School of Science and Technology

Department of Engineering

A Framework for Efficient Crowd Management with Modern Technologies

Ph.D. Thesis

By

Mishaal M. Almutairi

Internal Supervisors

Professor David Stupples
Dept. of Electrical and Electronic Engg.
School of Science and Technology
City, University of London
London, UK
d.w.stupples@city.ac.uk

Dr Dimitra Apostolopoulou
Dept. of Electrical and Electronic Engg.
School of Science and Technology
City, University of London
London, UK
dimitra.apostolopoulou@city.ac.uk

External Supervisors

Professor George Halikias
Department of Mathematics
University of Athens
Greece
ghalikias@math.uoa.gr

Professor Mohammad Yamin
School of Computing
College of Engineering and Computer Science
The Australian National University
Canberra, Australia
mohammad.yamin@anu.edu.au

March, 2024

Declaration

I, Mishaal Mofleh F. Almutairi, hereby confirm that the work presented in this thesis is my own. Any information derived from other sources has been properly acknowledged and cited within the thesis. The figures and graphics used in this thesis are either my own work, in the public domain, licensed under Creative Commons, or free to use with no copyright restrictions.

Abstract

Crowds are an inevitable part of society. Sometimes crowding, rather a degree of congestion, can benefit lifestyles in certain ways, particularly from a business and economical point of view. But at other times, crowding is detrimental to social progress. While businesses may prosper in areas with high human traffic, many lives are also lost due to crowding. Some of the reasons crowds are organised are for social gatherings (musical corsets, beach fronts), business activities (restaurants, fairs), sports, religious activities, political rallies, funeral and wedding processions, and so on. Managing crowds effectively and efficiently remains a challenging issue.

Tens of thousands of people have lost their lives due to the poor organisation of crowds. Several stampedes have taken place in both developed and developing countries. The reason for these disasters can be attributed to poor organisation, lack of infrastructure and technology. The literature review finds some studies aimed at providing ways to manage crowds. However, these studies concentrate on limited aspects of crowd management, and do not provide a comprehensive solution for all issues related to crowding.

This research presents a comprehensive framework leveraging modern technologies for effective crowd management, addressing the multifaceted challenges of handling large gatherings through a staged approach, including privacy and security considerations. It aims to systematically address crowd management issues from planning to post-event stages, each tailored to meet specific requirements.

In the Planning Stage, the focus is on establishing vital infrastructure and crisis management strategies, highlighted by the creation of an innovative automatic classification algorithm using machine learning and deep learning. This algorithm assesses event reservations based on criteria like event type and expected attendance, marking a significant advancement in structured event planning.

The Organization and Monitoring Stage integrates cutting-edge technologies like IoT, AI, drones, and fog and cloud computing, enhancing event organization and ensuring detailed monitoring. Features such as real-time data collection via IoT and smartphones, rapid data processing through fog computing, and automated access

control exemplify the stage's sophistication. Algorithms for analyzing drone images and incident reports further boost situational awareness.

The Flow Regulation Stage shifts attention to managing crowd flow with digital tools for precise gateway control, essential for avoiding bottlenecks and ensuring orderly, safe movement. Additionally, the Additional Issues Stage encompasses health monitoring and waste management, emphasizing a holistic strategy that considers environmental and health impacts post-event.

Significantly, the research explores privacy and security solutions for crowd-generated data, introducing methods like Private Information Retrieval (PIR) and Double Protecting Approach for data privacy, utilizing fog computing to enhance security without compromising personal information integrity.

This framework represents a pivotal advancement in crowd management, combining planning, organization, flow regulation, and privacy/security measures into a cohesive, technology-driven strategy. It not only addresses current crowd management challenges but also lays the groundwork for future innovations, offering a holistic approach to managing crowds effectively and securely.

Table of Contents

List of Abbreviations

Acronym	Full Form
Arafat	A valley outside Makkah
Arbaeen	Annual day of mourning the death of Imam Hussein
DB	Database
Fog	Fog node
GCC	Gulf Cooperation Council
Hajj	Annual pilgrimage to Mecca
IoT	Internet of Things
Ka'aba	A cubic structure for Circumambulation around it
Kumbh	Kumbh Mela
KSA	Kingdom of Saudi Arabia
LBS	location Based Services
Makkah	Mecca
Mina	A tent city for Hajj
Muzdalifah	A plain between Makkah and Arafat
POI	Places of Interest
RFID	Radio Frequency Identification
SP	Service Provider
Tawa'af	circumambulation of Ka'aba
Umrah	Lesser pilgrimage to Makka
WSN	Wireless Sensor Network

Acknowledgements

I would like to thank Professor David Stupples and Dr Dimitra Apostolopoulou, my internal supervisors, also I would like to thank Professor George Halikias and Professor Mohammad Yamin, my external supervisors, for their continuous and full support, encouragement, and suggestions during the course of this thesis. I also thank Dr Adnan Ahmed Abi Sen for his advice and support during the course of my research.

I am very thankful to my mother Norah and wife Amal, without their help, it would have been very difficult to complete this project.

Lastly, but not least, I am thankful to the Graduate Studies Office of the City University, and in particular Nathalie Chatelain for her support during the course my studies.

Chapter 1: Introduction

Tens of thousands of people have lost their lives in crowd related incidents. Unfortunately, despite the availability of tremendously improved technologies, very little to nothing has been done to effectively prevent the reoccurrence of crowd related disasters. On the contrary, the number of stampedes have increased with the passage of time. Indeed, crowd management continues to remain under-developed in most parts of the world. Surprisingly, whenever a stampede occurs, no government department or organisation is held responsible for the disaster. This chapter outlines the background and context of the research and its purposes. Significance and scope of this research are also discussed and an outline of the remaining chapters of the thesis is provided.

During the first half of 2021, three stampedes, one each in Israel, Tanzania and Afghanistan, took place, killing more than one hundred people and injuring many more. In 2020, a total of six stampedes took place. With these and other incidents, as shown in Table 1, crowd management hasn't yet evolved an effective strategy to stop or minimize such disasters from occurring. It is worth noticing that the number of stampedes have increased from forty five in the 20th century to one hundred and twenty two in the 21st century (see Table 1). During the first twenty-one years of the 21st century, 7628 people have lost their lives to stampedes compared to 6124 in in the entirety of the 20th century. These statistics are a clear demonstration of the deterioration in crowd management against the expectations of improvement due to the passage of time and availability of better technologies. We rarely find examples of better crowd management. However, one incident where management did an excellent job took place on 30th October 1993, in which seventy-three students were crushed in a charge of supporters to the field to celebrate the Wisconsin Badgers' win in which, fortunately, there were no fatalities. We frequently witness spectators charging on to sports fields if their team wins or loses, some incidents of which have resulted in multiple deaths (Mammana, 2016). This practice should be effectively prevented.

1.1 FAMOUS CROWDED EVENTS

Most crowding events, particularly the larger ones, are recurring and usually for religious rituals. Indeed, religious events are difficult to be managed due to the sensitives associated with them. The largest gathering of people, known as Kumbh Mela (Figure 1.1), to be referred simply as Kumbh (Verma & Sarangi, 2019), takes place in India every three years. The event rotates among four cities situated along the Ganges (Ganga) river, which is regarded as sacred by many in India. Most prominent of these four events takes place every twelve years in Prayag (Allahabad), a city situated at the meeting point of three sacred rivers, namely Ganges, Yamuna and Sarasvati, the last of which is symbolic and does not physically exist.

Table 1.1 ("List of Human Stampedes and Crushes," 2021)

Stampedes in the last four centuries

Century	Fatalities	No of Stampedes	No of Countries	Comments
18th	3000	2	2	Stampedes were caused by mismanagement of large crowds
19th	7150	11	7	Stampedes occurred due to poor management, triggering panic as a result of some unexpected incident such as a building collapse, terror attack, fire, etc.
20th	6124	45	29	The number of large events increased but the number of fatalities from stampedes reduced by more than a thousand. However, the number of stampedes and fatalities is alarming.
21st	7628	122	56	The number of events in this century have already surpassed previous records and are diversified across the world. Fatalities in the relatively shorter period are quite alarming. Crowd management needs massive improvements.

This event attracts tens of millions of devotees (sometimes one hundred million) over a period of about six weeks. Kumbh attracts between fifty to one hundred million pilgrims over a period of six weeks. On their auspicious day (Somwati Amavasya or Mesh Sankranti) the number of pilgrims may swell to several millions within a

relatively small area of up to twenty square kilometres. In 2021, amidst the ongoing COVID-19, Kumbh Mela took place in Haridawar, a city in north India. Kumbh Mela has accounted for thousands of deaths so far ("List of Human Stampedes in Hindu Temples," 2021).

Table 1.2

Stampedes of last five years

Year	Fatalities	No of Stampede	No of Countries	Comments
2017	107	16	13	India tops the list both in number of stampedes and fatalities.
2018	48	10	8	The number of stampedes and deaths reduced significantly.
2019	67	6	6	The number of stampedes and fatalities continues to reduce considerably.
2020	141	7	7	The number of stampedes and fatalities is the highest of the last five years.
2021	90	2	2	Still a very high number, which is a sad reflection of crowd management.

Figure 1.1: (commons.wikimedia.org, 2019) Kumbh 2019

The second largest gathering of people on our planet takes place every year in Iraq. The event is known as 'Arbaeen', in which about fifteen million people from several countries gather to mourn the assassination of Imam Hussein, a grandson of

Prophet Muhammad. About three million pilgrims from over fifty countries gather in Karbala (a city in Iraq), and walk barefoot from different places in Iraq. The Arbaeen has also witnessed several stampedes, killing hundreds of people. The last stampede took place on 10th September 2019, in which 31 people died (BBC, 2019).

Figure 1.2 (commons.wikimedia.org, 2019) Arbaeen (Karbala, Iraq)

The third largest gathering of people is Hajj (Yamin, 2018), the annual pilgrimage to Makkah (Mecca) in Saudi Arabia (Figures 3a and 3b). This is a highly organized event in which about three million pilgrims take part. Most of the pilgrims travel from close to two hundred countries to perform Hajj. Although Hajj is only a five day event, most of the pilgrims end-up spending about five weeks due to travel limitations. Hajj includes very intense and en masse rituals in which all pilgrims must take part at the same place (like in Arafat or Mina), involving very frequent travel to move pilgrims from one site to another. The hajj is a highly organised event, despite witnessing a number of stampedes killing thousands of pilgrims over the years. More information about Hajj and its management will be provided in in the future research. There are many other religious events which take place periodically. A description of some of them are detailed in a study by Yamin (Yamin, 2019).

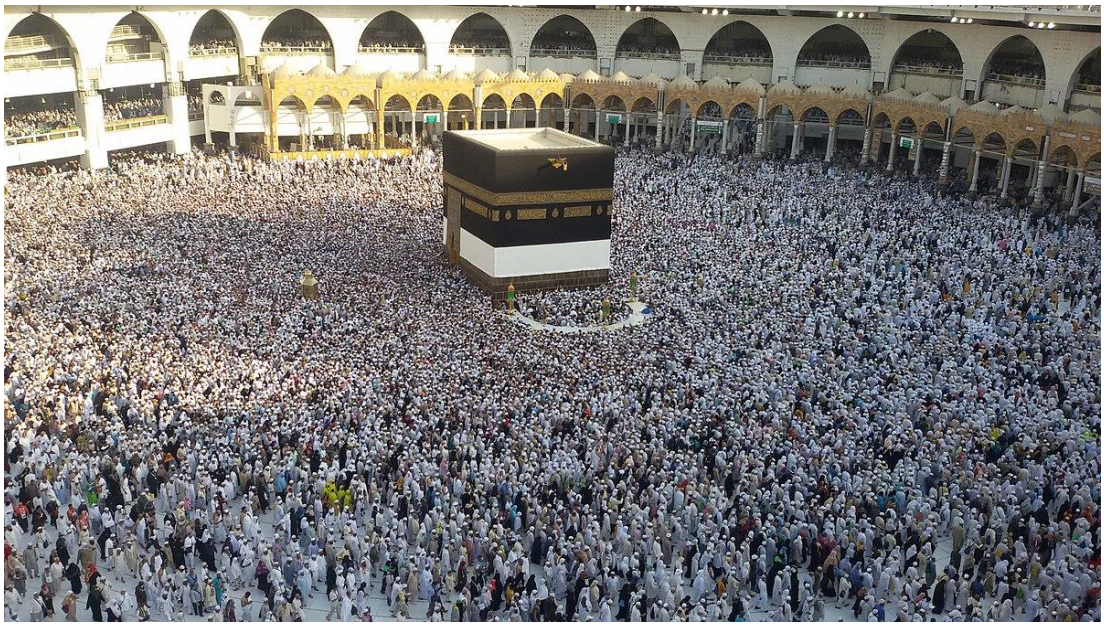

Figure 1.3 (commons.wikimedia.org, 2018) Tawa'af (circumambulation) of Ka'aba during Hajj

1.2 COVID-19 & CROWDED EVENTS

COVID-19 is the disease caused by Novel Corona Virus or SARS-CoV-2, which was first discovered in Wuhan city, China in late 2019 (Yamin, 2020). Shortly after, the World Health Organisation (WHO) declared it as a global pandemic (World Health Organization, 2020). To date (September 2021), the pandemic has infected approximately 231 million people, killing more than 4.75 million people (Worldometer, 2021). To prevent this virus from spreading, the use of face masks, social distancing, strict hygiene, and vaccination are recommended.

Figure 1.4(a): Wembley Stadium (11th July, 2021) (commons.wikimedia.org, 2021a)

Figure 1.4(b). A large crowd outside Wembley Stadium on 11th July, 2021(commons.wikimedia.org, 2021b).

In order to contain the virus from spreading, crowded events must strictly adhere to the guidelines agreed to by the international community to contain the spread of the virus. As a result, within three months of first coronavirus case being detected, many religious gatherings were either banned or curtailed to comply with the social

distancing norms. Unfortunately, despite restrictions and prohibitions of crowding, numerous crowding events have taken place without any COVID-19 restrictions, which may have contributed to the spread of the virus. On 11th July 2021, a Euro 2020 match took place at Wembley Stadium (Figure 1.4 (a)). The entry to the stadium was granted based on furnishing a proof of vaccination or a negative COVID-19 test result. As can be seen, the spectators were not using face masks, which is recommended even for vaccinated people. The match was won by England, after which, as can be seen in Figure 1.4 (b), a massive crowd of supporters descended to the streets outside Wembley stadium. As can be seen, all the COVID-19 precautions were flouted by the crowd, which may have caused further spread to the ongoing epidemic of the Delta strain in the UK and Europe.

Another example of unmanaged crowding during the pandemic is that of Kumbh which took place in Haridawar, a northern city of India, in March 2021. It should be noted that the Delta variant of COVID-19 was already causing havoc in India at the time. The Kumbh in Haridawar (Figure 1.5) was open to all, which attracted millions of devotees. There were no checks in place for the entry of the participants. On April 12 (Somwati Amavasya) and April 14 (Mesh Sankranti), about five million people took part in the bathing ceremony without any COVID-19 protocols to reduce the virus' spread. A total of 1,701 people tested positive for COVID-19 in the Haridawar Kumbh Mela area from April 10 to 14 (commons.wikimedia.org, 2014), confirming fears that one of the world's largest religious gatherings may contribute further to the rapid rise in coronavirus cases in India. It is a general view that this event would have served as a 'super spreader' in the deadly second wave of the Delta variant of COVID-19, which has killed tens of thousands of people. Several aspects of massive crowding of Kumbh have been discussed by Quadri and Padala (Quadri & Padala, 2021).

Figure 1.5 (commons.wikimedia.org, 2014) Kumbh Mela (June 2014)

Not all crowded events during the COVID-19 pandemic are unruly and unorganised. There are many examples of crowded events which were meticulously organised and well managed, adhering to all precautions and restrictions to contain and control COVID-19. The grand mosque in Makkah (Figure 1.6&1.7) was closed for months in 2020 in order to contain the pandemic. It should be noted that the grand mosque in normal circumstances can accommodate more than two million people to pray in congregation, and more than fifty thousand pilgrims can perform Tawa'af (Figure 1.6). When it opened in October 2020, only a few hundred worshipers were allowed to congregate in shifts with social distancing (Figure 1.7). Hajj, which can accommodate about three million pilgrims, was only made available for ten thousand people in 2020. Again in 2021, Hajj was only performed by sixty thousand fully vaccinated people in the age group of 40-50. In this manner, the opening of the grand mosque for a manageable number of people or having a much-curtailed Hajj pilgrimage did not result in further spread of the virus. Through effective management, no virus cases are known to have resulted from these events.

Despite the ongoing COVID-19 pandemic, the annual pilgrimage of Arbaeen 2020 did take place but only with a smaller number of pilgrims. Each country was allowed only one thousand pilgrims except for Iran, which was allowed to send two thousand and five hundred pilgrims. Overall, COVID-19 has severely impacted the region's tourism (di Giovine, 2020).

Figure 1.6(commons.wikimedia.org, 2020) Hajj 2020 (Umrah Pilgrimage)

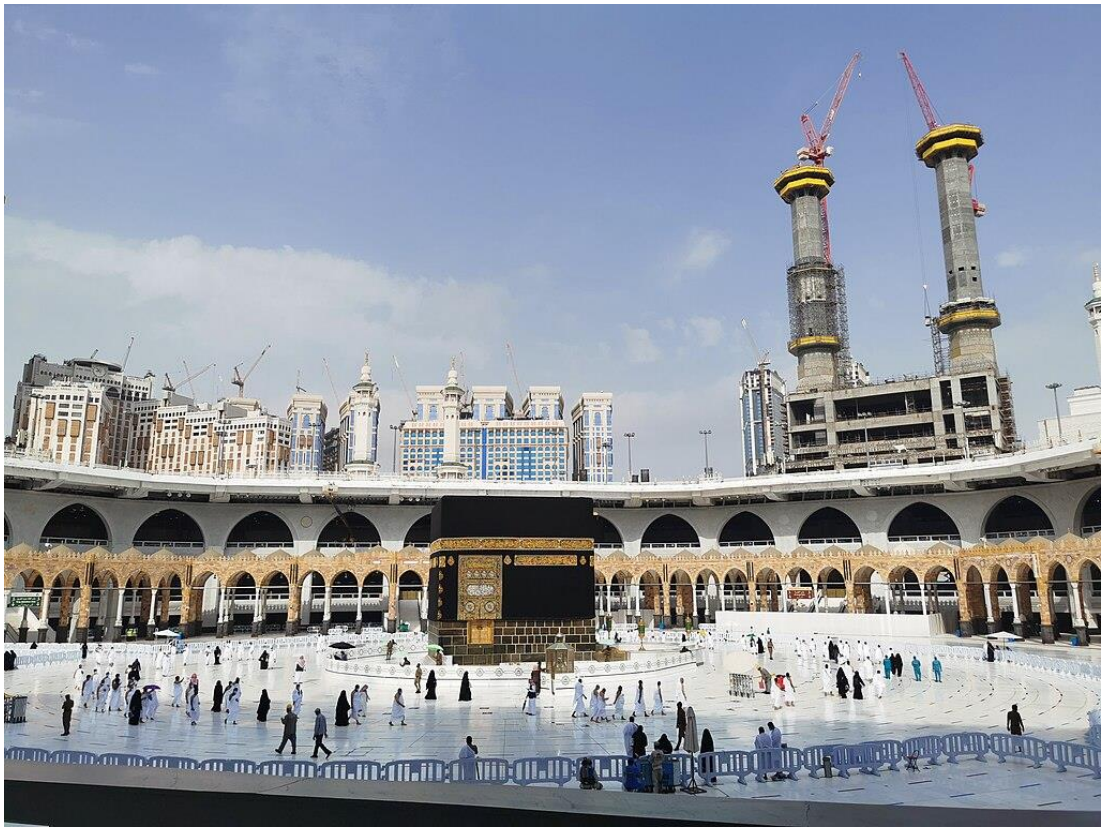

Figure 1.7 (commons.wikimedia.org, 2021) Hajj Dec, 2021

1.3 AIM & CONTRIBUTION OF THIS RESEARCH

The aim of this research is to provide a general framework for managing all aspects of large crowds with the help of the latest technologies. As the occurrence of stampedes is the major issue of crowded events, components of the proposed framework are designed to effectively prevent stampedes from occurring, which will be discussed in detail. Selective use of technology, which is critical in managing crowds and preventing disasters like stampedes, will also be discussed in detail. The aim and contributions can be summarized as follows:

Aim:

- To propose a comprehensive framework for managing crowds efficiently with the aid of modern technologies.

- To address the inherent challenges in managing large crowds across various stages, incorporating privacy and security solutions.

Contributions:

- Development of an automatic classification algorithm using machine learning and deep learning techniques for event reservation assessment.

- Enhancement of structured event planning through consideration of event type, expected attendee numbers, dates, and durations.

- Integration of advanced technologies (IoT, AI, drones, fog, and cloud computing) for improved event organization and meticulous monitoring.

- Achievement of real-time data acquisition via IoT, smartphone applications, and social media platforms.

- Implementation of automated gateways based on IoT for attendee regulation, and algorithms for processing drone-captured images and analyzing volunteer-reported incidents for enhanced situational awareness.

- Management of crowd flow using digital methodologies for precise direction and control of gateways, ensuring orderly and safe crowd movement.

- Addressing health monitoring and waste management to mitigate pollution and ensure attendees' health post-event.

- Introduction of innovative solutions for protecting individual data and biometrics within crowd management contexts.

- Proposal of the Private Information Retrieval (PIR) approach and techniques for enhancing privacy and security in crowds using fog computing.

- Introduction of the Double Protecting Approach for data privacy and the Double Cancelable Hashing for protecting users' biometrics.

The thesis presents a significant contribution to the field by tackling the complexities of crowd management through a multi-staged, technology-driven approach. It provides a holistic strategy for effectively and securely managing crowds, laying a foundation for future research and practical applications in this critical area.

Chapter 2: Literature Review

Large gatherings, or crowds are characterised by people with varying behaviour ranging from exuberant to hostile, and aggressive to peaceful. These crowds are accompanied by varying levels of chants, noises and even bands in some cases, and they are often alarming to private security, the police, and the public in general. Some of the most common large gatherings that require the services of crowd management personnel include sports events such as the Olympics, festivals, concerts, protests and demonstrations taking place in large cities and towns, community fiestas and fundraisers, and religious gatherings and events, among others. Moreover, Ahmed & Memish, (2019) claim that there are crowds everywhere including at the beach, at the train station, in restaurants and their surrounding environments, at various concerts. There are crowds when walking down the streets where various activities including demonstrations and protests occur every day, as well as product launch events which can also lead to crowding. It is inevitable for crowding to occur, especially in cities.

2.1 CROWD MANAGEMENT BACKGROUND

Crowd management is about ensuring safety and security of the members of the crowd, citizens, and their properties. Unruly crowds may damage public property, spark disasters like stampedes and fires, and affect the freedom of the citizens. In order to ensure safety and security, crowds must be managed properly.

Yamin et al., (2018) propose a framework for Crowd Control and Health Management System (CCHMS). This examines the usefulness and effectiveness of CCHMS components in real life with particular reference to Hajj and Kumbh Mela, which attracts millions of participants.

There are regular and irregular crowds. Kumbh, Hajj and Arbaeen are regular crowded events, whereas musical concerts, funeral processions, and political rallies are irregular and spontaneous crowds. It has been witnessed many times that some irregular crowds grew beyond all expectations, causing a nightmare for management and resulted in stampedes. Annadurai's funeral in 1969, the Protest March in London in 2003, the funerals of Khomeini in 1989 and Diana, the Princess of Wales in 1997,

and the wedding of the adopted daughter of Jayalalithaa in 1995 are all historically large and irregular crowded events.

2.2 INADEQUATE CROWD MANAGEMENT

In their book Crowd management: risk, security and health, O'Toole et al., (2020) explore crowds from a Complexity Theory perspective. As such, they maintain that a crowd is a complex paradigm because every individual in a crowd is a free agent, and they tend to respond to the people around them differently, thus, their attitudes and behaviours spontaneously affect other individuals. As a result, a crowd forms relationships between different individuals which creates a certain crowd behaviour. O'Toole et al., (2020) claim that this situation is beyond complicated because the causes and effects of a crowd are integrated in multiple attitudes and behaviours that are in constant movement, and that are developing. Emergent behaviour is one of the key aspects of a crowd's complexity, and it refers to the unpredictable behaviours that arise from different individuals in a crowd. In such a complex situation, it is extremely difficult for one to predict exactly what is going to happen every time since even the smallest alteration in a crowd may be intensified throughout the entire crowd (O'Toole et al., 2020). For instance, if a car breaks down near a crowd, different types of crowds will react differently to the situation. Some crowds may ignore the breakdown altogether while it may cause panic in other crowds, and in such a case, people may start rushing away or towards the broken down car. The uncontrolled movement then causes more panic within the crowd, which ultimately creates a disaster.

2.3 STAMPEDES AND DEATHS

A 2017 report by BBC highlighted that approximately 1500 people were wounded in Turin city in Italy after a firecracker evoked a stampede on a Saturday night. On that night, thousands of football fans had gathered in Cardiff to watch a live broadcast of Juventus' Champions League final against Real Madrid (BBC News, 2017). Suddenly, the spectators heard a loud bang, and within seconds, rumours of an explosion had already spread throughout the crowd causing mass panic. In the next ten minutes, crowds were hastily rushing from Cardiff stadium, crushing people against each other and against barriers. Individual possessions including bags, shoes, and other belongings were left scattered everywhere on the ground as people ran out of the square haphazardly while screaming. Immediately, the underground car park gave way

due to the force applied by the crowd. The barrier around the square entrance opened and people trampled over each other, causing severe injuries to some. The report indicated that most of the people in the crowd were injured, evidenced by small cuts on their arms and legs (BBC News, 2017). At least seven of the injured individuals, including a seven-year-old boy, were hospitalized as they were in critical condition after they were stamped on by others as they rushed to escape the stadium. The community expressed their anger at the authorities for not putting in place adequate crowd management and control measures to mitigate such incidences. They further expressed their concerns regarding inadequate crowd management, as a considerable number of Juventus fans expressed that this incident triggered traumatic memories caused by the Heysel stadium catastrophe that took place in 1985 due to crowd mismanagement (BBC News, 2017). Fans revealed that thirty-nine people died after being squashed against a wall, which then eventually collapsed and killed more people before the end of the game which was the European Cup final with Liverpool.

In light of this, effective crowd management calls for authorities, in conjunction with the event coordinators, to understand that crowds are complex because they are made up of individuals with diverse attitudes and behaviours. This understanding could have helped authorities devise effective strategies and techniques to manage the crowd in the occurrence of such emergencies, hence minimizing stampedes and the resulting injuries. For example, Kingshott (2014) recommends drafting standard crowd policing rules within an interlinked framework which would clearly exemplify effective crowd management to all the parties involved in a crowded event, including participants, organizers, casual spectators and bystanders, and those stakeholders tasked with crowd management and control. This framework helps all the stakeholders to understand and acknowledge the complexity of a crowd, hence make it easy for fair and equitable law and order maintenance in a crowd situation. Besides, this framework favours the coordination between law enforcement, crowd management, and the public under the community policing paradigm, with the central goal of maintaining peace and order and preventing public disorder during major events (Kingshott, 2014). This coordination is achievable through cooperation and consultation as a key requirement for a community policing paradigm. In their meetings with law enforcement and other stakeholders such as medical services, local councils, and crowd managers, event coordinators should discuss the following: Objectives, the proposed date and time of the event, the event's location, the event's itinerary, the event's time scale, the number

of attendees and their demographic information, and the proposed communication methods and techniques with the crowd, organizers, crowd managers, and other stakeholders (Kingshott, 2014).

Research conducted by Yamin Basahel & Abi Sen (2018) to investigate deaths and injuries caused by poor crowd management shows that over twelve thousand people lost their lives due to stampedes and other crowd related mishaps between 1980 and 2015. Despite such concerning findings, crowd managers across the world do not seem to have learnt anything from such past experiences, especially regarding notable crowd events. For this reason, the death toll since 2015 shows that there have been over seven thousand deaths related to ineffective crowd management, which is already more than what was recorded in the previous century (Yamin Basahel & Abi Sen, 2018). This research determined that the root causes of stampedes are overcrowding and crowd mismanagement. Therefore, this massive loss of lives could have been reduced or even avoided through better crowd management and control. Additionally, another research by Owaidah (2015) shows that a considerable number of people die every year due to poor organization and management of crowded events. The study reveals that thousands of people have perished in the recent past, especially due to fires and stampedes caused by overcrowding and crowd mismanagement. However, Owaidah (2015) maintains that it is possible to manage overcrowding, and in turn prevent catastrophes related to overcrowding through efficient and effective crowd management using more advanced modern technology. For instance, before the commencement of the summer Olympic games in 2004, the event's organizers contracted an American crowd management company known as Contemporary Services Corporation (CSC) to manage and control people in the event. During the opening and closing ceremonies, crowd managers from the contracted company ensured that there was order throughout the event by helping the spectators find their seats in an orderly manner. They also provided both the players and the spectators with general information about the stadium including its features and arrangement. The personnel also ensured that the crowd found their exit in an orderly manner once the event was over. As a result of effective crowd management, there were no fatalities during the game, and only a few spectators acquired mild injuries from crowding related incidents. The success of this event demonstrates that crowd management is possible, and it prevents catastrophes related to overcrowding through efficient and effective crowd management techniques.

2.4 CROWDS AND INFECTIOUS DISEASES

There has been an increase in the growth and spread of highly infectious diseases in the recent past. Some of the most contagious diseases witnessed include EBOLA, HIV/AIDS, Severe Acute Respiratory Syndrome (SARS), different strains of the influenza, Swine flu (H1N1 and H1N2) and Middle Eastern Respiratory Syndrome (MERS). These diseases have mainly been observed in Africa and the Middle East, but they are also scarcely distributed in other parts of the world, especially Asia (Yamin, 2020). The spread of these communicable diseases in crowds could be deadly, and their treatments are an extremely challenging endeavour. Therefore, those tasked with crowd management including the police, private security, and the public, must take adequate measures to ensure that the spread of these diseases is minimized, as well as to put up effective and reliable treatment plans in play in case there is an outbreak of any disease. Owaidah (2015) claims that most crowded events attract people from hundreds of different cultural and language backgrounds, which creates significant communication challenges for crowd managers. For instance, Hajj is an annual pilgrimage that is undertaken by Muslim worshippers to Mecca in Saudi Arabia every year during the Arabic Lunar month of Dhul Hijjah. Both interstate and international travels take place during this time, and they involve mass movements of large groups of people from different parts of the world to gather in a few identified sites in Mecca. According to Yamin & Ades (2009) up to six million people from across the world participate in Hajj every year. Such large crowds can make it difficult for crowd managers to control medical and other catastrophic emergencies related to overcrowding. For instance, the EBOLA outbreak that occurred in West Africa in 2014 was fuelled by overcrowding, and it did not only lead to mass panic, but it also caused serious challenges to the global health sector. Despite the World Health Organization's (WHO) determination to control the spread of the disease, it quickly spread throughout Guinea and its bordering countries including Sierra Leone and Liberia. The densely populated capitals of the three countries were more affected than any other parts as they provided an unparalleled opportunity for transmission.

2.5 THE COVID-19 PANDEMIC

The Coronavirus pandemic, which started in 2019, has had significant economic effects around the world. However, the level of impact depends on an organization's level of dependence on face-to-face interactions. For instance, industries such as hospitality, retail, and transportation have particularly experienced high impacts due to the nature of their operations. Each country has taken control measures to manage the spread of the pandemic based on various guidelines from health authorities. Currently, the standard control measures include wearing masks, observing social distancing, sanitizing using antibacterial gels, temperature controls, and utilizing disinfectant mats, among others. Nevertheless, these control measures do not avert the risks of being in a crowd. According to O'Toole et al., (2020), this is because crowds are complex paradigms as every individual in a crowd is a free agent, tending to respond differently to other people around them. As a result, people's attitudes and behaviour within a crowd are bound to affect other individuals spontaneously. O'Toole et al., (2020) further claim that such a situation is highly complex because the causes and effects of a crowd are integrated in multiple attitudes and behaviours that are in constant movement, and that are developing. In this light, crowds are a key source of the transmission and spread of COVID-19, and crowd mangers have come up with various ways to mitigate its spread.

Cities around the world have come up with measures to ensure that people are observing COVID-19 guidelines. Miles & Shipway (2020) argue that urban centres across the world have been expanding progressively in the past few years. This means that the world will keep facing key projections of booms in the urban centres even in the coming years. Specifically, major cities such as the city of Wuhan in China, where the Coronavirus started, among other cities such as Paris, where multitudes of people died from the outbreak, are expanding at an alarming rate. These cities already accommodate millions of people. This development and expansion of major cities has caused overcrowding, thus increasing the susceptibility of the spread of highly infectious diseases such as the COVID-19. This makes crowd management in urban centres very important, and although the complexities of modern urbanism make it more difficult to manage a pandemic such as COVID-19, most cities have tried implementing various crowd management techniques. For instance, major cities such as Paris and New York, among others, have taken measures to ensure that people are meeting the 1.5 metre social distancing guideline as directed by the WHO (World

Health Organization, 2021). The key to achieving this effort has been in the ability of crowd managers in these cities to obtain a continuous and real time view of how usually overcrowded and busy public spaces are faring so that they can take the necessary steps when certain areas become overcrowded. Essentially, crowd management experts around the world have been tracking the movement of people around urban centres in an effort to optimise the flow of people, hence managing the spread of the virus (Dey et al., 2021). Particularly, city authorities have been utilizing a human centric design that allows them to harness data and organize public spaces to adapt to people's needs, which are constantly changing. This data also helps crowd managers to track visitors and assess their compliance with the strategic guidelines and policies implemented by city authorities (Yu et al., 2021). This step has resulted in uninterrupted access to public spaces, improved comfort, improved safety, and better crowd management by city authorities.

In addition, several countries across the world have developed and implemented contact tracing apps in the past few months. These tracing apps alert the crowd management team when someone who they have been in contact with later tests positive for COVID-19 (Yu et al., 2021). However, all the contact alert apps are different in different countries because they are based on varying alert thresholds, which are achieved through a combination of distance between two contacts, and the amount of time they have been in contact. Also, the thresholds are country specific. For instance, in Germany and Italy, the contact alert apps detect people who have been in contact for more than 15 minutes, with a distance less than two meters between them (Yu et al., 2021). The adequate balance of these key aspects, time and distance, is fundamental as it helps the management team to avoid getting numerous false positives or negatives as a result of various factors such as high or low risk of exposure, and the inaccuracy in estimating distance due to the strength of Bluetooth signals. In this regard, concerned authorities have been analysing the combination of contact times for specific distances between two people in different key urban settings to acquire key information to gauge the contact tracing apps before using them in different contexts.

However, Shambour & Gutub (2021) point out that there are various challenges associated with the human centric design, which utilizes automated monitoring of people in crowds to ensure they are maintaining social distancing. The first challenge is that crowd managers have to adopt privacy techniques and sensors to ensure that they are respecting the privacy of everyone. These privacy sensors and techniques

must ensure the privacy of every individual while simultaneously providing the crowd management team with accurate time-space information on the position of every individual with sub-meter accuracy. Failing to do this, the automated monitoring fails to achieve its objective, thus becoming very difficult to control the spread of the coronavirus. Secondly, the crowd management team needs to establish an algorithm that is capable of simultaneously identifying families and their family members, and distinguishing them from strangers, with utmost accuracy, while at the same time preserving their privacy. Since this identification should be done in real time, the entire process raises various technical challenges for crowd managers.

2.6 LOST IN THE CROWD

Some people go missing in large crowds for different reasons, and this poses a significant challenge for them as they track their way back, especially in foreign countries with notable transportation and communication problems. Crowd managers have the responsibility to manage and control these kinds of emergencies to ensure the safety of everyone. For instance, being one of the most overcrowded events of the year, one of the most upsetting aspects of Hajj is the management and control of the huge number of pilgrims gathering in Mecca (Owaidah, et al., 2019). Although the authorized number of pilgrims that are issued travelling permits by their immigration offices in different parts of the world are only about three million, the number of unauthorized pilgrims in some years, such as 2012, is nearly equal to the number of authorized pilgrims. It becomes extremely difficult for crowd managers to control such a large number of people gathered in one place. As a result, chances of managing issues such as tracking missing persons, minimizing the spread of disease, controlling life threatening emergencies such as fires, stampedes, and drowning among others, becomes an extremely challenging task for crowd managers. In light of this, (Owaidah et al., 2019) recommend having adequate binding international and interstate standards aimed at limiting the number of people that should be allowed to gather in a specific area at the same time. These binding standards would make it easier for crowd managers to control crowds and manage all the emergencies related to large crowds, especially for crowd events that involve the gathering of millions of people at once.

2.7 CROWDS AND TERRORISM

Many parts of the world are facing the risk of terrorism, and crowded places are more plausible to being subjected to terrorist attacks. According to Baxter, Flinn & Picco (2018), a progressively homogenized world with integrated nations, cities, and regions often seeks to develop a portfolio or an anthology of cultural assets in an effort to establish and amplify their destination image and position themselves in the highly competitive marketplace. Key events usually form a central part of this anthology because they act as a showcase for their destinations (Baxter, Flinn & Picco, 2018). These events act as tourism drivers as they draw large numbers of people in the host country. They do this by providing a unique opportunity to market the destination country to a potentially extensive global audience through the substantial media attention that they attract. Therefore, event professionals play a significant role in contributing to the general image of the country or city where the event is taking place (Baxter, Flinn & Picco, 2018).

However, while large events yield notable benefits to the destination countries, cities, or towns, they may also garner significant negative attention that is likely to undermine and diminish the appeal of the destination if not managed properly. Recent events have proved that the nature of major events make them more receptive to terrorist attacks, which is extremely detrimental to the reputation of the destination. Baxter, Flinn & Picco (2018) claim that not only does the size of major events afford a country or city the opportunity to impose major damage, the media coverage of such events gain an extensive audience, thereby consummating the goals of terrorist groups of creating widespread fear and anxiety by obtaining global recognition. In this regard, Baxter, Flinn & Picco (2018) infer that the event's organizers and coordinators must exercise effective crowd management to ensure that nations and cities can leverage such big events safely and securely to facilitate tourism and enhance their brand image. Event managers must effectively plan, prepare and manage all eventualities before hosting an event, which means putting all the diverse risks associated with hosting a major event into consideration. They must consider the possibility of terrorist strikes and then ensure that their crowd management strategy includes plans and measures to reduce the threat of terrorism as well as an effective approach to the aftermath in case terrorism occurs.

Historically, major events have been linked to terrorist activities. For instance, the most noteworthy attacks based on MERT research include the terrorist attack on the Olympic Games in Munich in 1972, and the terrorist attack on the Atlanta Olympic Games in 1996. These attacks were then followed by the 9/11 attack, which consisted of four coordinated terrorist attacks against the United States by the Al-Qaeda on 11th September 2001. Since then, western societies have encountered an increase in terrorist activities, and major events have been a highly sought-after target according to Spaaij (2016). Most of the academic literature detailing terrorism and crowd management focuses majorly on sporting events including the two mentioned above. However, there are more events that have experienced terrorism attacks in the recent past due to inadequate crowd management including the Boston Marathon bombing in 2013, and the Paris attacks that happened in 2015. These attacks negatively affected the security plans, measures, and budget set for the UEFA championships that were set to take place in 2016 (Shepard, 2016). According to Spaaij & Hamm (2015), the recent increase in these attacks stipulates that these cultural events have increasingly become a target for terrorist attacks, which gives grounds for the need to evaluate the perceptions of event professionals and the implications for managing these events in a more safe and secure manner, especially in western cities, which are more susceptible to these attacks. Research by Spaaij (2016) exploring the challenges faced by an event's professionals in delivering safe and secure events in major cities shows that overcrowding and crowd management is one of the greatest challenges faced by these professionals. As a result, event managers must effectively plan, prepare and manage all eventualities before hosting an event, which means putting all the diverse risks associated with hosting a major event into consideration.

2.8 CROWDS AND INTOXICATION

Most major events that are attended by large crowds, except religious gatherings, are usually complicated by the availability of alcohol and other recreational drugs. All these substances undermine the ability of the individual to act in a composed manner and behaving in a protective manner towards the vulnerable members of the crowd, hence promoting safety within the crowd. According to Lombardo et al., (2020), most of these events are open air events, which means they are usually held in undesignated locations, especially music festivals, and electronic dance parties, which are mostly never organized and coordinated by experienced and professional event

organizers. In some cases, these informal events are held in underground sites, which are not designed to accommodate such large gatherings. Most participants in these informal events are young people, at times younger than those allowed to attend formal religious and sporting events. Lombardo, et al., (2020) further maintain that informal events such as music festivals, specifically the electronic dance music events, are highly associated with intoxication, which makes the crowd more susceptible to danger as a result of disorderliness. These events target young people between the ages of fifteen to twenty-five and attract large crowds often in unregulated sites and venues, which are increasingly found in purpose-built locations in the contemporary world.

