Short Abstract (25-30 words):

Long Abstract (120 words):

Commented [SF(1]: This is a peculiarity of what the journal will ask for.

The Internet of Things (IoT) is prevalent within smart homes. However, the security of such devices is often considered a limitation and user authentication relies on approaches that have considerable weaknesses and impracticalities. Continuous authentication has been considered a promising form of authentication for the future, shown to accurately collect and authenticate a continuous stream of biometric user data from user devices (e.g. smartphones). However, its application within IoT is currently in its infancy, and the limitations of sensors, power and processing capabilities present challenges when compared to traditional user devices. This article examines how the functionalities of multiple IoT devices may be utilised in a federated architecture such that the different capabilities of each device can be intelligently combined to authenticate users in real-time.

Continuous Authentication for IoT Smart Home Environments

Max Smith-Creasey, Security & Cyber Defence, Applied Research, BT plc, Adastral Park, UK. max.smith-creasey@bt.com
Steven Furnell, School of Computer Science, University of Nottingham, Nottingham, UK. steven.furnell@nottingham.ac.uk
Muttukrishnan Rajarajan, Information Security Group, City, University of London, London, UK. r.muttukrishnan@city.ac.uk

The Internet of Things (IoT) has expanded rapidly in recent years. The total number of active IoT device connections are set to overtake non-IoT devices and reach 30 billion by 2025 [1]. Today, these devices are abundant within the smart home environment. However, the purpose of each IoT device is often vastly different, each sensing and processing to fulfil a particular task. For example, some IoT devices are in operation for surveillance purposes and utilise a camera feed, others monitor the environment to control lighting or temperature, and others may be wearables that are worn by a user and collect heart rate and movement information. The diversity of devices means that they are constructed with specific sensing and processing technologies that they require to perform the task they were designed for. These devices will often have the capability to store or provide access to private information about the user or their environment. This is a data privacy concern that might lead to impostors gaining access to private data [2]. However, due to the breadth and variety of devices there is no standard way of authenticating a user [3]. Furthermore, around 80% of IoT devices fail to implement passwords securely [2]. In fact, lack of robust authentication is one on the key IoT security vulnerabilities [4]. This creates a clear risk that of unauthorised user access.

Unfortunately, traditional authentication techniques cannot be implemented effectively on most IoT devices because they lack conventional user interfaces through which the username and password might be implemented [3]. Furthermore, studies consistently show that such knowledge-based authentication mechanisms are not utilised securely by users and commonly found to be inconvenient. Tokens are also not generally suitable for user authentication in the IoT space because they generally require close physical contact to the device (e.g. for NFC-based tokens) which cannot be guaranteed to be viable in all cases. The use of common biometrics such as faces and fingerprints also has limitations because not all IoT devices

would have the sensors required, and processing may be intensive for an IoT device (especially for face recognition).

One approach to user authentication that has gained traction within the last decade is *continuous authentication* (CA). This concept constructs user profiles based on continuously collected biometrics from devices. Subsequent biometric samples from the device can be used to authenticate the device user beyond the point of entry. However, there are several key differences between devices on which continuous authentication may be applied (e.g. laptops and smartphones) and IoT devices within the smart home. First, there is a substantial difference in sensing, processing and power capabilities; these are often more limited in the context of IoT [5]. Secondly, many CA systems authenticate users during physical device interaction (such as keystrokes or touchscreen gestures), but it is not always the case in IoT that the user will be physically close to the device (e.g. a smart speaker) or explicitly interact with it (e.g. a temperature sensor). Finally, a smart home may be expected to have many IoT devices containing a variety of different sensors each.

There are relatively few studies proposing CA frameworks for IoT devices in the smart home. Those that do offer solutions are limited in the approaches they take, focusing on one type of IoT device or on one type of biometric, and so the challenges remain [5]. In this discussion we propose an intelligent CA solution for IoT devices based on multi-modal biometrics obtained from multiple IoT devices.

