Computers in Biology and Medicine 167 (2023) 107702

Contents lists available at ScienceDirect

Computers in Biology and Medicine

journal homepage: www.elsevier.com/locate/compbiomed

Identity resilience in the digital health ecosystem: A key recovery-enabled framework

Chetana Pujari [a], Balachandra Muniyal [a], Chandrakala C. B [a,*], Anirudha Rao [a], Vasudeva Sadiname [b,1], Muttukrishnan Rajarajan [c]

[a] Department of Information and Communication Technology, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, Karnataka, 576104, India
[b] Vachan Clinic, Vadiraja complex, Udupi, Karnataka, India
[c] School of Mathematics, Computer Science and Engineering, City University of London, London, EC1V 0HB, UK

ARTICLE INFO

Keywords:
Trust
Healthcare
Security
Privacy
Attribute-based access control
Blockchain
Decentralized identity
Key recovery
Verifiable credentials

ABSTRACT

In response to the evolving landscape of digital technology in healthcare, this study addresses the multi-faceted challenges pertaining to identity and data privacy. The core of our key recovery-enabled framework revolves around the establishment of a robust identity verification system, leveraging the World Wide Web Consortium(W3C) standard for verifiable credentials(VC) and a test blockchain network. The approach leverages cryptographic proofs embedded within credentials issued by various entities to securely validate the legitimacy of identities. To ensure standardized identity establishment, the roles and responsibilities of entities align with the UK digital identity and attribute trust framework, resulting in a cohesive verification process. Embracing self-sovereign identity (SSI), encrypted credentials are stored within the owner's device, empowering individuals with data control while prioritizing privacy and security. Furthermore, the work introduces an algorithm that places paramount importance on owner-centricity, trustworthiness, and privacy-aware handling of SSI credentials, subjected to threat modeling through the Owasp Dragon tool. A key recovery algorithm, a key component of our Recovery-Enabled Framework, empowers users to regain credentials using a trustee-based recovery system with a memorized PIN, eliminating the need for third-party reliance. Furthermore, a trust score, a crucial component of the framework, assesses the conformity of verified credentials with stated standards, boosting trust in established identities. Leveraging the modularity of Hyperledger Fabric, the work utilizes smart contracts to impose context-aware attribute-based policies, ensuring controlled access, traceability, and auditability, consequently strengthening security. Through comprehensive development, refinement, and rigorous testing, the prototype emerges as a potent tool for enhancing security within the Digital Health Ecosystem. It equips organizations with the means to navigate this digital landscape while inspiring trust among stakeholders, significantly contributing to the resilience of identity in the digital health ecosystem.

1. Introduction

Electronic healthcare encompasses various components, including a medical monitor Internet of Things (IoT) device like a wearable smart healthcare device, along with electronic health records (EHRs). A wearable device monitors health activities, for example, a fitness watch can measure blood pressure, heart rate, step count, and blood oxygen level. EHRs contain sensitive healthcare information, such as treatment plans, diagnoses, and test results. To provide timely, accurate, and better healthcare service, healthcare data is accessed and shared among all stakeholders involved in the healthcare ecosystem, including doctors, healthcare service providers, and healthcare research institutes.

As stakeholders regularly engage with the public, it becomes crucial to establish a reliable and verifiable decentralized identity that fosters trust. In the realm of identification, trust typically pertains to the confidence and belief that an individual, system, or business can be trusted to accurately and securely handle an individual's or organization's identity information. To achieve this, the ecosystem must ensure integrity, authentication, authorization, and privacy preservation, collectively forming a foundation for a trusted and resilient identity establishment.

* Corresponding author.
E-mail addresses: chetana.pujari@manipal.edu (C. Pujari), chandrakala.cb@manipal.edu (C.C. B).
[1] Consultant Psychiatrist.

https://doi.org/10.1016/j.compbiomed.2023.107702
Received 4 July 2023; Received in revised form 17 October 2023; Accepted 7 November 2023
Available online 13 November 2023

Identity establishment is a significant challenge in the digital era. For example, recent incidents regarding a fake doctor at Bankstown Hospital in Australia [1] and Missouri [2] have raised considerable alarm in the medical community. In light of the pandemic, there is a shift to online medical services [3–7] all over the world, hence wearable device data and EHRs are crucial for remote monitoring.