According to research conducted by Bullock et al., (2018) investigating the effects of intoxication in informal events that are mostly attended by young adults, the results show that overusing alcohol and other recreational drugs such as Marijuana is highly linked to these informal events, and they escalate the rate of injuries, stampedes and deaths. The research reveals that in 68 deaths related to alcohol poisoning and drug overdose at informal electronic dance music events have been recorded in the past fifteen years (Bullock et al., 2018). Violence was also identified in these events with a considerable number of participants claiming that they were beaten and stabbed, with a few stabbed so deeply that it resulted in needing tube thoracotomy. Matters get even worse at these events because some participants get intoxicated even before they attend them, which is a common practice in most American events, which occurs during pre-event gatherings typically around their cars and trucks (Bullock et al., 2018). Excessive drinking and drug use increases the risk of committing offenses and causing injuries, extreme behaviours such as fire jumping and others that increase the risk of contracting sexually transmitted diseases. Particularly, Ahmed & Memish (2019) elaborate more on fire jumping, which is a celebratory activity that arises when one team, especially in a sports or musical event, wins a tournament or a match. They describe the unsolicited gathering consisting of 52,000 fans who gathered in St. Louis, Missouri in the United States to watch a basketball game where the University of North Carolina's team played in the Final Four Semi-finals and National Championship games. Since two matches had gathered back in the main team's home state, two large unorganized crowds gathered on two successive nights where they lit bonfires to celebrate their teams while fire jumping and dancing through the flames, while performing their victory dances (Ahmed & Memish, 2019). By the end of the second night, 78 fans needed immediate medical attention and 50 of them needed emergency admission

because they were severely injured in these unsupervised activities. Besides, 67% of the crowd had alcohol poisoning, and they had suffered severe burns from fire jumping, thus they also required medical attention (Ahmed & Memish, 2019). In this regard, informal events undermine the ability of experienced professionals to organize and coordinate events, hence diminishing their efforts to manage crowds and mitigate all the negative consequences associated with inadequately managed crowds.

Crowds, which people witness every time, differ in various ways. A crowd may be caused by events, which either occur on a regular or irregular basis. Events such as the Kumbh, Hajj, and Arbaeen occur on a regular basis, so they are predictable, otherwise irregular events such as protests, election rallies, celebration marches, musical and sporting events and funeral processions among others are routinely unpredictable and spontaneous in nature (Yamin et al., 2018). Therefore, their sizes and the crowds that emerge from them can build up spontaneously, and easily become uncontrollable. It is extremely difficult to predict the nature and size of irregular and spontaneous crowds because they are surrounded by numerous uncertainties. For instance, it was unpredictable that over fifteen million people would gather at the funeral of Annadurai, a South Indian politician, in 1969 (Eladly, 2019). This funeral was so overcrowded that it was entered into the Guinness Book of World Records for the event with the greatest number of people. As a result, it was extremely difficult to manage the crowd, which caused a stampede that led to the deaths of at least twenty people and the hospitalization of sixty-two people nursing serious injuries. Although it is more difficult to manage irregular crowds, Eladly (2019) notes that it is equally hard to manage regular crowds because although it seems like the management of regular crowds is easier, the reality is that most stampedes associated with crowds have occurred in regular events such as the Kumbh Mela and Hajj. Nonetheless, technologies such as WNS, RFID, Fog, and Cloud have proven efficient in the management of regular crowds, although they may not be feasible in the management of spontaneous and irregular crowds.

2.9 MATHEMATICAL MODELLING OF CROWDS

Mathematical modeling plays a critical role in understanding crowd dynamics, helping to predict the behavior of large groups of people during high-risk scenarios like evacuations or mass events. Various models have been developed to simulate crowd behavior, focusing on different levels of abstraction. These models fall into four categories: microscopic, mesoscopic, macroscopic, and hybrid models. This review explores these methods, highlighting their use in real-world scenarios, and simplifying the key equations involved where applicable.

1. Microscopic Models

Microscopic models simulate the behavior of individual agents in a crowd, modeling each pedestrian separately with specific movement rules. These models are excellent for understanding detailed interactions, such as avoidance and decision-making.

One common microscopic approach is the social force model, which uses simple physics-based equations to simulate pedestrian movement. In this model, each pedestrian is subject to forces that guide their behavior. The equation for a pedestrian's movement is based on a balance of these forces:

$$F_i = m_i \frac{dv_i}{dt} = F_{\text{goal}} + F_{\text{repulsion}} + F_{\text{interaction}}$$

- F_{goal} : force moving the pedestrian toward their goal (destination),
- $F_{\text{repulsion}}$: repulsive forces to avoid collisions with others or obstacles,
- $F_{\text{interaction}}$: social interaction forces, such as staying near companions.

This model was applied to the Love Parade disaster in 2010 to simulate crowd behavior leading to the tragic stampede. Helbing et al. (2011) used the model to understand how overcrowding in bottlenecks contributed to the event.

Microscopic models were also employed in the Hajj pilgrimage to simulate the Tawaf ritual, where millions of pilgrims circumambulate the Kaaba. The model helped identify potential areas for crowd congestion and improve safety measures (Moussaïd et al., 2011).

2. Mesoscopic Models

Mesoscopic models strike a balance between microscopic and macroscopic models by grouping pedestrians into clusters, treating each cluster as a single unit while simplifying individual-level behaviors. These models are computationally efficient while still capturing important group dynamics.

An important case study involves Shibuya Crossing in Tokyo, where a mesoscopic model was used to simulate pedestrian flows. Pedestrians were grouped based on direction and speed, and their movement was modeled using equations from kinetic theory, which describes the flow of gases but can also apply to crowds.

The main equation used in mesoscopic modeling is the Boltzmann-like equation:

$$\frac{\partial f(x,v,t)}{\partial t} + v \cdot \nabla f(x,v,t) = Q(f)$$

Where:

- $f(x,v,t)$: the density of pedestrians at position x with velocity v at time t,
- $v \cdot \nabla f(x,v,t)$: the advection term, representing pedestrians moving,
- $Q(f)$: the interaction term, representing changes in velocity due to interactions with others.

This model was effective in optimizing pedestrian flow and minimizing congestion at Shibuya Crossing (Takizawa et al., 2018).

3. Macroscopic Models

Macroscopic models describe crowd behavior using fluid dynamics, treating the crowd as a continuous flow rather than focusing on individual pedestrians. These models are based on principles from fluid mechanics and are especially useful for large-scale simulations.

A commonly used macroscopic model is derived from conservation laws similar to those used in traffic flow modeling. The continuity equation for pedestrian density ρ(x,t) is:

$$\frac{\partial \rho(x,t)}{\partial t} + \nabla \cdot (\rho(x,t)\,\mathbf{v}(x,t)) = 0$$

Where:

- $\rho(x,t)$: pedestrian density at position x and time t,
- $v(x,t))$: the velocity field of the pedestrians.

This equation represents the conservation of mass, ensuring that the number of pedestrians in a given area changes only due to movement into or out of the area. Hughes (2002) used a macroscopic model to simulate pedestrian flows during the 2012 London Olympics, helping planners manage crowd movement in transportation hubs and venues.

Macroscopic models were also used at the Tianjin Railway Station in China to optimize the design and prevent overcrowding during peak hours, significantly improving safety and efficiency (Zhou et al., 2019).

4. Hybrid Models

Hybrid models combine elements of microscopic, mesoscopic, and macroscopic approaches, allowing for detailed simulations in areas where individual behaviors matter while simplifying the collective behavior in less critical areas. This approach is particularly useful for large and complex environments.

A notable example of hybrid modeling was at the Tokyo Train Station, one of the busiest transit hubs in the world. The station used hybrid models to simulate both the individual behavior of pedestrians at ticket counters and the macroscopic flow of passengers through the station during peak hours (Kretz et al., 2008). The microscopic component used equations from social force models to capture individual behaviors, while the macroscopic component used fluid dynamics equations to represent crowd flow.

Another example is the use of hybrid models during large events on the Sydney Harbour Bridge, where authorities combined microscopic and macroscopic simulations to ensure safe crowd movement during public celebrations such as New Year's Eve. This hybrid approach allowed for efficient crowd control and minimized the risk of accidents (Georgoudas et al., 2012).

2.10 TECHNOLOGIES FOR CROWD MANAGEMENT

Recent developments in the technological field have provided some of the finest tools and gadgets which can be immensely useful and helpful in managing crowded events. Here we provide a table followed by the description of some of the technologies and their capabilities.

Table 2.1

Crowd management technologies

Name	Usages in our CMS.
WSNs	Monitoring and sensing important indicators about the environment in relation to some conditions such as oxygen level, the level of pressure, pollution, and heat, all of which are very significant in the management of health and crowd conditions (Yamin, Basahel, & Abi Sen, 2018).
RFID Tags	Detecting the location and identity of objects in the targeted local area, which is important in the calculation of the number of participants in a specific area, as well as for searching and identifying different objects within the crowd (Rajaraman, 2017).
Drones	Observing the crowd vertically from overhead positions in all directions. Additionally, the drones can be used in this system to promptly deliver some material and medical supplies in areas that lack feasible ground transportation. Since they are fitted with sensors, they can perform quickly and accurately, especially in mapping the area under surveillance, and analysing footfall, assessing crowd distribution, evaluating and estimating the duration of stays and revisit patterns at these events. Drones for monitoring events in this way have proven to be an incredibly cost effective and flexible solution for obtaining event analytics in real time, which aids in planning (Vattapparamban, Güvenç, Yurekli, Akkaya, & Uluagac, 2016).
Airships	If GPS, Cellular network and Internet Connection do not work on the ground, airships can be deployed as the best alternative (Sun, Wang, & Xie, 2018).

IP cameras	They are used to take photo frames to obtain crowd segments' headcount before sending them for processing as an input for the proposed stampede detection algorithm in the article (Cusack & Tian, 2017).
Smart phones and devices	They can be used in the place of either WSN, RFID or Alarm in cases where there is availability of Cellular/Wi-Fi connection. They can also be used for other applications provided for the system (Chang & Chen, 2016).
Digital street	They transform vulnerable areas into a screen of LEDs to create a tool and a platform to alert crowd administration and control crowds (Fujdiak, Mlynek, Misurec, & Slacik, 2017).
GPS	Used to find objects' global location as well as tracking them (Guan, Shao, & Wu, 2017).
FOG	Used for caching and speeding up the processing of the data generated using various devices and tools that are mentioned in this table. The experiment favours Fog over cloud because Fog minimizes latency in communicating, transferring data, and decision-making. In a sensitive system such as CCHMS, latency can lead to system failure (Dastjerdi, Gupta, Calheiros, Ghosh, & Buyya, 2016) and (Yamin, Basahel, & Abi Sen, 2018).
Cloud	It is leveraged for its ability to store and process historical data into a data warehouse in preparation for data mining and big data analytics (Mach & Becvar, 2017).

2.11 RADIO FREQUENCY IDENTIFICATION (RFID) AND WIRELESS SENSOR NETWORKS

According to (Yamin et al., 2018), Radio Frequency Identification (RFID) technology and tools have proven effective in the management of some of the most rampant problems associated with crowding. For instance, RFID has already successfully been implemented in tracking the movement of goods, vehicles, and with people using RFID chips in the form of tags connected to a GPS, Wireless Sensor Network (WSN) or cellular (3G/4G) network. Yamin et al., (2018), further claim that deciding on the best network to select for any event highly depends on the path traversed by the RFID chip or the topography in which the RFID chip is positioned. If the RFID chip is positioned in an urban area, crowd managers have to consider issues such as the width of the streets, congestion, the density of buildings, and other related areas.

Additionally, a Wireless Sensor Network (WSN) is a collection of a large number of sensors, all of them assigned a unique task of monitoring and detecting physical events and phenomenon such as heat, light, pressure, RFID tags, and pressure. WSNs have extensive scalability and they are highly flexible because they are wireless (Yamin et al., 2018). Therefore, using WSNs to obtain signals from RFID tags is particularly effective, and it provides highly accurate and reliable latitudinal and longitudinal coordinates. However, their positioning or deployment and installation is very costly and risky, especially in places with certain limitations. In addition, effective tracking and crowd management using Cellular 3G/4G requires numerous repeaters to warrant access to all possible areas of RFID tags. Furthermore, Yamin et al. (2018), argue that it is widely understood that GPS is ineffective in certain locations such as densely built-up areas and tunnels. Similarly, some RFID tags may be undetectable in some areas such as in extremely densely populated locations, and the local sensor network cannot be positioned in places with limited space. Regardless of these limitations, these technologies have significantly transformed the processes of tracking and retrieving information and intelligence from obscure places (Yamin et al., 2018). Besides, these technologies have paved the way for Internet of Things (IoT), hence establishing a launching pad for a great number of applications. The table below outlines a comparison between RFID and WSNs.

Yamin and Ades (2009) argue that many pilgrims are reported missing and others require urgent medical attention during extremely crowded religious events such as the Kumbh Mela and Hajj. Such events lead to the occurrence of jams in human traffic, which in turn leads to overcrowding. Almost always, overcrowding results in stampedes, yet not all of them are covered in the press due to either political or safety reasons. Overcrowding also increases the possibility of the spread and acquisition of highly contagious diseases such as HIV/AIDS, bird flu, swine flu, and hepatitis among others (Eladly, 2019). Security issues are also of high consideration in these overcrowded events. As a result, crowd managers have to be realistic and practical in deciding what is important, useful, economic, feasible, and manageable for dense and large crowd management.

Table 2.2 (Alharbi, 2021)
Comparison between RFID and WSN

Factor	WSN	RFID
Main goal	Monitor and sense the environment	Detect location and Identity
Tasks	Collect, Process, Transfer, and Store information or data.	Ideally, RFID reflects RF signal transmitted from Reader to identify the location of an attached object
Element	1 Sink aggregates the information from sensor nodes. 2 Sensor node with sensing, Computing, and communicating elements.	**T**ag (Passive/Active) stores the unique serial number, and it provides memory for some additional info. Passive tag is used only for reading info by a Reader. Active tag supports two-way communication with higher signal strength and can store some information, but it is costly. **R**eader can read or write data on Tag and pass it to the host. Capable of sending messages to an individual tag or broadcast to all tags within range. **H**ost Computer analyses data
Range	Does not support long range of communication, therefore, it uses multichip to reach the Sink Node and increase the range.	Usually has a small Range of communication, where Passive Tag, which is about 2-3 meters, and Active Tag, which is between 100 to 200 meters. However, it is costly relative to its abilities

Applications	It has applications in numerous fields including Safety and Wellbeing, Healthcare, Smart-Grid, and Environment.	The basic applications include Tracing, Security & Access Control, Healthcare, Crowding, Clothes stores, among others
Protocol of connection	Wireless connections include Wi-Fi 802.11WLAN but it is High on power, Bluetooth 802.15.1 WPAN, ZIGBEE 802.15.4 Low Power WPAN	RFID Protocols (Air-Interface) (IOS-x), LF, UHF, and NFC among others.
Communication and Connection	Multi-hop to increase strength of signal, and WSNs can link to each other (Ad hoc).	Single-hub and there isn't communication between RFIDs.
Mobility	Usually, static	Usually, mobile
Programming	Supported	Not supported
Deployment	Random or fixed	Attached to or embedded in objects
Power and energy	Battery for sensors, and power supply for Sink Node	No need for battery for Passive Tag, but powered-battery is needed for Active Tag, and power supply for Reader
Usability	In cars, phones, clothes, and electronic devices, among others.	In cards, bracelets, phones, and car, among others.
Limitation	Range, Architecture, massively heterogeneous, Real-Time Apps, Privacy & Security, among others.	Power, Communications, Cost of Active Type, Security & Privacy, among others.

Soman & Jacob (2018) argue that one of the most fundamental aspects of any crowd management techniques is to collect, assess, and organize data about the involved entities including the palm, finger, and retina, and then feed it into a database using a distributive database management system (DBMS). This system must be

capable of effectively and efficiently searching through extensive data. Acquiring pilgrim data is easy and straightforward because most of them prepare their information during their visa application process (Soman & Jacob, 2018). However, Yamin & Ades (2009) maintain that Kumbh currently lacks an effective mechanism for collecting and organizing their data, which poses significant management issues. Once a database is established, it can be utilized to obtain and disseminate data for planning and administration purposes in these events in coordination with other wireless and sensor technologies and tools (Yamin & Ades, 2009). Other studies like those conducted by Yamin et al. (2018); Yamin & Ades, (2009) assert that RFID chips have proven effective in tracking and monitoring both people and goods. For instance, the Malaysian government has ensured that all the passports for Malaysian citizens are RFID enabled, which has hastened the processing process at Malaysian airports, thus minimizing congestion and overcrowding. Since Yamin & Ades (2009) have acknowledged that it is essential to track pilgrims in religious events for administrative and management purposes, the RFID technology, through wireless sensor networks such as cellular (3G/4G) network or GPS tracking devices can be used to track pilgrims throughout their spiritual journey, thus making crowd management easier. However, Yamin & Ades (2009) ascertain that RFID presents accuracy, reliability, and other performance related issues if every person in a large and dense crowd carries an RFID chip. As a result, the installation of wireless sensor networks to sense and read RFID chips would have significant economic implications where irregular events such as Kumbh Mela keep happening (Yamin & Ades, 2009). However, RFID technology is highly effective for tracking and identification reasons. A human readable ID coded RFID is able to in identify, outline, report, and assist people in need of urgent attention. Ordinary people must be able to read the ID for them to report effectively (Yamin et al., 2018). Ideally, these RFID contain some PDA and readable data, which is useful for uniting lost and found pilgrims with their groups or units, as well as for medical plights. For maximum efficiency, the RFID is connected to the event database to enhance the recovery of data and ease updates when need be.

Concurrently, Nasser et al., (2017) claim that the extensively used ICTs such as smartphones, WSN, RFID, e-bracelets, and Wi-Fi have challenged researchers to establish solutions for crowd monitoring and management at irregular events such as Hajj. According to them, current solutions deal with facilitating the processes related to performing religious rituals and ceremonies such as offering the LBSs during Hajj

rituals (Nasser, et al., 2017). These solutions are responsive to what happens, but they have not yet been tested in wide area case studies. Today's smart devices such as mobile smartphones have built in technologies such as Wi-Fi, GPS, LBSs, AGPS, and digital compasses. In a smartphone, the GPS is used to pinpoint the exact location of the smartphone, the LBSs technologies work in conjunction to determine exact positions, and the Wi-Fi minimizes the search time for the closest GPS satellite. In this regard, these software applications in-built in today's smartphones have been designed to specifically use the phone's geographic location to provide various facilities and services. Some of these services include locating and map navigation, and they are extremely useful in crowd management. Yamin et al., (2018) and Nasser et al., (2017) acknowledge the above ICT technologies for addressing crowd monitoring and management in events such as Hajj have both advantages and disadvantages. The advantages stimulate the development of solutions aimed at supporting crowd management in these events, while the disadvantages such as bandwidth, distance, energy cost, rate, among others determine the type of applications that can be designed to improve the process. They claim that even RFID technologies are still inadequate and inefficient in outdoor system application when it comes to crowd management in large religious events such as Hajj, yet they are widely adopted for the same purpose (Nasser et al., 2017). Besides, mobile technologies equipped with GPS applications only function effectively in outdoors settings if the sky is clear to allow the GPS receivers to work properly. Otherwise, the satellite signals are either unreliable or blocked completely in tunnels or closed buildings. Furthermore, crowd sensing using mobile devices, and utilizing social network data to create applications to guide pilgrims who are at risk due to overcrowding are not appropriate because not all the pilgrims are in possession of a smartphone during these events, and those who carry them may not know how to use the tracking and sensing applications installed in them (Nasser al., 2017). Also, it is impossible to recharge the smartphone in such crowded places, and the network is also usually very low, thus slowing down all forms of communication. Although there are several methods for tracking individuals in these events, especially the use of image processing techniques, only a few have demonstrated efficiency in real time. In this regard, more practical crowd management techniques must be designed to manage these events.

2.12 FOG AND CLOUD COMPUTING

Yamin et al., (2018) define Fog as a computing model that was introduced by CISCO back in 2012 for the key purpose of minimizing or eliminating some cloud computing limitations. As such, Fog is an extension of Cloud to the edge of a network containing a smaller processing power and memory, which means that any smart device that can do storage and computing. Considering this, Fog is unlike Cloud in that it is closer to the end-user, and it reinforces the distributed computing model. The comparison between Fog and Cloud is represented in the table below.

Table 2.3

A comparison of Cloud and Fog

Fog	Cloud
It can be any device with the ability to compute and store data, as well as network.	It is only set for servers
It supports time sensitivity applications. Particularly the ones that deal with emergencies, where Fog usage minimizes latency while increasing response rate, and decreasing traffic on the provided links.	Does not support time-sensitive applications such as the ones dealing with emergencies, thus it is difficult to achieve goals such as reduced latency, increased response speed, and diminished traffic on the links
The Fog Node is usually closer to the end-user; thus, it is suitable for data filtering and processing before sending it to the Cloud. This leads to reduced overhead processing on the Cloud, and minimized traffic on the network and the links. It can easily process images and identify key features before sending features, rather than images, to the Cloud.	Cloud is exclusively used to store all the information and utilize big data applications to investigate and uncover unknown data associations.
Fog may sometimes implement significant access restrictions on data before transferring it to Cloud, which mostly occurs for IoT objects that do not have enough processing power and memory to perform identical tasks.	Cloud cannot do this.

Fog can be implemented as smart traffic to facilitate mobility applications and foster crowd management.	Cloud can be implemented as smart traffic to facilitate mobility applications and foster crowd management, but not as effectively as Fog.
Fog increases the availability service	Cloud is extremely beneficial in crowd management
It is possible to scatter numerous Fog Nodes to cover large areas, such as in case of densely crowded events such as Kumbh Mela or Hajj.	Cloud does not support the Computing distributed model as competently as Fog.
Fog Node has limited resources, which gives rise to the persistent need for Clouds.	Cloud offers unlimited resources.
Fog supports awareness location	Cloud does not support awareness location.
Users can have full control.	Users have limited control because there are only three control models, which include SaaS, PaaS, and IaaS

According to Yamin et al., (2018), crowd managers should make the best use of Fog technology by dividing the crowded area into many different cells, each of them containing Fog to ensure that there is a connection in all the objects in a particular cell. This subdivision ensures that Fog accurately computes the number of event participants, normally with tags, in every cell to ease their management by supporting certain services. Fog Nodes in every cell then feed the aggregate of the results acquired after data processing in a specific cell to the Core Fog. The Core Fog is also capable of performing some key operations before transferring the data to Cloud. In the Cloud, data is mined, and big data analysis is performed. In case of an emergency in a crowded event, Fog can make decisions directly without latency.

Similarly, Abdulqadir et al., (2021) argue that the augmented growth of the Internet of Things (IoT) technology has posed substantial challenges to the definitive cloud computing prototype. These challenges include high latency, network failure, and limited capacity. Cloud computing and Fog computing brings the Cloud nearer to IoT computers in an effort to overcome these challenges. Both Fog and Cloud provide IoT storage and processing services locally rather than sending them to the Cloud. Besides, Fog and Cloud offer better efficiency as well as faster reactions cooperatively with cloud, thus they are viewed as the safest and most reliable advance towards

ensuring that IoT delivers stable and reliable resources to different IoT customers. However, (Abdulqadir et al., 2021) noted that some applications and services still cannot benefit from Cloud-Fog computing despite its extensive utilization. The reason this computing paradigm is still inefficient is because of Cloud's inherent problems ranging from a lack of location awareness, lack of mobility support, and high latency. As such, they suggest that crowd managers should make the best use of Fog technology, which has emerged as an outstanding infrastructure to issue resources at the edge of network elasticity.

Ullah et al., (2018) also emphasize on the efficiency of Fog computing and the need to leverage its benefits in crowd management. They study some of the key utilizations of Fog computing and its performance under diverse approaches and implementations. First, they proposed an environment for Fog computing, and demonstrated an accurate testbed for use in different scenarios. They particularly investigated three user scenarios and designed their Fog computing platform for each of them (Ullah et al., 2018). The three scenarios include Fog computing of crowd-sourced, dissemination of content in challenged networks, and programmable IoT analytics. In each scenario, they solved optimization problems through novel algorithms, and the findings were such that the recommended algorithms outperformed baseline algorithms with respect to the key efficiency metrics of the three scenarios by at least 30%, 20%, and 90% respectively. A number of ongoing activities aim at implementing the recommended Fog computing model for providing network services, adapting system dynamics, and predicting device availability to facilitate crowd management (Ullah et al., 2018). Specifically, the Fog computing of crowd-sourced scenario details the efficiency of Fog computing in managing crowds. Ullah, et al., (2018) maintain that Fog Nodes, the network computing devices that are deployed near end users towards the edge of a network, can apply some processes on data mining, gathering, cleaning, filtering, summarizing, storing, sharing, and transferring it to Cloud. They argue that Fog computing is effective in crowd management because Fog Nodes minimize latency in crowd-related emergencies such as stampedes without returning to Cloud because they use a wireless connection.

Concurrently, Alraddady et al., (2019) add that due to the sudden and progressive increase in the number of requests for network resources, Cisco invented the idea of introducing the process of computing to the edge of the network in 2012. This idea also included deploying the computational process geographically in the

vicinity of the end users to offload bandwidth and the main Cloud to increase the response rate and minimize costs. Alraddady et al., (2019) leverage this concept of IoT and cloud computing technologies to propose a novel Fog computing-based framework to alleviate the issue of packet delay and bandwidth bottleneck during Hajj where millions of pilgrims gather in Mecca, Saudi Arabia along with the security personnel, health providers and other service providers. The latest data from Saudi Arabia's general authorities for Hajj season, the highest number of pilgrims segregated in Mecca was witnessed in 2018, and they added up to 1,867,678 (limited to actual Hajj, General Authority for Statistics KSA, 2019). Without a proper crowd management framework, such a high number of people concentrated in one area over a long period of time increases susceptibility for crowd related emergencies such as stampedes, injuries, deaths, terrorism attacks, and fires, among others. As such, Alraddady et al., (2019) assert that pilgrims should be properly directed to take the designated route to their destination in an orderly manner. The current crowd management system used during the Hajj season consists of only a cloud server where the data they provide before acquiring their travel permit (including important personal details) is stored. Each pilgrim is issued an identification card containing this information, and an attached quick response code is scanned for the event personnel to obtain all their information in an organized structure. Alraddady et al., (2019) argue that the management of the huge crowd formed by pilgrims every Hajj season presents numerous challenges because the cloud server system in place suffers from high latency since all the pilgrim data is supposed to be retrieved or transmitted from the cloud server, which leads to heavy network traffic.

In light of this, the authors suggest employing a fog computing system to help crowd managers alleviate some of these challenges at a low cost. The central idea behind fog computing in this case is that it will move storage and processing away from the cloud server and closer to the end user. The result of this is that there will be lower energy consumption and a faster response time because the amount of data that will be retrieved and sent to the cloud is minimized. To this end, Alraddady et al., (2019) recommend a framework that will help event coordinators in irregular events such as Hajj to maximize the number of requests being processed at the Fog level and avoid processing them at the central cloud server to minimize the response time, thereby attaining a high quality of services, especially for requests with non-delay tolerance. The framework is designed to assist pilgrims arrive at their destination using

their assigned route in a more orderly and effective manner. The framework also aims at expediating inquiry requests for health providers and security personnel, who are tasked with the responsibility of managing crowds at critical events to mitigate risks. Similar to the findings of Yamin et al., (2018); Abdulqadir., et al (2021) and Ullah et al., (2018), Alraddady et al., (2019) attest that leveraging Fog in crowd management helps minimize or eliminate the most pervasive cloud computing limitations.

To test whether such a framework would work, Alraddady et al., (2019) conducted an extensive literature review to uncover standard Fog-based frameworks that have worked before. Their findings were that several scholars have proposed and tested Fog computing models that have proven effective. For instance, Hong (2017) suggested and tested a Fog computing framework known as Crystal. In the framework, a Fog agent decomposes a Fog application into small services, referred to as crystals in this model, which can be mined using any processing unit such as a Fog Node, an end user or even a Cloud server. Crystals have the capacity to identify and select the most suitable Fog Node to deploy a service based on the Fog's obtainable resources and the processing requirements of the crystal. These crystals are auto-scaling, self-healing and they support mobility such that when a Fog Node dissipates for any reason, the crystals heal themselves and then they attach on to the next accessible Fog Node (Hong, 2017). As a result, app developers do not have to write codes that are completely accurate and error-free because the framework depends on two key Fog Nodes: Fog agents and Fog trackers. Fog agents are tasked with the responsibility of decomposing and crystalizing the processes of the Fog application. Secondly, Fog trackers have a responsibility of receiving periodic check signals from resources of Fog agents in the same cluster, as well as sending messages to other Fog trackers on different clusters to ensure that they utilize all the available resources within the system. Besides, Hong (2017) presented a Fog application referred to as Fog MapReduce with an aim of processing the requested services that are geographically close to the end user to increase privacy for highly confidential and sensitive data, minimizing response time. The framework was also designed to compare the performance of its applications with those of Apache Spark.

On the other hand, Jeong., et al (2017) proposed and tested a framework that enables secure communication between a cloud server and an IoT device through mobile edge computing. The first phase of the framework involves the registration of an IoT device at the cloud provider using an encrypted password and username. The

purpose of the registration process is to verify and authenticate clients when they request to be connected to a mobile edge provider (Jeong., et al 2017). After the authentication of a client's request, the cloud provider examines the availability and accessibility of the mobile edge nodes, and then selects the most appropriate edge nodes with reference to the node's geographical location as well as the request requirements in regard to security, bandwidth, and delay. After the selection of the most suitable node, the second phase begins. This phase involves the cloud server sending the network address together with a temporary identification number to the client, accompanied by a password for the selected mobile edge node (Jeong., et al 2017). The temporary ID that is issued is then sent to allow for the IoT device to be utilized in authenticating the communication between the IoT device and the edge node to guarantee the safety and privacy of the IoT device. After the IoT device or the client is connected to the edge node, data transmission using a secret key that is only familiar to the edge node begins in the third phase (Jeong., et al 2017). Eventually, the edge node transmits the processed data to the cloud without the need to involve the client. Should the client require to make changes to the edge node for any reason such as due to roaming, the registration process needs to be repeated from the first phase through to the third.

The success of the two described Fog frameworks is an indication that the one proposed by Alraddady et al., (2019) to ease the management of pilgrims in Hajj events will be successful. The framework focuses on retrieving the information of the pilgrims in case of a crowd related emergency, which means that it is not as complex as Hong's (2017) Crystal framework that requires processes of decomposition and crystallization. Secondly, Alraddady's et al., (2019) framework bestows features that will ensure that processing requests are geographically near the end user, although a part of the crowd managing procedure will still rely on Cloud. The framework will be more effective and efficient for crowd management in relation to Hajj pilgrims if it has a single and separate layer used to control and manage fog nodes to minimize latency. This is because solely depending on the main cloud server presents the challenge of traffic congestion during a high-density event such as Hajj. Alraddady's et al., (2019) framework is even more efficient because it considers several privacy and security issues ranging from confidentiality to integrity to middleman attacks. However, just like other proposed frameworks, the designers acknowledge that this framework presents a limitation in that it may not be possible to solve the bottleneck issue that the

study aims at addressing using the registration process in the framework. This is because these events have a high number of clients who will all be trying to connect to the main server. If the clients must first connect to the main cloud server for them to be redirected to Fog, the cost of the entire process will be unbearable in regard to the system's response time and bandwidth. As such, Alraddady et al., (2019) upgraded their framework into a 3-layered framework that leverages the benefits of IoT technologies and cloud computing to minimize the problems of packet delay and bandwidth bottleneck during Hajj events. The recommended 3-layered framework consists of: End User Layer, Fog Node Layer and Main Cloud Layer. The End User Layer acts as an interface between the Fog Nodes, located in Mecca offices and other ritual sites such as Muzdalifa, Mina, and Arafat, and the end users. The Fog Node Layer provides a middleware, which connects to the Main Cloud Layer, while the Main Cloud Layer provides a storage platform for all the input data, which is also updated periodically while in storage (Alraddady et al., 2019).

2.13 PRIVACY AND SECURITY

PIR TECHNIQUES FOR PRIVACY IN IOT

Preserving privacy and security of users' information is one of the most challenges for the recent technologies like Internet of things (IoT) and its smart applications and adaptive services. Private Information Retrieval (PIR) is one of the most common and strong approach for preserving privacy in IoT applications and especially with Location Based Services. However, most of users cannot use like this technique because it requires to print a huge size of data from server provider to the cache user's device and that impossible and illogical in many of devices and cases according to the resources and overhead. This section presents new method called Fog-PIR to deal with PIR by depending on the fog computing with will solve previous issue in PIR and enhance the privacy of users. Simulation confirms the superiority of Fog-PIR to normal PIR according to performance and privacy.

Most of recent services and applications depend on the concept of client-server. Thus, the service provider (SP) in the cloud will answer any request come from devices of users as smart-phone, smart-car, or any other devices. IoT paved the road to finding millions of these smart applications and adaptive services in all fields (Business, Health, Transportation, Education, etc. (Qian & Wang, 2012; Zhao et al., 2010).

Location Based Services are very popular in these days and is being used with great momentum in many applications and systems as searching for PoI, find shortest path, delivery issue and shopping online, emergency cases and request the ambulance or police, etc. In general case, the query from SP has specific format (Identity of user, Query | Data, Location coordinates, Time, [range]). So, user has to send this data with each query or each specific period to SP to get response and information, or to save this data for more sophisticated services (Zhao et al., 2010; Qian & Wang, 2012; Huang et al., 2018; Chen et al., 2017; Yamin & Sen, 2018).

The main issue in the previous scenario are the privacy and performance in addition to resources of user, where the resources are not enough to receive and process huge amount of data from SP. Some solutions as we discussed in the next section, depended on another server to address this issue, but in the same time it has created another issue related to the need trust to this third party (TP). In this work, we propose a new solution for the both previous issues (Performance and resources, and Trust to TP) depending on the fog computing and its hierarchical structure (da Cruz et al., 2018; Mostafavi & Shafik, 2019).

Fog computing is a type of edge computing, posed in 2012 by Cisco, to solve many issues in the Cloud Computing and support new types of applications. Fog locates in the edge of network close to the end user, where many of nodes are distributed density in different cells. Each node manages specific area and the objects in this area. In a similar scenario there are many of core fogs, and each core node manage many of fog nodes (Sen & Yamin, 2020). Fog nodes can apply police on data to enhance privacy and security before sending to cloud. Moreover, it can process and filter data before sending it to cloud to reduce the time and delay in the cloud, in addition to response directly for critical and emergency cases (Sen et al., 2019).

In this work we employ the fog nodes and their features to provide a new enhancement method instead of the normal PIR approach. More details about the proposed method will be in the third section, while next section will review the previous techniques for preserving privacy in addition to the previous methods in enhancement of PIR approach.

According to the importance of privacy and protecting users' data, many methods have been suggested to preserve privacy. The most important of these methods (Sen et al., 2018) are:

 Encryption: Data is encrypted between the sender (the user) and the receiver (the service provider), but it is assumed that the service provider is a trusted party (Yamin et al., 2019).

 Dummy: The user sends some fake queries in addition to his real query to mislead the service provider about his request (Basahel et al., 2019).

 Obfuscation: The user conceals his precise location within a certain area or sends a location further than his precise location to protect his privacy. He may use the method of adding noise to some data or changing it in some applications, but on the condition that it does not affect the results of the main service (Albouq et al., 2020; Alsaawy et al., 2019).

 Cooperation: A group of users in one region collaborating to exchange some available information without the need to contact the service provider or send them all at once, and thus the identity of all of them will be hidden within the group of cooperating users (Yamin & Sen, 2020; Sen et al., 2018).

 TTP: Instead of trusting the service provider and contacting him directly, an intermediary server is used to hide the identity of the users from the service provider and thus protect their privacy, but the issue of trusting the intermediary server is another problem [Sen et al., 2017; Gertner et al., 2000).

 PIR: It is a method that allows the user to inquire from the server without the service provider knowing what the real or accurate query the user wants, and thus usually a large amount of information is queried in each query (Ghinita et al., 2008).

In this work, we focus on PIR approach specifically and the methods that have advanced this approach as an improvement on the basic principle:

A. First Method

It is considered the simplest method. The data in the server are divided into numbered areas so that the user sends the number he wants (that is, the part from which he wants to obtain his data) to the server, and the server returns the results for this area, in this way PIR can be likened greatly to the principle Cloak Area or Obfuscation, where the user protects his privacy by hiding himself within a zone of confusion or a lock zone, so that the malicious service provider or the external attacker does not know what the real query the user wants within this area, nor does he know the exact location of the user within this area (Ghinita et al., 2008).

But in this way, the service provider still has information about the area in which the user wants to obtain inquiries within it, and this query can be known if the points of interest in this area are homogeneous, and the service provider can track the user's path over time (Ullah et al., 2020)..

B. Second Method

An improvement to the previous method, the user sends a ray of zeros and ones, for example (,0,0,1,1, ..) where 1 corresponds to the cells or areas that the user wants to obtain from the service provider, and thus it will be difficult for the service provider to track the user And defining its purpose, especially that some of the required areas will be false, meaning that the user does not want it basically, but rather was requested to mislead the service provider, which is similar to the concept of Dummy (Alsaawy et al., 2019).

C. Third Method

It came as an improvement to the previous method by including the concept of encryption, so that the data on the server is encrypted in addition to the query in order to prevent any access to it by the external attacker (Ernvall & Nyberg, 2003).

D. Fourth Method

To increase the level of protection, it has been suggested to rely on more than one service provider, so that each service provider has a different cell numbering of its own, the user creates a beam with the required cells and distributes them to the servers and therefore the user will not need to request fake cells here as in the second method, and at the same time, no service provider will be able to know exactly what the user wants (Zhao et al., 2007).

But here, the results coming from each server will contain many areas that are not needed, and the user will collect all of them and then choose the area he wants from each server, and here we notice the presence of a double load on the user. It is also expensive in the process of data transmission (Zhao et al., 2007). The paper also discussed the issue of the DNS being exploited to breach privacy by malicious service providers. But in the event that the performance is a sensitive issue for the user, then the part of the data that the user wants must be requested from each server, instead of completely from one server, and thus the user must collect the returned results.

Therefore, there is privacy protection here, but it is not complete, as there is a part of the required data exposed for each server.

E. Fifth Method

Some have used the concept of Anonymizer to increase the level of protection, so that there is a TTP that requests a large amount of data from the service provider to completely isolate its ability to penetrate the privacy of users, and then TTP responds to user queries. It was applied to health sector queries by creating an unhelpful user profile by masking the user's identity (Khan et al., 2020). To measure the effectiveness of the proposed solution, machine learning algorithms were employed to measure the distance between each user's query with his / her profile.

F. Sixth Method

It employs the technology of cooperation between users in forming one beam and then sending it to the service provider, after which the result is distributed to all users so that each user filters his own results only, and some have suggested using other methods to protect privacy with PIR (Fung et al., 2015).

Unfortunately, despite all the previous methods of PIR, they all still suffer from problems in performance, connection costs and computing costs, which we seek within the proposed solution to address it (Zhang et al., 2019). In (Grissa et al., 2017; Angel et al., 2021), the authors tried to solve this issue in different ways. In (Grissa et al., 2017) statistical methods were employed about previous queries to increase efficiency in performance without sacrificing privacy, but with tolerance for some errors, and (Angel et al., 2021) it was suggested to use special data coding or compression for queries so that performance is improved and the volume of data sent is reduced.

PRIVACY AND SECURITY IN CROWDS USING FOG COMPUTING

Thousands of crowded events take place every year. Often, management does not properly implement and manage privacy and security of data of the participants

and personnel of the events. Crowds are also prone to significant security issues and become vulnerable to terrorist attacks. The aim of this work is to propose a privacy and security framework for large, crowded events like the Hajj, Kumbh, Arba'een, and many sporting events and musical concerts. The proposed framework uses the latest technologies including Internet of Things, and Fog computing, especially in the Location based Services environments. The proposed framework can also be adapted for many other scenarios and situations.

Crowd management is an important but very complex management exercise due to the difficulty in controlling large numbers of people for long periods of time. If a crowd is not controlled properly, it may cause disasters resulting in the loss of lives. Crowd management requires the integration of many systems such as security and safety, healthcare, housing, transportation, and other services and processes (Lee & Ahmed, 2021). Most countries witness events that gather hundreds of thousands of people in one place, such as demonstrations, political rallies, funeral processions, or religious gatherings, among others. Figure 6.1(a) and 6.1(b) Chen et al. (2017) show crowds associated with the finals of the Euro 2020 in London in 2021. Sometimes the number of participants in a crowding event reaches several million. For example, Kumbh Mela in India attracts several million people. Likewise, the Hajj, in Makkah (Mecca) attracts more than two million pilgrims every year, see Figure 6.2(a) (Chen et al., 2017), and 6.2(b) (Yamin et al., 2018).

To manage large, crowded events, governments pay great attention and seek to find an effective way to monitor and control crowds efficiently. For these events, governments do their best to successfully organize and plan for gatherings and events in order for them to run smoothly (da Cruz et al., 2018). The Kingdom of Saudi Arabia is considered one of the leading countries in crowd management, as it has employed many modern technologies to control the Hajj commute between locations without any problems or threats (Mostafavi & Shafik, 2019; Sen & Yamin, 2020).