The anatomy of a smart home

There may be a number of different IoT devices within the smart home. Utilising built-in sensors they can fulfil a plethora of purposes including safety, power efficiency and comfort, health and well-being, and help for the elderly or disabled [4]. However, unlike other devices (such as laptops) IoT devices are hugely variable and not often alike; the smart speaker is vastly different to the smart light can comes with a different sensors, interfaces and capabilities. Some of the IoT devices within the smart home may be portable (such as wearable devices) whereas others might stay relatively static within the smart home (such as smart fridges). It might also be the case that some devices require authentication (or at least a level of authentication) to provide functionality, when others do not. Some devices will also have greater sensing capabilities than others and might be able to collect considerable biometric modalities, whereas other devices may not collect any meaningful biometrics. Figure 1 shows some devices that might be found within a smart home.

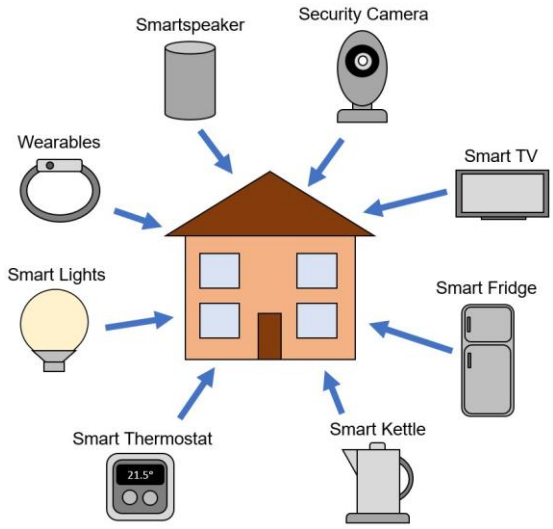

Figure 1. Illustrating the range of IoT devices in a smart home

The IoT devices that may be found within a smart home have sensors from which biometrics can be collected. Some indicative options include the following, and Table 1 indicates how these are often associated with particular forms of IoT device:

- **Microphone**: This can most commonly be found in smart entertainment systems (e.g. speakers and televisions).
- **Camera**: The camera sensor collects images or videos, often in RGB. The quality of the capture may be effected by the camera resolution. Cameras are commonly found in smart home security/monitoring systems.
- **Accelerometer**: The accelerometer sensor measures acceleration in the *x*, *y* and *z* axis. These sensors are common in devices that detect movement, such as wearables.
- **Touchscreen**: The touchscreen can sense touch-gesture based information such as swipe behaviour. This sensor is usually found on devices that might have a touchscreen interface (such as a home management panel).
- **Temperature**: The temperature sensor can detect the current temperature and is commonly found in smart home thermostats that report the temperature.
- **Ambient Lighting**: These sensors detect illumination levels in the environment. They can be found in IoT devices related to smart home lighting systems.
- **Passive Infrared (PIR)**: Measures infrared light radiating from objects. It can detect movement but not images (which would require an imaging IR sensor). These sensors are usually found in security systems.

	Sensors						
IoT Device	Microphone	Camera	Accelerometer	Touchscreen	Temperature	Ambient Lighting	Passive Infrared
Smart speaker	✓						
Security camera	✓	✓				✓	✓
Smart TV	✓						
Smart fridge				✓	✓		
Smart kettle					✓		
Smart thermostat				✓	✓		
Smart light						✓	
Wearable	✓		✓	✓			

Table 1: Typical sensors within smart home IoT devices

Many of these sensors are embedded within the IoT devices for the processing of specific smart home purposes and may not be able to derive biometrics. However, other sensors are able to capture biometric information from a proximate user or via an interaction from a user. Biometrics are measurable characteristics of human beings and fall into two main categories of biometrics. The first is *physiological* biometrics [10], these are intrinsic to a user's physiology such as their fingerprint, iris, and face. The second is *behavioural* biometrics [10], which are derived from a user's behaviour such as the way they walk or type. Many different biometrics can be collected from the sensors found in IoT devices [11]. Some of these include:

- **Face**: The faces of individuals is one of the primary ways humans recognise each other and work has been done for decades to authenticate via the face with computers.
- **Voice**: Utilising voice (known as speaker recognition) to authenticate can be done text-dependently or text-independently, i.e. specific text or any text, respectively.
- **Gait**: Gait recognition recognises the way users walk. It can be done either on the user (via an accelerometer) or off the user (via a camera).
- **Gestures**: The way users interact with touchscreens that might be on smart home IoT devices can yield distinguishable traits based on speed, pressure, etc.
- **Keystrokes**: Keystroke dynamics is concept that has been around for decades and has shown effectiveness in authenticating individuals.
- **Behavioural Profiling**: Behavioural profiling represents the capture of user behaviours, such as their habits (e.g. if they are in a certain room at a certain time).

This is a non-exhaustive list of biometrics, and others may also be captured from sensors within smart homes (including some soft biometric traits [12]). Of course, not all of these biometrics can be collected continuously from a sensor (e.g. voice may only be obtained when a user talks and gait will only be obtained as a user walks). This will need consideration in the *continuous* authentication framework in order to leverage the best source(s) available at any given point.

User authentication in the IoT

The fields of continuous authentication and IoT have both grown rapidly over the last decade, and there have already been some works that sought to consider them together. For example, Shahzad and Singh assessed how devices within the IoT might collect and authenticate biometrics [3]. They make a distinction between IoT devices that maintain contact with the user (e.g. fitness trackers) and those that do not (e.g. smart speakers) and evaluate some of the biometric information that might be collected. The authors conclude by producing their own IoT continuous authentication framework for a set-up comprising of a wi-fi sender and receiver. They authenticate users via gait based on the interference with the wi-fi signal and achieve accuracies of up to 93.0%. However, the continuous aspect of the framework is limited because gait recognition can only be collected when users walk.
Furthermore, the study does not consider utilising multiple biometrics or combining biometrics from multiple devices.

A solution for context-aware CA in IoT environments is proposed in [6], and is motivated by the lack of CA schemes for devices that are not in the possession of a user. The study performs a simulation to obtain some experimental results but does not go into depth on the types of biometrics that might be used and also does not present a smart home use case.

Krasovec et al. [7] utilise behavioural biometrics and employ multiple IoT devices to avoid a single point of failure (such as a solution hosted solely on a smartphone). When a user enters a room the authors immediately begin sensing via movement sensors on the keyboard, passive infrared (PIR) sensors in the room, and force sensors around the user's keyboard and mouse. The authors show that continuous authentication is possible from these sensors with an equal error rate (EER) as low as 7.9% when comparing windows of data to recently observed behaviour. Whilst the study does authenticate via sensors embedded within the user's environment, they do not appear to consider sensors on popular IoT devices that one might find in the smart home.

Meanwhile, Nespoli et al. provide an overview of different IoT, sensing, biometric, and machine learning components that can achieve continuous behavioural biometric authentication for IoT devices [8]. They note that utilising behavioural biometrics (over physiological biometrics) comes with benefits to security, continuousness, unobtrusiveness and cost effectiveness. However, while the paper provides a comprehensive overview of many different components that might be used within a CA scheme for IoT devices they do not present a framework and do not discuss how to optimally combine the components.

Gonzalez-Manzano et al. present a survey of CA solutions for IoT devices [9]. They define four categories of IoT devices including wearables (e.g. smartwatches), implementable devices (e.g. health monitoring), external devices (e.g. in smart homes), and portable devices (e.g. smartphones, though it is noted that not all literature considers them as part of the IoT). They divide the biometric features that can be extracted from IoT sensors as raw (a direct reading) or derived (requiring pre-processing). The authors conclude with some challenges, including the need for lightweight CA for IoT devices.

Another survey is presented in [5] for CA methods in IoT environments. Some issues with CA for IoT are discussed, including i) resource constraints, ii) bandwidth/communication, overhead, iii) scalability, and iv) privacy. The authors note device limitations with some only having several MHz of CPU as well as maybe only 100KB of RAM or ROM. It is also shown

that few other surveys have considered IoT environments and most focus on specific portable devices (as noted in [6]) which limits the usefulness. The survey states that the surveyed approaches for IoT continuous authentication are dependent on a single device and there is a general lack of trust management mechanisms for IoT-based CA.

Towards a more comprehensive approach

We envisage a modern smart home equipped with a variety of IoT devices, such as previously shown in Figure 1. Some of these devices are capable of collecting biometric information from the sensors available on the device. For example, a security camera might be able to recognise the gait or faces of users. Some of the devices may provide access to privileged information, such as a user's purchase history via a smart television or smart speaker. The increase in home working during the COVID-19 pandemic means that we are surrounded by smart home IoT in both personal and professional settings.

The traditional forms of authentication are often not readily applicable to IoT devices, particularly because of the variety of user interfaces involved [3]. We therefore propose a continuous authentication approach. However, unlike some other schemes we will utilise an intelligent framework that factors in the real-world nuances of the IoT and uses multiple biometrics from multiple IoT devices to achieve an overall trust measure available to all IoT devices.

The IoT devices in the smart home will continuously collect and authenticate what biometrics they can (some devices may not be able to gather biometrics at all, or all the time). If the IoT device is capable of collecting multiple biometrics, trust scores computed for each one can be fused locally using standard fusion techniques (as discussed bwelow), achieving a *local trust*. However, this local trust may be based on a single biometric modality and may not alone be sufficient to authenticate the user (e.g. a low resolution camera may produce unreliable face recognition scores).

In the event a privileged event needs to occur on a smart home IoT device or a user interaction is performed that requires authentication, the device can use the local trust score (if it has one) and request the local trust scores of other devices within the smart home. These trust scores can then be fused on the device requiring authentication. The frequency that an IoT device might request scores from other devices registered to the smart home might range from continuously (for high security devices) to per event (for devices needing event-specific authentication).

There are certain nuances that this type of system must consider. Firstly, there may be a varying set of IoT devices within the smart home; devices may be added, removed or be in the smart home for only a period (e.g. a wearable). Secondly, devices may receive differing levels of interaction from a user, with some devices capturing a continuous feed of biometrics (e.g. a camera-equipped device), others only capturing one-off events (e.g. when spoken to), and others capturing no usable biometrics. Lastly, it may be that different devices require different levels of authentication.

Achieving Continuous Authentication

Traditional authentication is a point-of-entry assessment, which means that once an IoT device that has been authenticated may be used by impostors if left unlocked. Additionally, traditional methods may be difficult to implement on an IoT device because such devices may not have standard user interfaces (e.g. keyboard input) [3]. Lastly, each IoT device will often perform authentication individually, without making use of the other devices within the smart home.

The advantage of continuous biometric authentication stems from it being more usable (requiring no explicit interaction to authenticate) and more secure (in that it authenticates throughout a session). These systems carry the benefit of providing security, but also being highly usable in that they are transparent to the user and require no explicit interaction from them (such as a PIN). It has been suggested in multiple surveys that many users would opt for using such systems to authenticate their devices [14]. This form of authentication can therefore be seen to suffer few of the discussed shortcomings of other authentication solutions discussed.

Achieving continuous authentication within this smart home IoT context will see lightweight machine learning models (possibly TensorFlow Lite models [15]) being used to train a system on biometrics collected for a training period. After training the IoT devices will (if applicable) utilise the sensors to collect one or more biometric(s) from the user, compare the biometric(s) to the trained profile and produce a local trust score.

In some multi-sensor devices it may be that only one sensor is able to gather biometrics (e.g. the face, but no voice as the user did not talk). This can also cause disparity in the times since a certain biometric or device was authenticated. This is considered in the score fusion in which the biometric scores are fused with respect to their temporal state, such that most recent scores have a higher weighting.

This process will occur whenever an IoT device connected within the smart home requires a current authentication score; local trust scores of each IoT device will be sent to the authenticating device which will then fuse them with its own local score. The final score will be compared to a threshold in order to assess if the authentication is maintained. This process may occur at different intervals depending on desired security, e.g. it may occur continuously on some devices (for high security) and per event/interaction on other devices. The collection of multi-device scores to form a robust trust score for continuous authentication is shown in Figure 2. This shows a devices responding to a request for local scores such that a device may form a robust combined trust based on all available biometrics. Note that in the case of device 3 no related biometric sensors are present, and in the case of device 4 it may not always be present.