(a)

(b)

Fig. 6.1(a)(b) Crowd during and after the 2020 Euro Cup Final Wembley Stadium (11th July, 2021) (commons.wikimedia.org, 2021 a,b)

The integration of modern technologies has contributed to the provision of many adaptive services, electronic systems, and applications that work on smartphones, in addition to some supportive tools such as Radio Frequency Identification (RFID), bracelets and cards that enables attendee locations when needed, as well as

many different types of network sensors and cameras that provide permanent monitoring of the crowds. In addition to this, smartphones aid attendees and have important applications in them that keep them in contact with the specialized teams directly as well as with each other and with their families (da Cruz et al., 2018; Yamin et al., 2018; Mohamed et al., 2018).

(a) Ka'ba before COVID-19

*Fig. 6.2 (*commons.wikimedia.org *2016,2021) (a)(b) Hajj pilgrims before and after COVID-19*

Despite all those great efforts and the various techniques employed to control crowds, some other problems have emerged in regard to protecting the privacy and security of user data and keeping it from being breached or disclosed to unauthorized persons. Continuous monitoring, collecting, and analyzing people's data may reveal a lot about their behavior, hobbies, and qualities. For example, tracking their location permanently may reveal sensitive data such as their religion, morals, social and economic status, and other information that may expose some users to a real threat to their safety (Sen et al., 2018; Sen & Basahel, 2019).

The issue of privacy has become a major issue for many societies and individuals, especially with the digital revolution and the appearance of smart cities, homes, and phones. These developments have forced governments to make special laws to prevent companies and service providers from exploiting their users' data and the need to adhere to rules and policies that prevent the violation of their privacy. General Data Protection Regulation (GDPR) is an example of these laws that were issued in 2016 and came into force in 2018 within the European Union, in addition to similar laws in America, China, etc., and recently Saudi Arabia (Yola et al., 2019; Goddard, 2017).

The amounts of collected data within the crowds are extensive, and this data is shared by the crowd participants with their families, support teams, organizers, government services, and other smart applications. Most of this data is sensitive and needs protection to prevent it from being disclosed by malicious parties such as medical data, and the disclosure of some sensitive or private data by malicious parties may lead to inconvenience and harm to people that may amount to a real threat to their safety. Therefore, protecting the privacy within the crowd is very important, whilst also being a complex issue to address at the same time (Santana et al., 2020; Rahman et al., 2017).

This research presents a new idea of protection for the privacy and security of the data of individuals within the crowd based on fog computing, after presenting a brief reference study for the most famous methods of privacy protection. In the end, future directions are discussed as well as the mechanism for implementing the proposed technology.

Crowd management does not only mean monitoring and directing the movement of the crowd, but also managing their housing, health and transportation, and therefore

there is a great amount of diverse data that is stored about each person, and this diverse data and associated applications can be exploited by malicious parties by analyzing this data and discovering a lot of private and sensitive information about the behavior, and the physical, social and health status of individuals. Thus, we need special methods to protect this data from being hacked or disclosed. Although there are laws regulating the issue of privacy, as in the GDPR in European countries and others, these laws are not sufficient, as they depend on the commitment of service providers to these laws and not to circumvent them. Therefore, researchers presented various other ways to protect privacy that do not require absolute confidence in the service provider, which may be malicious at times and exploit the data collected by it about its users to reveal additional information about them or leak data to other parties (Santana et al., 2020; et al., 2017; Ludwig et al., 2015).

Privacy is the right of people to decide who has access to their data, according to the terms of the owner of that data, for example, what data they give access to, when and what can be accessed, etc. Therefore, no party that provides a service and needs users' data can use this data in a way other than the intended purpose of the service, as this party would be breaching the data owner's privacy. Thus, the term privacy is different from data security, which is concerned with protecting the confidentiality, integrity, and availability of data on a permanent basis. A commonly referenced example of the wrong use of an advertised service is what some search engines do, which is to analyze the terms that each person searches for to understand the behavior of the individual and then sell this data to advertising companies. Another example is related to location-based services. Instead of these services being specialized only in directing the person to reach target destinations, some malicious servers create a profile for each user containing the places they visit with the time stamp of their visit. Through a simple analysis of this data, a lot of a person's sensitive data can be revealed, such as the times they are not home, their religion, place of work, marital status, behavior and morals and many other private data that may pose a great danger to the person if the data is obtained by a malicious person or entity. The same also applies to medical services (Yang et al., 2017; Mendez et al., 2018).

Crowd management is a complex process that requires the integration of many services, such as medical services, location-based services or tracking, saving personal data, and keeping track of purchases, searches, and others. This indicates that there is a significant threat to the privacy of participants. Some of the most popular ways to

protect privacy have been suggested by previous research (Sen et al., 2018; Chanal & Kakkasageri, 2020).

The Trusted Third Party (TTP) method relies on an intermediary server instead of relying on the main service provider, but its problem is that the intermediary party may be a threat as well. Recently, Fog computing has been used like Trusted Third Party (TTP) instead of depending on the cloud only (Yamin et al., 2019; Sen & Yamin, 2020). Dummy: The user camouflages himself by sending a lot of false information to the service provider, but such methods may cause an additional load on the user on the one hand and may not suit many applications that require the correct information about the user (Yamin & Sen, 2018; Shady et al., 2017).

Obfuscation: The user obfuscates some data, such as changing their real location to another place close to themself, or changing some data about their age or gender so that the service provider cannot form an analysis of their personality or reveal accurate information about themself, but it may also lead to overloading the user due to processing inaccurate results and it also may not be suitable for applications that require accurate user information such as medical (Albouq et al., 2020; Yamin & Ades, 2009).

Anonymity: It is a simple method that hides the user's ID or replaces it with a hash code or a pseudonym. But this method is easy to break if the collected data indicates the identity of the user (Sen et al., 2021; Sen et al., 2020). Mix-Zone: It is an enhancement for the previous technique, the nickname is changed periodically to increase the level of protection and make the attacker's task to link data with user and create file for him more difficult (Sen et al., 2021; Butun et al., 2019). K-Anonymity: Anonymity user within group of K users, so the attacker or malicious service provider cannot differentiate between them, but it requires the presence of K users in one place and their consent to cooperate together to protect their privacy or rely on the Anonymizer (administrator of a specific geographic area) to manage the cooperation process (Sen et al., 2022).

Cache: Relying on some of the previous results and storing them for later use to reduce the number of contacts with the service provider, an approach that needs to be integrated with other approaches mentioned previously, such as TTP or Cooperation between Peers, for it to be an effective method (Sen et al., 2018). Private Information

Retrieval (PIR): The user must retrieve or query a huge amount of data from the service provider (SP). Hybrid: It is the integration of more than one approach to create a more efficient approach, for example, cooperation between Dummy and Cooperation or K-Anonymity and Obfuscation (Almutairi et al., 2021; Yamin & Sen, 2020). Other related issues are discussed in (Yamin, 2018; Chetty et al., 2022).

All the mentioned methods have advantages and disadvantages and each of them are suitable for dealing with a certain type of service, but in the issue of crowds, the matter is a little different. We often need accuracy in data whilst also having performance speed in addition to protecting privacy. Most of the previous methods suffer from these requirements. Additionally, the issue of crowding is a complex issue that contains many diverse sub-systems and therefore needs to propose a different, dynamic or hybrid approach to achieve better protection and adapt to the nature of each service, system or user. Therefore, a new approach based on fog computing is proposed that can provide important additional advantages associated with crowd management in addition to its role of protecting privacy, which is explained in detail in the next section.

PROTECTING FOR DATA PRIVACY

The rise of vigilant and malicious hackers has led to an increase in direct threats, blackmail, hacking, and data theft. Consequently, there's an urgent need for robust privacy protection methods to safeguard user data against both malicious attackers and unreliable service providers. This study introduces a dual-strategy approach to enhance data privacy within crowds, drawing on a systematic literature review to evaluate existing technologies like encryption, data mining, obfuscation, dummies, and Trusted Third Parties (TTP). However, these technologies fall short in fully securing and protecting data due to significant weaknesses. The proposed approach aims to bolster the efficacy of current privacy methods without compromising their performance, catering to complex systems, including crowd management applications. By combining various technologies under two main tenets: doubling the efforts of traditional data protection techniques and leveraging fog computing. The new strategy promises improved efficiency and performance. This innovative approach is designed to effectively support the diverse and complex systems and applications utilized in managing crowds.

Protecting privacy means protecting the right of people to determine who uses their data, when they use it, how they use it, and when they use it. This has become more difficult with modern technologies such as the Internet of Things and its various applications, such as smart cities, smart homes, innovative health, and intelligent transportation, as the Internet of Things tools are everywhere (Lee & Ahmed, 2021). For instance, the "About Us" page on any website collects data about people all the time, sending it to the cloud to be analyzed and study the behaviour of individuals to determine their preferences and then provide more intelligence and adaptive services (Jakimoski, 2016). Therefore privacy has become a real threat in the face of development or the onset of modern technologies. Techniques to provide privacy protection for users using these services are necessary to solve this problem.

Many countries have announced privacy laws and procedures that companies and service providers must adhere to achieve data protection and privacy. European countries announced the GDBR law for protecting users' privacy in 2016. This law also entered into force in 2018 (Edwards, 2016). The Kingdom of Saudi Arabia announced a similar law in 2020, but this law may not be considered sufficient or a guarantee for private individuals (Sirur et al., 2018). Communication has become more difficult in an era where information has become the real wealth because there is the threat of many malicious attackers seeking to collect data about people and selling it in masses to other criminals on the dark web (Alkhali et al., 2021).

These people may directly threaten or blackmail individuals, stealing or hacking their data. Some malicious servers play the role of the attacker by stealing the data of its users or leaking it to other parties such as advertisers and promoters, or as happens in some medical centers when some patient data is leaked to insurance companies or employment companies (Sirur et al., 2018). This poses a significant danger to users, and laws cannot be the only solution to such Threats. Therefore, it is necessary to build effective privacy protection methods and techniques to guarantee users' data privacy even when a malicious attacker or an unreliable service provider is present.

Privacy differs from security in various ways, and some researchers may consider it more difficult to achieve data privacy than security. According to

Jakimoski (Jakimoski, 2016), security is concerned with protecting the confidentiality of data and not revealing or exposing it when it is sent between two parties that trust each other, such as A and B. This can be easily achieved through the use of encryption algorithms. Security is also concerned with another standard of integration for data Integrity. Therefore, it is a guarantee that the data will not be modified when it is sent from A to B, who, as we indicated, trust each other (Sirur et al., 2018). The last criterion for security is availability, i.e. from A and B of penetration, the three security interests can be expressed in the CIA trio, which differs from the corresponding trio in the field of privacy, where privacy is concerned with protecting the user's anonymity, identification. Therefore, it is about sending data from A to B. Knowing that A is a user and B is a provider, A may not want to reveal the identity of B or to reveal the identity of any external attacker who eavesdrops on the data sent between A and B knowing that in privacy the transmitted data may not itself be data Confidentiality (Jakimoski, 2016).

The second criterion for privacy is to prevent tracking, which means protecting the user's location from being tracked by any external attacker or service provider. Protecting the user's location is crucial because it is unacceptable for the service provider to completely track the user's movements and whereabouts as this data is associated with services that depend on the location and which are shortened LBS-location-based services (Zakhary et al., 2013). Accessing such information may lead to significant threats to the user, up to a threat to his life or theft of his property if he is not at home (Zakhary et al., 2013). In addition, tracking may expose many secrets of users' privacy, such as the degree of their wealth or marital status, places of work, the nature of their work, their behaviour, morals, religion, etc. So, the third concern for privacy is to prevent profiling or to build a complete profile about the user by collecting all the inquiries and operations that they perform so that an external attacker or service provider can analyze this data to reveal a lot of user behaviour (Lee & Ahmed, 2021). For example, by collecting different user requests, we can determine a lot of information, whether the user is rich or poor, generous or stingy, the number of his family members, is there a person is carrying a child, are there children in the house or not, and any other private and personal information including average income of the user (Lee & Ahmed, 2021). The data can also reveal if users refuse to provide all this information to service providers. Therefore, privacy can be

summed up or defined by another definition linked to its trilogy concerning preventing an external attacker or service provider from disclosing or tracking a user's identity by building a file about their interests, behaviour, personality and preferences (Albouq et al., 2020).

This study finds that many technologies have been advanced to protect privacy, the most famous of which are dummies, obfuscation, k-anonymity and cooperation-peers to hide identity. This study has also discovered other methods, highlighted in the next section, which overviews the previous studies. Unfortunately, these methods have some weaknesses related to their impact on the quality of the basic service, their significant impact on performance or the ineffectiveness of some of them and the possibility of penetration easily. We called it so that the way each previous approach works is doubled, but in a way that does not negatively affect the level of performance, and at the same time, it will improve the level of protection achieved and address weaknesses in each approach. A: This is what we will prove by detailing the proposed approach and the results of the comparison. In this, we seek to protect privacy within an application of complex applications with smart technologies, which is crowd management. Crowd management is considered one of the problematic issues and challenges for most countries that conduct events and activities involving large crowds, especially when hundreds of thousands or millions of people gather in one place (Al-Shaery et al., 2020). For example, the Kingdom of Saudi Arabia witnesses more than 6 million Pilgrims gather in a specific area, such as the Arafat area or within the Two Holy Mosques in Mecca and Medina during the Hajj season (Felemban et al., 2020). Also, in the Karbala region, nearly 30 million people gather to visit a specific area, and in Kanpur, India, more than 150 million gather to perform Hindu religious rites (Felemban et al., 2020). Additionally, countries that host the Olympics or the World Cup tournaments also witness the presence of large numbers of people. Countries also witness large crows in specific areas during demonstrations, marches, celebrations or festivals. Thus, there is also a challenge to the method of protecting users' data privacy. For example, in the Kingdom of Saudi Arabia, the Ministry of Hajj provides thousands of services and applications that support these people (Al-Shaery et al., 2020). Pilgrims come from all world countries and have to deal with different service providers and many applications that facilitate their tasks during the Hajj period

and within the crowds. The challenge is how the country can ensure the privacy of users' data is protected during these periods. Our contributions to this research can be summarized as follows: A reference study of the existing methods of protecting privacy and identifying their weaknesses and drawbacks.

Propose a new approach to privacy that can enhance the level of effectiveness of previous or current methods without a significant impact on performance. Employing fog computing to enhance the level of performance and efficiency of some methods. Provide a case study for using the proposed model to protect privacy in crowds.

A comparison between the proposed approach and the traditional methods to prove the superiority of the proposed approach.

Based on what was previously discussed, we noticed that protecting the security and privacy of users is one of the most severe challenges facing the future of modern technology, smart services, and related applications. In this section, we will review the most well-known methods that were presented in order to protect users' privacy while highlighting the weaknesses of each of them.

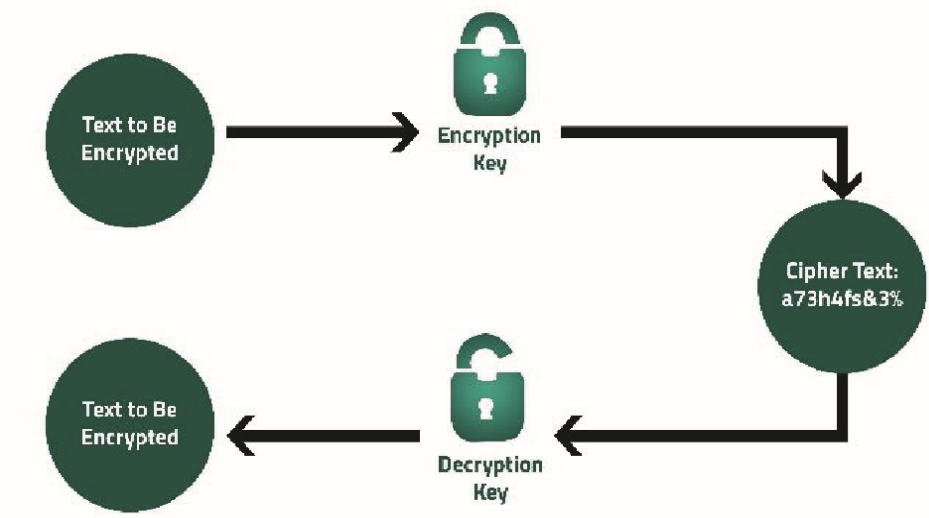

Fig. 6.3 Data Encryption Strategy

A. Encryption

First, encryption is a simple and common technique to protect the privacy of users' data from an external attacker.

However, the encryption process needs to be improved because, with the development of attackers' tools and capabilities, attackers can break this

encryption sometimes (Daniel & Momoh, 2021). In addition, if the service provider is hacked or the service provider itself is a malicious party, the encryption will not affect the protection of its activation, and the privacy of users will be easily compromised. Figure 6.3 shows the data encryption strategy.

B. Laws and Regulations

These laws and regulations require companies and service providers to give the user complete freedom to manage their collected data with the service provider and to delete or modify whatever data they want (Sloot & Zuiderveen Borgesius, 2018). In addition, these laws give the user the right to choose when service providers want to share, analyze, view or access his data. Despite the importance of laws to regulate the work of companies, they are not sufficient to protect the privacy of users when there is a malicious party that can circumvent laws, in addition to the fact that an external attacker can steal user data before it reaches the service provider and implement policies related to laws on it (Sloot & Zuiderveen Borgesius, 2018). Therefore, there are better solutions to protect privacy than laws.

C. Use of Statistical Techniques or Data Mining

This method is used in some systems and is effective in systems where the user is not required to send detailed data (Haoxiang & S, 2021). For example, such as systems that manages electricity consumption in smart homes. In these systems, techniques can be used to collect data and send a summary instead of sending Detailed data about the times of turning on and off devices at home, which may lead to a significant breach in the privacy of the user daily, but these methods can only be used in restricted and specific applications, and they also need to employ

an intermediate layer between the user and the service provider to achieve effective performance (Haoxiang & S, 2021).

D. Anonymity, Concealment of Identity

It is done by the user using a pseudonym, symbol, code, or hash code to hide his original identity from the service provider (Saeed et al., 2022). These methods are valid for dealing with the service provider for one time. However, in the event of continuous dealings with the service provider, the service provider can collect data or for an external attacker to collect data about the user and then reveal his fundamental identity, especially since the IP number is often the same in most connections (Saeed et al., 2022). Therefore this approach is not considered a practical approach to privacy in the event of continuous or repeated queries.

E. Mix-zones

It is considered a development of the previous approach because it can be used in systems that require dynamic queries or that the user raises during his movement, i.e. the user is not static and therefore requires the user to work on setting or changing his username or alias when entering a new zone every period of time (Khodaei & Papadimitratos, 2021). Time to improve the level of privacy, but unfortunately a malicious service provider or the attacker can also, in the event of tracking the user, re-associate the new name of the user with the data sent in the event of monitoring the footprint or the time of transmission with the site of the transmission for the use of the user and the nature of the query (Khodaei & Papadimitratos, 2021). Therefore, this method will not be effective in this case especially if the attacker has experience in the geographical areas within which the user moves.

F. Dummies

With this technology, the user sends a set of dummy queries accompanying his original query or sporadically sends dummy queries, and with every period of time, sends one of the actual query services (Wu et al., 2020). This approach is suitable for single queries where the user does not move. However, suppose the user moves and sends queries. In that case, dummy queries can be isolated from the actual query by tracking the time or the nature and type of this

query on the one hand, and on the other hand, the use of such methods may affect the performance of some services (Wu et al., 2020). For example, in crowds or congestion, sending dummies may increase the expected number of users in the service provider or their locations and thus will affect the main service related to managing and organizing crowds.

G. Cooperation

Users may cooperate with each other to hide their identities or mislead the service provider by sending a user to query another user or sending all users for the same query (Khosravi & Fereidunian, 2019). A sufficient number of users to apply what is known as k-anonymity, that is, to hide users within k-peer.

H. Obfuscation

The user modifies some private data before sending it to the service provider. For example, the user can change his primary location by choosing a location near or a certain distance away, according to the nature of the jamming or the level of protection he desires (Al-Balasmeh et al., 2021). However, this method may also affect the accuracy of the private data of the user, just as in the previous example of managing crowds or congestion on the one hand, and on the other hand, in the event of user movement and sending successive queries, the attacker or malicious service provider can draw a unique path for the user's movement (Allen, 2015). Similarly, in an area-attack attack, the attacker can draw a path for places the user navigates, thus revealing a lot about the user's data, tracking him, and breaching his privacy.

I. TTP

When we do not trust the service provider, we can rely on another provider for the protection service only so that the queries are sent to him so that he sends the queries on behalf of the users to the service provider (Soomro et al., 2016). However, the problem of the outside attacker remains on the one hand, in addition to the possibility of hacking the TTP itself, as it will also be a source of danger or The TTP itself may be malicious and thus penetrate the total privacy of the users cooperating with it (Kaur & Gupta, 2021). This technique may develop into a cloak area, a development of the previous technology by dividing the TTP into many TTP. However, each of them is responsible for a small area, a specific area, so that all users within this space are sent to this server, which only sends data about the region's

location and not the exact locations of the users within it (Kaur & Gupta, 2021). It then sends all the queries collected in one query to prevent the service provider from creating a profile for each user (Kaur & Gupta, 2021). This happens especially when there are not enough users within the region, and the cooperation of the TTPs responsible for the region, if it is malicious and cooperates with the service provider, can be compromised User privacy.

CANCELABLE HASHING FOR PROTECTING BIOMETRICS OF USERS IN CROWD

Smart gates are considered one of the most important methods for managing crowds. Often, methods of authentication and verification of users depend on the user's biometric fingerprints, such as hand or eye prints. Sending a picture of the fingerprint or eye to the server for verification is deemed unacceptable, especially in crowds, as it will significantly impact service performance in addition to imposing a heavy load on the network. Another, more serious challenge is related to the security and privacy of this data. If a user's fingerprint is stolen, it implies that all systems and services related to it, whether financial, medical, or otherwise, will be vulnerable to hacking. Unfortunately, the use of the traditional hash function is not sufficiently strong against a Replay Attack, and integration with blockchain requires substantial resources and suffers from delays that may impact the quality of sensitive services. In this solution, a Hash Function is proposed to enhance the level of privacy and security of biometric information. The hashing process will be doubled on one hand, and fog computing will be employed as an intermediary and additional protection on the other hand. Finally, the proposed technology will provide a solution to the problem of Relay Attack. The effectiveness and applicability of the proposed approach will be implemented and assessed.

Crowd management is regarded as one of the significant issues faced by most countries, particularly those hosting events with large gatherings such as sporting or religious events. The Kingdom of Saudi Arabia is among these countries, annually witnessing huge crowds exceeding 6 million people in one location during the Hajj season or the month of Ramadan (Yamin, 2019; Basahel et al., 2021) Fig. 6.4 shows an example of crowd.

Previous studies have looked at preserving privacy in IoT through various approaches (Sen et al., 2018). Wireless and mobile technologies can also help manage crowds by enabling contact tracing and mapping crowd dynamics (Yamin et al., 2018). During the COVID-19 pandemic, frameworks have been proposed for crowd management using AI to enforce social distancing and monitor health status (Almutairi et al., 2022).

While biometric identification provides high authentication reliability, it faces two main challenges for use in crowds. The first is time delay during matching of biometric data, especially with large volumes. Fog computing could help offload authentication processes from the cloud to reduce delay (Yamin, 2019). The second challenge is security and privacy of stored biometric templates. Revocable biometrics approaches that replace templates like variable hash codes have been suggested to address this (Yamin, 2019; Sen et al., 2018).

*Figure 6.4(*commons.wikimedia.org*, 2016) Example of Crowded in the Hajj*

This research aims to propose a solution for biometric authentication in crowds that addresses performance and privacy concerns. Additionally, a case study of the solution's application for Hajj crowd management in Saudi Arabia will be presented. The contributions will include a framework employing fog nodes and variable hash codes to enhance security, privacy, and reduce authentication delays in large crowds. The proposed framework addresses

performance and privacy issues related to biometric identification, providing a potential solution to improve security and decrease authentication delays in large gatherings. Additionally, the application of this solution in managing crowds during the Hajj in Saudi Arabia has important implications for enhancing safety and efficiency during the pilgrimage. This research contributes to advancing the available knowledge about crowd management and strengthens security in high-density environments by examining new methods including fog nodes and changeable hash codes.

With the technical development and the digital revolution, crowd management solutions have become smarter, and these solutions can solve many crowd problems. For example, the use of surveillance cameras and drones had a good effect in preventing unwanted or unauthorized persons from sequencing to gathering places. In the Kingdom of Saudi Arabia, a person needs a permit to obtain permission to perform Hajj, whether from inside or outside the Kingdom. There are many security barriers and an extensive deployment of security men who check the permits of every person who wishes to enter or behaves suspiciously. Electronic permits have also become one of the technologies used recently in crowd management and some other applications. Especially with smart devices, QR technology, and the availability of the Internet everywhere. All of this greatly facilitated the electronic authentication process, which depends on comparing inputs with data stored in databases. It can be divided into three basic types:

- An ID with a password, which is the easiest, most accessible, usable, and least costly, but it is also the most vulnerable to hacking. It has been newly developed with a third level of protection by sending a code to the mail or mobile phone as an SMS message.
- Code with a piece of hardware such as credit cards and electronic keys. This method is safer than the previous one, but at the same time, the hard piece may be stolen or forgotten by the user, who must always carry it. Thus, it is less usable, available, and more expensive than the first method. We note that both methods, unfortunately, cannot solve the problem of denial on the one hand, and on the other hand, still suffer from the problem

of fraud or theft, and therefore, complete reliability cannot be obtained by using electronic permits based on a code or an ID number.

- The third solution is biometric features, which is an alternative solution to the two previous methods. This method achieves very high, undeniable reliability, as it is always associated with the person, unless it is copied or forged. There are two types of these: first, physiological features, such as a face print, fingerprint, iris, or DNA, which are fixed and do not change with time. However, it is more expensive, so it is not commonly found in public places. The second type is behavioral, which may change with time, such as sound and signature.

Unfortunately, even biometric identifiers are vulnerable to attacks such as copying and reusing, and here the risk will be doubled, due to the non-change with time, and therefore the same fingerprint of a person can be used in another application or system (Ahmad & Shin, 2022). This type of authentication is used in many companies, universities, airports, and in many smart city applications. For example, attendance and departure systems often use a fingerprint, as well as entry operations to rooms that contain confidential or personal data also use this type of protection (Ahmad & Shin, 2022). Therefore, this type can also be used within crowds to ensure that no unauthorized person is defrauded or infiltrated, and also to give crowd management the ability to easily track people within crowds.

There are two main challenges to using this type (Biometic one) of authentication in crowds:

The first challenge is related to performance and the problem of time delay in the authentication process, especially in the case of big data that requires high computing power to process images and measure the similarity ratio, in addition to the accompanying encryption processes (Yamin et al., 2018). Within crowds, the process becomes more complex and may lead to long queues at security checkpoints. Relying on crowd capabilities to solve this problem is also not considered a sufficient solution, as even the cloud may suffer from delays when there are a large number of queries at the same time, such as in crowds (Yamin et al., 2018). Fog nodes, in their integration with the cloud, may play a positive role here, which will be discussed within the proposed solution.

The second challenge is related to the extent of the threat to the security and privacy of this confidential information for people. Data is often stored in the form of an arithmetic representation that can be called a template, and sometimes it stores more than one image. But what if this information is leaked or the server is hacked, people may be exposed to a real threat, as this data is often linked to sensitive systems such as financial or government systems. Thus, this information may be greatly misused. Unfortunately, encryption cannot be considered a sufficient solution in such cases, due to the possibility of penetration, especially with the development of the attackers' computing capabilities, in addition to the problem of Replay Attack.

Therefore, it is imperative to use a revocable biometrics approach so that the user biometric can be replaced as a password. There are many ways to achieve this, the most important of which will be mentioned in the next section. This research will discuss the solutions that have been presented in other researches and dealt with this issue on the one hand, and on the other hand, we will present a new proposed solution to the two previous challenges. Thus, the contributions to this research can be summarized as follows:

- A reference study on the challenges of using biometric fingerprint authentication in crowds.
- Proposing electronic gates in crowded areas with biometric identifiers to improve the level of privacy and security.
- Employing fog nodes to play a positive role in reducing the load on the cloud or service provider in the authentication process and to enhance the level of security as well.
- Suggesting the idea of a variable (replaceable) Hash code instead of a fixed one or a biometric fingerprint template.
- Presenting a case study on the application of the proposed solution in the Kingdom of Saudi Arabia.

The following parts will be a reference study for the current solutions in the field of biometric authentication, then we will discuss in detail the proposed

solution and finally we will discuss a case study on the application of the proposed solution within the Kingdom of Saudi Arabia.

In systems where high reliability is required, biometric identifiers must be used as an authentication method. However, this method itself may be vulnerable to security and privacy threats unless four necessary characteristics are observed:

- Diversity and non-correlation: ensuring that the same template cannot be used in another application.
- Revocability: that is, the template becomes useless if the system is hacked.
- Irreversibility: preventing the original data from being retrieved from the template.
- Performance The template generation method should not degrade system performance.

In Pillai et al. (2010) study, they used irreversible transformations by employing the signal field with linear and nonlinear transformations. While [Y] used hashing functions to access a unique, non-reversible token. Both solutions were to prevent the original image from being stored in databases and also to prevent it from being retrieved from its template. However, at the same time, the previous two solutions did not prevent some attacks, such as reuse or copying. Thus, a set of solutions to this problem were presented, which were discussed in several studies, including:

Sanjay et al. (2009) used the Salting feature, i.e. adding a password to the image of user's biometric before performing the conversion or hashing process, to obtain a distorted copy of the biometric data so that it cannot be used in another application. However, this method may fail if the password used is stolen.

Bolle et al. (2002) they used the idea of multiplying the die by itself again via XOR to create different variables, but this solution greatly affected the performance.

Johnson and Lindenstrauss (1984) used the displacement process, which is similar to the previous idea, but here using a random key, so the problem remains in stealing the key as well.

Rathgeb et al. (2014) random projections were used for some biometric features instead of using the whole template, but this method slightly affected the accuracy of the identifier in identifying the owner.

Alessandra and Loris (2007) they improved the previous method by using a random projection matrix, but it did not completely solve the accuracy problem, especially if the same matrix was used by different users.

Kanade et al. (2009) they reconfigured the fingerprint block in a different way, such as cutting the image into parts, then randomly changing its arrangement, and then performing the conversion process. Also, this method did not solve the problem of reuse when copying.

Hao et al. (2006) bio-Hashing They arranged the template in the form of a vector and then rearranged the bits or took bits from certain numbers only and not all of them.

"Multi-biometrics based cryptographic key regeneration scheme" they used the Bloom filter technique as an array of ones and zeros with a hash function, in which bits are replaced by corresponding bits.

Malallah et al. (2014) they used a special table to manage the process of rotating the bits to the right or left, after dividing the block into words and encrypting them.

We note that all previous methods tried to achieve the four basic features to provide protection in the event of a breach of one of the systems used for biometric identifiers, and therefore this system will not affect other systems that the user himself needs. But at the same time, these methods suffered from a major problem related to the possibility of reuse in the event of copying within the same system, on the other hand, some methods suffered from the performance issue. Therefore, in this paper, we present a different way to solve the two previous challenges, whereby we introduce the idea of a biometric identifier that changes periodically through an improvement on the Salting approach. Instead of using a fixed password added to the hash function of the fingerprint, an automatically increasing number will be used with each new authentication query.

More than that, we suggest the use of fog nodes that will be distributed in the crowd area as companions to digital gateways, as these nodes improve the performance of the authentication system by performing some processing operations on behalf of the end user and the server by the fog node.

The following table shows a quick comparison between the previous methods in terms of the way they work and their limitations.

Table 6
Previous Methods Comparison

These studies collectively aim to address the critical aspects of biometric template protection, considering factors like irreversibility, revocability, diversity, and performance. However, each method has its own set of limitations that need

Study	Title & Authors	Method	Limitations
[1]	"SECTORED RANDOM PROJECTIONS FOR CANCELABLE IRIS BIOMETRICS" - K. Pillai, M. Patel, Chellappa. Rama, K. Ratha	Irreversible transformations using signal field with linear and nonlinear transformations.	Prevented image storage but didn't fully guard against attacks like reuse or copying.
[2]	"Cancelable Iris Biometrics and Using Error Correcting Codes to Reduce Variability in Biometric Data" - K. Sanjay, D. Petrovska-Delacrétaz, D. Bernadette	Utilizes error correcting codes to reduce variability in biometric data.	Reduces variability but not foolproof against data theft
[3]	"Biometrics Perils and Patches" - M. Bolle, H. Connel, K. Ratha	XOR multiplication of data for diversification	Performance degradation due to XOR multiplication.
[4]	"Extensions of Lipschitz Maps into a Hilbert Space" - W. Johnson, J. Lindenstrauss	Implements the Salting feature to distort biometric data.	Vulnerable if the added password is stolen.
[5]	"On the Application of Bloom Filters to Iris Biometrics" - C. Rathgeb, F. Breitinger, C. Busch	Uses random projections for some biometric features.	Slightly affected accuracy in identifying users.
[6]	"An Improved BioHashing for Human Authentication" - L. Alessandra, N. Loris	The study presents an improved BioHashing method for human authentication.	Limited accuracy improvement, especially for shared projection matrices.
[7]	"Application of Biometrics to Obtain High Entropy Cryptographic Keys" - S. Kanade, D. Camara, D. Petrovska-Delacrétaz, D. Dorizzi	Utilizes displacement process with a random key.	Vulnerable if the random key is stolen.
[8]	"Combining Cryptography with Biometrics Effectively" - Hao, F., Anderson, R., Daugman, J.	Combines cryptography with biometrics for security.	Effectiveness depends on the strength of encryption.
[9]	"Multi-Biometrics Based Cryptographic Key Regeneration Scheme"	Uses Bloom filter technique for cryptographic key regeneration.	Efficacy relies on the robustness of hash functions.
[10]	"Non-Invertible Online Signature Biometric Template Protection via Shuffling and Trigonometry Transformation" - F. Malallah, S. Mumtazah, W. Adnan, S. Yussof	Involves rotating bits using a special table and dividing the block into words. |	Security dependent on the secrecy of table and key.

to be carefully assessed in the context of specific applications and security requirements. Further research is necessary to refine and improve these techniques while mitigating their limitations.

2.14 HEALTH AND WASTE IN CROWDS

Park et al. (2021) explored the impact of the COVID-19 pandemic on travelers' preferences for crowded versus non-crowded travel options. They found that the pandemic has led travelers to favor less crowded destinations and activities, with this preference influenced by individual factors such as sensation seeking and a need for uniqueness. This shift has significant implications for tourism management and marketing strategies during health crises.

Shambour and Gutub (2021) explore the integration of IoT technologies in managing the Hajj and Umrah pilgrimage, emphasizing the potential of such innovations to enhance the efficiency and safety of these significant religious events. Their review categorizes existing research into areas like crowd management, housing services, and the application of smart technologies, underscoring the importance of IoT in improving the pilgrimage experience for millions of Muslims annually.

Pouw et al. (2020) developed an efficient framework for real-time monitoring of physical distancing in crowded spaces, utilizing pedestrian tracking data to distinguish between family members and non-family members in compliance with COVID-19 guidelines. This approach enables effective crowd management and physical distancing enforcement, highlighting the potential of technology in supporting public health measures during the pandemic.

Abdulrazaq et al. (2020) developed an IoT-based smart helmet for early COVID-19 detection, utilizing thermal imaging and facial-recognition technologies to identify fever symptoms in crowds with minimal human interaction, potentially reducing virus spread.

Fedele and Merenda (2020) developed an IoT system aimed at enhancing social distancing and emergency management in smart cities, utilizing multisensor data to enable real-time planning and crowd management. This system employs IoT-based Wireless Sensor Networks (WSNs) and algorithms for identifying safe exits and managing overcrowding, demonstrating a significant application of technology in urban safety and quality of life improvement.

Waste management has long been a critical issue for urban areas, grappling with the dual challenges of efficiently managing increasing volumes of waste and

mitigating environmental impacts. The COVID-19 pandemic has further complicated these challenges, introducing new dimensions such as the disposal of personal protective equipment and the need for contactless waste collection mechanisms (Onoda, 2020).

Alshalani et al. (2020) emphasize the significance of incorporating ICT systems into crowd management, indirectly highlighting the potential for similar technologies to enhance waste management in densely populated settings.

The insights provided by Alshalani et al. (2020) and Onoda (2020) underscore the critical role of technological innovations in transforming waste management practices, highlighting the potential for these advancements to contribute to the sustainability and resilience of urban areas in the face of ongoing and future challenges. As cities worldwide strive towards the vision of smart urban living, integrating smart waste management systems will be crucial in achieving these goals, ensuring a healthier, more sustainable, and efficient urban environment.

Sosunova and Porras (2022) sheds light on the multifaceted nature of waste management challenges and the necessity for a holistic approach that encompasses not only technological solutions but also considers the roles and interactions of various stakeholders involved in waste management processes. From municipal authorities to citizens and waste management companies, each stakeholder plays a pivotal role in the ecosystem of smart waste management, and their engagement is crucial for the successful implementation and operation of SWM systems.

Smart cities promise a lot of progress and development in the level of services for their residents and in all areas of life, such as health, transportation, education, energy, entertainment, and others. Waste management is one of the important areas for which smart cities promise to provide effective solutions. The importance of these systems comes from the fact that they overlap and integrate with other systems such as transportation and health. It also greatly reflects the level of development in cities and plays an important role in displaying them in the most beautiful way.

The matter can become more complicated in cases of crowds, which produce huge amounts of waste in a short time, and if it is not treated correctly and in a timely manner, it may cause many health problems or even stampedes and crowding incidents.

Chapter 3: A Framework for Crowd Management

The aim of this chapter is to provide a summary of the research conducted so far. In particular, we shall present a design and architecture of a comprehensive framework for the Crowd Management System (CMS) to manage and control the crowds and issues arising in event management. We shall also discuss various details of the CMS.

Crowd management requires integration of multi domains and many of their services and technologies. There is no single service or application which can solve this issue completely. The proposed CMS works under the umbrella of the IoT, in addition to components of many new technologies and techniques. While combination of several technologies and tools has its merit in solving critical issues, it also raises the issues of security and privacy in addition to the issue arising by interoperability.

It is well known that most of the crowd related issues arise due to overcrowding and congestion. The proposed CMS has been designed to provide a comprehensive solution for the most critical and underlying issues of crowding like stampedes, healthcare and emergencies, transportation, and entry permits.

The Crowd Management System (CMS) framework was developed using the traditional four-layer IoT architecture, consisting of the Sensing Layer, Fog Computing Layer, Computing Layer, and Application and Services Layer. Each layer integrates various technologies to manage and control crowds effectively.

The Sensing Layer is crucial for collecting real-time data through a variety of devices and technologies, including Wireless Sensor Networks (WSNs), Radio Frequency Identification (RFID), smartphones, and smart vehicles. This layer gathers real-time environmental and crowd-related data, forming the foundation of the CMS framework. According to Pister, Kahn, and Boser (1999), the concept of "smart dust" enables wireless networks of sensor nodes, which are integral to the CMS framework's sensing layer for capturing detailed crowd movement and environmental conditions.

The Fog Computing Layer processes the collected data locally to reduce latency and allow rapid decision-making. Akyildiz, Su, Sankarasubramaniam, and Cayirci (2002) highlight the importance of distributed sensor networks in environments requiring real-time data analysis, such as crowd management. The Fog Computing Layer provides localized, decentralized data processing, which is essential for mitigating crowd-related issues before they escalate.

The Cloud Computing Layer enhances the fog layer by providing large-scale data storage, computational power, and long-term data analytics. Buyya, Yeo, Venugopal, Broberg, and Brandic (2009) note that cloud computing is emerging as the fifth utility in IT, offering scalable computing power that is crucial for processing massive datasets generated by IoT devices and ensuring the seamless functionality of the CMS framework.

Finally, the Application and Services Layer integrates the processed data into useful applications, such as crowd flow management, emergency detection, and health monitoring. This layer offers services that directly interact with end-users, ensuring that real-time information and guidance are provided during crowded events. Kim, Ramos, and Mohammed (2006) emphasize the role of the Internet of Things (IoT) in building next-generation pervasive systems that are vital for crowd management applications, offering comprehensive solutions for event organizers and participants.

In view of the ongoing COVID-19 pandemic, we shall also present a framework for managing and controlling crowded events, which is a part of the Application & Services Layer of the CMS framework. The CMS uses current technologies, including Artificial Intelligence (Machine Learning and Regression), Internet of Things, Cloud and Fog computing, and digital gadgets and tools. The current and future research will relate to this framework.

Technical architecture of the CMS is shown in Figure 3.1. It has four layers, which, with the help of technologies, provide a comprehensive solution to the problems of congestion, stampedes, healthcare, safety, security, transportation, awareness, and guidance. Each layer outlines several modules, which are dependent on technologies included in the layer. One of the most important components of the proposed framework is a model of Crowd Flow Management (CFM), which uses

different technologies and tools like high resolution cameras, Image processing, IoT, Sensor Networks, Cloud and Fog Computing, Smart Street, Location based Services (LBS), GPS, and RFID to detect and mitigate stampedes before they cause any damage.

CONTRIBUTION TO THE FRAMEWORK DEVELOPMENT AND IMPROVEMENTS:

The author's contribution to the CMS framework includes significant improvements by incorporating new technologies and expanding the system's capabilities to address modern challenges. One key contribution was the enhancement of the Sensing Layer by incorporating advanced sensor networks and IoT devices to collect more accurate and timely data on crowd behaviors. This aligns with the principles outlined by Pister et al. (1999) in utilizing smart dust and sensor nodes for real-time environmental monitoring.

Further improvements were made in the Fog Computing Layer by integrating advanced data processing techniques to allow for immediate crowd control interventions based on real-time analytics. The distributed nature of this layer, as described by Akyildiz et al. (2002), enables faster responses to potential crowding issues, improving overall system responsiveness.

In addition, enhancements to the Cloud Computing Layer improved the scalability and efficiency of data storage and processing. This layer's ability to handle large datasets and perform complex analytics aligns with the vision of Buyya et al. (2009), who describe cloud computing as a powerful IT utility for handling large-scale, real-time data processing.

Finally, improvements were made to the Application and Services Layer by developing user-friendly applications for crowd management, including tools for crowd flow tracking, emergency response, and health monitoring. These tools provide

real-time feedback and guidance to both event organizers and participants, reflecting the integration of IoT and pervasive systems as highlighted by Kim et al. (2006). These contributions significantly advanced the CMS framework's ability to manage large crowds safely and efficiently, particularly in high-risk environments such as large events or religious gatherings.

3.1 LAYERS OF THE PROPOSED FRAMEWORK

There are four layers in the CMS, and each layer has several modules. In this section, we shall describe these layers. We shall also describe the underlying technologies, and their role in the proposed framework as shown in figure 3.1. Our description of layers follows the bottom-up approach.

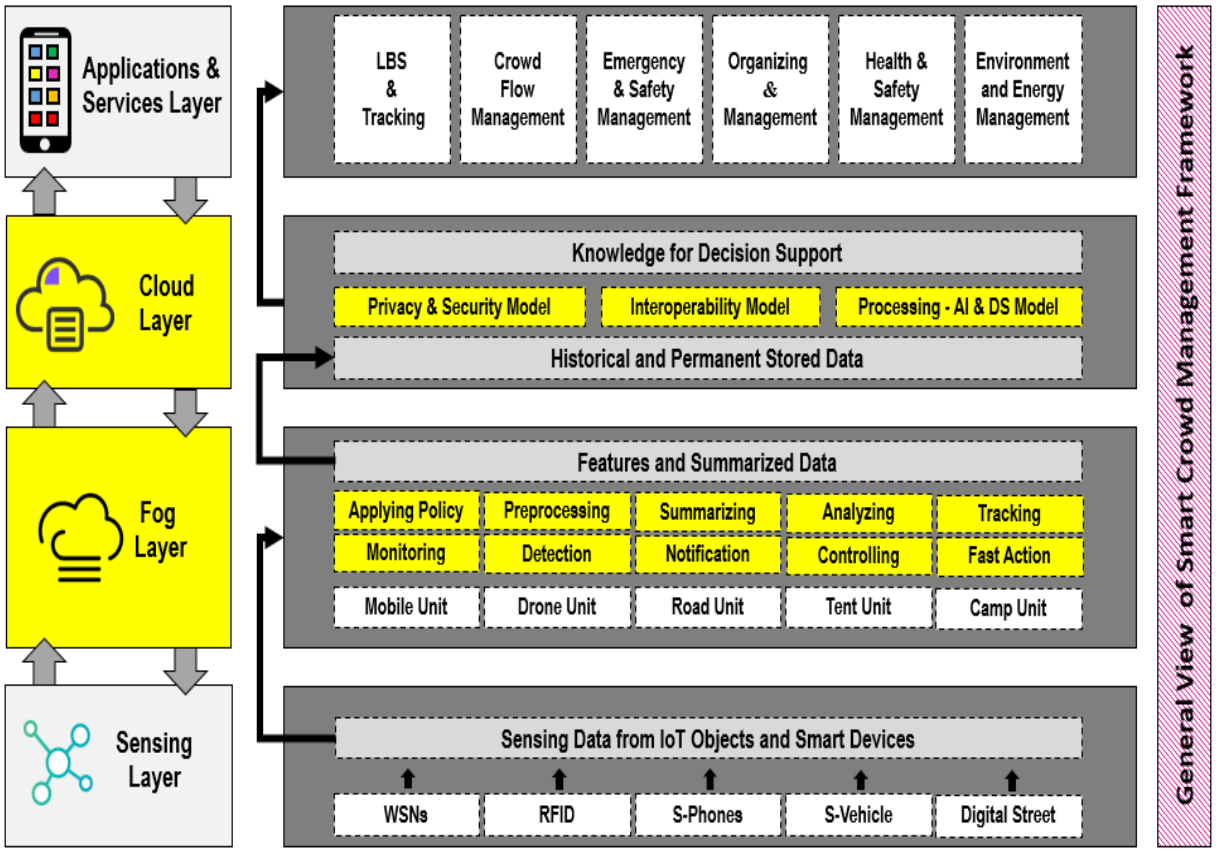

Figure 3.1: Architecture of Crowd Management System (CMS) framework

3.1.1 SENSING LAYER

The sensing layer, depicted at the bottom of the CMS architecture in Figure 3.1, and is crucial for the system's functionality. It incorporates Wireless Sensor Networks (WSNs), Radio Frequency Identification (RFID), Smartphones, Smart Vehicles, and Digital Streets. These components execute distinct tasks but, when combined, they facilitate comprehensive solutions, addressing numerous challenges and alleviating traffic-related issues efficiently.

The sensing layer also uses different objects and technologies for collecting data from users or environments like WSNs, RFID, S-Vehicle like Drones, Smart Phone and some specific applications, or social medial, in addition to Digital Street which will play an important role in the control flow of the crowd. More details about each possible thing in each type of sensing resource is presented in Figure 3.2.

3.1.2 FOG COMPUTING LAYER

Chapter 2 discusses Fog computing's role in rapid data processing and its critical function in preemptively identifying stampedes, thereby preventing disasters. Fog computing supports necessary calculations for Sensing layer tools and technologies, offering an effective environment for these operations. Additionally, it serves as a temporary data storage solution for applications, enhancing the overall efficiency and responsiveness of the system.

Fog node can be a drone, unit on the road, or the mobile phone of the users themselves. A large number of these nodes have to be distributed to cover the entire crowd area, where each node will be responsible for cluster of sensing objects. That will create a hierarchy of nodes and provide a faster response. Moreover, fog nodes will provide other important services like pre-processing and analysing data, monitoring signs, detecting any event, applying policies on data for more security and privacy, and notifying users in the sensing layer and guiding them. Then all the summarized data will be sent to the cloud for more computing power and permanent storage.

3.1.3 COMPUTING LAYER

Chapter two compares Cloud and Fog computing, highlighting Cloud Computing's essential role in wireless applications. It details specific roles for both technologies, emphasizing that Cloud Computing enhances Fog's functionality, particularly in detecting stampedes, by extending its capabilities.

As we know, besides other functionalities, cloud computing is used for storing data and providing three important functionalities:

a) Processing historical data to detect new useful knowledge from previous experience by using DS algorithms and techniques

b) Protecting the privacy and security model with the proposed approach on the data of users to prevent any potential attack

c) Enabling different services and devices to work together by providing an interoperability method for heterogeneous services and devices.

3.1.4 APPLICATION AND SERVICES LAYER

This layer supplies all the necessary applications for stampede detection, with their foundation extending from the Sensing layer up to the Cloud computing layer, making them available for use at this layer. A summary of these services is provided following this section.

In this layer, we have proposed six service domains for important sub-systems that have a direct or indirect effect on crowd management, which are: LBS & Tracking, Crowd Flow Management, Crisis & Stampede & Emergency Management, Organization issues, Health & Safety, and Environment & Energy. Each sub-system has many important services to help us comprehensively manage the crowd related issues, which are mentioned in Figure 2.

3.2 MODULES IN THE APPLICATION LAYER

Frontline activities are part of the Applications layer. Following is the description of the modules, services, tasks, and activities of the Applications layer.

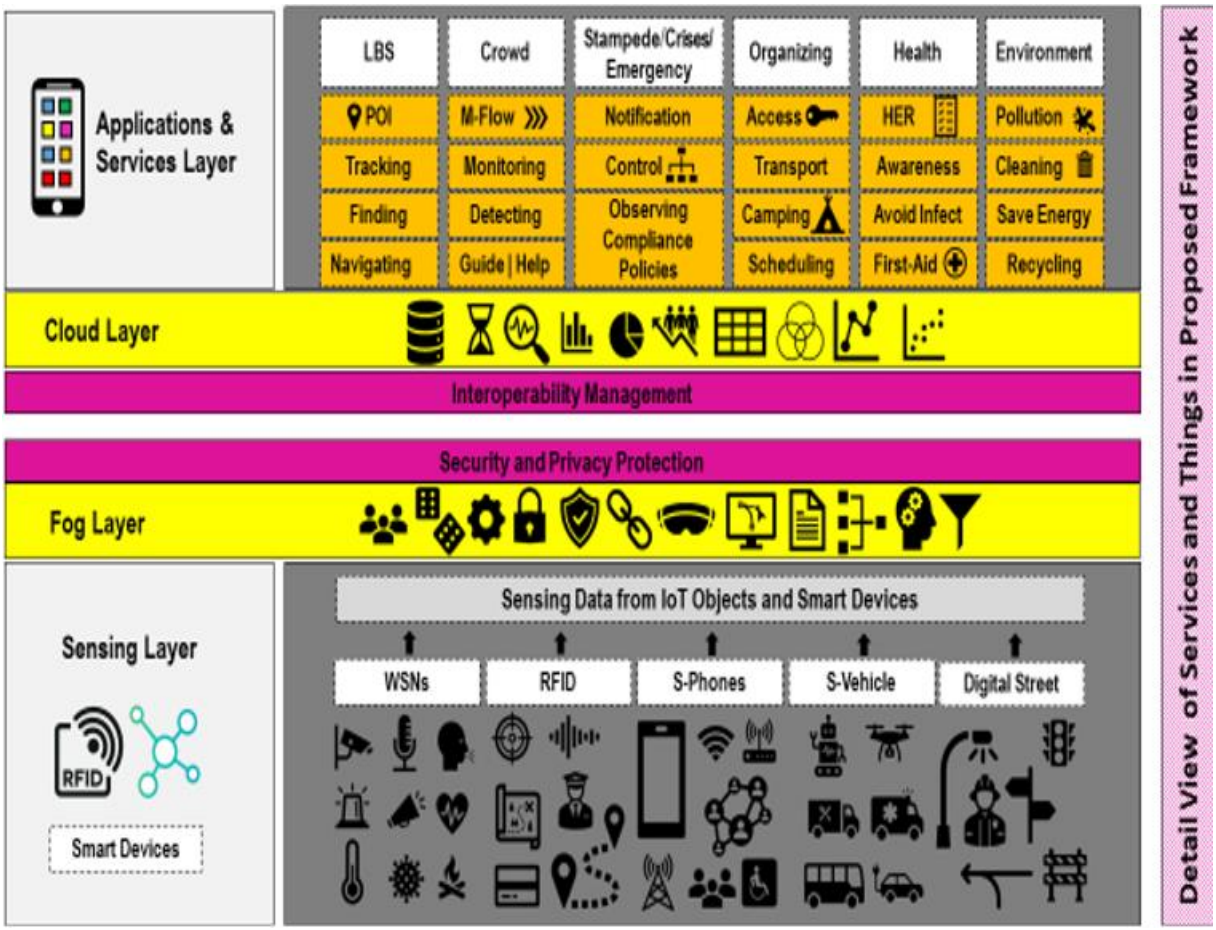

Figure 3.2: Modules in Smart Traffic Framework

3.2.1 LOCATION BASED SERVICES (LBS)

Location based Services (LBS) is an environment to provide many services to different kinds of users. Many IoT and Digital Street Applications take place with the LBS. In the LBS, there are privacy issues, especially the need to protect Identity, and location privacy from the SP themselves. As will be seen later, the Stampede and Crises Management would make use of the LBS for some applications. Privacy and security issues also use the LBS. A list of applications in the LBS follows:

3.2.1.1 PLACES OF INTEREST (POI)

This service is aimed at helping the user (a member of the crowd) search for specific services centres, restaurants, police, or a medical centre. This will be required in future studies with the implementation of a mobile application.

3.2.1.2 TRACKING

Tracking is used by users to get information about their location and the health and safety condition in each cell or area of the crowd. This would be useful for implementing the framework in relation to keeping track of the participants of a crowded event. In future studies, we shall provide the tools and scenario of applying this service. This service will be facilitated by RFID.

3.2.1.3 LOCATION OF MISSING ITEMS

This service will be used to find lost items such as a personal item of luggage or person. This service can only track the items which are tagged with the RFID. We shall provide this service in the proposed mobile application.

3.2.1.4 TRAVEL NAVIGATION

This service will help user to select the best route to reach their destination in the crowd. We will provide this solution for the internal and external environment.

3.2.2 CROWD FLOW

This service application is designed to ensure smooth crowd flow, which is critical in avoiding a stampede. Several actions are involved in this process, which are described as follows.

3.2.2.1 MANAGE FLOW

This service aims to regulate crowd movement effectively by selecting the most appropriate solutions based on the specific circumstances, including the use of digital streets, drones, and providing instructions to crowds via mobile applications.

3.2.2.2 MONITORING

This service will monitor the flow of the crowd and confirm it is flowing smoothly without problems. Smart algorithm will monitor crowd flow by Image Processing and RFID Tracking.

3.2.2.3 DETECTING

This service will depend on previous information to detect any anomalies and abnormal trends in the crowd. A Smart Algorithm is used to detect any abnormal event

in the crowd by Text mining through social media, notifications of users in the crowd, and image processing.

3.2.2.4 GUIDANCE AND SUGGESTIONS

This service will enhance the awareness of users in a crowd about the timing, events or activities, signs, and other relevant information. We shall provide this service in the proposed mobile application.

3.2.3 STAMPEDE, CRISIS AND EMERGENCY MANAGEMENT

There are several tasks and activities for the Crisis and Stampede management to deal with and response to. These are listed and summarised below.

3.2.3.1 NOTIFICATION

The framework provides scanning mechanisms for surveillance facilities to detect and mitigate issues before they arise and cause harm. Whenever any abnormal activity is detected in the crowd, it would be duly notified to the management and to the participants depending on the relevance. This would facilitate for management and participants to take the appropriate course of action. There would be ways of reaching the participants, usually through apps mandated by the management and subscribed to by the participants, or by announcements on the PA system and digital media.

3.2.3.2 CONTROL

This task would come into action once a notification is received by management to control the crowd in abnormal situations like a stampede, fire, flooding, or in crises like the one which has been created by COVID-19. We shall provide a new protocol to deal with crowds in the case of crises, in addition to providing a method to control CrowdFlow after a crisis (stampede or other disasters) to prevent any disaster.

3.2.3.3 COMPLIANCE

This activity is to check that the participants and organizers are complying with the norms and procedures. It would trigger an alarm if there is non-compliance. This activity is for both normal and abnormal situations. In normal situations, it is to enforce and ensure that all users adhere to the rules safety to avoid all manmade disasters. We shall provide an algorithm for auto monitoring of users to enforce compliance in normal and abnormal situations.

3.2.4 ORGANISING

Organising is one of the most important functions of the any management. There are many tasks linked to Organising. In the context of crowd management, several activities of procuring and providing services to the members of the events require organisation. Here, we provide the details of some of them.

3.2.4.1 ACCESS CONTROL

This functionality is to prevent unauthorised people gaining access to any part of the system. This task is important to safeguard the information on the system. At a later stage, we shall provide a comparison between many different methods for physical access and proof of their presence.

3.2.4.2 TRANSPORT

Often there are significant issues in transporting participants from one location to another. Sometimes, the event also needs to organise the transportation of participants from the relevant airports to the event and vice versa. Transport may include several means (buses, trains, ships, and aeroplanes), depending on the nature of the event. Transport also requires web applications to manage trips, buses, trains, routes, among others.

3.2.4.3 CAMPING (TEMPORARY ACCOMMODATION)

In some crowded events, it may be a good management practice to divide users in to groups and each group would be a cluster in the same camp to help manage them efficiently. For example, in Hajj, about two million pilgrims are provided tent accommodation in Mina, comprising of tents of different sizes.

3.2.4.4 SCHEDULING

This activity deals with organizing the periods of activities for each group in order to reduce the overload on any area or service during the course of the event. It would often utilize a web service to manage the activities, timing, and locations, among other functions.

3.2.5 HEALTH AND SAFETY

The Health and Safety unit would be operated with the help of the Electronic Health Record (EHR), whose details follow. An Electronic Health Record will be created for all participants (users) in the crowd. This would include biometric data, which would play a highly critical role in identifying the injured and deceased participants and officials. This functionality would be very useful in emergent cases and challenging situations (stampede, fires, and earthquakes). We shall provide a web application to comprehensively manage the health data with many electronic services using WSNs, RFID, Surveys, etc.

3.2.5.1 AWARENESS

This function will be used for regular health advice and alerts to the participants. This will help participants to protect their health in crowds. The messages would be sent to the registered mobile numbers of the participants through mobile applications.

3.2.5.2 INFECTION TRACKING

This is another messaging service designed to protect participants from becoming infected by different viruses and diseases. This service would operate by detecting and tracking infected participants and isolating them to a safe environment. In this way, other participants can be prevented from becoming infected. We shall provide an algorithm to detect and track infected participants and notifying others of possible exposure with infected people. As a result, they would be quarantined for a specified period. An algorithm would be provided for observing precautionary rules and detecting violations.

3.2.5.3 FIRST AID

Crowded events usually get a significant number of accidents, some of which result in injuries. These and other emergency cases should be provided medical attention and treatment, if required. We shall provide:

- A Smart Application to enable users to help themselves in emergency cases.
- A Smart algorithm and tools to enable the relief team to arrive quickly to the incident location in the crowd.

3.2.6 ENVIRONMENT AND ENERGY

In some congested events, environmental issues, such as pollution, have become critical issues. This requires monitoring weather on a continuous basis, and taking appropriate actions.

3.2.6.1 POLLUTION

In the case of a worsening situation, management is alerted and notified of any change in the regular ratios.

3.2.6.2 CLEANING

Cleaning during congested areas is not an easy task because access is often blocked. This can turn some parts of the crowded areas into waste dumps. If the waste is not removed within 72 hours, then the waste generates bacteria, which can cause an endemic. Therefore, timely cleaning must be given priority. This would preserve the environment and prevent the spread diseases. We suggest smart containers and smart method to collect waste in crowded events. We also advocate for a mobile service for waste collection.

3.2.6.3 PREVENTION OF ENERGY WASTAGE

Energy is a precious and costly resource, and it must be preserved. Saving energy results in a positive impact on the carbon footprint of an event as well as money saved. Smart technology will be used here in order to conserve and generate energy. We shall provide a checklist of requirements which should be agreed upon by the event organisers.

3.2.6.4 RECYCLING

Dealing with the waste has now become a global issue. Many ways have been suggested to deal with household waste. One of them is recycling, which preserves resources and hence the ecosystem, whilst also limiting a contribution towards global warming. We suggest auto health screening of crowd waste in order to promote a healthy environment. We shall provide an algorithm for filtering waste in the crowd.

3.2.7 OTHER FUNCTIONS

Apart from the above-mentioned utilities and applications, there would be some other functionalities to improve the safety and wellbeing of the event participants. For example, there may be a need to provide a web based automated and secure parking system, enabling participants to book a parking spot before arriving at the event. This would help alleviate undue crowding in the search of parking.

Another very useful utility would be to provide an environment to protect participants' security and data privacy. For this, a method to protect data privacy relevant to crowding will be proposed.

Chapter 4: Managing Crowds during COVID-19

COVID-19 has warranted the management of crowded events to enforce restrictions to contain the spread of the virus. Unfortunately, as discussed in the previous chapters, we have witnessed numerous events that have not enforced these restrictions, resulting in an increased spread of the virus, in numerous cases. In order to contain the spread of such a highly contagious disease, several restrictions, including wearing face masks, maintaining social distancing, and adhering to regular cleaning and sanitisation are critical. At times, events in some parts of the world occur spontaneously and can often grow into an unmanageable crowd. Controlling spontaneous crowded events, such as political rallies, protest marches, funeral processions, and musical concerts can be quite a daunting task, especially during the current COVID-19 crisis. In this chapter, a framework for organising crowded events during COVID-19 is proposed. This framework would be identified as COVID-19Crowd. During future studies, to guide the proposed framework, an algorithm will be proposed, modelled with machine learning and regression analysis. Validation of the proposed algorithm would also be provided. As the proposed framework mandates participants to register for the event and acquire entry permits, event data can be collected and analysed to improve future organisation and management.

Organisation of crowded events often involves complex tasks. But to organise them during an ongoing crisis or pandemic, such as COVID-19, which requires adherence to many restrictions, would be much more difficult. However, persuading or forcing participants to maintain adequate social distancing is very difficult. Currently we are passing through the COVID-19 pandemic. Several aspects of this pandemic have been discussed (Yamin, 2020; Bardesi et al., 2021; Bajaba et al., 2021; Yamin et al., 2021), which was first detected on 31st December 2019 in the Wuhan city of the Wuhan Province of China. Global efforts to check the spread of the virus has so far received mixed success. Most countries have been passing through multiple waves of the virus. Sadly, since its start, several variants of COVID-19 have emerged. The Delta variant of COVID-19, which was first detected in December 2020 in India (Planas et al., 2021), has spread into many parts of the world causing a large number of deaths in many parts of the world (del Rio et al., 2021).

The World Health Organisation (WHO) has approved several vaccines for emergency use but their effectiveness, especially against the Delta variant, is questionable (Solis Arce et al., 2021; Sanderson, 2021). There has been very little success in the treatment of the COVID-19 disease (Rodriguez-Guerra et al., 2021; Nalbandian et al., 2021). However, certain measures recommended by the WHO have been proven to be effective to contain the COVID-19 virus and are agreed upon globally. These include social distancing, limiting exposure, wearing a mask in public places, regular cleaning, especially of hands, using gloves, regular sensitisation, and others.

Crowded events, especially social, religious, recreational, and political gatherings, are part of our life. We have witnessed the cancellation or downsizing of many events due to the ongoing pandemic. Unfortunately, we have also seen many out-of-control crowded events with or without the involvement of the regulatory bodies (government of the country or the region). Some important crowded events which have taken place during this pandemic are analysed below.

We have witnessed several regular and irregular organised events with crowds during the COVID-19 pandemic. While some of them mandated and implemented the pandemic restrictions, others have failed to do so. Most of these events are religious in nature so the reasons for failures to comply with COVID-19 restrictions may be due to religious perceptions.

We can find many crowded events with a lack of proper management or poor organisation, which may have contributed to the spread of COVID-19. As the pandemic goes on, so do these kinds of events in different parts of the world. The ongoing mismanagement and poor organisation has encouraged us to provide a framework for organising crowded events. Section 4.1 outlines details of the proposed framework.

PURPOSE OF THE FRAMEWORK AND CONTRIBUTION

The primary goal is to manage large crowds effectively during pandemics like COVID-19, ensuring that health protocols such as social distancing, mask-wearing, and sanitization are maintained. The framework is designed to minimize the risks of contagion and streamline event management through smart technologies.

My contribution to the framework appears to involve the structuring of its key components, particularly the use of advanced technologies such as machine learning, RFID, cloud computing, and data analysis to enhance crowd management.

The framework is composed of several modules that work together to manage crowds and ensure safety:

- Smart Application for Interface and Communication.
- Data Transfer for Connection and Networking.
- Information Gathering from Sensing Components.
- Data Analytics.
- Semantic Modelling and Reasoning.
- AI Model for Decision Making.

JUSTIFICATION AND DEVELOPMENT PROCESS

The development of the framework was influenced by:

- **Observation of Failures in Event Management During COVID-19**: Many crowded events lacked proper management and resulted in further virus spread, necessitating a better framework for handling such events.
- **Technological Integration**: The decision to integrate machine learning, AI, and IoT technologies was based on their ability to process large amounts of data in real-time, predict outcomes, and provide knowledge-driven decision-making.
- **Adaptability**: The framework is designed not just for COVID-19 but for any similar crisis, making it a flexible solution for crowd management in pandemics or natural disasters.

The decisions to incorporate these specific technologies and methods were driven by the need to manage large gatherings effectively during crises like pandemics. The framework integrates:

- **Machine Learning**: For predictive analytics and data-driven insights, machine learning models allow for adaptive learning from event data, improving future event planning and management.
- **RFID and Sensors**: These technologies provide real-time data on crowd movement and environmental factors (like temperature or proximity), ensuring health guidelines are maintained.
- **AI-based Decision Making**: The AI model was justified because of its ability to process large datasets and provide real-time insights without human intervention, reducing human error and improving the response time for critical decisions.

This development process involves systematic integration of real-time data collection, processing, and analysis, ensuring that the framework not only addresses current needs during COVID-19 but is also adaptable for future crises.

4.1 PROPOSED FRAMEWORK

Figure 4.1 depicts a model for the proposed framework for organising crowded events during the ongoing pandemic. The framework is designed for crowded events during the COVID-19 pandemic but can also be used during other pandemics and crises caused by natural disasters or other similar events. This framework uses several tools and technologies including Machine Learning, RFID, Cloud Computing, APIs, sensing tools, and data analysis and processing.

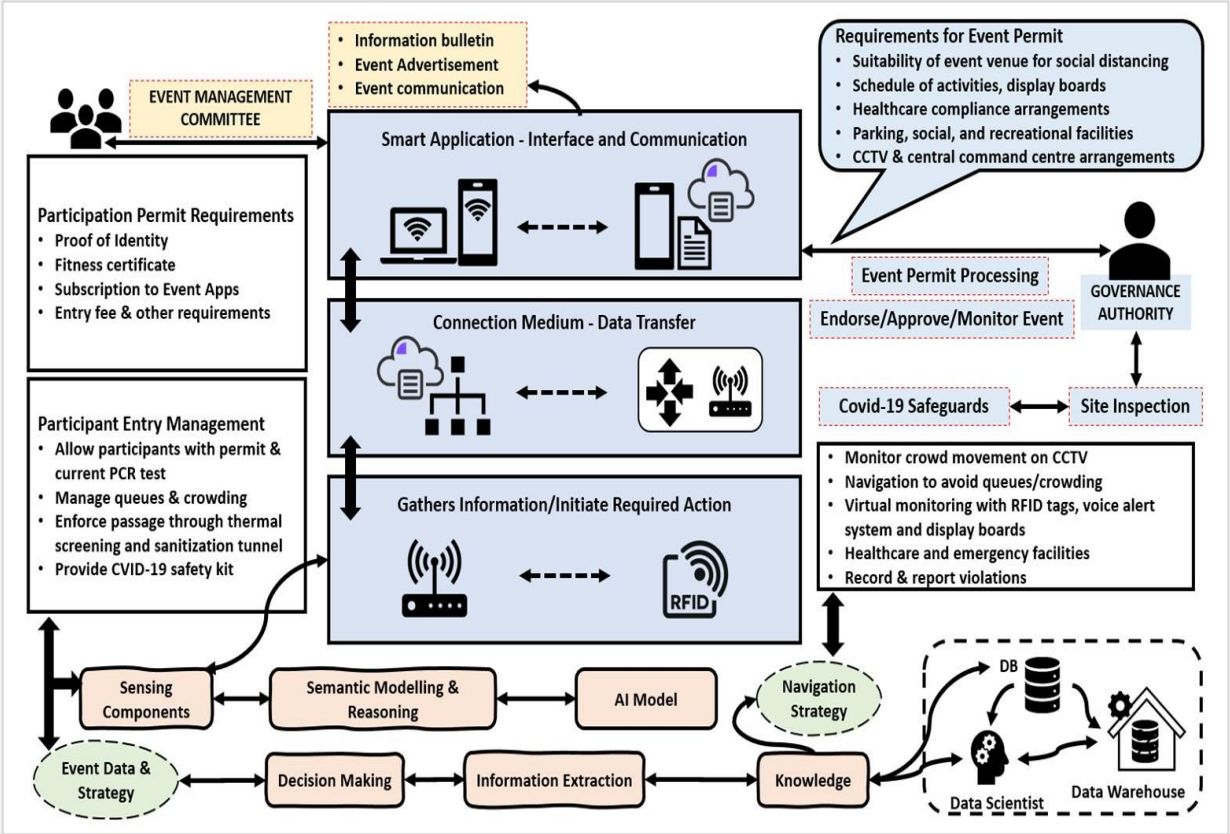

Figure 4.1: A framework of crowd management during a pandemic (COVID-19Crowd)

4.2 COMPONENTS OF COVID-19 CROWD

Following is the description of the components of COVID-19Crowd and their functions.

4.2.1 SMART APPLICATION FOR INTERFACE AND COMMUNICATION

The smart application of the proposed model receives and delivers requests/responses to the users (event management committee and governance authority) of varying roles. This layer deploys applications for smart event

management to offer various services including; applying for an event permit, Endorse/Approve/Monitor event, guidelines for the event/participation, and so on.

4.2.2 DATA TRANSFER FOR CONNECTION AND NETWORKING

The data transfer module of the proposed model connects and transfers the data for processing. The data is collected from various smart devices through sensors and this module is responsible for connecting to other devices, servers, etc., over the network. Different things/devices involved in event conduct/crowd management through arrangements, security, virtual visits, and inspection, etc. are connected and data is transferred by using this module.

4.2.3 INFORMATION GATHERING FROM SENSING COMPONENTS

Various sensors such as temperature sensors, infrared sensors, proximity sensors, optical sensors, etc. are part of an event management system for detecting and gathering data about the environment. Information is extracted through this module to initiate necessary action in and around the event timeline.

4.2.4 DATA ANALYTICS

The crowd (event attendees) could provide input during the event through various activities and strategies. By means of sensing components or event-based decisions, the data are captured and applied with semantic modelling and reasoning through a machine learning model. The data are stored in a database and will also participate in model fitting, prediction, and forecasting for future actions. In the distributed event environment, all such data origins produce databases and are extracted, transformed, and loaded into the data warehouse. A data scientist makes use of statistical and operational data from the data sources to analyze, predict, and forecast the acquired decisions.

4.2.5 SEMANTIC MODELLING AND REASONING

Semantic modelling and reasoning do the following:

- Enrich the meaning of the data being collected from various IoT sensors and actuators.
- Hides the device heterogeneity and allows for efficient integration.

4.2.6 ARTIFICIAL INTELLIGENCE MODEL

Using semantic web ontologies, a set of new rules are inferred based on the prevailing information.

4.2.7 KNOWLEDGE-DRIVEN DECISION MAKING

An AI model provides knowledge-driven decision-making for cognitive and physical tasks to support event users. This module allows tasks to be accomplished faster and better through better decisions for the event, without human intervention.

Better design and implementation of event strategy and navigation strategy are observed and achieved through AI-based decision making.

Chapter 5: Integrative Technologies for Real-Time Crowd Management: A Case Study of the Hajj

Crowd management is a very complex process, which requires the integration of many technologies together to create a reliable tool in crowd flow control. The historical events resulting from stampedes are the greatest evidence of the need for an effective solution. Relying on one method is not a reliable solution in such critical systems that require real-time response. The purpose of this solution is to develop a smart framework that uses Artificial Intelligence (AI) and other technologies to control and manage crowds. The methodology involved conducting literature review and using a case study of Hajj event to develop a Python-based solution for running the framework. The findings shows that the framework is effective in crowd management, but it would be improved using advanced machine learning techniques. The proposed approach will help government agencies and other bodies to focus on adopting modern levels of technology in crowd management.

5.1 INTRODUCTION

Across the globe, countries have documented historical events on stampedes. These situations are associated with challenges in the management and control of the crowd. As such, nations organize for large events that involve attendance of millions or thousands of individuals. These events include political activities, sports, and religious functions. Hence, governmental heads have the responsibility to provide safe and secure areas for public gatherings while taking into consideration of various issues such as health, transportation and security, among others (Hassanein et al., 2019; Wijermans et al., 2016). Unfortunately, governments often face the challenge of crowd management. The problem emerges because of lack of the resources and tools for people organization (Yamin, 2015; Almutairi et al., 2021). Consequently, the large gatherings have turned out to be sources of huge disasters in society.

The purpose of this Solution is to present a smart framework that uses artificial intelligence (AI) as an effective strategy for controlling crowd. The proposed framework involves the integration of different layers, algorithms, distributed services and new technologies that help in offering an efficient and safe crowd organization and management. The research also uses Hajj Event as the case study, which helps in understanding the deep impact of problems in crowd management.

A. Terms used in this Proposed Solution

• Artificial Intelligence (AI) is a terminology, which indicates the ability of machines or robots or software to engage in performing tasks similar to what humans can do.

• Crowd control is a term that depicts the use of different resources to manage a crowd when things turnout negative or unexpected.

• Crowd management indicates a strategy, which works before, after, and during an event. As such, the strategy entails assessing the situation, as well as maintaining the same and guaranteeing that individuals in a group are kept orderly and under safe control.

• Data privacy or information privacy indicates a principle that requires individuals to have maximum control of their personal data including deciding how third parties collect, store and use the data.

• Data security refers to the approach adopted by organizations and individuals to engage in the protection of the digital data from data breach and cyber theft.

5.2 PROPOSED FRAMEWORK

This study proposed a platform that supports the integration of four basic steps that were proposed and developed to provide integrated information on the state of crowds within the area that was divided into a group of cells. In each cell a fog node was added to provide automatic data processing without delay and relieve pressure on the cloud that stored information permanently for deeper analysis in the future and the discovery of new knowledge. In the first stage, we relied on smart gates, which provided real-time information about the number of people in each area as illustrated in Figure1. This was made possible by relying on the Internet of Things, specifically RFID Reader and Tags. The second stage was based on processing the images captured by the drone that can provide coverage for the entire cells without creating additional

obstacles in order to offer instant information about the places of crowd distribution within the cells and the percentage of congestion in each locality that cannot be reached through the digital gates However, the gate provided information about the current direction of crowd flow also.

In the third stage, we relied on Crowdsourcing, i.e. the information sent by the same people within the crowd, through the mobile application, which contributed to alerting to anomalies that are difficult to count and detect through accurate image processing such as a stampede, fire or any other event according to the received reports. Therefore, immediate action was undertaken as a response to the occurring event. Finally, the data prior to the three phases was collected within the fog node, which applied a simple algorithm to analyze the gathered data and then executed an optimal action. Moreover, we proposed using hardware tools for creating smarter system. As such, we suggested a digital- street in addition, smart gates, and smart bracelets in order to provide effective crowd control and alerting and avoid jams or crowds or any causes of crowds.

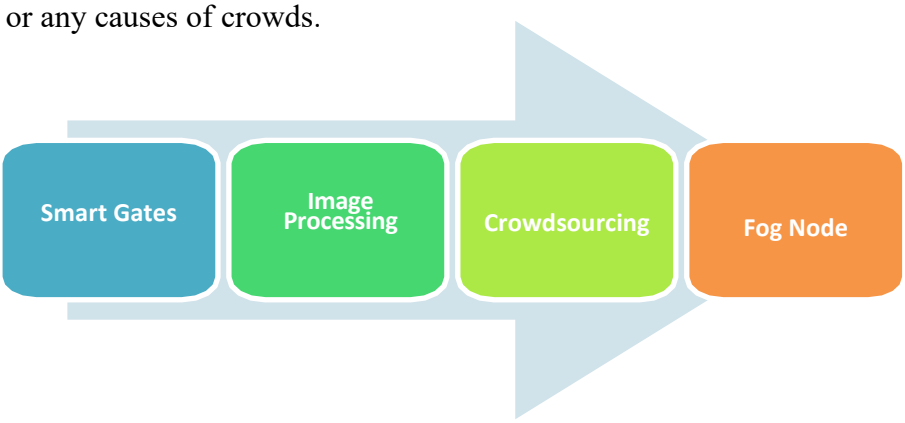

Fig. 5.1 Stages for the framework

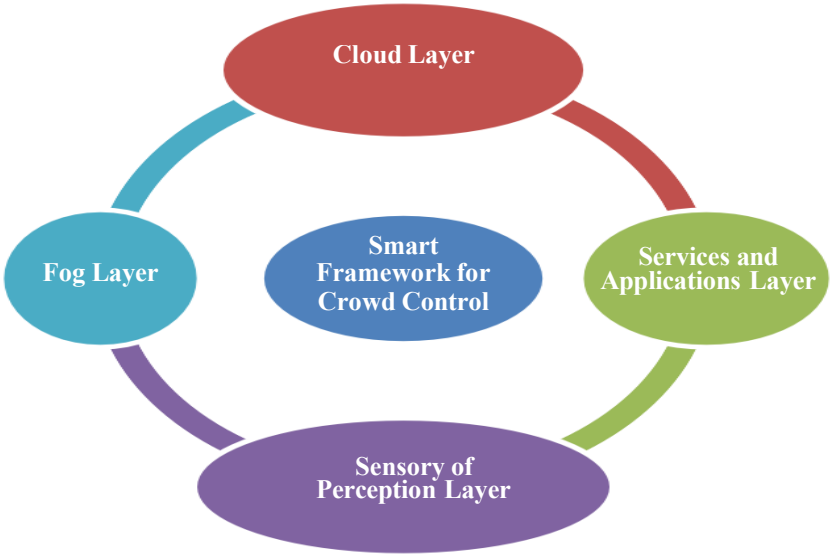

Fig. 5.2 Proposed Framework Layers

A. Framework Layers

The Internet of Things architecture has been relied upon, so the proposed framework consists of four main layers, which performs many functions and tasks as illustrated in Figure 5.2. The following points explain the main classes and their respective tasks:

• The sensory or perception layer: which contains Internet of Things objects, such as wireless network sensors, radio identifiers, and smart devices such as phones, vehicles, and digital roads. This layer is responsible for providing data, sensing it, and sending it to the next layer.

• Fog layer: One of the most important layers in the proposed framework. Fog nodes are responsible for receiving, collecting, and processing data in principle in real time without delay, as fog nodes are close to the data source (sense layer) at the end of the network. Also, the communication between the IoT objects and the fog node is via a local wireless connection. In the proposed system, the fog node is a smartphone, a drone, a road unit (roadside), a smart tent or a camp. The fog node application collect data, clean it, delete anomalies from it, and applies policies to it to unify it, and then summarize and analyze the data to make a quick decision in the event of any threat. The decision will be to control the gates in order to direct the crowds and send alerts in different ways to people within the crowd.

• Cloud layer: It receives all data from the fog nodes and stores it permanently. It also protects the stored data and its privacy and ensures the unification and integrity of the data to facilitate the process of using it by different services. Finally, the most important task is to process and analyze historical data by employing machine learning and artificial intelligence to deduce rules that enable the fog node to detect and classify the degree of threat based on the data received from the sensor layer in real time.

• Services and applications layer: It was divided into six main areas: tracking services and location-based services, flow control services and congestion information, services for managing emergency situations such as crowds and congestion, organization and management services for crowd events, health services, and services related to the environment and energy such as management. Waste in the crowd. All previous applications, systems and services rely on data collected in the cloud in order to provide services that are more intelligent and adaptive to users within the crowd.

An essential element in the success of the proposed framework is the availability of the necessary infrastructure, so Figure 3.1 in (chapter 3) displays the proposed structure integrated with the proposed framework.

Figure 5.3 shows the division of the crowd area into cells, so that in each cell there is a group of wireless network sensors that monitor physical data from the surrounding environment, such as temperature, pressure, noise, etc. There is also a smart gate in each cell at entry and exit in order to accurately calculate the number of people within the crowd. Each cell also contains a digital street that lights up in different colors that suit the nature of the crowding or the nature of the road in order to direct the crowds. The red color indicates that the road is closed or very crowded, while the green road indicates that there is no congestion. Digital street lighting is controlled through road units that represent fog nodes based on the level of congestion and the condition of each cell. Fog nodes that are distributed on lighting devices or within drones, process data coming from sensors, smart gates, and cameras using rules received from the cloud based on proposed algorithms based on machine learning. The evidence also shows the existence of a special application for security and civil defense teams to facilitate the communication and management process between the teams on the ground and the command and decision support centers. Further, the application would be used for crowds that offer several essential services.