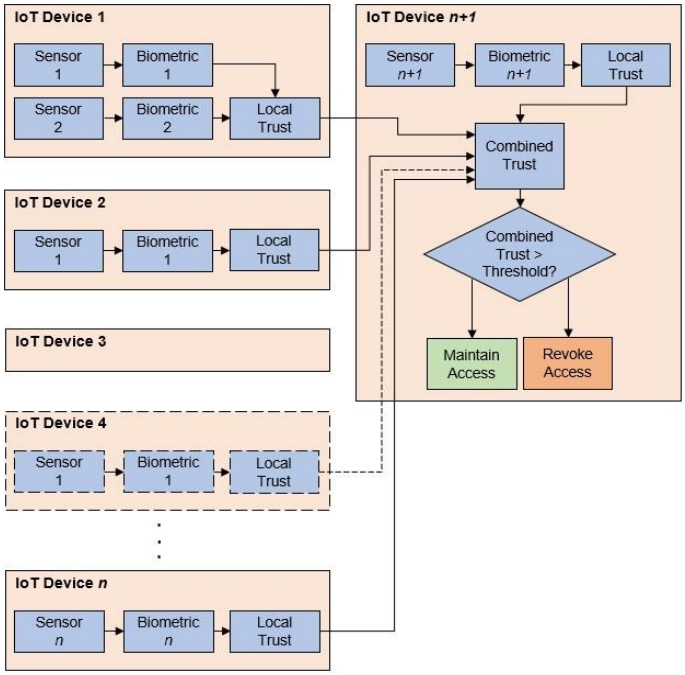

Fig. 3. The approach for intelligent continuous authentication for smart home IoT devices.

Some of the aforementioned IoT devices can collect multiple biometric modalities, e.g. a security camera with an embedded microphone might collect face *and* voice biometrics. Utilising multiple different biometrics together has been shown to both yield improved performance (in terms of the Equal Error Rate) and increase the difficultly for an impostor to attack the system [16]. However, there are multiple methods to fuse biometrics together. One common method is at the score-level, at which scores from biometric comparisons are combined. This also applies to the fusion of the fused scores from multiple IoT devices to produce a single *combined trust* score from all contributing IoT devices. This fusion would be take place on each IoT device if there are multiple biometric scores. The weighting applied to each biometric will decay with respect to time such that, for example, a biometric that is 30 minutes old will yield less trust to the overall score. This fusion would also take place on the IoT device requesting the score from all other IoT devices within the smart home after it has received the scores. The weighting applied here (if any) might be the reliability of that IoT device based on past accuracy.

Moving forward

Whilst this discussion has presented a continuous authentication approach for IoT devices, there are still some existing challenges that remain. The first is with regard to assessing real-world performance and limitations on various IoT devices with different amounts of processing and storage. This will allow for optimal selection of biometrics on different IoT

devices, ensuring they are capable of handling the capture and authentication. This might also see heavy processing done on non-IoT devices (e.g. in the cloud) to provide efficiency. The second area of future work would be to consider and protect the system from potential attacks. These attacks might take place at the communications level (e.g. a man in the middle attack) or at the presentation level (at which an attacker might present a forged biometric).

The trajectory of the IoT shows that is is a rapidly growing area. This comes with a plethora of security concerns. One of these security concerns is authentication. However, IoT devices are vastly different and may not have standard authentication interfaces. We propose the use of continuous multi-modal biometric authentication via a variety of different devices connected within the smart home to provide robust trust scores in real-time. We have explored the state-of-theart and discussed the components and nuances of continuous authentication for IoT to define how our framework could be implemented. We concluded by highlighting the need for future work within this field.