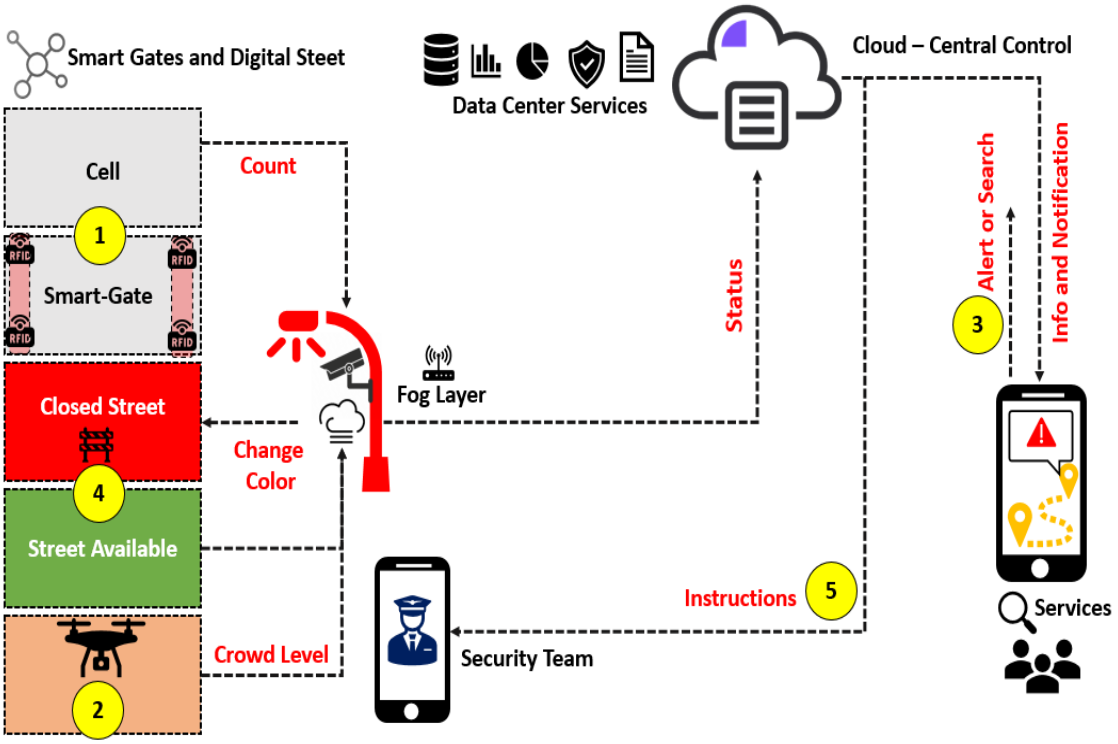

Fig. 5.3 Main **C**omponent of **P**roposed **S**olution (Deployment View)

Chapter 6: Privacy and Security of individuals in Crowded Events

Privacy and security are an important aspect of Crowd management. It assumes even a greater importance in large and intense crowded events like the Kumbh, Hajj, and Arabian. Some of these and other crowded events are religious in nature. Consequently, they attract politicians and social activists, which could be targeted by some organisations and countries. Safeguarding their personal information, movement and whereabouts is an integral part of crowd management.

This chapter provides innovative methods to protect the privacy and security of the participants of crowded events. These methods do not exist and is a contribution by the author.

Due to the rapid expansion of technologies such as the Internet of Things (IoT) and smart applications, the need to protect users from intrusion of personal information has become more pressing than ever. This chapter focuses on the innovative solutions to protect personal privacy and security to mitigate the risks associated with data breaches and unauthorized access.

Protection of individual privacy concerns in a crowds, such as those during large events, is a complex task pose unique challenges due to the scale of available data collection and monitoring techniques. The chapter provides an in-depth survey of traditional privacy protection methods, including encryption, dummy queries, obfuscation, and the use of trusted third parties (TTP). However, these methods, while effective to some degree, often fall short of providing robust, efficient, and scalable solutions.

The main contribution of this chapter is the introduction of several novel approaches, including the Fog-PIR technique, which leverages fog computing to address the

limitations of traditional Private Information Retrieval (PIR) approaches. The Fog-PIR method enhances privacy while reducing the performance and resource overhead.

6.1 PIR APPROACH AND ITS TECHNIQUES FOR PRESERVING PRIVACY IN IOT

6.1.1 PROPOSED SYSTEM

The basic idea of the proposed solution is to distribute the load and not trust a single server, by employing the hierarchical structure of the fog nodes. Each fog node on behalf of the user will manage a specific region and request all its data from a central fog node, which in turn is responsible for a group of regions (multiple fog nodes), and requests its data from the cloud or service provider. Thus, the data of the service provider will be divided into many parts and distributed near the user, and synchronized every period according to the nature of the application. Fog Node will divide its results and the results stored in the cache into smaller regions and parts and number them with specific numbers. When a new user comes, he can request all the data in the fog node or request several parts only according to the nature of the resources he has. Thus, the data requested by the user will be much less than that of traditional PIR, but enough to protect its privacy from the fog node that is responsible for a specific area only, and thus the load will be lower on the user which means that the system performance will be better. As for the privacy of the service provider, it will be fully protected, because the user will no longer need to deal with the service provider at all. (see Fig. 6.1)

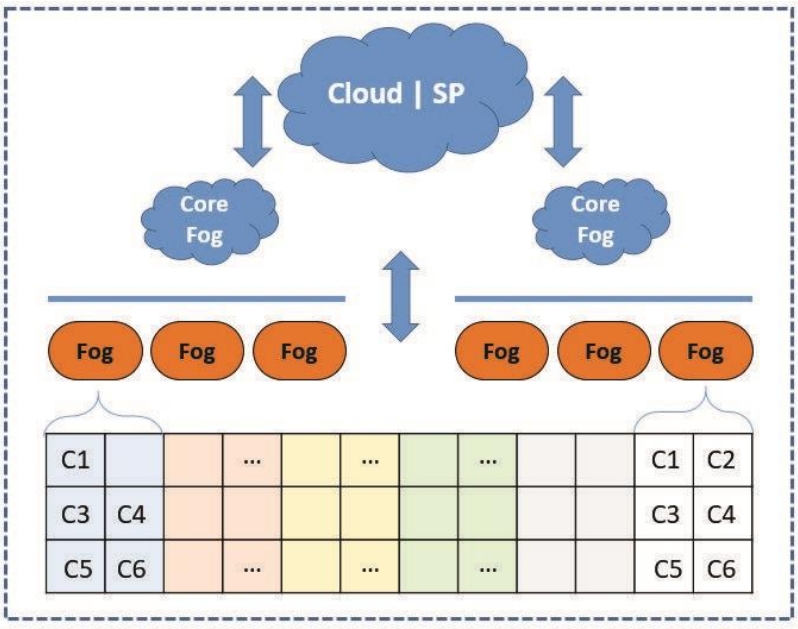

Fig. 6.1 Structure of proposed method (Fog-PIR)

6.1.2 SIMULATION AND RESULTS

Entropy, in the context of information security and privacy, refers to the measure of uncertainty or unpredictability regarding the data an attacker possesses about a target user. It quantifies the degree of certainty an attacker can achieve when receiving data that may be partially or fully associated with the intended target. Consequently, if the user refrains from transmitting any information that is directly attributable to them, the level of entropy remains maximized. This implies that the attacker will have minimal to no accurate information about the user, thereby preserving the user's anonymity and security.

To prove the superiority of the system in terms of performance and privacy, a simulation was performed according to the following assumptions:

- Dividing the area into 100 equal cells and putting a fog node in each cell.
- Assuming that the data contains information about 100 different points of interest.
- Fog Node updates its data every 2 hours from the central fog node which updates its data from the cloud.
- There are 100 users.

To measure performance, the volume of sent data will be based on the number of required queries, while the level of privacy will be measured according to the K-Anonymity criterion, i.e. the number of queries that are stored at the service provider about a specific user. A comparison will be made between the proposed improved method, the conventional PIR technique, and the trusted third-party TTP based PIR method.

Fig. 6.2 shows the superiority of Fog-PIR in terms of privacy, as it achieved the highest Entropy, considering that the user does not contact the service provider completely, as in the method based on a trusted third-party TTP-PIR, unlike the traditional PIR, in which the server can collect more information about the user with Time passes and after every query.

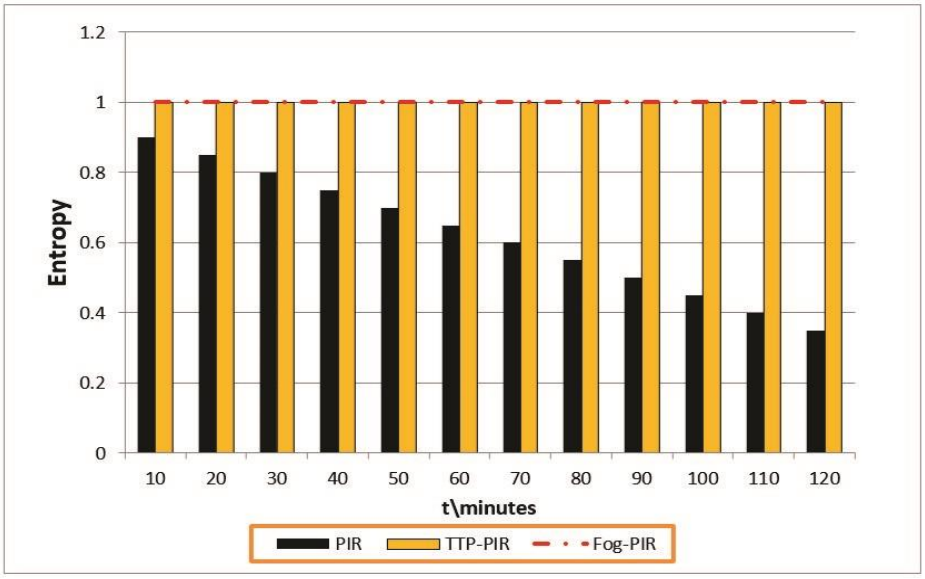

Fig. 6.2 Entropy comparison for privacy level

Fig. 6.3 shows the superiority of Fog-PIR in terms of response time, due to its reliance on a local connection with the near fog node at the end of the network, instead of connecting to a remote server via the Internet, and therefore with the increase in the number of queries, the improvement in response time will be greater.

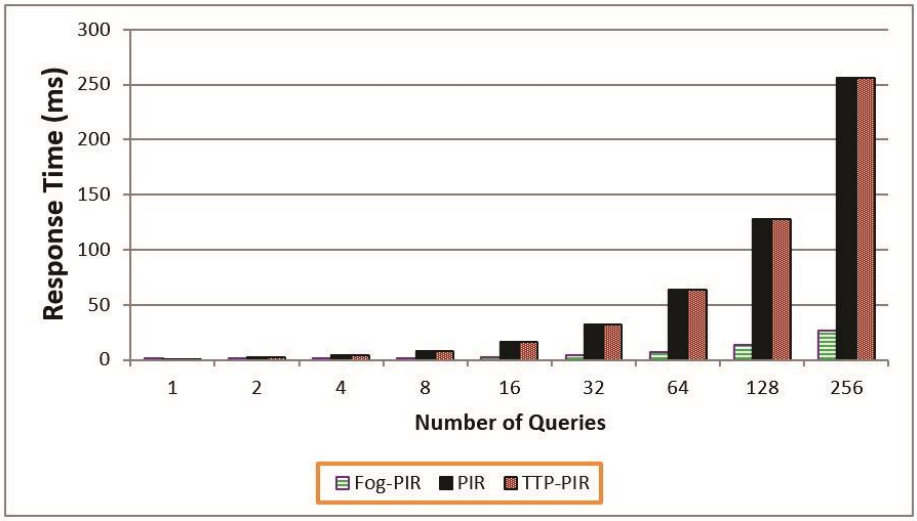

Fig.6.3 Comparison response time for performance issue

Regarding performance issues, this challenge is a common concern for any privacy technique that relies on cooperation between multiple parties. However, in our proposed method, we address this challenge by leveraging fog nodes as static and stable components with caching mechanisms along the data transmission path to improve availability. In the primary scenario, the process can terminate before sending a query to the service provider (SP). If the user does not receive a response within a predefined threshold time (the average time for a typical query), they must resend the

query, resulting in increased time costs and delays due to duplication. By utilizing a cache, this issue can be mitigated, as the user will retrieve the query result directly from the cache upon resending, significantly reducing the time cost.

We have evaluated this issue in a simulated environment using Cisco Packet Tracer, with Ping Testing employed to calculate the average query time as shown in figures 6.4 (a, b and c).

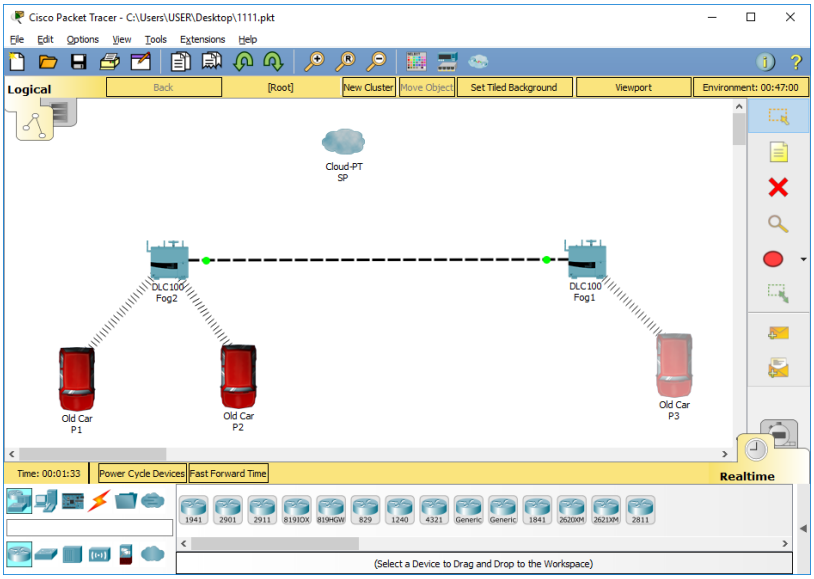

Fig. 6.4(a) Simulation environment by Cisco Packet Tracer

```
C:\Users\USER>ping www.google.com

Pinging www.google.com [216.239.38.120] with 32 bytes of data:
Reply from 216.239.38.120: bytes=32 time=102ms TTL=112
Reply from 216.239.38.120: bytes=32 time=97ms TTL=112
Reply from 216.239.38.120: bytes=32 time=109ms TTL=112
Reply from 216.239.38.120: bytes=32 time=93ms TTL=112

Ping statistics for 216.239.38.120:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 93ms, Maximum = 109ms, Average = 100ms
```

Fig. 6.4 (b) Average time (AT) of connection to SP by Internet

```
C:\Users\USER>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=6ms TTL=64
Reply from 192.168.1.1: bytes=32 time=25ms TTL=64
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 25ms, Average = 9ms
```

Fig. 6.4 (c) AT of connection to fog node or another peer by Wi-Fi

The connection among peer will be in WIFI. In addition, each peer has his private Internet connection so he can send the query of others to SP also.

We implement this issue by (Asp.net c#) to inform the capability of applying our method, in addition we applied the main scenario on the Packet Tracer Simulator.

Formal Analysis

We are compared our techniques to the scenario of dealing with SP without any protection method, then we compared it to Dummy approach, Obfuscation approach, and BTP (encryption) approach. The used metrics are:

- K-Anonymity: simple metric for finding the percentage of misleading the SP

- Entropy: The entropy (E) of identifying the real location or data out of the anonymity set is defined

- Estimation Error (EE), the percentage of error that attacker can fill in if he tries to determine the real query or location of peer.

- Cache Hit Ratio (H), percentage of query that can be found in the cache, to reduce the number of connections to the SP

- Cost measure by both the time of response (T) & the size of transferred data (S)

We will calculate the previous metrics according to the SP which can be the most threat on the privacy of user because it saves the whole received data.

Firstly, without any protection technique the values will be:

- K-Anonymity = 1/1 = 1 that mean SP insure that the query belongs to submitted peer.

- $E = -\sum_{i=0}^{k} Pi * Log_2(Pi)$ Where Pi is the probability of that query belongs to submitted Peer ➔ Pi=1 ➔ E=0.

- EE = E *100% = 0 The SP will not fill in error if he estimates that received query belongs the sender.

- H = maximum rate because only real queries are saved in the cache.

- Cost_Time = T the time of sending query to SP and receive the result.

- Cost_Size = S The number of byte that send to the SP for each query = Size (Q).

S(Q) = Identity(int32) + Latitude(double) + longitude(double) + POI (String) + Range(int16).

S(Q) = 4+8+8+50+2 = 72 Byte < 1KB for each sent query.

So to enhance the privacy we have to:

Reduce the K-Anonymity, Increase the E and EE, Increase the H, and do not increase the T and S.

1- **Dummy approach** sends many of false queries with the real one (K queries):

- K-Anonymity1 = 1/(1+K) so if we increase K that will enhance the privacy.

- E1 only if all generated queries are very similar to real queries, so all of them has same probability and E will be maximum ➔ Max(E) = $\mathrm{Log}_2(\mathrm{K}+1)$

Actually, that is impossible in the dummy approach because It is very difficult to generate dummies similar to real quires in the dynamic environment, so the E will be enhanced but will not reach to Max (E).

- H1 will be smaller ➔ adversely affect because dummy data stored in the cache.

- T1 will be T*(K+1) ➔ adversely affect.

- S1 will be S(Q)*(K+1) ➔ adversely affect.

2- Obfuscation approach, changes the location before sending query to SP (it just for location privacy)

- K-Anonymity2 = 1/D where D is the distance between real location and obfuscated one. So, more distance more privacy but sure that will effect on the result accuracy adversely

- E2 = $-\sum_{i=0}^{D} \mathrm{Pi} * \mathrm{Log2(Pi)}$ where D is the number of possible locations for the user.

- H2 = H because same query saved in the cache ➔ No effect

- T2 = T + Time of mapping response to real location ➔ bad effect

- S2 = S

3- Encryption approach (BTP)

- K-Anonymity3 = maximum = 0 because user doesn't deal with SP in normal case.

- E3 = Max (E)

- H3 = 0 because encrypted data cannot be stored in the cache ➔ bad effect

- T3 = 2*T + Time of encryption and decryption ➔ bad effect

- S3 ≥ S according to size of last block in the data in addition to the size of key ➔ bad effect

4- The Approach technique – For example: Double Swap Two Peers and Two Fog Nodes.

- K-Anonymity4= Maximum = 0 for the P1 and P3 where P1 doesn't connect to SP, and P3 send one dummy query not belongs him.

- E4 = Max(E) for P1 because he doesn't connect to SP, while E4 of P3 will be enhanced in total because K will become K+1 after each new query.

- H3 > H because two caches are employed here, and only real queries are saved in the cache.

- T4 = T + Time of swap between P1, P2, Fog1, Fog2, P3 ➔ Bad effect, however H3 will relaxing this issue as we discussed in result.

- S4 = S no changing on the main size of query

Based on the previous discussion, it is clear that our dual-protection approach offers enhanced privacy protection without significant effect on the cost.

Performance Measure based on number of queries and Cache-hit-ratio --- By C# and Asp.net as shown in figures 6.5 (a and b).

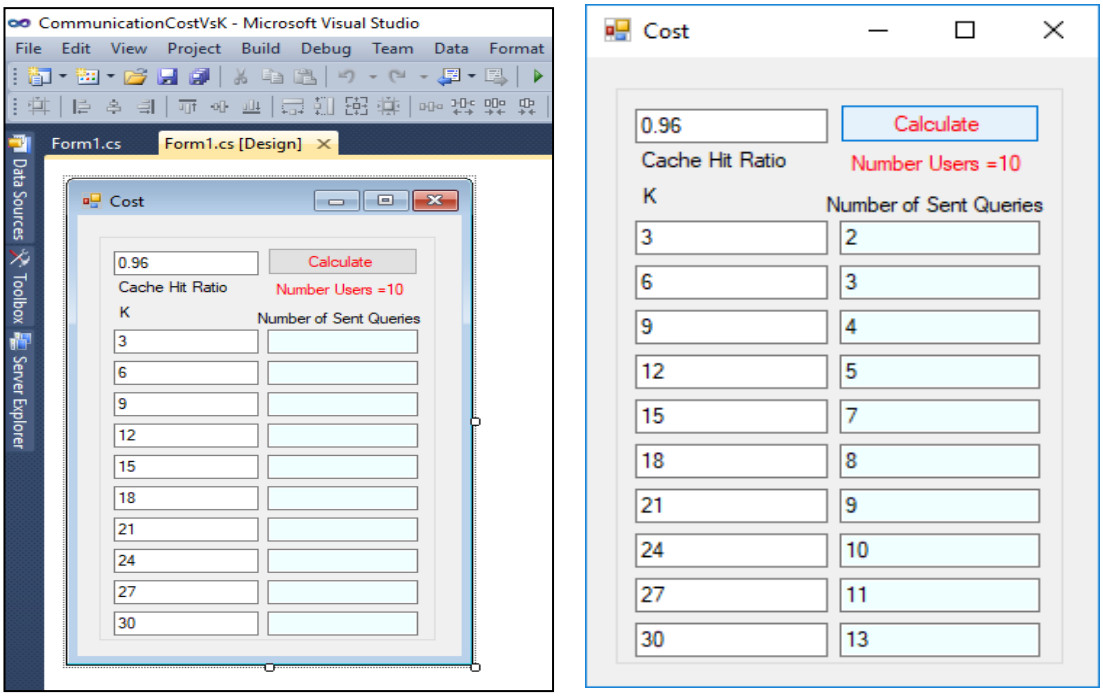

Fig. 6.5(a) Number of Queries based on Cache

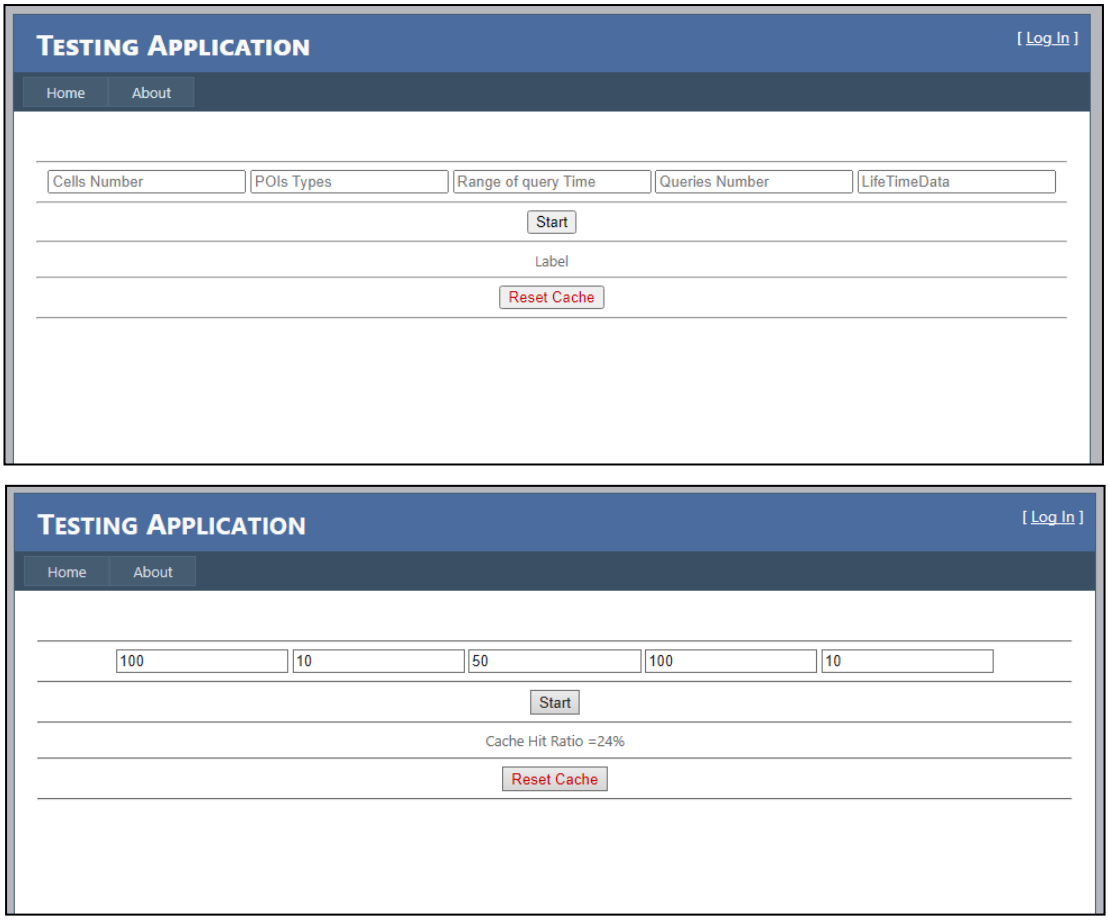

Fig. 6.5(b) Cache-Hit-Ratio based on Number of Queries

A. Advantages of the Proposed Solution

The proposed Fog-PIR approach has following advantages:

- Introducing an improved method that is applicable within the PIR approach.
- Reducing the user load.
- Increase the speed of system performance, as the user requests data from the fog node near him instead of the service provider, as the fog node keeps the data in its cache.
- Providing a solution to the problem of protecting the privacy of the user's query from the fog node, and sufficient protection for his location by requesting more than one part or requesting all the information stored in the fog node, so that it is impossible to know what the user wants exactly, and his exact location cannot be determined.
- Take benefits of the advantages of the fog knot in the rapid response to some emergencies.
- Complete protection of the user's privacy from the service provider, as the user will never deal with him.

B. Disadvantages of the Proposed Solution

Fog-PIR suffers from the following limitations:

- The need for a special environment for achieving the system (smart cities)
- Protecting the user location from the fog node is achieved, but if more than one malicious fog node cooperates, the user's path can be exposed.

6.2 ENHANCING PRIVACY AND SECURITY IN CROWDS USING FOG COMPUTING

SUGGESTED APPROACH

The basic idea of the proposed hybrid protection method came from the necessity of having an integrated crowd management framework, where the framework manages the cooperation between various technologies, services, and smart things. This framework deals with data generated from the crowd in a way that preserves the privacy and security of this data. The proposed framework includes four main layers; firstly, the Internet of Things, which is responsible for providing data about the environment and people in realtime, additionally, the cloud and fog computing layer for processing this data, and finally the services and applications layer. Figure 6.6 represents the common form of systems architecture related to the Internet of Things, and Figure 3.1 in (chapter 3) represents a proposed model for a crowd management framework and shows the number of systems, services, and technologies needed.

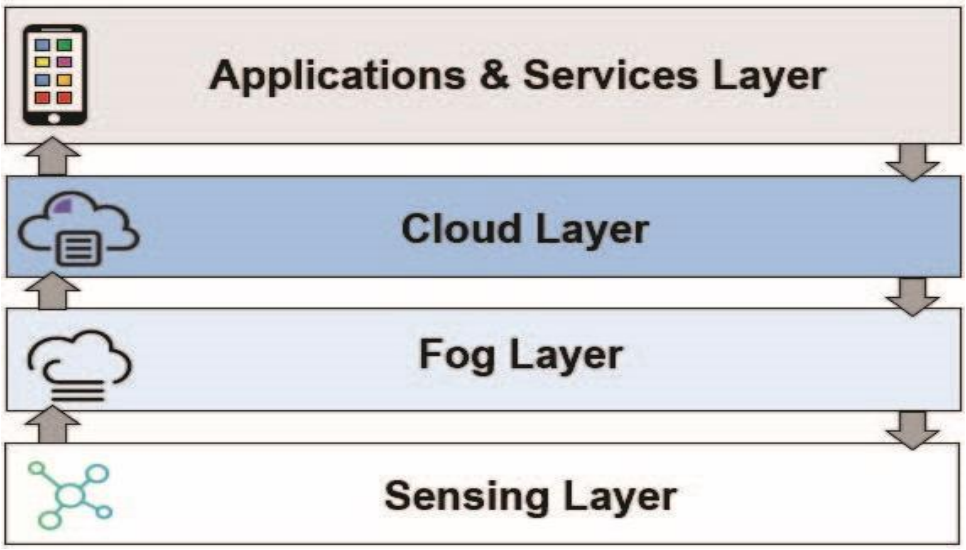

Fig. 6.6 Common Structure of IoT

To elaborate, the first layer in the framework contains various forms of IoT objects that collect different data about the crowd (people and the environment), while the fog computing layer provides quick response and initially processes data, in addition to the new component which provides data privacy and security protection. The cloud computing layer stores data permanently and provides the needed computing power for the processes and algorithms that operate on large amounts of data. The last layer is the services and applications layer, which contains many useful and supportive services in crowd management. This layer takes advantage of the stored

data in the cloud, which came of generating too much data and to provide a response in real through the fog node. Thus, in any modern crowd processing time (RT) to some emergency event. Each fog node is business environment, there must be a large number of fog responsible for a specific sector or area within the crowd nodes integrated with the cloud in order to solve the problem area.

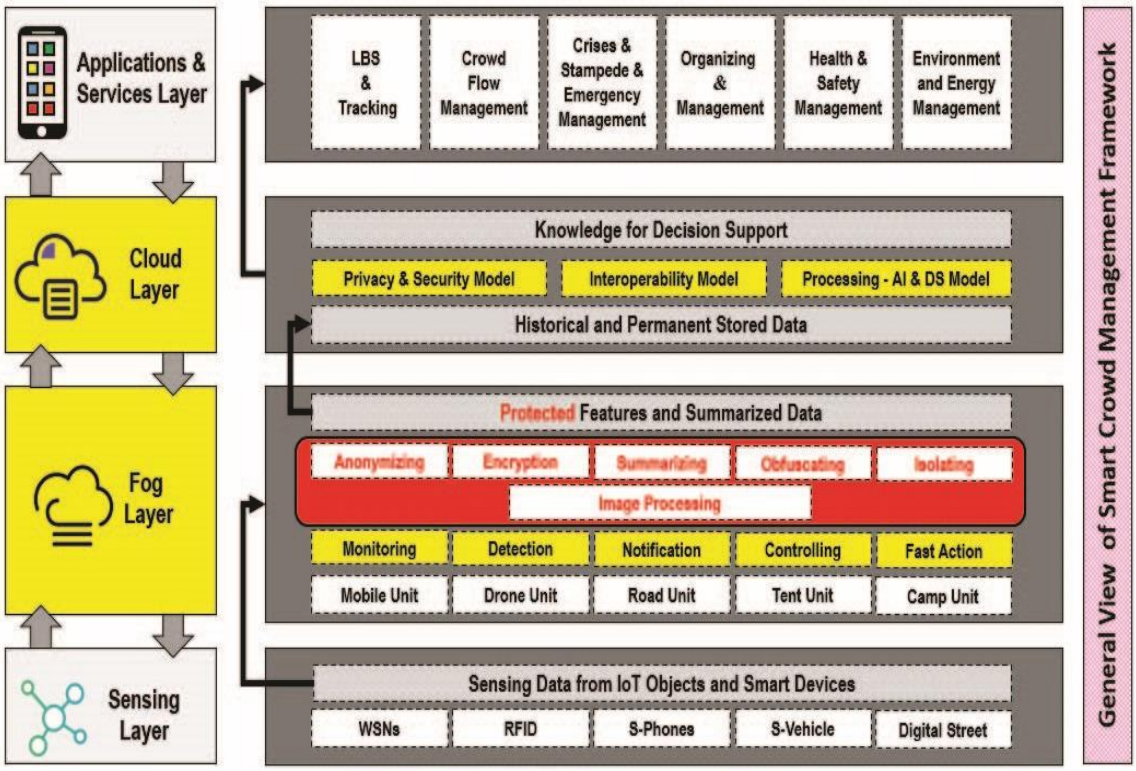

Fig. 6.7 Proposed Framework for Crowd Management t with new protecting privacy and security component

This research proposes the idea of a hybrid protection technology (the integration of a number of different protection methods) based on fog computing, because the fog layer is close to the user at the end of the network. It does not save data permanently and is only dealt with while the user is in its specified area. Thus, a new component has been added to the fog nodes that can perform new functions in crowd management and data processing in a way that contributes to enhancing the privacy and security of this data. In other words, the fog node processes the data before sending it to the cloud in a way that prevents the privacy of this data being breached when it is transferred away from the user to the cloud or the service provider.

Privacy is often breached by collecting data within the cloud for a while and then analyzing it and linking it with the owner of this data to create their profile. Therefore, if the fog node isolates personal and sensitive data before sending it to the cloud

without affecting the quality of provided service, this will improve the level of privacy. Thus, the idea of the proposed method depends on adding a protection component within the fog node responsible for protecting privacy through several new functions that are inspired by several traditional common privacy protection methods (TTP, Clack Area, Obfuscation, Mix-Zone, and Encryption) so that we have a new protection method that is more adapted to different applications and various services within the crowd and compatible with the requirements of each user.

The new functions can be summarized by the following points, which were added to the proposed structure in red, as shown in Figure 6.7:

- Fog can play the role of anonymizer by concealing the identity of users connected to the service or its provider.
- Fog can summarize some data to obscure the details, for example calculating the average consumption of electrical energy instead of the times of turning the devices on or off.
- The fog node can encrypt some sensitive data before sending it or apply some policies to it.
- Fog can process some images, specify sensitive data in them, camouflage, hide or cut them before sending the image, or even send features instead of the image if the image is sensitive, such as a face or fingerprint. x Fog can add confusion to some data before it is sent.
- Fog can isolate some personal data and ask the user whether he wants to send it or not to the service provider.

But to truly activate this approach and create an intelligent adaptive protection approach, the fog node must be able to specify and discover sensitive data from user data. On the other hand, the fog node must determine the basic data that will be provided to a particular service provider and the level of accuracy required in this data based on the nature of the service.

As for sensitive data, in the current stage, it relies on the level of user awareness, so that each user builds a personal file that contains the preferences and the required level of protection by specifying sensitive data, highly sensitive data, and data that can be sent to service providers.

As for the data required from service providers, we suggest forming a knowledge database by experts in the first stage so that the basic data needed by each service are determined according to its type. After that, we will build an automated model and train it on this data by the time. The focus of next research will be creating an automated detector for sensitive data based on ML techniques.

6.3 DOUBLE PROTECTING APPROACH FOR DATA PRIVACY

PROPOSED APPROACH

A double-approach approach is proposed to provide protection and maintain the security and privacy of data more effectively and in a way that supports complex systems such as crowd management systems, which organize a wide variety of applications and support services. The umbrella approach includes many technologies, but all depend on two primary conditions. The first condition, which is the basic idea on which this approach depends, involves doubling the work of traditional protection methods. The second condition is the effective use of the fog node or fog computing to improve the performance and efficiency of the proposed methods. Since this approach relies on multiple methods, it will have a significant role in Serving different systems and applications, as we have indicated in complex systems such as crowd management.

Beginning with encryption, we have suggested double steganography encryption, which means the process of concealment or concealment. Analysis and breaking of traditional cryptographic techniques have been developed into the science of steganography by hiding information encrypted with cryptographic techniques such as DES encryption within a template that does not attract the attention of attackers, such as a picture of a landscape, for example, and then send it in this way. We suggest doubling the process, that is, the encrypted text is first hidden in a template, and then the template itself is hidden in another template to increase the complexity and level of security. The user will perform the first encryption process to hide his original data, and then perform Fog node in the second process to reduce the load on the user without breaching the user's privacy because his data is basically encrypted in the first template and then sent to the service provider.

The second method is double obfuscation. We noticed that double obfuscation suffers from two problems. The first problem is the possibility of a region tracking attack, and the second is the difficulty of processing the returned data, which may affect the accuracy and quality of service based on the location of the new or accurate user. The obfuscation process was divided into two stages. In the first stage, the user performs a little obfuscation because it deals with the

fog node only once or twice rather than as a service provider that deals with it continuously. Then the same fog node reconfigures a second, wider region that contains the first region, and therefore the service provider to whom the request comes from the fog node will not be able to associate it with an identity; the user, on the one hand, to track the area, and on the other hand, the result returns to the fog node, which divides it into several sections: northeast, southwest, middle, and the central region is the user's primary region. Also, for the problem of accuracy of the returned results and reduce the burden on the user in processing all the returned results.

In the issue of peer collaboration, a double cache technique was proposed, whereby in each fog node, there are two caches. The first is unique in that users put their queries without the need to deal with each other, and the second is specific to the results of these queries. The query that answers more queries is prioritised in the order of queries that it needs within the first cache. This problem will also solve another problem in improving the privacy of cooperating individuals, as the user who sends a query that does not belong to him will enhance his privacy and shade the service provider, who will consider it a unique query for the sending user. Thus we will also solve the problem of false dummies that can be discovered by using a query that cannot be detected as a dummy because it is an actual query for another user.

The next method is a double swap. Also, this issue will address a problem in the traditional collaboration approach. When users are in one area, the collaborator will reveal the privacy of his location because he is in an area close to the user. Double-swap was proposed to solve this problem and enhance the level of cooperation between users and motivate them to do so. It will first be swapped between two users and then between two fog nodes. Thus, the focus will move from the user who sent the query to a user who belongs to a fog node in another region to appear as if he is in the main region. Thus, the required protection of the policy will be achieved without affecting the privacy of the collaborator, the sender of the query, or the privacy of his location.

Another approach is a double-server, which divides user data when the server is reliable, as in the case of some government agencies. It also manages crowds, where personal information is isolated from identity information. Each is

placed in a private server so that if one of the servers is hacked, the attacker or hacker cannot benefit from the data because it is not linked to specific users. If the identity server is hacked, the attacking hacked user will not obtain detailed information about these users, thus enhancing the level of protection in such methods. Another method is double cancellable hashing for biometrics. In some crowd management systems, we must identify people through a Biometric fingerprint to prevent denial and impersonation. Such systems may cause danger if biometric data is stolen from users. To solve this problem, it is suggested to use hash code or data transformation. Biometric fingerprint instead of using the fingerprint itself with the addition of some change to this fingerprint. Therefore, no attacker can recover the primary fingerprint data from the sent hash code so that it can be used again in another application or system, or it poses a threat to the user to enhance this protection. Also, this process was suggested by double adding a number that increases periodically in each new query so that a different hash code is generated each time. Therefore, this code will only be valid for one time. The exact process to ensure the user's presence in a specific place first in the same place as the crowd and thus is reliable on the one hand. On the other hand, double the jamming process or hashing the data so that the malicious task attacker becomes almost impossible to reveal any helpful information about the Biometric fingerprint.

Regarding double mix-zone, as mentioned in the previous works, we mentioned that its negative effect is that the ability to track the path and re-route the user through the temporal and spatial sequence makes it easier for the nature of the queries to be revealed, especially if the attacker has information about the region. To solve this problem, a double mix-zone is proposed as in Figure 6.8.

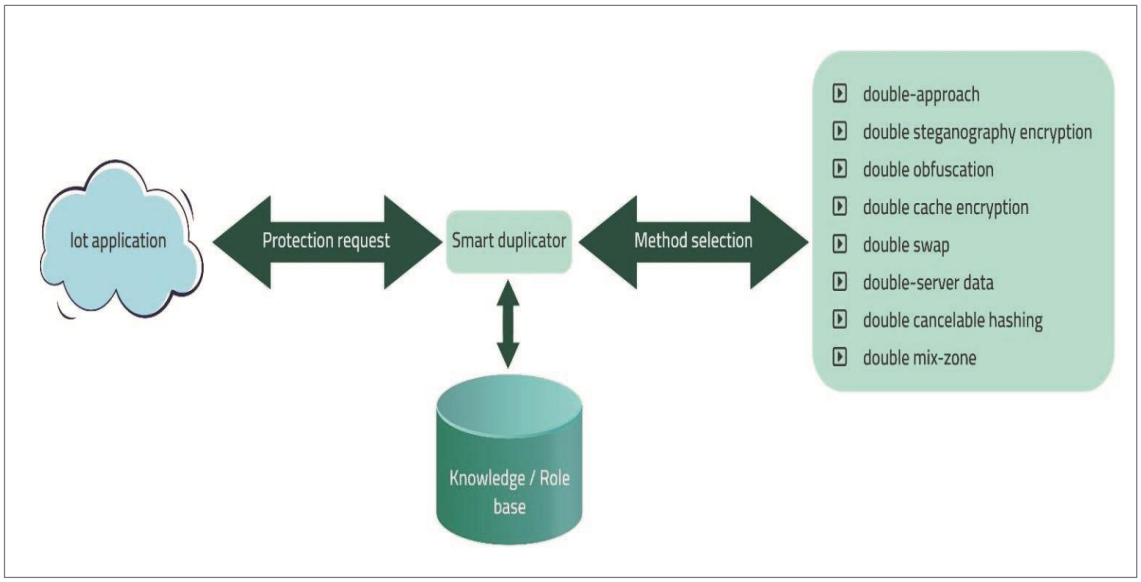

Figure 6.8 A Proposed double mix-zone

The user sends his destination only to the fog node with an initial nickname, and then the fog node exchanges the nickname with another user who heads in the opposite direction so that the user uses this nickname sends it and communicates with the service provider. The service provider will not suspect a change in the user's identity but will link another user's data as the primary user, thus incredibly misleading the service provider. We note that we have proposed a large group within the framework of double obfuscation. Some of these methods have been published in previous research, and others are in the works. As for this work, we summarize all these methods under one approach that we call double obfuscation to adapt this approach to protecting privacy in crowds. This is what, that will be explained using the case study.

CASE STUDY

As we indicated earlier, many applications and systems exist in the crowd management process. Some applications are health applications that require accuracy in user data, others depend on Biometric fingerprint, and some depend on tracking the user’s location to guide him to the nearest point of interest, such as the nearest restaurant, health center, or hotel. Others are related to crowd management to measure the number of those present in a particular place to determine and manage crowding rates. A standard traditional approach cannot manage all these methods to solve all these systems and provide them with privacy. Therefore, it needs a complex approach, as in the double-approach, for example, for the fingerprint. Biometric fingerprint and double cancellable hashing will be employed, while in the point of interest issue, double obfuscation can be used efficiently or double mix-zone for movers. As for calculating

the number of crowds, the double-swap approach can be used. It will not affect the number of people but will swap between their locations without affecting It depends on the number of people present in each region. However, in medical data, for example, double-server data can be used, where data and pain will be separated. Reviews and medical records about the identity of users in another server, so the database knowledge or smart note will be placed responsible for determining the appropriate technique from the previous methods based on the nature of the user's query and requests, which is the basic idea of this approach, and therefore the double-approach approach will be able to fulfil the protection of users' privacy within the crowd.

DISCUSSION FOR SUPERIORITY

In order to prove the superiority of the proposed approach over the traditional methods in contrast to the basic feature that involves the idea that the proposed approach can be applied to complex systems other than the traditional methods because it contains many methods with a smartnode to choose the most appropriate method for each application, we will prove in the following the superiority of the improved methods over their counterpart Traditional methods. We will rely on two basic criteria in measuring the effectiveness of privacy. We will rely on k-anonymity or the entropy criterion. The amount of actual real information that can be collected on the server and related to the user who owns this information. The user to do it in double-swap we note that the entropy of the traditional swap technique or cooperation between users located in one area will inevitably be less than one due to the presence of some correct spatial information related to the user's whereabouts given that the users are located in one area will differ. This percentage depends on the distance separating the two users from each other. In the case of a double-swap, the protection will be absolute. The entropy at its highest value will be equal to one because the user who sent the query is located in a completely different place than the owner of the main query, and it is thanks to the swap between two fog nodes in the second stage of the swap.

In double obfuscation, we note that the entropy ranges from zero to completely smaller than one in traditional obfuscation. This ratio is related to the size of the jamming area. However, the more significant the jamming area in size, the more performance will be negatively affected. The user needs to recalculate the results returned compared to his new location, but in double obfuscation, the

user does not send any query. However, the fog node sends on its behalf, and therefore there is complete concealment of identity, and the entropy will be at its highest value. As for the performance issue, the fog node was employed to divide the results into five sections so that the user chooses the result in the location closest to his location without revealing that to the fog seat. Alternatively, the service provider and thus improve the performance and accuracy of the results returned. In the mix-zone, the entropy is related to the user's delay in sending his query so that the new alias is not detected and linked with the user's data, but there is a section of this data that is always linked to the user's name, and therefore the value of the entropy will also be less than one, but in the double mix- zone, the user sends a pseudonym to another user located in the same area, and therefore all his data will be assigned to this user without any doubt from the service provider, and therefore a file will be formed after several inquiries and exchanges that do not give any accurate information if the service provider analyzes it, and the entropy will also be in the highest values. In the field of encryption, here we care more about the level of protection and the inability to break it. It is much more difficult for an external attacker compared to traditional encryption. Also, in the field of biometric fingerprinting, we have improved performance. With the traditional approach, a biometric fingerprint cannot be used in other applications, but the attacker can use it in the application—the hacker himself. In our technique, the attacker cannot benefit from his penetration of the Biometric fingerprint. Even in the following query within the system itself, we notice the superiority of the proposed approach over other corresponding approaches in all its forms without a clear impact on the level of performance.

6.4 DOUBLE CANCELABLE HASHING FOR PROTECTING BIOMETRICS OF USERS IN CROWD

PROPOSED APPROACH

By reviewing previous works, the importance of using a technique that changes the template of the biometric fingerprint becomes evident, ensuring that there is no correlation between the fingerprint of a specific person within more than one application. Additionally, in the event that the template is stolen by penetrating the server or monitoring the entertainment on the network and decrypting it, significant harm to the user cannot be caused by the attacker, especially in the event that the attack is of the Active type, where an act that indicates direct action is performed by the attacker. Then, the user can communicate with the server to cancel their fingerprint by changing the shared key between them. However, in the case of a passive attack, the existing application can be accessed by the attacker, and user data can be stolen.

Therefore, to address this issue, a method of double and continuously changing authentication is proposed. This ensures that if the data for a particular authentication query is stolen, the attacker will not be able to benefit from it for another login.

More than that, reliable Fog nodes have been employed as intermediate points through which the service provider is contacted, and thus the user first needs to authenticate with the Fog node and prove his identity, and then authenticate with the help of the Fog node with the service provider. The user communicates with the Fog node via Wi-Fi while the Fog node communicates with the Service Provider over the Internet. This means providing a higher level of availability for the user even if he does not have an Internet connection, especially in private places that witness crowds. Such solutions can be applied to ensure that all users within the crowd are connected to service providers.

On the other hand, fog nodes are useful in improving the level of performance and reducing the number of connections with the service provider in some other queries that do not require authentication, as the fog node can perform the caching process for some results for the most requested or frequent queries within the crowd, and thus reuse them in answering future queries. Without the

need to contact the main service provider. In this way, fog nodes can greatly improve the performance of systems and provide immediate response in some emergency events within the crowd.

To achieve the process of automatic change of the biometric information template, a random number, N, was generated when registering with the server for the first time, to be added to the hash function of the revocable biometric fingerprint. But N in each query will change its value by adding 1 to it to create a more complex template on the one hand, and most importantly, it will only be effective for the current authentication.

In general, the steps for the validation process within the proposed approach can be summarized in the following points, which are also shown in Figure 6.9:

1) The user will rely on the throwable template Hash0 resulting from calculating the hash function of the biometric fingerprint with the shared key with the service provider, then the user will recalculate a new hash function for the previous template with the number N added to it. In the next times and when performing an authentication process, the user will add 1 On the number N and then insert it into the process of generating the hash instead of N, thus generating a new unique template that is completely different from the previous one.

2) The user sends the hash1 with the user number in the service provider to the fog node and modifies the value of N in his internal memory to become N + 1.

3) To increase the level of protection, the fog node will generate a new Hash by re-encapsulating Hash1 by adding UserID and sending it to the service provider with the user number.

4) The service provider will first verify that the query is coming from a validated fog node within the list of validated fog nodes. Then the service provider based on the user number will retrieve the template stored for this user with the Key with the last N used. It will then compute the Hash1 again from the stored template with the value N+1 added to it.

5) The server will adjust the value of N in its databases to N+1.

6) The server will calculate Hash2 through the value of Hash1 added to UserID.

7) Finally, the server will match the Hash2 received from the fog node.

8) If the match is successful, a temporary and encrypted token will be generated to enter the system and sent to the Fog node, which will then return it to the requesting user.

9) If the authentication is not successful, 1 will be subtracted from the value of N.

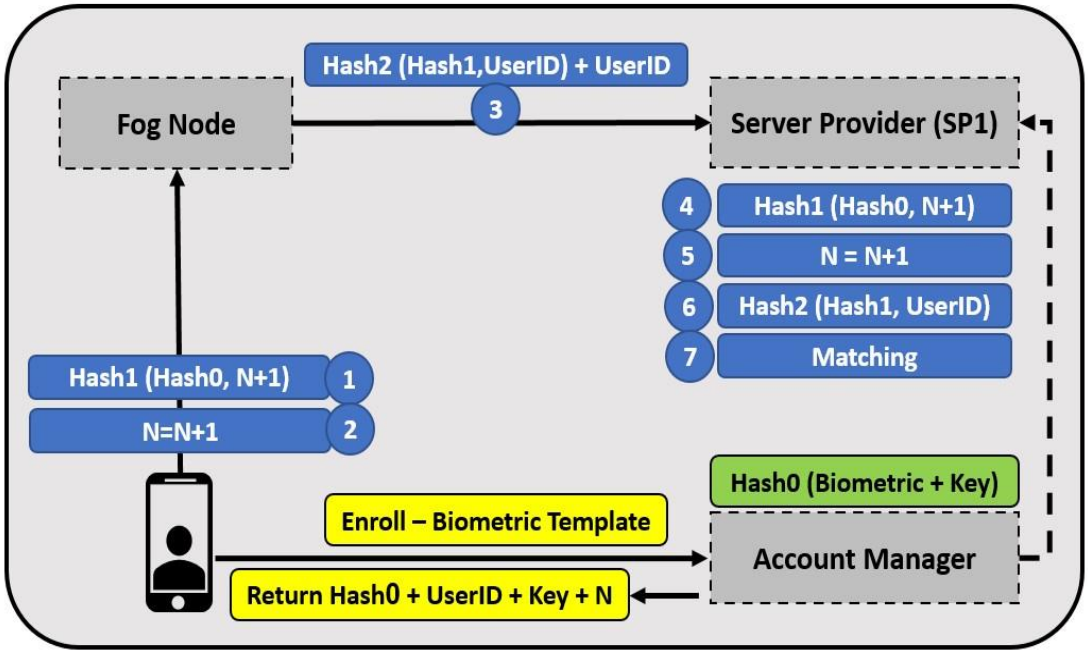

Fig. 6.9 Proposed model architecture for revocable authentication

Features of the proposed method compared to the existing methods

The proposed method achieves the four basic features that must be available in a removable biometric fingerprint template, namely:

1- Diversity: the same template cannot be used for a user in more than one application, due to the use of Key + UserID in the fingerprint generation process, and this data is impossible to be repeated in two different applications

2- The ability to cancel is also achieved within the proposed method by just changing the Key. More than that, the proposed approach is superior to the additional advantage that the template is basically valid for one use, that is, it changes every time through the variable N

3- Irreversibility: Also verified, we use the method of segmentation functions, which gives a unique code with a size of 128 characters, and

therefore it is impossible to extract the original data of the fingerprint if this code is revealed.

4- Performance: The process of hashing is easier and faster than the methods of casting arrays, projection, displacement, rotation, or transformation, which are used in other methods to generate a nullable template. The doubling process added an additional feature to increase the level of security and complexity in penetrating the system on the one hand. On the other hand, the use of the fog node will play a major role in reducing the burden on the service provider in the operations following the authentication process and in enhancing security as well. Where the connection to the fog node ensures that the person is in the same place, and the connection between the fog node and the service provider via the Internet is therefore the most vulnerable to attack, and therefore doubling the hashing process here will greatly complicate the attacker's task.

All of the above confirms the superiority of the proposed approach in terms of the level of security and performance. Figure 6.10 shows the pseudocode of the proposed method. We know that the code for the proposed method has been implemented within the Visual Studio .Net environment in C#.

```
// User
Hash0, N = Read_LocalMemory ();
Key = EnterKey();
Hash1 = Hash ( Hash0, N+1 , Key );
Send_To_Fog ( Hash1, UserID);
//Fog
Hash1, UserID = Received_New_Reqeust ( );
Hash2 = Hash ( Hash1 + UserID );
Biometric_Authentication (Hash2, UserId, FogID);
//Server Provider
Biometric_Authentication (Hash2, UserId, FogID);
Begin
    Fog = check_List_Trusted_Fog ( FogID )
    If ( Fog )
        N, Hash0, Key = Get_User_Info(UserID);
        H1 = Hash ( Hash0, N+1, Key);
        H2 = Hash ( H1, UserID);
        If ( H2 == Hash2)
            Update AccountTable N=N+1 where UID=UserID;
            Return SessionToken; //Ture
    Return False;
End Function
```

Figure 6.10 pseudocode of the proposed method

CASE STUDY

The Kingdom of Saudi Arabia witnesses annually, especially during the periods of Hajj and the month of Ramadan, a large crowd in Medina and Makkah Al- Mukarramah, especially within the Two Holy Mosques, where more than 6 million people gather in a specific area. Many service providers in all fields seek to serve the guests of Rahman (pilgrims), as the Kingdom of Saudi Arabia calls them. The most important thing for the government is to prevent hackers from obtaining a false permit or impersonating other people who have a permit. There is no solution for this except through the biometric fingerprint, as it is linked to the same person and cannot be used by another person. However, the government fears the theft of this data, which serves as an entry key for all service providers within the Hajj journey in all fields (hotel and flight reservations, money transfers, transfers, entry permits to Hajj areas, comprehensive medical file, etc.).

To solve this problem, it was proposed to build smart gates distributed in different places of the area that witness crowds, so that the authentication processes are distributed to several outlets to reduce pressure, and the user can use his smart phone with an application for Hajj management to find the biometric fingerprint. According to the proposed authentication policy, the user has to enter the key value with the modified N value in addition to the biometric information. Then to go through the same approach steps. Fog nodes were distributed to cover the entire Hajj area to solve the problem of unavailability of internet connection for some users.

Figure 6.11 shows a visualization of the locations of the digital gates in the Grand Mosque (Red Spot), and they could be in the entry points of Makkah Al-Mukarramah.

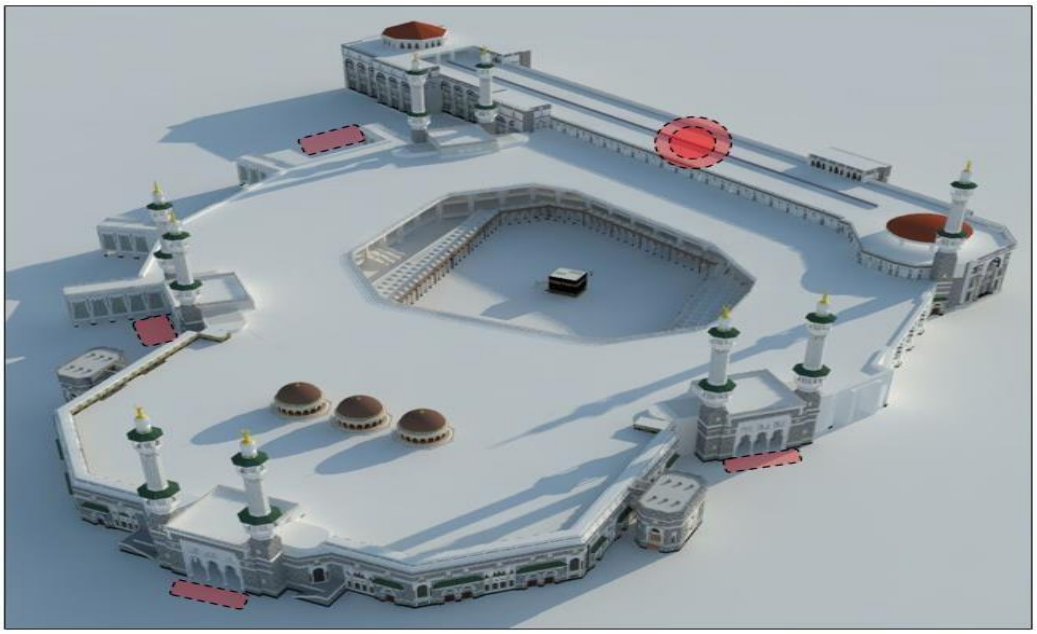

Fig 6.11 Proposed places for the distribution of digital gates in the Prophet's Mosque

The proposed novel outlines a biometric authentication approach using double cancelable hashing and fog computing to improve security and performance, particularly in crowded environments like the Hajj pilgrimage. The key features and validation of the core aspects will be presented in the following:

Features:

1. Double Cancelable Hashing:

o Uses a biometric fingerprint with a dynamic key and a variable number N that increments with each authentication attempt. This ensures that each authentication generates a unique hash, preventing reuse of stolen data.

o The system allows easy cancellation by changing the key, enhancing security if a template is compromised.

2. Fog Computing:

o Utilizes fog nodes as intermediaries between users and service providers, providing faster and more secure authentication without the need for constant internet connectivity. This is especially useful in crowded environments where internet access might be limited or slow.

o Fog nodes can cache frequent queries and act as gatekeepers, reducing load on the service provider and enhancing system performance.

3. Performance and Security:

o The system improves security by making it harder for attackers to reuse stolen data. It also reduces network delays by offloading some processing to fog nodes, thereby speeding up authentication processes.

4. Case Study in Hajj:

o The implementation in the Hajj crowd demonstrated its effectiveness in managing large crowds, improving security, and providing reliable authentication even in areas with poor internet access.

Validation of the System:

1. Security Validation:

• Cancelable Hashing with Dynamic Keys and N-Values: The use of cancelable biometrics, where the key and a random number N change with each authentication attempt, is a robust validation technique. By introducing N, which is incremented with each query, the system guarantees that even if an attacker captures the hash from a previous session, they won't be able to reuse it. This ensures non-reusability of authentication credentials, a major challenge in traditional biometric systems.

The system validates that the new hash (Hash1) is always distinct by adding the incremented value of N to the hash, confirming that the captured data from any session is no longer valid in future attempts.

• Fog Node Verification: Each fog node must authenticate itself to the service provider before any user data is processed. This process involves the verification of the fog node using a list of trusted nodes maintained by the service provider. Any authentication attempt from an unverified fog node is rejected, ensuring the integrity of the network. This double authentication (user and fog node) provides an additional security layer that can be validated by checking the correctness of the fog node's credentials.

• Data Confidentiality & Token Generation: If the match between the calculated Hash2 (based on the stored template and modified N value) and the one sent by the fog node is successful, a temporary, encrypted token is generated.

This token allows the user temporary access to the system. The validation here lies in generating and securely transmitting this token, ensuring that only authenticated users can proceed.

2. Performance Validation:

- Reduction of Server Load: By utilizing fog nodes to handle some authentication requests and caching frequent queries, the system significantly reduces the number of direct connections to the central server. This distribution of workload enhances system performance, especially during peak times, as validated in environments with large crowds like the Hajj pilgrimage, where millions of users are involved.

Validation in this case could involve testing system response times and server load during high-demand periods. The reduction in network traffic and improved latency are key indicators that the fog nodes are effectively performing their role.

- Caching Mechanism: Fog nodes are capable of caching responses for commonly requested data. This improves response times for repeat queries, reducing the need for redundant communication with the service provider. The effectiveness of this caching can be validated by testing scenarios where frequent queries occur and measuring the decrease in response time when cached responses are used.

- Immediate Response in Emergency Situations: In scenarios that demand immediate action, such as emergency events in a crowd, the system ensures a quick response by utilizing local fog nodes to handle requests without needing to contact the central service provider. Validation of this feature would involve stress-testing the system under simulated emergency conditions to ensure that fog nodes respond quickly and appropriately.

3. Scalability and Availability Validation:

- Support for Large Crowds: The system has been designed to handle millions of users, as seen in the Hajj case study, where it managed to authenticate pilgrims across multiple locations using a distributed network of fog nodes. Validation of scalability involves simulating high-traffic environments

with multiple fog nodes and verifying that the system can handle peak loads without significant degradation in performance.

- Offline Capabilities via Fog Nodes: In situations where users may not have internet access, fog nodes ensure continued availability of authentication services. This can be validated by simulating environments with intermittent or no internet connectivity and ensuring that users are still able to authenticate and access services through fog nodes operating in local-only mode.

4. Integrity and Error Handling Validation:

- Error Handling During Failed Authentication: The system's error handling ensures that if authentication fails (e.g., due to mismatched hash values), it subtracts 1 from N and retries the process. This rollback mechanism ensures that false negatives (i.e., legitimate users being denied access) are minimized, without compromising security.

Validation here involves testing various failure scenarios, such as incorrect hash values, untrusted fog nodes, and corrupted data transmissions, and ensuring that the system responds appropriately by either retrying or securely aborting the process.

5. Practical Case Study: Hajj Validation:

- The Hajj case study serves as a real-world validation for the system. With over 6 million people in a limited area, the system had to manage biometric data, prevent unauthorized access, and ensure seamless user experiences under pressure. The successful deployment of smart gates with fog computing during Hajj proved the system's ability to scale, maintain security, and perform efficiently.

Validation was conducted through field tests, which showed reduced waiting times at entry points and fewer security breaches due to unauthorized access. These results are critical for validating the practical applicability of the system in real-life scenarios.

6. Validation of Privacy:

- The system addresses concerns about privacy by ensuring that even if biometric data is intercepted, it cannot be used in another context due to the unique key and N value. This validates compliance with privacy standards,

especially in sensitive environments like Hajj, where personal and sensitive data is handled on a large scale.

- Privacy validation can involve auditing the system for compliance with data protection regulations and running penetration tests to ensure that intercepted data cannot be reused or linked across applications.

The proposed system's validation process covers all critical aspects—security, performance, scalability, error handling, and privacy. Field tests, especially in high-stress environments like the Hajj pilgrimage, provide strong evidence that the system functions as intended.

BENEFITS OF THE PROPOSED APPROACH

The proposed approach has the following benefits:

- The proposed solution addresses performance and privacy concerns associated with biometric authentication in crowds.
- Fog nodes enhance security, privacy, and reduce authentication delays in large crowds by offloading authentication processes from the cloud.
- Improved availability for users, even in areas with no Internet connection, through the utilization of fog nodes.
- Fog nodes improve system performance by caching frequently requested data and providing immediate responses during emergency events within crowds.

LIMITATIONS OF THE PROPOSED APPROACH

The proposed approach suffers from the following limitations

- Implementation of fog nodes and variable hash codes may require initial infrastructure investment.
- Managing fog nodes and ensuring their secure operation presents a substantial challenge.
- Overreliance of fog nodes and service providers on network connectivity for communication purposes.

FINDINGS AND OUTCOMES OF THE STUDY

The case study conducted during the Hajj crowd management in Saudi Arabia demonstrated the efficiency of the proposed approach in enhancing security, privacy, and authentication speed in overly crowded environments. First, the proposed biometric authentication led to enhanced security and privacy. This is because implementing smart gates equipped with biometric authentication technology significantly enhanced security measures during the Hajj pilgrimage. By linking biometric fingerprints to individual identities, the risk of unauthorized access or identity theft was greatly reduced. This ensured that only legitimate pilgrims were granted access to essential services and facilities, such as hotel reservations, flight bookings, and medical services. Secondly, utilizing biometric fingerprints as authentication keys addressed concerns related to data theft and unauthorized access. By employing revocable biometrics and variable hash codes, the risk of biometric data theft or misuse was minimized, thereby minimizing anxiety among pilgrims and government authorities responsible for managing the crowd.

Furthermore, distributing smart gates across various locations within the Hajj area facilitated smoother authentication processes for pilgrims. Decentralizing authentication procedures minimized the pressure on individual entry points, leading to shorter waiting times and improved crowd flow management. Pilgrims were able to authenticate their identities efficiently using their smartphones and biometric information. It is also important to note that placing fog nodes across the Hajj area resolved issues with internet access for users. Fog nodes acted as intermediary points for facilitating communication between pilgrims' devices and service providers, enabling consistent connectivity even in regions with restricted internet availability. The incorporation of fog computing technology greatly improved the availability and reliability of authentication services during the trip.

Chapter 7: Health Management in Crowds

7.1 HEALTH MANAGEMENT IN CROWDS

Maintaining health in society: a fundamental matter that all countries and governments seek. After the Corona pandemic, the importance of health prevention and adherence to preventive measures has increased. It gets more complicated in crowds. It requires special treatment and protocols. This research provides a comprehensive framework for managing and promoting health and safety within crowds. The platform provides a set of important procedures, monitoring, tracking, and alerting algorithms, and a set of supporting health services that it provides via a smart application. The platform will contribute to promoting health and safety within crowds.

7.1.1 INTRODUCTION

• Health

Due to the increasing interest in public health after the historical events accompanying human life, and historically technology has helped and contributed to the remarkable development of the health sector from traditional health to smart health through several stages, namely traditional health, then electronic health, then mobile health, to smart health using smart devices and sensors, all the way to algorithms. Predictive health conditions, health incidents and finally Ubiquity Health.

• Crowds

Due to the crowding of people in a certain place, these crowds may be a major cause of the infection spreading faster, and a shortage of oxygen may also result in cases of narrow or closed spaces, which affects some age groups or some medical cases. Some crowds may also lead to disasters, affecting the Safety Therefore, we need special treatment for crowd situations to contribute to the protection of these crowds.

7.1.2 CONTRIBUTIONS:

1. An algorithm to detect numbers in crowds.
2. An application to collect and track vital data on an ongoing basis and monitor them within crowds.
3. Employing fog nodes to pre-predict and alert users in the event of a threat.
4. Employing a Drone to quickly deliver medicines and first aid kits to hard-to-reach places.
5. Volunteers and encouraging volunteers.
6. Measuring the level of compliance with precautionary measures.

In this research, we seek, through the previous points, to provide a comprehensive framework for successful health management within crowds, as the proposed framework consists of the usual main layers, which are four layers as follows:

•**Perception layer**, which is the layer responsible for providing data through smart phones or Internet of Things devices such as smart watches, wearable sensors, and radio IDs.

•**Fog layer**, which divides crowd areas for clusters to facilitate data handling, speed up data analysis in real time, predict in advance any anomalous data, and respond to emergency situations.

•**Cloud layer**, which collects all data, stores it, then analyzes and compares it with historical data and applies algorithms for analyzing big data, which we cannot deal with in the fog layer.

•**Application layer**, which is the layer for providing many health services that must be available to manage crowds, such as alerting in the event of sudden crowding, as the application provides appropriate guidance to avoid this emergency and encourage volunteers.

PROPOSED APPROACH:

Successful health management requires the presence of special protocols for dealing with crowds or prevention, in addition to continuous monitoring and finally timely alert, in addition to the possibility of flexible communication in the supporting medical units in the event of crowding, whether during medical consultations or in the event of delivering medicine to difficult-to-reach places. Thus, the research seeks through the framework of work presented to achieve the previous points of the proposed protocol as shown in Figure 7.1.

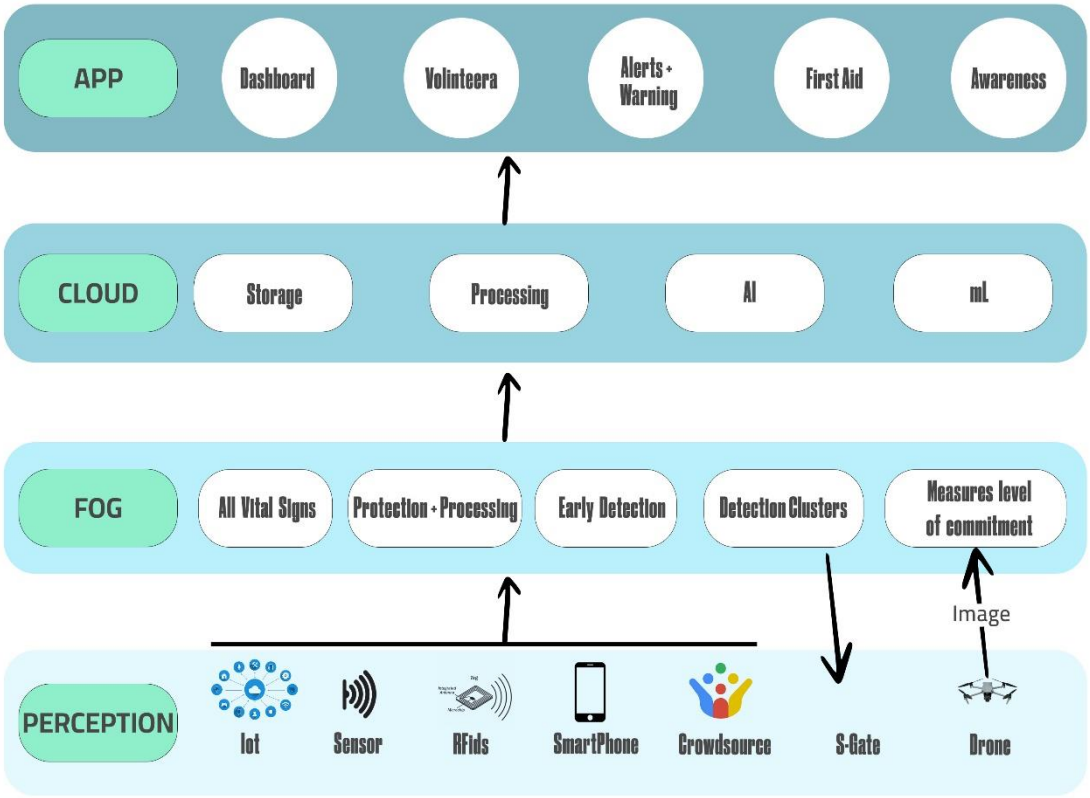

Fig 7.1: health Management Framework

1- **Special protocol**:

A special protocol for working with crowds during electronic registration processes to ensure that individuals coming to the crowds have the necessary vaccines, control the total registered numbers, verify the identity of the individuals, and give each individual one bracelet as a unique identity.

2- Continuous monitoring:

which two algorithms will be used to implement:

• An algorithm for controlling the number of users in each sector to prevent crowding that leads to crowding or dangerous crowding through the smart bracelet and gate.

• An algorithm for monitoring vital data through a smart bracelet or through an electronic service through the application that asks the user every certain period of time to enter his vital data, with the option of sending an urgent status in the event of any change in the vital data.

3- Tram:

This is the stage of measuring the level of compliance with preventive measures, which is carried out through two sections:

• Monitoring the level of distancing by analyzing images of gatherings or via a smart bracelet and location.

• Analyze the facial image and alert in the event of non-compliance with wearing masks.

4- Advance warning:

• By analyzing fog nodes for vital data and detecting any change or potential threat, thus alerting the person directly.

• Be alerted in advance if there are stampedes.

• Advance percentage through cloud sourcing analysis coming from within the crowds.

5- Effective communication:

o Through an electronic consultation application.

o Using Drons to quickly deliver emergency materials to hard-to-reach areas.

o First aid and volunteers.

o Ambulances closest to the centers or points.

o Preventive and medical advice and alerts to enhance medical awareness, provide general news, appropriate rationalization of crowds, and direct appropriate movement for them.

Chapter 8: Implementations, Findings and Discussion

8.1 MANAGING CROWDS DURING COVID-19

8.1.1 IMPLEMENTATION of the Algorithm for Proposed Framework

For the proposed algorithm, classification is more relevant than regression as we only deal with applications requiring accept (true) or reject (false) decisions. In general, one can also choose different machine learning models for an algorithm. A particular algorithm may be better than another (type of data, size of training data, selected features, etc.). On the other hand, some algorithms may have very similar accuracy. In such situations, one may opt to use multiple models with similar accuracy as a committee instead of using the one with the best accuracy. These models can be used to achieve significantly better and reliable results. These matters are discussed in Tajti (2020), where new voting functions for neural network algorithms are discussed.

Here, we provide an algorithm to support the proposed framework. We have chosen two thresholds: Threshold1 is for accepting or rejecting a model based on its accuracy, whereas Threshold2 is used for checking the number of accepted models in order to ensure reliability. The algorithm uses two functions, one for event planning, and another for event approval (See Algorithm 1).

***Algorithm 1**: Algorithm for Proposed Model.*

```
Input: Get input/request related to event from smart mobile/web application
Output: decisions to execute event or not
Step-1: Start
        Step-2: User Apply Request for Event E1 through the System/App
        Step-3: System Receive the Request and Call AI_Driven_Smart_Event (E1) for Evaluation
        Step-4: Response to Request by Rejection or Acceptance
        Step-5: If Accepted then Call Event_Execute Process
Step-6: Stop
function AI_Driven_Smart_Event (Event_Request E1)
#Start
            flag = Null;
            do // Waiting Until Final Decision
               Location Loc = E1.getLocation(); // Get Location of Planning Event Area
               Datasources ds = Get_Historical_Data_of_Area (Loc); //get collected data of selected Area
            // protocol = {MQTT, HTTP, CoAP}
            // Data will be time-series of WSNs Reads, Area Information and Capacity, Time-series of infected
        No.
            //Preprocesing_Data (ds)
            //Preprocess (dataset), contains many steps
```

```
        One_hot_encoder (ds.CategoricalPart); //label encoder for categorical data (dataset)
        Replacement_Null_Value (ds.NumericalPart); // Using Median or Average Function
        Feature_Scaling (dataset); // if there are different numeric features with different scaling
        [Training, Testing] = data_split (ds, 0.8, 0.2, Random); // Divide dataset to 20% for Testing
        Max_Accuracy = 0;
        Num_of_Accepted_Models = 0;
        Model Best_Model = Null;
        For i = 0 To Models.Count-1 // Models is list of common ML models (Regression and
    Classification)
                M = Apply_Machine_Learning_Model(Training, Testing, Models[i]);
            If (Threshold_of_Accuracy < M.Accuracy) Then
                    Num_of_Accepted_Models ++;
            If (Max_Accuracy < M.Accuracy) Then
                    Max_Accuracy = M.Accuracy;
                    Best_Model = Models[i];
            End If;
        End For;
      If (Num_of_Accepted_Models >= Threshold_of_Approve) Then flag = True;
      //Initial Accept for Request
        Else
       //Model_Reasoning
            flag = Ask_For_Manual_Decision_Admin(Best_Model, Max_Accuracy,
      Num_of_Accepted_Models);
      // Admin will show visualization results and decide manually (True or False)
        End If;
      While (flag == Null); // Until Flag has result automatically or manually
            If (flag) Then // If Flag = True
      //Check there is no other approved request for Event in the same Date
      flag = Check_ DateOverlapping (E1.StartDate, E1.EndDate); // Check there is no
      other Event in same date
      If (flag == False) Then Update_Request_Status (E1, "Reject", null, "Select other
      Date Please"); // Rejection
      Else //Event_Planning
      Certificate C= Generate_Certificate (E1); // Certificate for Approval
      Update_Request_Status (E1, "Approve", Cert, Guidelines_Doc);
            End If;
      Else
            Update_Request_Status (E1, "There is Threat, So the request is
      rejected"); // Rejection
      End If;
      Return flag;
      #End
function Smart_Application (String eventType, Location eventLoc, Date
evenStartDate, Date eventEndDate)
      #Start
            //Create New Event_Request by the received event from Input
            Event E1= new Event (EventType, EventLoc, eventStartDate,
            eventEndDate);
            Result = AI_Driven_Smart_Event (E1); //Send Request
            If (Result)
                  Show_Alert ("Approved, Check Your Request Status for
            Details"); // The response of
      your request
            Else Show_Alert ("Rejection, Check Your Request Status for Reason");
      // The response of
      your request
      #End
```

Important Procedures and Policies for Event Execution

Here, we list some procedures and policies to be made available during the execution.

Release Info_Bulletin

- Release Event_Advertisement

//event_strategy

- Allow participants with a valid permit and a current PCR test;
- Provide a kit with essential items (i.e., mask, sanitizer, etc.) and a leaflet of information;
- Manage queues by enforcing adequate social distancing;
- Thermal screening, passing through a sanitization tunnel;
- Provide RFID-tagged bracelet for tracking and providing emergency help.

//navigation_strategy;

- Monitor crowd movement on CCTV;
- Manage movement to prevent crowding;
- Track individuals with RFID tags as and when required;
- Broadcast alerts through loud speakers and billboards;
- Provide healthcare and emergency support;
- Report violations.
- Collect, store, and manage data from activities and devices (sensors, reports, etc.) for current and future use.

8.1.2 Explanations and DISCUSSION of Main Functions of the Algorithm

The algorithm is designed to function in the following manner:

1. The applicant (host/owner/event management committee) would use the Smart Application form to apply for an event permit by inputting the type, location, number of participants, and start and end dates of the event.
2. The Smart Application function will then receive it as a new request and start evaluating the request by invoking the "Smart Event" function, which would process the application through the following steps:
    a. Historical data about the selected location (from previous event(s)), which include reports of incidents and infections of previous events for the selected area, would be retrieved. Data from IoT sensors about the pollution and congestion or crowd ratio of the area (time-series) will also be analyzed.
    b. Preprocessing of the available data according to its type (numeric or nominal) would take place, which would consist of replacing the null values, scaling numeric values, and encoding the nominal values.
    c. The function will then apply common machine learning (ML) models (by going through each of them, one by one), and calculate the accuracy of each step. Note that the function has a list of common ML classification models (managed by the admin), for example, linear regression, log regression, SVM, naive Bayes, decision tree, etc. Thus, the proposed framework depends on different kinds of machine learning models, not just regression but also classification.
    d. Then, the data will be divided randomly, with training being 50% and testing making up the other 50%.
    e. The function will calculate the number of models that have an acceptable accuracy (larger than a specific threshold).

f. The function will compare all accuracy values and find the ML model with the maximum value and save this result (to support the admin when managing the list of ML models in the future).

g. The function will check if the number of accepted models is large enough (the threshold can be adjusted by the admin). If so, the function will accept the request automatically when it is verified that there are no threats in this area to host the event.

h. In case the number of accepted models is less than the threshold, the function will request manual reviewing with the accuracy result of the best ML model, in addition to the number of accepted ones.

i. If the return decision is to reject the application, the function will send an alert to the applicant citing safety concerns.

j. If the automatic or manual decision was to approve, the function will check for the availability of the date(s). If the desired date(s) is not available, the function will send a rejection message and advise the applicant to choose another date(s).

k. If the applicant's request is approved, the function will update the status of the request, notify the applicant, send guidelines, generate the certificate of approval, and invoke the Execute Event function (to send an alert to teams to start the process of preparations).

3. It should be noted that we mentioned an important procedure, which contains a number of tasks related to the organization of the event (e.g., alert teams, send ads, monitoring event condition, and feedback). However, all data collected from sensors during the event will automatically be sent to the cloud, as shown in the proposed framework.

4. Feedback and other relevant data will be merged with previous historical data for future evaluation.

8.1.3 Factors for Validation for ML Model

As a result of data not being available, there is no real validation in this work. Instead, here, we set out a scheme for future validation of the framework, which can be used to support decisions concerning the management of events during the pandemic situation and other similar scenarios. In other words, our results are simply recommendations, along with some metrics for validation in the future.

The following paragraph provides some common metrics to test ML models in general, which can also be used for the proposed framework, and collect and organize real data (dataset). The dataset can be built manually from the reports of all events and associated applications. Data about COVID-19 from its beginning to up until now would also be useful.

Optimization: Avoiding Model over Fit with an Additional Handout Set

For training in a machine learning model, we usually split data into two parts: 80% for training and 20% for testing. The machine learning model provides a data split function to achieve this splitting. After data splitting, the model can do training and testing on these parts, and provides some metrics through which we can verify whether the results are acceptable or not.

8.1.4 K-Fold Cross Verification

1. Using classic F-fold cross validation by splitting data into k-folds, k = 5;
2. Observations: All combinations and averages of both the test and validation observations;
3. Validated against: Computational complexity and validation accuracy;
4. Optimization: Improving stability of the machine learning model across several data inputs.

This approach splits the given input dataset into K groups (K-fold) of sections of equal sizes. For every learning set, the K-fold prediction function takes (k − 1)-folds, and the remaining folds are reserved for the test set. Using this method, the output is observed as less biased when compared with other methods. This method takes a group as the standby or test data set, takes the remaining groups as the training dataset and tries to fit the model on the training set, and assesses the performance of the model using the test set for each group to improve the stability of the model.

8.1.5 Nested Cross Validation

1. Using nested cross validation strategy;
2. Observations: Use inner loop (two-fold) for hyper parameter tuning, use outer loop (five-fold) for accuracy estimation;
3. Validated against: Error estimation;
4. Optimization: Improving hyper parameter tuning and estimating accuracy.

The nested cross-validation approach separates the hyper-parameter tuning step and the error estimation step. This process uses the inner loop for hyper-parameter tuning and the outer loop for estimating accuracy.

8.1.6 Time-Series Cross Validation

1. Using F-fold CV by splitting data into k-folds;
2. Observations: Entire training data occurs before your test data;
3. Validated against: Over fitting;
4. Optimization: Improving stability of the machine learning model across several data inputs.

The drawbacks of traditional CV techniques are addressed by using this approach through splitting time series data without instigating data outflow, and using a nested CV to get an impartial estimate of the error on an independent test set and CV with datasets that hold multiple time series. This approach improves the stability of the machine learning model across several data inputs and avoids overfitting.

8.1.7 Model Comparison

1. Using method 5 × 2CV paired t-test from Scikit-learn Python machine learning library;
2. Observations: Statistically significant;
3. Validated against: p-value; 4. Optimization: Choose the best model.

Based on the statistical significance of the machine learning models, the best model that fits the data to provide better predictions is identified. A 5 × 2CV paired t-test model is used to relate machine learning models based on their strong statistical foundation. This model would split the data into training (80%) and testing (20%), and

select the testing part (20%) randomly five times. Let Ca, Cb, Cc, Cd, and Ce be five classifiers, test each classifier on the training data, and compute (DiffAi) the difference in the accuracy between these classifiers. In this way, the process goes through five iterations, which can be used to compute the mean variance (S2). Then, t-statistic can be computed from the following formula:

$$\text{t-statistic} = \frac{DiffA_1}{\sqrt{\frac{1}{5}\sum_{i=1}^{5} S_i^2}}$$

where DiffA1 is the mean variance of the first iteration.

8.1.8 Future Research

In future research, we will provide validation of the proposed algorithm using a suitable dataset from the operations of the system. Additionally, we will provide methods to manage and ensure privacy and security in the proposed framework. We will also deal with the interoperability issue for converting heterogeneous to homogeneous data so as to better support different applications.

8.2 INTEGRATIVE TECHNOLOGIES FOR REAL-TIME CROWD MANAGEMENT: A CASE STUDY OF THE HAJJ

8.2.1 IMPLEMENTATION AND RESULTS

The implementation process is described with following stages:

A. Smart Gates Stage

Smart gates employed Internet of Things technology and fog computing, by distributing electronic gates (RFID readers consisting of two pieces at both ends of the path or the entrance to each area, and the reader can be one piece placed on top). Further, electronic bracelets are distributed to the crowd participants for automatic identification. Thus, the smart gates enabled them to track the numbers of people entering and leaving a certain area, which assisted the administration to control the distribution and flow of numbers flexibly, effectively and automatically in real time because the gate can also be locked automatically when the numbers exceed a certain threshold. The proposed smart gates achieved several additional features in crowd management to raise the level of safety and prevent heavy traffic. These features include:

• Provide a tracking mechanism for specific people at the time of need within the crowds.