About the authors

Max Smith-Creasey is …

Steven Furnell is a professor of cyber security at the University of Nottingham. He is also an Honorary Professor with Nelson Mandela University in South Africa and an Adjunct Professor with Edith Cowan University in Western Australia. His research interests include usability of security and privacy, security management and culture, and technologies for user authentication and intrusion detection. He has authored over 350 papers in refereed international journals and conference proceedings, as well as books including Cybercrime: Vandalizing the Information Society and Computer Insecurity: Risking the System. Prof. Furnell is the Chair of Technical Committee 11 (security and privacy) within the International Federation for Information Processing, and a board member of the Chartered Institute of Information Security.

Muttukrishnan Rajarajan is …

Commented [SF(2]: Please complete the bits for yourselves.

References

Commented [SF(3]: We can go through these at the very end, and work out which ones are still referenced and in what order … and then renumber as appropriate.

[1] L. S. Vailshery, “Global iot and noniot connections 2010-2025,” Mar 2021. [Online]. Available: https://www.statista.com/statistics/1101442/iot-number-ofconnected-devices-worldwide/

[2] E. Bertino, “Data privacy for iot systems: Concepts, approaches, and research directions,” in *2016 IEEE International Conference on Big Data (Big Data)*, 2016, pp. 3645–3647.

[3] M. Shahzad and M. P. Singh, “Continuous authentication and authorization for the internet of things,” *IEEE Internet Computing*, vol. 21, no. 2, pp. 86–90, 2017.

[4] D. Bastos, M. Shackleton, and F. El-Moussa, “Internet of things: A survey of technologies and security risks in smart home and city environments,” in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 2018, pp. 1–7.

[5] F. H. Al-Naji and R. Zagrouba, “A survey on continuous authentication methods in internet of things environment,” *Computer Communications*, vol. 163, pp. 109–133, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366420319204

[6] P. Nespoli, M. Zago, A. H. Celdran, M. G. Perez, F. G. Marmol, and F. J. Garcia Clernente, "A dynamic continuous authentication framework in iot-enabled environments," in *2018 Fifth International Conference on Internet of Things: Systems, Management and Security*, 2018, pp. 131– 138.

[7] A. Krasovec, D. Pellarini, D. Geneiatakis, G. Baldini, and V. Pejovic, "Not quite yourself today: Behaviour-based continuous´ authentication in iot environments," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 4, no. 4, dec 2020. [Online]. Available: https://doi.org/10.1145/3432206

[8] Y. Liang, S. Samtani, B. Guo, and Z. Yu, "Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 9128–9143, 2020.

[9] L. Gonzalez-Manzano, J. M. D. Fuentes, and A. Ribagorda, "Leveraging user-related internet of things for continuous authentication: A survey," *ACM Comput. Surv.*, vol. 52, no. 3, jun 2019. [Online]. Available: https://doi.org/10.1145/3314023

[10] A. K. Jain, A. A. Ross, and K. Nandakumar, *Introduction to Biometrics*. Springer Publishing Company, Incorporated, 2011.

[11] M. S. Obaidat, S. P. Rana, T. Maitra, D. Giri, and S. Dutta, *Biometric Security and Internet of Things (IoT)*. Cham: Springer International Publishing, 2019, pp. 477–509.

[12] J. F. Roscoe and M. Smith-Creasey, "Unconventional mechanisms for biometric data acquisition via side-channels," in *13th International Conference on Security of Information and Networks*, ser. SIN 2020. New York, NY, USA: Association for Computing Machinery, 2020. [Online]. Available: https://doi.org/10.1145/3433174.3433600

[13] S. W. Shah and S. S. Kanhere, "Recent trends in user authentication – a survey," *IEEE Access*, vol. 7, pp. 112505–112519, 2019.

[14] S. Rasnayaka and T. Sim, "Who wants continuous authentication on mobile devices?" in *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, 2018, pp. 1–9.

[15] "Tensorflow lite: Ml for mobile and edge devices." [Online]. Available: https://www.tensorflow.org/lite

[16] M. Smith-Creasey and M. Rajarajan, "A continuous user authentication scheme for mobile devices," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, 2016, pp. 104–113.