• Avoiding cases of loss and enabling pilgrims to know the location of their current campaigns or members of their families and friends.

• Preventing unauthorized persons from entering, for example, a person entering a camp other than his camp or an area other than his

• Detecting fake or duplicate permits.

• Distribute the load on a regular basis on the tracks, regions and cells.

• Automatic closure of areas when numbers reach a certain limit.

• Employing smart fences to provide smart alerts for people with special needs (in proportion to the condition of the disability)

• Facilitate crowd control and management

Figure 8.1 and 8.2 show a conceptual form of the proposed smart gates' mechanism of action, where two types of gates (two-piece or one-piece) appear with

the communication mechanism between the gates and the fog node. These are in turn connected to the data center and the main processor. It should also be noted that the gates monitors entry or exit from the areas, and therefore there must be a control center with the gates of a specific area. Hence, the fog node plays this role in addition to a central controller that can create integration in the work of all the gates for the studied area.

B. Monitoring Phase via Drones and Photos

The proposal indicates that drones that can reach any area should be used. These drones should not cause additional barriers. Hence, they can be allocated in two ways, either as a complete coverage of the area or by sending them to areas where the numbers exceed a certain threshold.

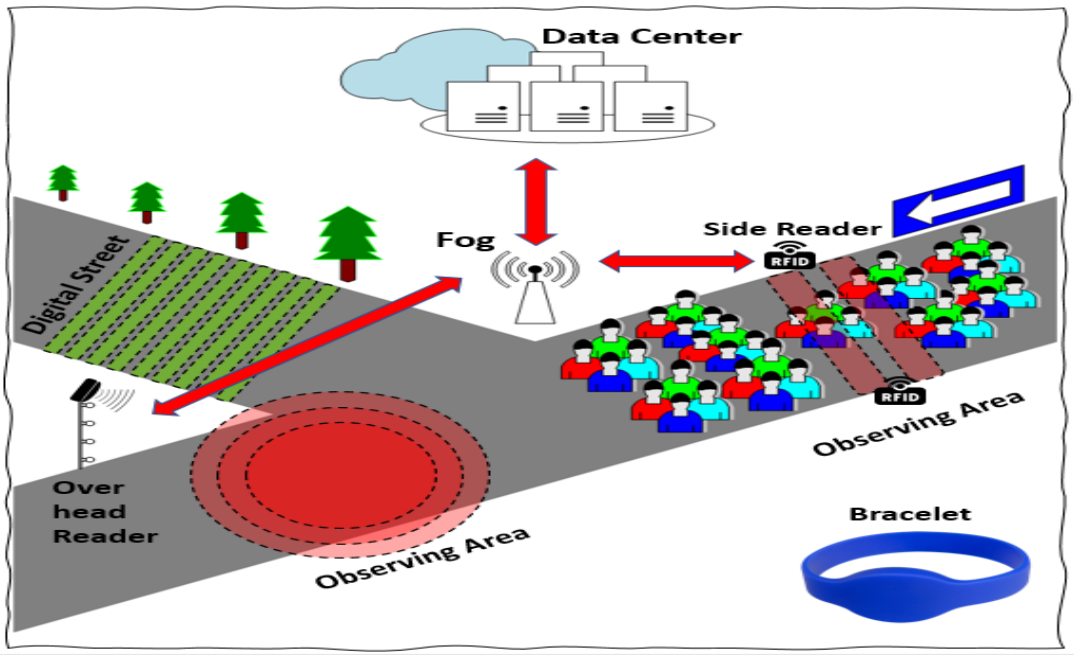

Fig. 8.1 Proposed smart gate for crowd-managing (I)

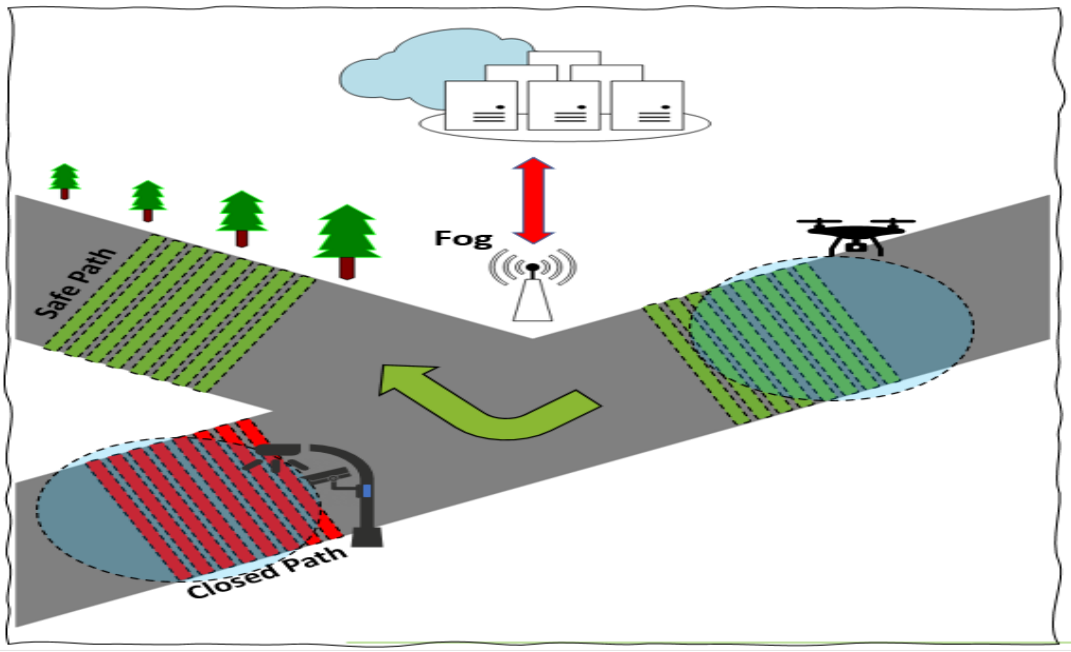

Fig. 8.2 Proposed smart gate for crowd-managing (II)

At this stage, we provided an instant image processing algorithm, and therefore the algorithm had to be light in order to enable the microprocessor in the drone to process it immediately and send text values instead of images to the fog node to make the final decision based on the information collected from more than one source as we mentioned earlier.

Thus, the proposed algorithm relies on several steps, where the original image size is first adjusted to a uniform size to adjust for standardization of the ratio calculation process and to reduce the image size and speed up the processing process Figure 8.3 Then the image is converted from RGB to gray to isolate the influence of color compounds on the calculation process and to work with One layer and speed up the calculations, and then a filter is applied to remove noise from the image to isolate some of the anomalies Figure 8.4 In the third step the Canny filter is used in order to calculate the edges of the objects in the image and to convert the image to black and white.

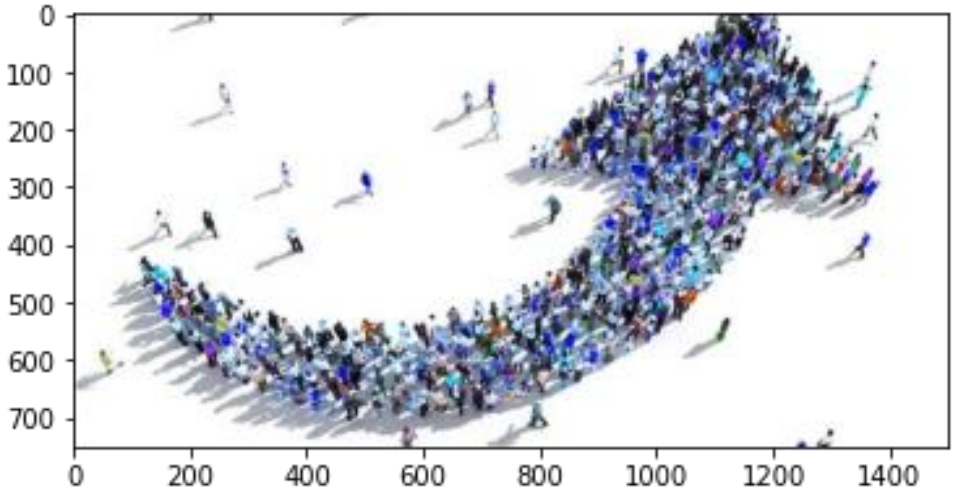

Fig. 8.3 Example of image processing algorithm (I)

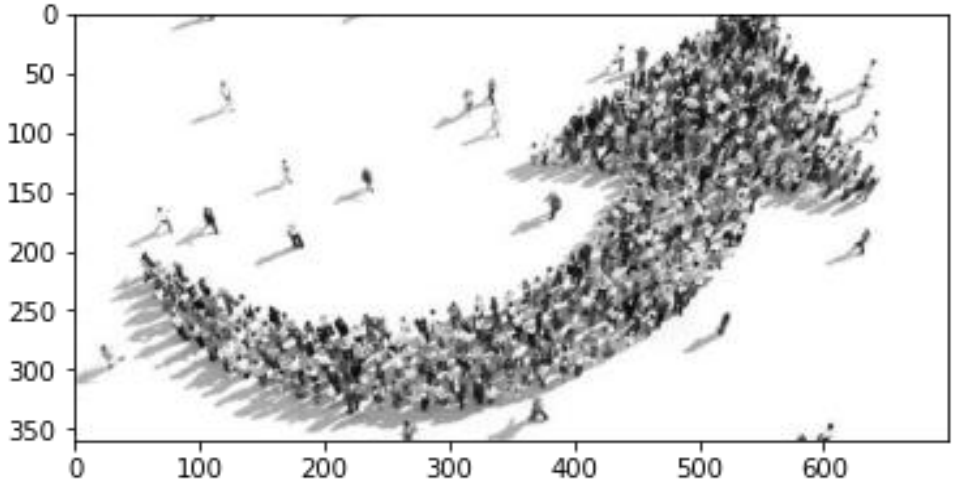

Fig. 8.4 Example of image processing algorithm (II)

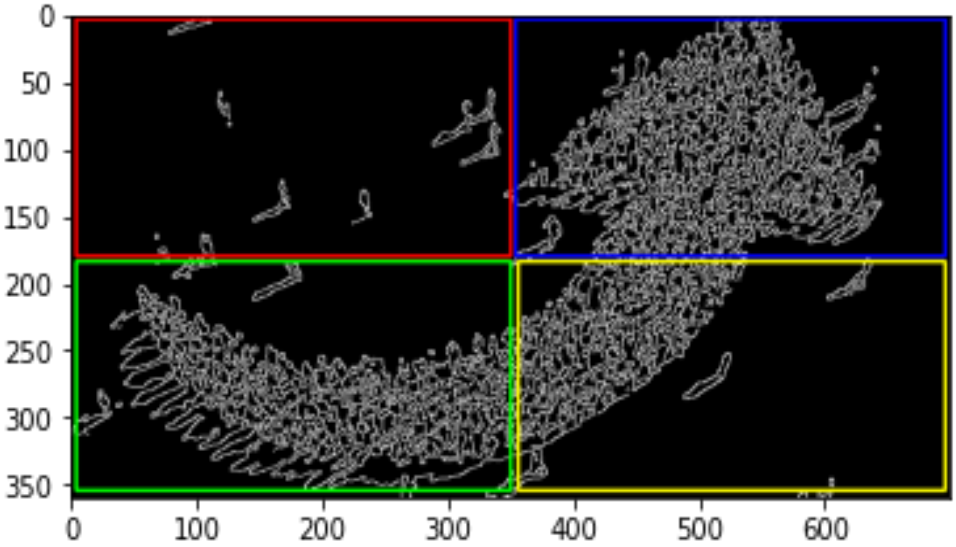

Fig. 8.5 Example of image processing algorithm (III)

The image is then divided into four equal sections as illustrated in Figure 8.5 so that the ratio of white pixels to black pixels in each section is calculated. The resulting ratio is then multiplied by an adjustment factor X, which is controlled by the administrator according to the plane's distance, image and cell size.

In Figure 8.5,

- *Percentage in Red is: 7.3%*
- *Percentage in Green is: 52.4 %*
- *Percentage in Blue is: 65.9%*
- *Percentage in Yellow is: 40.7 %*

The resulting ratio represents the congestion value in each sector. While the division process will contribute to enabling the fog node to determine the direction of crowd movement, and thus dynamic control of the smart gates, so that some gates are locked or opened to control crowd movement. Digital streets are also controlled to illuminate in colors that make it easier for crowds to easily follow directions and know the instructions to be followed to ensure the safety of crowds and stay away from areas Rally and avoid scrambling.

Algorithm1- Detect the rate of crowd in each cell

```
Double CrowdRate[] Calculate_Crowd_Ratio (Image x, Int Width, Int Height, Int Cols, Int Rows)
Start
        Img = Read_Image(x)
        Gray_Img= Convert_RGP2GRAY (Img)
        Gray_Img= Resize_Image(Width, Height)
        Img_Edge= Canny_Filter(Gray_Img, Threshold)
        W= Width / Cols
        H= Height/ Rows
        Rectangle [] R = New Rectangle [Cols*Rows]
        W1=0
        H1=0
        Index =0
        For (int i=0; i< cols; i++)
                For (int j=0; j< cols; j++)
                        W=W*i
                        H=H*j
                        R[Index]=Img_Edge(W1:W, H1:H)
                        Index++
                End For
        End For
        For (int i=0; i<R.Count;i++)
                Res = Sum (R[i]) / (R[i].Rows*R[i].Cols)  // Calculate
                Rate of Crowd (Percentage of weight pixel)
                CrowdRate.Add(Res)
        End For
        Return CrowdRate
End Function
```

C. Crowdsourcing Stage and Smart Phone Applications

Smartphones have become one of the basics of life and an essential companion for almost everyone, especially with millions of mobile services and applications that have facilitated and changed the concept of access to basic and daily services in our lives. Also, the data flowing from these applications has become an important resource for many systems. In this research, we developed a special application that enables crowds to send information about any abnormal event such as stampede, medical condition or fire so that appropriate action can be taken directly while providing a live image of the site to the decision-maker in addition to automatic control through gates and digital methods. In order to control crowd movement and control the event before it turns into a disaster the application also makes it possible to send useful information to crowds about crowded places and about some important alerts and warnings. Figure 8.6 shows the default interfaces for the proposed application. More than that, the application can be developed to provide information in cases of loss or loss through integration with digital portals. Further, Figure 8.7 shows the main screen in the application, which enables the user, after logging in (to ensure reliability), to inform about the occurrence of a specific event to appear on the map to others, with the possibility of confirming an event or denying a specific event that was reported by another user.

Fig. 8.6 Application main screen for user login

Fig. 8.7 User Interface for Event Management

D. Digital Street Stage

When an event or congestion is detected in a specific area or path, alerts will be sent directly to the digital streets, which are luminous pieces of different colors LED Pieces that are inexpensive and are planted in parts of the paths floor of the crowd gathering area. So that the colors guide the people within the crowd and the security and safety men to crowded or closed areas that should not be approached (in red) and to safe and less crowded paths that are illuminated (in green). Of course, smart gates will achieve physical locking of some areas when necessary. The importance of the proposed digital street is that the lighting of the streets On which crowds walk in different colors will be easy to notice and will reduce the need for the use of a large number of security men, in addition to being understood by all individuals of different languages or customs in various gatherings such as Hajj in the Kingdom. To achieve this, the illuminated pieces are distributed in different places on the street, not on the entire track, in order to reduce costs. The mobile application also sends alerts and instructions to individuals, as well as to security and safety teams.

Figure 8.9 shows an example of using the digital street, closing some lanes or areas in red, and lighting alternative lanes in green.

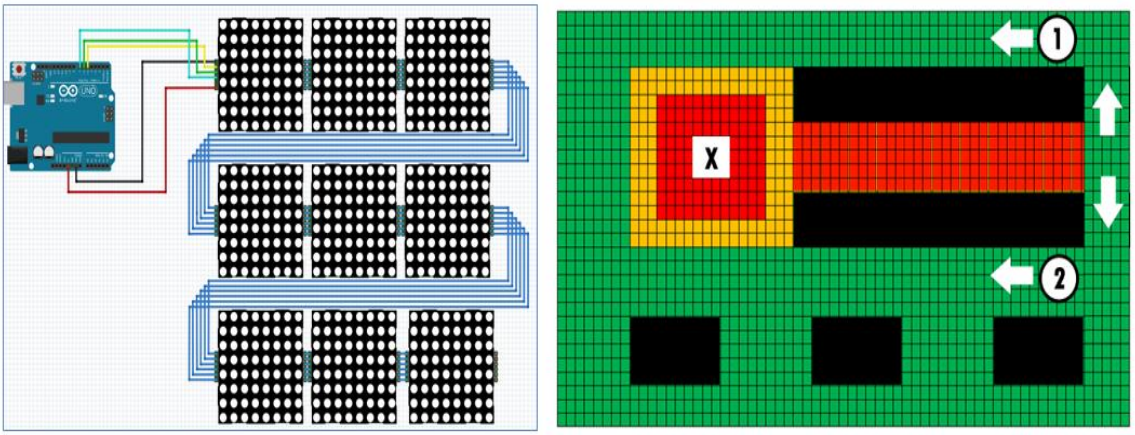

Fig. 8.9 Digital Street Stage

Case study

To evaluate the proposed framework, it must be tested in an actual environment. The Kingdom of Saudi Arabia is considered one of the countries that witnesses crowded crowds throughout the year, especially during the month of Ramadan and the sacred months in the Mosque of Mecca, the Mosque of the Prophet, and the areas of the holy sites for more than a billion and a half Muslims.

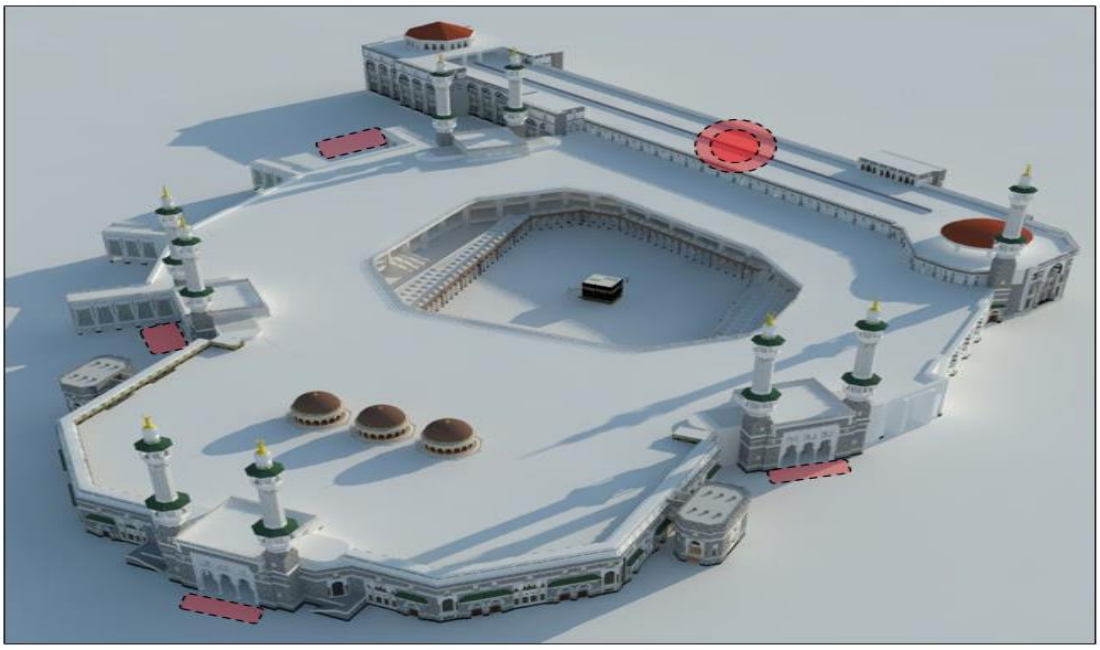

Fig. 8.10 Imaginary diagram of the distribution locations of smart gates within the Grand Mosque in Mecca

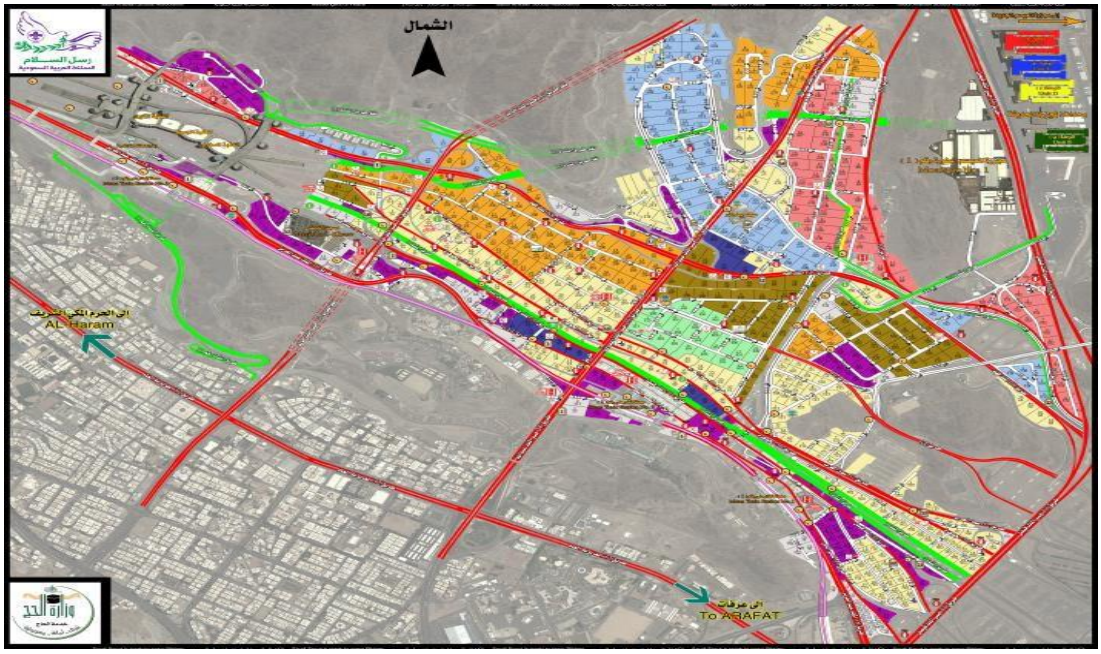

Fig. 8.11 (Scouts.org.sa, 2011) Distribution of Mina and Muzdalifah into sectors

Since more than 7 million people are gathered in one place, many safety measures and crowd management policies must be applied in order to be able to control and manage crowds flexibly. The proposed framework greatly assists in the success of the process of effectively organizing crowds during the seasonal period. Thus, Figure 8.10 shows an imaginary diagram of the distribution locations of smart gates within the Grand Mosque in Mecca (the areas shaded in red), which ensures obtaining very accurate information about the number of crowds in the circumambulation area and in each sector within the Grand Mosque. Figure 8.11 issued by the Hajj and Umrah Management Authority indicates how the Mina and Muzdalifah regions are distributed into sectors, in addition to the main routes that crowds take during the Hajj period. This image confirms the possibility of applying the proposed approach within the emotions area also by distributing fog nodes across sectors and preparing digital routes within the roads and branches taken by crowds so that they can be easily controlled based on the proposed algorithm and through the applications and services available on the proposed application.

The following section refers to the source code that was implemented using the Python language on the Google Colabs platform, in addition to the results obtained about congestion rates when experimenting on multiple images.

A. Python Code

```
#Load libraries  import pandas as pd  import numpy as np
import matplotlib.pyplot as plt
from sklearn import model_selection
from sklearn.metrics import accuracy_score
import cv2
images_array=["s.jpg"]
for img in images_array:
 image = cv2.imread(img)
 plt.imshow(image)
 plt.show()
 gray_image = cv2.cvtColor(image,cv2.COLOR_BGR2GRAY)
 gray_image = cv2.resize(gray_image,(700,360))
 edged = cv2.Canny(gray_image, 100, 500)
 ret,thresh = cv2.threshold(gray_image,220,255,0)
 gray_image = cv2.cvtColor(gray_image, cv2.COLOR_BGR2RGB)
 edged = cv2.cvtColor(edged, cv2.COLOR_BGR2RGB)  plt.imshow(gray_image)
 plt.show()
 edged = cv2.cvtColor(edged, cv2.COLOR_BGR2RGB)
 ##---------------------------------------------
 cv2.rectangle(edged, (4,4), (350,180), (255, 0, 0), 2)
 cv2.rectangle(edged, (4,184), (350,354), (0, 255, 0), 2)
 cv2.rectangle(edged, (354,4), (696,180), (0, 0, 255), 2)
 cv2.rectangle(edged, (356,184), (696,354), (255, 255, 0), 2)
 #white= Total - cv2.countNonZero(img[1])  Rows - Cols
 Red_white = np.sum(edged[0:180, 0:350] == 255)
 Red_black = np.sum(edged[0:180, 0:350] == 0)
 percent1 =  (Red_white/Red_black)*100*3
 #print('Number of white pixels:', Red_white)
 #print('Number of black pixels:', Red_black)
 print('Percentage in Red is:', round(percent1,1),'%')
 Green_white = np.sum(edged[180:360, 0:350] == 255)
 Green_black = np.sum(edged[180:360, 0:350] == 0)
 percent1 =  (Green_white/Green_black)*100*3
 #print('Number of white pixels:', Green_white)
 #print('Number of black pixels:', Green_black)
 print('Percentage in Red is:', round(percent1,1),'%')
 Blue_white = np.sum(edged[0:180, 350:700] == 255)
 Blue_black = np.sum(edged[0:180, 350:700] == 0)
 percent1 =  (Blue_white/Blue_black)*100*3
 #print('Number of white pixels:', Blue_white)
 #print('Number of black pixels:', Blue_black)
 print('Percentage in Red is:', round(percent1,1),'%')
 Y_white = np.sum(edged[180:360, 350:700] == 255)
 Y_black = np.sum(edged[180:360, 350:700] == 0)
 percent1 =  (Y_white/Y_black)*100*3
 #print('Number of white pixels:', Y_white)
 #print('Number of black pixels:', Y_black)
 print('Percentage in Red is:', round(percent1,1),'%')
 plt.imshow(edged)
```

Chapter 9: Future Research

To date, there is no comprehensive solution for crowd management. Most of the historical research presents individual solutions for specific problems only. However, this research proposes a comprehensive framework by integrating many solutions, technologies, and tools to create an effective solution for all issues related to crowd control and management. In addition, the proposed framework will support interoperability between heterogeneous techniques and devices and provide a number of assistant services and applications.

One of the most important components of the crowd management framework is continuous monitoring of crowds to detect any unusual activity or incident in order to help management to address it effectively and efficiently. In future research, there will be many different methods to detect unusual and suspicious activities. This would involve trust and cooperation among different layers and technologies of the framework including images processing, WSNs, RFID, and text analysis of social media. It is expected that timely detection of abnormal activities and issues would allow management to control the situation before it turns into a disaster.

Sometimes disasters occur despite best efforts to manage a crowd appropriately. The CMS is designed to prevent as well as manage disasters. One of the expected disasters in an intensely crowded event is a stampede. As part of the full thesis, a number of smart ways will be suggested to deal with the flow of crowds to avoid stampedes, and manage the emergency services and cleaning if one does take place. As part of the safety mechanism, several methods for notifying and guiding different people with disabilities, old age, cultural barriers, and communication and other issues would also be provided.

A crowded event, if not managed properly during COVID-19 pandemic, can become a super spreader of the infection. Managing crowds during a pandemic would require different protocols and strategies. As part of the future research, specific polices and method will be suggested for managing the health and safety of the participants.

In order to improve future management, collection and analysis of entire data about the activities of the event is a mandatory requirement of crowd management. Intelligence gained from data analytics is necessary for providing smart services. On

the other hand, issues of privacy and security of data are very sensitive and critical. As part of the full thesis, a new approach for preserving privacy and security in the crowd management context will be provided.

Mobile and web applications have become very useful, and more and more people are now using them. In order to enhance the quality of services of crowd management, the use of applications will be essential. As part of the future research, such applications would be provided to create awareness, provide guidance, locate POI, find lost articles, provide item and human tracking, and provide first aid, among other functions.

We shall provide simulations of Crowds with the help of MATLAB. With Hajj being an annual and highly organised crowded event, we shall discuss implementation of our framework and the Stampede Detection Model in the case of Hajj, We shall also provide algorithms for effective management of crowded events at a later stage.

9.1 STEMPEDES AND CRISES MANAGEMENT

There are several components for managing crowds and providing a stampede detection and mitigation system. Cloud and Fog computing, through its nodes, play a pivotal role in managing critical functions of crowd management. There will be several mobile units (including drones) which can be treated as fog nodes. A detailed description of them, including the following, will be provided in the future research.

9.1.1 Fog Layer

- A method of distributing a large number of nodes required to cover the designated area for crowd management
- A method of analysing data
- A method of detecting events, requiring actions, in the crowded area
- Policies on data for security and privacy
- Notification mechanism for alerts to the participants of the crowded events

9.1.2 Cloud Computing

- DS algorithms for detecting knowledge from previous experience
- Privacy and security model as per the proposed approach
- Interoperability method for heterogeneous services and devices

9.1.3 LBS and Tracking

- Apps to help the members of the crowd search for specific services (auto service centre, restaurant, police, or medical centre) will be provided
- For the purpose of tracking, the location of users to get information about the crowd in each area, as well as tools and scenario will be provided
- A Mechanism to detect lost items (including personnel) will be provided
- An appropriate app which allows users to select the most appropriate route and navigate to the desired destination will be provided

9.1.4 Crowd Flow

- In order to control the crowd flow, a web application to plan the flow with respect to time and location will be provided
- A smart algorithm using Image Processing and RFID Tracking to monitor the flow of the crowd and confirm its smooth flow will be provided
- A smart algorithm for detecting any unusual event in the crowd will be provided. This will be enabled with the help of text mining of social media sources, notifications of users themselves in the crowd, and image processing
- Advisory to enhance the awareness of users in a crowd about the timing, places, activities, signs etc. will be provided using one or more apps

9.1.5 Stampede, Crisis and Emergencies

In order to prevent disasters and hazards, the CMS will provide alerts and remedies. In particular, the CMS will:

- Provide a range of methods to notify and instruct participants to take prompt action in order to prevent disasters from occurring
- Provide a new protocol to deal with crowds in case of crises, in addition to a method to control flow after an abnormal situation to prevent a disaster
- Provide a new algorithm for auto monitoring the adherence of users in special situations
- Validate the algorithm

9.1.6 Organization of activities

Details of activities associated with the CMS require organisation, which would be discussed in detail in future research. In particular, the following will be provided:

- Prevent unauthorized users from entering any area or access to any service, which will control the maximum number of users and prevent random distribution
- Provide a comparison between different methods for physical access and the presence of available resources.
- Organise transport to move within the event perimeters as well as to connect with the external entities of interest
    - Web service to manage trips, buses, metro, and routes.
- Web service organize and divide groups' camping (Hajj case study)
- Web service to manage leisure activities, timing, and site seeing to reduce mental stress from the work environment.

9.1.7 Health and Safety

Most of the health and safety related activities are performed in relation to the Electronic Health record (EHR). The following is the list of activities which would be designed and discussed related to EHR or otherwise.

- Provide a web application for comprehensive health data with many of the electronic services that depend on WSNs, RFID, Surveys, etc.
- Service in the mobile application
- Algorithm to detect and track infected users and notify close contacts to be careful
- Algorithm to monitor the precautionary rules applied and detect violations
- Smart application to enable users to help themselves in emergency cases
- Smart algorithm and tools to enable a relief team to arrive quickly to the event location in the crowd

9.1.8 Environment and Energy

In order to have a successful event, the environment within and outside the event must be clean and free from bacteria. In order to take care of the environment related issues, the following tasks will be organised.

- An algorithm for filtering waste in the crowd will be provided
- Monitoring the condition or environment of a crowded area, and notifying for any change in the regular ratios to keep the environment free from pollution
- Cleaning to preserve the environment and crowd area from infections developing from waste material
- Providing smart containers and a smart method to collect waste in a crowd
- Mobile service for garbage collection
- An energy saving mechanism.

9.1.9 Implementation of CMS in the Hajj case

In order to provide evidence of suitability and applicability, a simulation of crowd management in the case of Hajj CMS will be conducted to provide evidence of successful operational capabilities. This would provide an example of the suitability of the technologies used for managing and controlling crowds.

The CMS contains additional components. Their validation or simulation will be provided in future studies.

9.2 WASTE MANAGEMENT IN CROWDS

Proposed approach

In this section, a detailed description of the proposed framework for effective waste management is presented in the form of an X. The proposed framework explains the layers used and the tools and tasks for each layer as shown in the next figure.

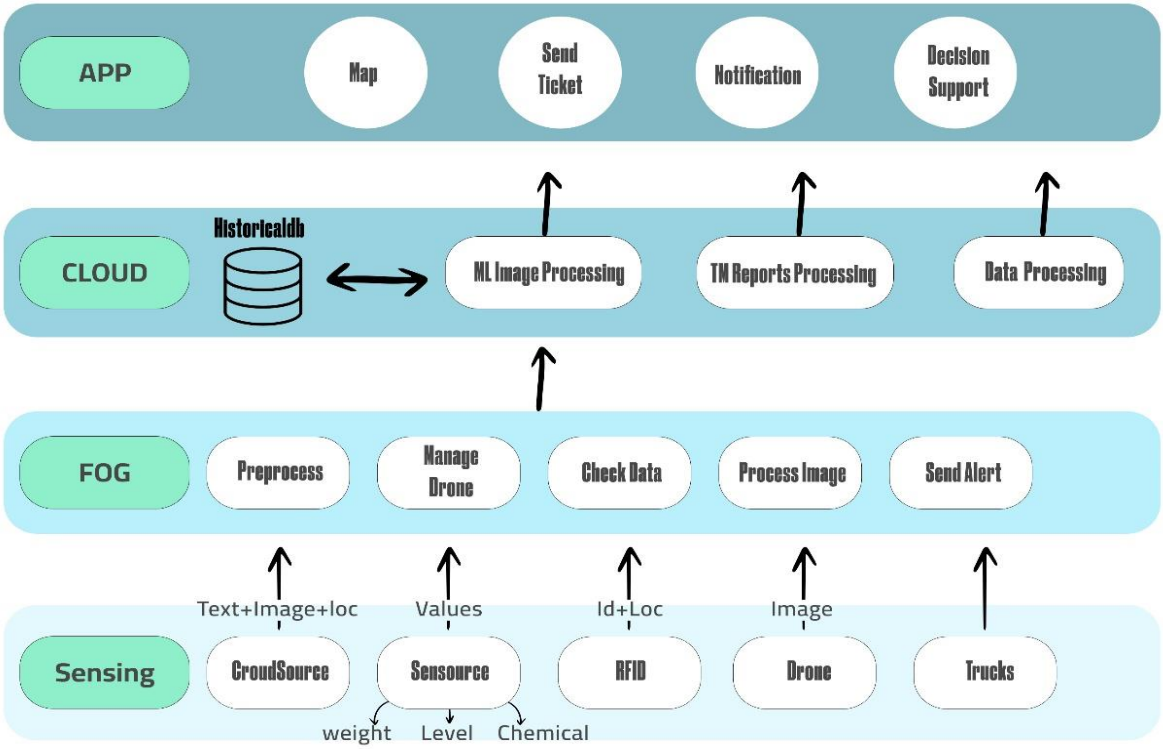

Fig 9.1 Waste Management Framework.

The first layer is the IoT layer where sensors are placed in each container with a radio ID to form smart waste containers, it is possible to track or build a historical record for each container through its unique identifier. The sensors also provide information about the level of fullness of the container, the weight of the waste, and finally the level of gases emitted. All this information is sent to the second layer (fog nodes).

Second layer: Each doctor node analyzes the received data based on a simple algorithm to support the decision of whether the container needs to be emptied or not.

In exceptional cases (crowds), the fog node can also send immediate requests for small-sized collection vehicles with special pressure compressors to deal with waste immediately. By integrating with the smart gate system, a safe path can be chosen for these vehicles without affecting the movement of crowds.

The third layer, the cloud, stores all previous data to form six important data to apply this data to the ML algorithm to draw the shortest path, in addition to pre-predicting the fullness of containers and choosing the most appropriate time for each of them based on the nature of the place in which it is located (location).

Fourth class applications

The layer contains two types of applications:

The first is for fleet management, as it displays a map with container distribution points and the status of these containers, in addition to the locations of vehicles in RT. This application will effectively support fleet control decisions.

The second is for users, as it enables the user to send a direct request in the event of a smell or an accumulation of waste in a specific place, where he sends a description with a picture and location.

Requests are handled, prioritized, and scheduled within the management system. An algorithm that verifies the login mechanism through a unified system

Fog nodes help in building a special schedule at the neighborhood or sector level, thus facilitating the management process and increasing the level of accuracy, as each neighborhood or location has its own nature.

Chapter 10: Conclusions

Crowd management is a complex exercise. Partly because of uncertainties surrounding the actual turn out of the number of participants. Common problems of crowd management continue to remain such as inadequate management, lack of experience and resources, and reluctance or inability to use technology. Addressing one aspect wouldn't fix the problem of crowding, rather it must be a comprehensive solution. A comprehensive solution, with the help of suitable technologies, such as provided in this thesis, can help reduce the number of problems encountered by the management of crowded events. In this thesis, we have developed and thoroughly evaluated a comprehensive framework designed for the efficient management of crowds utilizing the latest advancements in technology. Our research was motivated by the growing need to address the challenges of crowd management, which has become increasingly complex due to the rising scale of public gatherings and the inherent risks of stampedes, overcrowding, and the spread of diseases, as highlighted by recent global events, including the COVID-19 pandemic.

The framework presented herein leverages a multi-layered approach that integrates Cloud Computing, Fog Computing, the Internet of Things (IoT), and Artificial Intelligence (AI) to offer a robust solution capable of addressing the dynamic and multifaceted nature of crowd management. This integration not only aims at improving the efficiency and responsiveness of crowd management strategies but also at enhancing the safety and security of individuals in crowded settings.

A significant contribution of this thesis is the demonstration of how modern technologies can be synergistically harnessed to provide real-time monitoring and management of crowds. By deploying IoT devices for data collection and utilizing AI for data analysis, the framework facilitates swift decision-making and proactive management actions. Furthermore, the adoption of Fog Computing serves to minimize latency, ensuring that critical data and insights are processed closer to the source, thereby enabling faster response times to emergent crowd-related challenges.

Our research findings underscore the potential of this framework to revolutionize crowd management practices. Not only does it offer a scalable and flexible solution adaptable to various contexts and scales of gatherings, but it also presents a model that can be iterated upon and improved as technologies evolve.

The significance of this research lies in its holistic approach towards crowd management, encompassing the entire lifecycle of crowd dynamics from the planning phase to the post-event period. This comprehensive methodology enhances the effectiveness of the proposed solutions by addressing not merely a singular aspect or challenge but the entirety of the crowd's journey. Such an approach ensures that the solutions implemented are robust and can significantly improve the management of crowds more effectively than previous methods.

Furthermore, the research meticulously considers the critical issues of privacy and security, proposing solutions that surpass the capabilities of existing methodologies. A notable innovation introduced is the concept of digital gates, characterized by their exceptional accuracy and real-time processing capabilities, which facilitate precise counting of individuals without delays.

Additionally, the development of a lightweight and rapid image processing algorithm represents a significant advancement, offering quick implementation without computational delays. This algorithm is instrumental in assessing crowd density and generating timely alerts to prevent overcrowding.

Another innovative solution presented is the concept of a 'digital street', integrated with a mobile application. This platform proves highly effective in disseminating alerts, managing crowd flow, and providing a suite of additional services tailored to the needs of the crowd. These services include functionalities such as locating lost items, identifying points of interest, offering consultations and guides, and promoting cultural awareness, among others. Collectively, these features not only enhance the safety and efficiency of crowd management but also enrich the overall experience of the participants.

However, the deployment of such a comprehensive framework is not without challenges. Issues related to privacy, data security, and the ethical implications of surveillance in public spaces necessitate careful consideration and the implementation of stringent safeguards. Moreover, the success of this framework depends on cross-

sector collaboration, involving government bodies, event organizers, and technology providers, to ensure its effective implementation and integration into existing crowd management protocols.

In conclusion, this thesis contributes to the ongoing discourse on the application of modern technologies in public safety and crowd management. It offers a forward-looking perspective on how digital innovations can be leveraged to mitigate risks associated with large gatherings, ultimately fostering safer and more organized public spaces. As we advance, continuous research and development in this domain will be pivotal in addressing the evolving challenges of crowd management, ensuring that technological solutions remain adaptive, effective, and aligned with societal values and norms.

Bibliography

Abdulqadir, H. R., R. M. Zeebaree, S., M. Shukur, H., Sadeeq, M. M., Salim, B. W., Salih, A. A., & Kak, S. F. (2021). A study of moving from Cloud computing to Fog computing. *Qubahan Academic Journal*, *1*(2), 60–70. https://doi.org/10.48161/qaj.v1n2a49

AFP. (2017, November 11). *Arbaeen crowd, Karbala* [Photo]. https://www.dawn.com/news/1369782

Ahmed, Q. A., & Memish, Z. A. (2019). From the "Madding Crowd" to mass gatherings-religion, sport, culture and public health. *Travel Medicine and Infectious Disease*, *28*, 91–97. https://doi.org/10.1016/j.tmaid.2018.06.001

Alharbi, A. (2021). *A framework for controlling & managing traffic with modern technology*. https://openaccess.city.ac.uk/id/eprint/26510

Unpublished doctoral thesis - City University of London

Alraddady, S., Li, A. S., Soh, B., & Alzain, M. (2019). Deployment of Fog computing during Hajj season: A proposed framework. *Procedia Computer Science*, *161*, 1072–1079. https://doi.org/10.1016/j.procs.2019.11.218

Arab News. (2021, July 24). *Pilgrims do not need to test, isolate after Hajj*. https://www.arabnews.com/node/1899196/saudi-arabia

Bajaba, S., Mandurah, K., & Yamin, M. (2021). A framework for pandemic compliant higher education national system. *International Journal of Information Technology*, *13*(2), 407–414. https://doi.org/10.1007/s41870-021-00629-7

Bardesi, H., Al-Mashaikhi, A., Basahel, A., & Yamin, M. (2021). COVID-19 compliant and cost effective teaching model for King Abdulaziz University. *International Journal of Information Technology*, *13*(4), 1343–1356. https://doi.org/10.1007/s41870-021-00684-0

Baxter, D., Flinn, J., & Picco, L. F. (2018). Plan for the worst, hope for the best? Exploring major events related terrorism and future challenges for UK event professionals. *International Journal of Tourism Cities*, *4*(4), 513–526. https://doi.org/10.1108/ijtc-03-2018-0021

BBC. (2021a, July 8). [Euro 2020 Wembley crowd]. https://www.bbc.com/news/in-pictures-57743446

BBC. (2021b, July 8). [Euro 2020 Wembley crowd after match]. https://www.bbc.com/news/in-pictures-57743446

BBC News. (2017, June 4). *Turin stampede: "1,500 injured" at Juventus screening*. https://www.bbc.com/news/world-europe-40147813

BBC News. (2019, September 10). *Shia Muslim pilgrims mark Ashura in Iraq's Karbala*. https://www.bbc.com/news/av/world-middle-east-49653409

BI India Bureau. (2019, March 4). *Kumbh Mela: The world's largest religious gathering sets 3 world records*. Business Insider. https://www.businessinsider.in/kumbh-mela-2019-sets-3-guinness-world-record/articleshow/68250313.cms

Bullock, M., Ranse, J., & Hutton, A. (2018). Impact of patients presenting with alcohol and/or drug intoxication on in-event health care services at mass-gathering events: An integrative literature review. *Prehospital and Disaster Medicine*, *33*(5), 539–542. https://doi.org/10.1017/s1049023x1800078x

del Rio, C., Malani, P. N., & Omer, S. B. (2021). Confronting the Delta Variant of SARS-CoV-2, Summer 2021. *JAMA*, *326*(11), 1001. https://doi.org/10.1001/jama.2021.14811

di Giovine, M. A. (2020). Padre Pio, Pandemic Saint: The effects of the Spanish Flu and COVID-19 on pilgrimage and devotion to the world's most popular saint. *International Journal of Religious Tourism and Pilgrimage*, *8*(7), 129–154. https://doi.org/10.21427/9aw9-x346

Eladly, H. (2019). RIDR model for crowd management using RFID technology. *International Journal of Control Systems and Robotics*. Published.

https://www.iaras.org/iaras/home/caijcsr/ridr-model-for-crowd-management-using-rfid-technology

General Authority for Statistics KSA. (2020, November 18). *Hajj statistics*. General Authority for Statistics. https://www.stats.gov.sa/en/28

Hong, H. J. (2017). From Cloud computing to Fog computing: Unleash the power of Edge and End devices. *2017 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*. Published. https://doi.org/10.1109/cloudcom.2017.53

Jeong, T., Chung, J., Hong, J. W. K., & Ha, S. (2017, October). Towards a distributed computing framework for Fog. *2017 IEEE Fog World Congress (FWC)*. https://doi.org/10.1109/fwc.2017.8368528

Khanday, A. M. U. D., Khan, Q. R., & Rabani, S. T. (2020). Identifying propaganda from online social networks during COVID-19 using machine learning techniques. *International Journal of Information Technology*, *13*(1), 115–122. https://doi.org/10.1007/s41870-020-00550-5

Khanday, A. M. U. D., Rabani, S. T., Khan, Q. R., Rouf, N., & Mohi Ud Din, M. (2020). Machine learning based approaches for detecting COVID-19 using clinical text data. *International Journal of Information Technology*, *12*(3), 731–739. https://doi.org/10.1007/s41870-020-00495-9

Kingshott, B. F. (2014). Crowd management: Understanding attitudes and behaviors. *Journal of Applied Security Research*, *9*(3), 273–289. https://doi.org/10.1080/19361610.2014.913229

List of human stampedes and crushes. (2021, September 11). In *Wikipedia*. https://en.wikipedia.org/wiki/List_of_human_stampedes_and_crushes

List of human stampedes in Hindu temples. (2021, August 26). In *Wikipedia*. https://en.wikipedia.org/wiki/List_of_human_stampedes_in_Hindu_temples

Lombardo, P., Lim, A., Jones, A. A., Vigo, D., Honer, W. G., Duff, J., MacEwan, G. W., & Vila-Rodriguez, F. (2020). Impact of cannabis mass gathering events on mental health and health service utilization. *MedRxiv*. Published. https://doi.org/10.1101/2020.04.20.20073387

Mammana, G. M. (2016, March). *Sports-related riots: understanding group behavior to improve police strategy* (Thesis). http://hdl.handle.net/10945/48553

Miles, L., & Shipway, R. (2020). Exploring the COVID-19 pandemic as a catalyst for stimulating future research agendas for managing crises and disasters at

international sport events. *Event Management*, *24*(4), 537–552. https://doi.org/10.3727/152599519x15506259856688

Ministry of Hajj and Umrah. (n.d.). *Main*. Retrieved October 3, 2021, from https://www.haj.gov.sa/en

Nalbandian, A., Sehgal, K., Gupta, A., Madhavan, M. V., McGroder, C., Stevens, J. S., Cook, J. R., Nordvig, A. S., Shalev, D., Sehrawat, T. S., Ahluwalia, N., Bikdeli, B., Dietz, D., Der-Nigoghossian, C., Liyanage-Don, N., Rosner, G. F., Bernstein, E. J., Mohan, S., Beckley, A. A., . . . Wan, E. Y. (2021). Post-acute COVID-19 syndrome. *Nature Medicine*, *27*(4), 601–615. https://doi.org/10.1038/s41591-021-01283-z

Nasser, N., Anan, M., Awad, M. F. C., Bin-Abbas, H., & Karim, L. (2017). An expert crowd monitoring and management framework for Hajj. *2017 International Conference on Wireless Networks and Mobile Communications (WINCOM)*. Published. https://doi.org/10.1109/wincom.2017.8238202

O'Toole, W., Luke, S., Brown, J., Tatrai, A., & Semmens, T. (2019). *Crowd Management: Risk, Security and Health (Events Management and Methods)* (1st ed.). Goodfellow Pub Ltd.

Owaidah, A. A. (2015). *Hajj crowd management via a mobile augmented reality application: a case of The Hajj event, Saudi Arabia*. http://theses.gla.ac.uk/6330/

Doctoral dissertation: University of Glasgow

Owaidah, A., Olaru, D., Bennamoun, M., Sohel, F., & Khan, N. (2019). Review of modelling and simulating crowds at mass gathering events: Hajj as a case study. *Journal of Artificial Societies and Social Simulation*, *22*(2). https://doi.org/10.18564/jasss.3997

Planas, D., Veyer, D., Baidaliuk, A., Staropoli, I., Guivel-Benhassine, F., Rajah, M. M., Planchais, C., Porrot, F., Robillard, N., Puech, J., Prot, M., Gallais, F., Gantner, P., Velay, A., le Guen, J., Kassis-Chikhani, N., Edriss, D., Belec, L., Seve, A., . . . Schwartz, O. (2021). Reduced sensitivity of SARS-CoV-2 variant Delta to antibody neutralization. *Nature*, *596*(7871), 276–280. https://doi.org/10.1038/s41586-021-03777-9

Praveen, K. (2019). *Kumbh Mela crowd* [Image]. https://www.oneindia.com/photos/kumbh-mela-2019-57067.html

Press Trust of India. (2021a, April 15). *Crowding at Kumbh Mela* [Photo]. https://www.ndtv.com/india-news/over-1-700-test-covid-19-positive-at-haridwar-kumbh-over-5-days-official-2414270

Press Trust of India. (2021b, April 15). *Over 1,700 Test COVID-19 Positive At Haridwar Kumbh Over 5 Days: Official*. NDTV.Com. https://www.ndtv.com/india-news/over-1-700-test-covid-19-positive-at-haridwar-kumbh-over-5-days-official-2414270

Quadri, S. A., & Padala, P. R. (2021). An aspect of Kumbh Mela massive gathering and COVID-19. *Current Tropical Medicine Reports*, *8*(3), 225–230. https://doi.org/10.1007/s40475-021-00238-1

Rodriguez-Guerra, M., Jadhav, P., & Vittorio, T. J. (2021). Current treatment in COVID-19 disease: a rapid review. *Drugs in Context*, *10*, 1–8. https://doi.org/10.7573/dic.2020-10-3

Sanderson, K. (2021, August 19). *COVID vaccines protect against Delta, but their effectiveness wanes*. Nature. https://www.nature.com/articles/d41586-021-02261-8

Saudi Gazette. (2021, July 18). *WHO chief lauds Saudi Arabia's coronavirus measures during Hajj*. https://www.saudigazette.com.sa/article/608957/SAUDI-ARABIA/WHO-chief-lauds-Saudi-Arabias-coronavirus-measures-during-Hajj

Shambour, M. K., & Gutub, A. (2021). Progress of IoT research technologies and applications serving Hajj and Umrah. *Arabian Journal for Science and Engineering*. Published. https://doi.org/10.1007/s13369-021-05838-7

Shepard, S. (2016, March 3). *Euro 2016 security budget increased after Paris attacks*. Security Today. https://securitytoday.com/articles/2016/03/03/euro-2016-security-budget-increased-after-paris-attacks.aspx

Solís Arce, J. S., Warren, S. S., Meriggi, N. F., Scacco, A., McMurry, N., Voors, M., Syunyaev, G., Malik, A. A., Aboutajdine, S., Adeojo, O., Anigo, D., Armand, A., Asad, S., Atyera, M., Augsburg, B., Awasthi, M., Ayesiga, G. E., Bancalari, A., Björkman Nyqvist, M., . . . Omer, S. B. (2021). COVID-19 vaccine

acceptance and hesitancy in low- and middle-income countries. *Nature Medicine*, *27*(8), 1385–1394. https://doi.org/10.1038/s41591-021-01454-y

Soman, A., & Jacob, S. (2018). An Efficient and Decisive Crowd Management System Based On RFID Technology. *IJARIIT*, *4*(2), 443–446. https://www.ijariit.com/manuscript/an-efficient-and-decisive-crowd-management-system-based-on-rfid-technology/

Spaaij, R. (2016). Terrorism and security at the Olympics: Empirical trends and evolving research agendas. *The International Journal of the History of Sport*, *33*(4), 451–468. https://doi.org/10.1080/09523367.2015.1136290

Spaaij, R., & Hamm, M. S. (2015). Endgame? Sports events as symbolic targets in lone wolf terrorism. *Studies in Conflict & Terrorism*, *38*(12), 1022–1037. https://doi.org/10.1080/1057610x.2015.1076695

Ullah, A., Yaqoob, S., Imran, M., & Ning, H. (2019). Emergency message dissemination schemes based on congestion avoidance in VANET and Vehicular FoG Computing. *IEEE Access*, *7*, 1570–1585. https://doi.org/10.1109/access.2018.2887075

Verma, M., & Sarangi, P. (2019). Modeling attributes of religious tourism: A study of Kumbh Mela, India. *Journal of Convention & Event Tourism*, *20*(4), 296–324. https://doi.org/10.1080/15470148.2019.1652124

Wahid, A. (2018). *Kaaba* [Image]. Kaaba Crowd. https://unsplash.com/photos/cAQXApsh490

Word Health Organization. (2021). *Advice for the public*. WHO. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public

World Health Organization. (2020, March 12). *WHO announces COVID-19 outbreak a pandemic*. https://www.euro.who.int/en/health-topics/health-emergencies/coronavirus-covid-19/news/news/2020/3/who-announces-covid-19-outbreak-a-pandemic

Worldometer. (2021, October 3). *COVID Live Update: 235,489,356 Cases and 4,813,176 Deaths from the Coronavirus - Worldometer*. https://www.worldometers.info/coronavirus/?utm_campaign=homeAdvegas1

Yadav, R. S. (2020). Data analysis of COVID-2019 epidemic using machine learning methods: A case study of India. *International Journal of Information Technology*, *12*(4), 1321–1330. https://doi.org/10.1007/s41870-020-00484-y

Yamin, M. (2018). Managing crowds with technology: Cases of Hajj and Kumbh Mela. *International Journal of Information Technology*, *11*(2), 229–237. https://doi.org/10.1007/s41870-018-0266-1

Yamin, M. (2020). Counting the cost of COVID-19. *International Journal of Information Technology*, *12*(2), 311–317. https://doi.org/10.1007/s41870-020-00466-0

Yamin, M., Abi Sen, A. A., AlKubaisy, Z. M., & Almarzouki, R. (2021). A novel technique for early detection of COVID-19. *Computers, Materials & Continua*, *68*(2), 2283–2298. https://doi.org/10.32604/cmc.2021.017433

Yamin, M., & Ades, Y. (2009). Crowd management with RFID and wireless technologies. In IEEE (Ed.), *2009 First International Conference on Networks & Communications* (pp. 439–442). IEEE. https://doi.org/10.1109/netcom.2009.14

Yamin, M., Basahel, A. M., & Abi Sen, A. A. (2018). Managing crowds with wireless and mobile technologies. *Wireless Communications and Mobile Computing*, *2018*, 1–15. https://doi.org/10.1155/2018/7361597

Yu, Q., Hu, L., Alzahrani, B., Baranawi, A., Alhindi, A., & Chen, M. (2021). Intelligent visual-IoT-enabled real-time 3D visualization for autonomous crowd management. *IEEE Wireless Communications*, *28*(4), 34–41. https://doi.org/10.1109/mwc.021.2000497

Appendices

Appendix A

List of Published articles

Related to thesis

Almutairi, M. M., Apostolopoulou, D., Stupples, D., Sen, A. A. A., Yamin, M., & Halikias, G. (2023). A Double Protecting Approach for Data Privacy. In 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 360-366). New Delhi, India.

Almutairi, M. M., Apostolopoulou, D., Halikias, G., Sen, A. A. A., & Yamin, M. (2022). Enhancing Privacy and Security in Crowds using Fog Computing. In 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 57-62). New Delhi, India. doi: 10.23919/INDIACom54597.2022.9763199.

Almutairi, M. M., Apostolopoulou, D., Halikias, G., Sen, A. A. A., & Yamin, M. (2022). A Framework for Comprehensive Crowd and Hajj Management. In 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 63-68). New Delhi, India. doi: 10.23919/INDIACom54597.2022.9763174.

Almutairi, M. M., Sen, A. A. A., & Yamin, M. (2021). Survey of PIR Approach and its Techniques for Preserving Privacy in IoT. In 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 417-421). New Delhi, India.

Almutairi, M. M., Halikias, G., & Yamin, M. (2020). An Overview of Security Management in Saudi Arabia. In 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 261-265). New Delhi, India. doi: 10.23919/INDIACom49435.2020.9083725.

Almutairi, M. M., & Halikias, G. (2019). Identification and Management of Growing Security Threats towards KSA. In 2019 6th International Conference on

Computing for Sustainable Global Development (INDIACom) (pp. 1315-1321). New Delhi, India.

Almutairi, M. M., Yamin, M., Halikias, G., & Sen, A. A. A. (2022). A Framework for Crowd Management during COVID-19 with Artificial Intelligence. Sustainability, 14(1), 303. https://doi.org/10.3390/su14010303

A Smart Framework to control Crowd Flow based AI (Hajj Event) - (Communicated)

DOUBLE CANCELABLE HASHING FOR PROTECTING BIOMETRICS OF USERS IN CROWD - (Communicated)

HEALTH MANAGEMENT IN CROWDS - (Communicated)

WASTE MANAGEMENT IN CROWDS - (Communicated)

Existing

Almutairi, M. M., Yamin, M., & Halikias, G. (2021). An analysis of data integration challenges from heterogeneous databases. *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)*. https://doi.org/10.1109/INDIACom51348.2021.00061

Almutairi, M. M., Abi Sen, A. A., & Yamin, M. (2021). Survey of PIR approach and its techniques for preserving privacy in IoT. 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), 417–421. https://doi.org/10.1109/INDIACom51348.2021.00074

Almutairi, M. M., Halikias, G., & Yamin, M. (2020, March). An overview of security management in Saudi Arabia. *2020 7th International Conference on Computing for Sustainable Global Development (INDIACom)*, 352–356. https://doi.org/10.23919/indiacom49435.2020.9083725

Almutairi, M. M. (2020a). A review of cloud computing in education in Saudi Arabia. *International Journal of Information Technology*, *12*(4), 1385–1391. https://doi.org/10.1007/s41870-020-00452-6

Almutairi, M. M. (2020b). Role of Big Data in education in KSA. *International Journal of Information Technology*, *13*(1), 367–373. https://doi.org/10.1007/s41870-020-00489-7

Almutairi, M. M., & Halikias, G. (2019). Identification and management of growing security threats towards KSA. *2019 6th International Conference on Computing for Sustainable Global Development*, 1315–1321.

Almutairi, M, M, Yamin, M, Halikias, G, & Sen, A, A, A. (2021). A framework for crowd management during COVID-19 with artificial intelligence. *Sustainability, 14*(1), p. 303. doi: 10.3390/su14010303.

Hassanein, H., Zorba, N., Han, S., Kanhere, S. S., & Shukair, M. (2019). Crowd management. *IEEE Communications Magazine*, *57*(4), 18-19 doi: 10.1109/mcom.2019.8703458.

Sharma, D, Bhondekar, A, P, Shukla, A, K, & Ghanshyan, C. (2016). A review on technological advancements in crowd management. *Journal of Ambient Intelligence and Humanized Computing, 9*(3), 485-495. doi: 10.1007/s12652-016-0432-x.

Wijermans, N, Conrado, C, van Steen, M, Martella, C, & Li, J. (2016). A landscape of crowd-management support: An integrative approach. *Safety Science, 86,* pp. 142-164. doi: 10.1016/ j.ssci.2016.02.027.

Yamin, M. (2015). Health management in crowded events: Hajj and Kumbh. *BVICA M's International Journal of Information Technology, 7.*

Albouq, S, S, Sen, A, A, A, Namoun, A, Bahbouh, N, M, Alkhodre, A, B, & Alshanqiti, A. (2020). A double obfuscation approach for protecting the privacy of IoT location based applications. *IEEE Access, 8,* pp. 129415-129431.

Alsaawy, Y, Alkhodre, A, B, Sen, A, A, A, & Shoaib, M. (2019). Swap obfuscation technique for preserving privacy of LBS. *International Journal of Academic Scientific Research, 7*(2), pp. 11-19.

Alsaawy, Y, Alkhodre, A, Eassa, F, A, & Sen, A, A, A. (2019). Triple cache approach for preserving privacy and enhancing performance of LBS. In Proc. of the 6th *IEEE International Conference on Computing for Sustainable Global Development (INDIACom),* pp. 1277-1281.

Angel, S, Chen, H, Laine, K, & Setty, S. (2021). PIR with compressed queries and amortized query processing. In Proc. of the *IEEE Symposium on Security and Privacy (SP),* pp. 962-979.

Basahel, A, M, Sen, A, A, A, Yamin, M, & Alqahtani, S. (2019). Bartering method for improving privacy of LBS. *International Journal of Computer Science and Network Security, 19*(2), pp. 207-213.

Chen, L, Thombre, S, Jarvinen, K, Lohan, E, S, Alen-Savikko, A, Leppakoski, H, & Lindqvist, J. (2017). Robustness, security and privacy in location-based services for future IoT: A survey. *IEEE Access,* 5, pp. 8956-8977.

da Cruz, M, A, Rodrigues, J, J, Sangaiah, A, K, Al-Muhtadi, J, Korotaev, V. (2018). Performance evaluation of IoT middleware. *Journal of Network and Computer Applications, 109,* pp. 53-65.

Ernvall, A, M, & Nyberg, K. (2003). On server-minded computation for RSA protocols with private key splitting. In Proc. of *Nordsec.*

Fung, E, Kellaris, G, & Papadias, D. (2015). Combining differential privacy and PIR for efficient strong location privacy. In Proc. of the *International Symposium on Spatial and Temporal Databases,* pp. 295-312.

Gertner, Y, Ishai, Y, Kushilevitz, E, & Malkin, T. (2000). Protecting data privacy in private information retrieval schemes. *Journal of Computer and System Sciences, 60*(3), pp. 592-629.

Ghinita, G, Kalnis, P, Khoshgozaran, A, Shahabi, C, & Tan, K, L. (2008). Private queries in location based services: Anonymizers are not necessary. In Proc. of the *ACM SIGMOD International Conference on Management of Data,* pp. 121-132.

Grissa, M, Yavuz, A, A, & Hamdaoui, B. (2017). When the hammer meets the nail: Multi-server pir for database-driven crn with location privacy assurance. In Proc. of the *IEEE Conference on Communications and Network Security (CNS),* pp. 1-9.

Huang, H, Gartner, G, Krisp, J, M, Raubal, M, & Weghe, N, V,D. (2018). Location based services: Ongoing evolution and research agenda. *Journal of Location Based Services, 12*(2), pp. 63-93.

Khan, R, Ahmad, A, Alsayed, A, O, Binsawad, M, Islam, M, A, & Ullah, M. (2020). QuPiD attack: Machine learning-based privacy quantification mechanism for PIR protocols in health-related web search. *Scientific Programming.*

Mostafavi, S, & Shafik, W. (2019). For computing architectures, privacy and security solutions. *Journal of Communications Technology, Electronics and Computer Science, 24,* pp. 1-14.

Qian, Z, H, & Wang, Y.J. (2012). IoT technology and application. *Acta Electronica Sinica, 40*(5), pp. 1023-1029.

Sen, A, A, A, & Basahel, A, M. (2019). A comparative study between security and privacy. In Proc. of the *6th IEEE International Conference on Computing for Sustainable Global Development (INDIACom),* pp. 1282-1286.

Sen, A, A, A, & Yamin, M. (2020). Advantages of using for in IoT applications. *International Journal of Information Technology.*

Sen, A, A, A, Eassa, F, A, & Jambi, K. (2017). Preserving privacy of smart cities based on the fog computing. In Proc. of the *International Conference on Smart Cities, Infrastructure, Technologies and Applications,* pp. 185-191.

Sen, A. A. A., Eassa, F. A., Jambi, K., & Yamin, M. (2018). Preserving privacy in internet of things - A survey. *International Journal of Information Technology, 10* (2)., https://doi.org/10.1007/s41870-018-0113-4.

Sen, A, A, A, Eassa, F, A, Jambi, K, Bahbouh, N, M, Albouq, S, S, & Alshanqiti, A. (2017). Enhanced-blind approach for privacy protection of IoT. In Proc of the 7th *IEEE International Conference on Computing for Sustainable Global Development (INDIACom),* pp. 240-243.

Sen, A, A, A, Eassa, F, Yamin, M, & Jambi, K. (2018). Double cache approach with wireless technology for preserving user privacy. *Wireless Communications and Mobile Computing, 2018,* pp. 1-11. doi: 10.1155/2018/4607464.

Ullah, I, Boreli, R, & Kanhere, S, S. (2020). Privacy in targeted advertising: A survey. *arXiv preprint arXiv:2009*.06861,

Yamin, M, & Sen, A, A, A. (2018). Improving privacy and security of user data in location based services. *International Journal of Ambient Computing and Intelligence, 9*(1), pp. 19-42. doi:10.4018/ijaci.2018010102.

Yamin, M, & Sen, A, A, A. (2020). A new method with swapping of peers and fogs to protect user privacy in IoT applications. *IEEE Access, 8,* pp. 210206-210224. doi: 10.1109/ACCESS.2020.3038825.

Zhang, Z, Wang, K, Lin, W, Fu,, A, W, C, & Wong, R, C, W. (2019). Practical access pattern privacy by combining pir and oblivious shuffle. In Proc. of the 28th *ACM International Conference on Information and Knowledge Management,* pp. 1331-1340.

Zhao, F, Hori, Y, & Sakurai, K. (2007). Two-servers PIR based DNS query scheme with privacy-preserving. In Proc. of the *IEEE International Conference on Intelligent Pervasive Computing (IPC2007),* pp. 299-302.

Zhao, J, C, Zhang, J, F, Feng, Y, & Guo, J, X. (2010). The study and application of the IoT technology in agriculture. In Proc. of the 3rd *IEEE International Conference on Computer Science and Information Technology,* pp. 462-465.

Abi Sen, A. A., Alawfi, I. M. M., Aloufi, H. F., Bahbouh, N. M., & Alsaawy, Y. (2021). Comparison among Cooperation, Anonymity and Cloak Area approaches for Preserving Privacy of IoT. In 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 413-416). New Delhi, India.

Altamimi, B, A. (2021). Fog Mix-Zone Approach for Preserving Privacy

Area approaches for Preserving Privacy of IoT. *2021 8th*

Based Schema for Location Privacy Preservation. in *IEEE Transactions on Sustainable Computing, 4*(2), pp. 156-167. doi: 10.1109/TSUSC.2017.2733018.

Butun, I, Österberg, P, & Gidlund, M. (2019). Preserving Location Privacy Chanal, P, & Kakkasageri, M. (2020). Security and privacy in IoT: A survey. *Wireless Personal Communications, 115*(2), pp. 1667-1693.doi: 10.1007/s11277-020-07649-9.

Chetty, G, Yamin, M, & White, M. (2022). A low resource 3D U-Net based deep learning model for medical image analysis. *International Journal of Information Technology.* doi: 10.1007/s41870-021-00850-4.

Communications and Network Security (CNS), pp. 1-6, doi:

Communications. pp. 439-442, doi: 10.1109/NetCoM.2009.14

Development(INDIACom), pp. 413-416, doi: 10.1109/INDIACom51348.2021.00073.

doi: 10.1109/INDIACom51348.2021.00071.

Goddard, M. (2017). The EU general data protection regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research, 59*(6), pp. 703-705. doi:10.2501/IJMR-2017-050.

in Cyber-Physical Systems. *2019 IEEE Conference on*

in IoT. *2021 8th International Conference on Computing for*

International Conference on Computing for Sustainable Global

IoT. *2020 7th International Conference on Computing for Sustainable*

Ludwig, T, Reuter, C, Siebigteroth, T, & Pipek, V. (2015). Crowdmonitor. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems.* doi: 10.1145/2702123.2702265.

Mendez, M, Papapanagiotou, I, & Yang, B. (2018). Internet of things: Survey on security. *Information Security Journal: A global perspective, 27*(3), pp. 162-182. doi: 10.1080/19393555.2018.1458258.

Mohamed, M, Shabayek, A, & El-Gayyar, M. (2018). IoT-Based framework for crowd management. *Mobile Solutions and their Usefulness in Everyday Life,* pp. 47-61. doi.org/10.1007/978-3-319-93491-4_3.

Rahman, A, Hassanain, E, & Hossain, M, S. (2017). Towards a secure mobile edge computing framework for Hajj. *IEEE Access, 5,* pp. 11768-11781. doi: 10.1109/ACCESS.2017.2716782.

Santana, J, R, Sanchez, L, Sotres, P, Lanza, J, Llorente, T, & Munoz, L. (2020). A privacy-aware crowd management system for smart cities and smart buildings. *IEEE Access, 8,* pp. 135394-135405. doi: 10.1109/ACCESS.2020.3010609.

Sen, A, A, A, & Yamin, M. (2020). Advantages of using fog in IoT applications. *International Journal of Information Technology, 13*(3), pp. 829-837. doi: 10.1007/s41870-020-00514-9.

Shady, M, Usman, M, Abesen, A, & Arif, S. (2017). AES-route server model for location based services in road networks. *International Journal of Advanced Computer Science and Applications, 8*(8). doi: 10.14569/ijacsa.2017.080847.

Sustainable Global Development (INDIACom), pp. 405-408,

Technologies. *2009 First International Conference on Networks &*

Yamin, M, Alsaawy, Y, Alkhodre, A, B, & Abi Sen, A. (2019). An innovative method for preserving privacy in internet of things. *Sensors, 19*(15), p. 3355. doi: 10.3390/s19153355

Yang, Y, Wu, L, Yin, G, Li, L, & Zhao, H. (2017). A survey on security and privacy issues in internet of things. *IEEE Internet of Things Journal, 4*(5), pp. 1250-1258. doi: 10.1109/JIOT.2017.2694844.

Yola, G. et al. (2019). Location privacy in the wake of the GDPR. *ISPRS International Journal of Geo-information, 8*(3), p. 157. doi: 10.3390/ijgi8030157.

Al-Balasmeh, H, Singh, M, & Singh, R. (2021). Framework of data privacy preservation and location obfuscation in Vehicular Cloud Networks. *Concurrency and Computation: Practice and Experience, 34*(5).

Alkhalil, Z, Hewage, C, Nawaf, L, & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3.*

Allen, S. (2015). Remembering and forgetting-protecting privacy rights in the digital age. *European Data Protection Law Review, 1*(3), pp. 164-177.

Al-Shaery, A, M, Alshehri, S, S, Farooqi, N, S, & Khozium, M, O. (2020). In-depth survey to detect, monitor and manage crowd. *IEEE Access, 8,* pp. 209008–209019.

Daniel, A, & Momoh, M, O. (2021). A computer security system for cloud computing based on encryption technique. *Computer Engineering and Applications Journal, 10*(1), pp. 41–54.

Edwards, L. (2016). Privacy, security and data protection in smart cities: A critical EU law perspective. *SSRN Electronic Journal.*

Felemban, E, A, Rehman, F, U, Biabani, S, A, Ahmad, A, Naseer, A, Majid, A, R, Hussain, O, K, Qamar, A, M, Falemban, R, & Zanjir, F. (2020). Digital Revolution for hajj crowd management: A technology survey. *IEEE Access, 8,* pp. 208583–208609.

Haoxiang, W, & S, S. (2021). Big data analysis and perturbation using datamining algorithm. *March 2021*, *3*(1), pp. 19–28.

Jakimoski, K. (2016). Security techniques for data protection in cloud computing. *International Journal of Grid and Distributed Computing, 9*(1), pp. 49-56.

Kaur, G, & Gupta, R. (2021). A study on location based services and TTP based privacy preserving techniques. *2021 International Conference on Advances in Computing and Communications* (ICACC).

Khodaei, M, & Papadimitratos, M. (2021). Cooperative location privacy in Vehicular Networks: Why simple mix zones are not enough. *IEEE Internet of Things Journal, 8*(10), pp. 7985–8004.

Khosravi, M, & Fereidunian, A. (2019). Enhancing smart grid cybersecurity using a fuzzy adaptive autonomy expert system. *Smart Grid Conference (SGC).*

Lee, C., & Ahmed, G. (2021). Improving IOT privacy, data protection and security concerns. *International Journal of Technology, Innovation and Management (IJTIM)*, *1*(1), 18–33. https://doi.org/10.54489/ijtim.v1i1.12

Saeed, M, M, Hasan, K, Obaid, A, Saeed, R, A, Mokhtar, R, A, Ali, E, S, Akhtaruzzaman, M, Amanlou, S, & Hossain, A, K. (2022). A comprehensive

review on the users' identity privacy for 5G networks. *IET Communications*, *16*(5), pp. 384–399.

Sirur, S, Nurse, J, R, C, & Webb, H. (2018). Are we there yet? *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security.*

Sloot, B & Zuiderveen Borgesius, F. (2018). The EU general data protection regulation: A new global standard for information privacy. *SSRN Electronic Journal.*

Soomro, Z, A, Shah, M, H, & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2), pp. 215-225.

Wu, Z, Li, G, Shen, S, Lian, X, Chen, E, & Xu, G. (2020). Constructing dummy query sequences to protect location privacy and query privacy in location-based services. *World Wide Web, 24*(1), pp. 25-49.

Zakhary, S, Radenkovic, M, & Benslimane, A. (2013). The quest for location-privacy in opportunistic mobile social networks. *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC).*

Kanade, S., Petrovska-Delacrétaz, D., & Dorizzi, B. (2009). Multi-biometrics based cryptographic key regeneration scheme. In 2009 IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems (pp. 1-7). Washington, DC, USA. doi: 10.1109/BTAS.2009.5339034.

Alessandra, L, & Loris, N. (2007). An improved BioHashing for human authentication. *Journal of Pattern Recognition Society, 40*, pp.1057–1065,

Basahel, A, Alsabban, A, & Yamin, M. (2021). Hajj and Umrah management during COVID-19. *International Journal of Information Technology.* https://doi.org/10.1007/s41870-021-00812-w.

Bolle, M, Connel, H, & Ratha, K. (2002). Biometrics perils and patches. *Pattern Recognition, 35*(12), pp. 2727-2738.

Hao, F., Anderson, R., & Daugman, J. (2006). Combining Cryptography with Biometrics Effectively. *IEEE Transactions on Computers 55*(9) (2006) 1081–1088.

Johnson, W, & Lindenstrauss, J. (1984). Extensions of lipschitz maps into a hilbert space. *In Contemporary Mathematics,* pp. 189-206.

Kanade, S, Camara, D, Petrovska-Delacrtaz, D, & Dorizzi, D. (2009). Application of biometrics to obtain high entropy cryptographic keys. in Proceedings of the *2009 World Academy on Science, Engineering, and Technology,* Hong Kong.

Malallah, F, Mumtazah, S, Adnan, W, & Yussof, S. (2014). Non-invertible online signature biometric template protection via shuffling and trigonometry transformation. *International Journal of Computer Applications, 98*(4).

Pillai, K, Patel, M, Rama, C, & Ratha, K. (2010). Sectored random projections for cancellable IRIS biometrics. In proceeding of the *2010 IEEE Symposium on Acoustics, Speech and Signal Processing,* New York.

Rathgeb, C, Breitinger, F, Busch, C, & Baier, H. (2014). On the application of bloom filters to iris biometrics. *IET Journal on Biometrics, 3*(4), pp. 207-218.

Sanjay, K, PetrovaskaDelacretaz, D, & Bernadette, D. (2009). Cancelable IRIS biometrics and using error correcting codes to reduce variability in biometric data. *IEEE Conference on Computer Vision and Pattern Recognition,* USA.

Tajti, T. (2020). New voting functions for neural network algorithms. In Annales Mathematicae et Informaticae: Vol. Accepted manuscript. Annales Mathematicae et Informaticae - AMI. https://doi.org/10.33039/ami.2020.10.003

Ahmad, I., & Shin, S. (2022). Perceptual encryption-based privacy-preserving deep learning in internet of things applications. 2022 13th International Conference on Information and Communication Technology Convergence (ICTC). https://doi.org/10.1109/ictc55196.2022.9952589

Sosunova, I., & Porras, J. (2022). IoT-Enabled Smart Waste Management Systems for Smart Cities: A Systematic Review. *IEEE Access, 10*, [Pagination]. https://doi.org/10.1109/ACCESS.2022.3188308

Alshalani, H. J., Alnaghaimshi, N. I., & Eljack, S. M. (2020). ICT system for crowd management: Hajj as a case study. 2020 International Conference on Computing and Information Technology, University of Tabuk, Kingdom of Saudi Arabia, 11-15. https://ieeexplore.ieee.org/document/123456789

Onoda, H. (2020). Smart approaches to waste management for post-COVID-19 smart cities in Japan. IET Smart Cities, 2(2), 89-94. https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-smc.2020.0051

Fedele, L., & Merenda, M. (2020). An IoT-based smart city framework with real-time crowd management for safe reopening post COVID-19 lockdown. Algorithms, 13(10), 254. https://doi.org/10.3390/a13100254

Abdulrazaq, M. N., Alshekhly, M. N., Al-Zubaidi, S. S., Karim, S. A., Syamsudin, H., & Ramli, R. (2020). Novel COVID-19 detection and diagnosis system using IOT based smart helmet. International Journal of Psychosocial Rehabilitation, 24(7). https://doi.org/10.37200/IJPR/V24I7/PR270221

Pouw, C. A. S., Toschi, F., van Schadewijk, F., & Corbetta, A. (2020). Monitoring physical distancing for crowd management: Real-time trajectory and group analysis. PLoS ONE, 15(10): e0240963. https://doi.org/10.1371/journal.pone.0240963

Shambour, M. K. Y., & Gutub, A. A. (2021). Smart Umrah System Utilizing IoT Technologies to Serve Pilgrims and Facilitate Performing Umrah. Arabian Journal for Science and Engineering, 46, 10335–10349. https://doi.org/10.1007/s13369-021-05838-7

Pister, K. S. J., Kahn, J. M., & Boser, B. E. (1999). Smart dust: Wireless networks of millimeter-scale sensor nodes. Electronics Research Laboratory Research Summary, 39(4), 20-29.

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. IEEE Communications Magazine, 40(8), 102-114. https://doi.org/10.1109/MCOM.2002.1024422

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25(6), 599-616. https://doi.org/10.1016/j.future.2008.12.001

Kim, D., Ramos, C., & Mohammed, S. (2006). The Internet of Things: From RFID to the next-generation pervasive networked systems. Proceedings of the 3rd International Conference on Grid and Pervasive Computing Workshops, 53-62. https://doi.org/10.1007/11752834_5

Friedman, R. (2012). Crowd control at the London Olympics: A mathematical perspective. Mathematics Today, 48(2), 64-69.

Georgoudas, I., Papageorgiou, M., & Haj-Salem, H. (2012). Hybrid modeling of pedestrian crowd dynamics in public events. Journal of Transportation Research, 36(4), 419-434.

Helbing, D., & Molnár, P. (1995). Social force model for pedestrian dynamics. Physical Review E, 51(5), 4282–4286.

Helbing, D., Farkas, I. J., & Vicsek, T. (2011). Simulating crowd disasters using the social force model. Nature Physics, 6(5), 368-372.

Hughes, R. L. (2002). A continuum theory for the flow of pedestrians. Transportation Research Part B: Methodological, 36(6), 507-535.

Kretz, T., Grünebohm, A., & Schreckenberg, M. (2008). Experimental study of pedestrian flow through a bottleneck. Journal of Statistical Mechanics: Theory and Experiment, 2008(10), P10014.

Moussaïd, M., Helbing, D., & Theraulaz, G. (2011). How simple rules determine pedestrian behavior and crowd disasters. Proceedings of the National Academy of Sciences, 108(17), 6884-6888.

Takizawa, K., Tomita, T., & Yoshida, S. (2018). Mesoscopic modeling of pedestrian flow at Shibuya crossing using cellular automata. Transportation Science, 52(3), 672-685.

Zhou, M., Chen, Z., & Wang, X. (2019). Macroscopic modeling of pedestrian dynamics in railway stations. Journal of Transportation Engineering, 145(6),

Chang, S. H., & Chen, Z. R. (2016). Protecting mobile crowd sensing against Sybil attacks using cloud-based trust management system. Mobile Information Systems, Article ID 6506341. https://doi.org/10.1155/2016/6506341

Cusack, B., & Tian, Z. (2017). Evaluating IP surveillance camera vulnerabilities. In 15th Australian Information Security Management Conference (pp. 25-32). https://doi.org/10.4225/75/57a6fd111905e

Dastjerdi, A. V., Gupta, H., Calheiros, R. N., Ghosh, S. K., & Buyya, R. (2016). Fog computing: Principles, architectures, and applications. Internet of Things Journal, Article ID 7361597. https://doi.org/10.1109/JIOT.2016.2684354

Fujdiak, R., Mlynek, P., Misurec, J., & Slacik, J. (2017). Simulation of intelligent public light system in smart city. Progress in Electromagnetics Research Symposium-Spring, 2515-2519. https://doi.org/10.1109/PIERS.2017.7960298

Guan, K., Shao, M., & Wu, S. (2017). A remote health monitoring system for the elderly based on smart home gateway. Journal of Healthcare Engineering, Article ID 5843504. https://doi.org/10.1155/2017/5843504

Mach, P., & Becvar, Z. (2017). Mobile edge computing: A survey on architecture and computation offloading. IEEE Communications Surveys & Tutorials, 19(3), 1628-1656. https://doi.org/10.1109/COMST.2017.2682318

Rajaraman, V. (2017). Radio frequency identification. Resonance (Indian Academy of Sciences), 22(6), 549-575. https://doi.org/10.1007/s12045-017-0522-0

Sun, P., Wang, X., & Xie, W. (2018). Centrifugal blower of stratospheric airship. IEEE Access, 6, 10520-10529. https://doi.org/10.1109/ACCESS.2018.2817558

Vattapparamban, E., Güvenç, I., Yurekli, A. I., Akkaya, K., & Uluagac, S. (2016). Drones for smart cities: Issues in cybersecurity, privacy, and public safety. In 12th International Wireless Communications and Mobile Computing Conference (pp. 216-221). https://doi.org/10.1109/IWCMC.2016.757706004019020.