The EHRs from hospitals, wearable devices, and clinical data within different countries are fragmented on healthcare servers. The current setup involves centralized systems managed by a central identity provider with complete control over user identity credentials and service access. In contrast, federated identity management systems allow users to utilize a single identity for seamless authentication across different service providers, eliminating the need for separate credentials at each provider's end. As an example, we can utilize the credentials from our email account to log in to other service providers, eliminating the need to create an entirely new set of credentials. However, existing literature, such as [8–12] mainly concentrates on healthcare service providers, overlooking the potential risks to patient data. In this context, privacy protection laws imposed by governmental regulatory bodies, such as the Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR), are essential for regulating the healthcare industry. However, these laws are not sufficient to establish the right to privacy [13]. Healthcare data breaches and unauthorized information disclosure are major concerns [14]. Digital trust [15], interoperability, access control, and privacy are critical elements of the Self-Sovereign Identity (SSI) ecosystem which requires establishing the digital identities as well as the personas for this particular context [16]. In SSI, the owner can manage the attribute that defines their identity and have control over who can gain access to the identity credentials by using a decentralized identifier (DID) and cryptographically verifiable credentials (VC).

In the existing work [17–19], privacy is mainly referenced to session data. Even though attribute-based identity privacy is considered in [20,21], the proposed work could further improve by generating the codeword based on the cryptographically proven claims in the verifiable credentials. As in the SSI ecosystem, the user credentials and private keys are stored in the software agent called a wallet. If the wallet is lost, the user loses their identity-defining verifiable credentials and private key. A seed word-based and guardianship model is being proposed in the existing work [22,23]. The guardianship model relies on a third party for key recovery. The seed word-based recovery mechanism is ineffective as it is not easy to remember seed words after ten long years. Hence, the proposed work aims to ease the process of decentralized key management, which is user-centric.

In the proposed work, the different stakeholders involved in healthcare, including doctors, patients, hospitals, clinics, and research institutes, are identified and provided with verifiable credentials (VC) that offer cryptographic proof of their qualifications, citizenship, employment, and medical licenses. These VCs, along with decentralized identifiers (DID) and blockchain technology [24], are utilized to establish decentralized identities for all stakeholders and ensure the decentralization of both identity and health records. Within the proposed work, a tailored credential schema is meticulously constructed, and finely tuned to cater to the nuances of the healthcare ecosystem. In a significant stride towards safeguarding user privacy, the framework introduces compound proofs. These proofs intricately weave together claims extracted from diverse verifiable credentials. This integration is achieved using predicate-based zero-knowledge proofs, establishing an unyielding shield of privacy around user data.

Additionally, a pivotal advancement takes shape in the form of a trust score computation mechanism. This feature imbues the identity establishment process with heightened confidence. The trust score is meticulously calculated based on the repertoire of credentials possessed by stakeholders. This computation effectively aligns the verifiable attributes of stakeholders with predefined benchmarks, offering a tangible and quantifiable measure of trustworthiness within the healthcare identity framework. To enhance user privacy, the proposed approach separates identity from electronic health records (EHRs) and defines access policies at the attribute level using smart contracts.

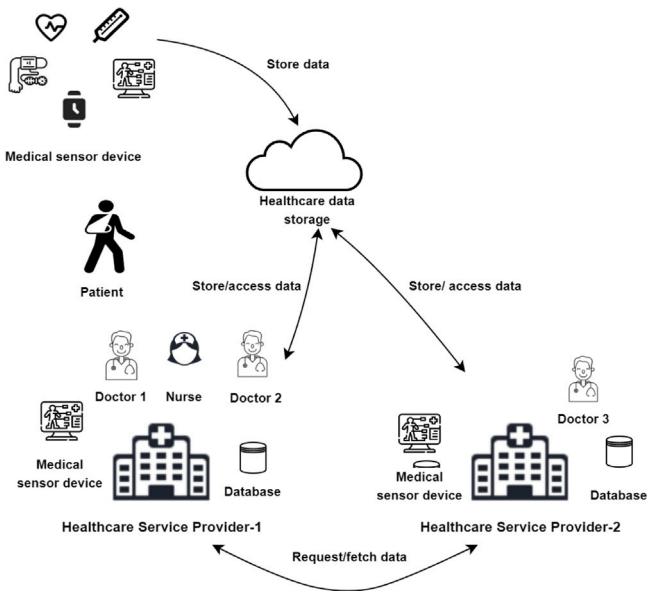

Fig. 1. Use case depicting the need for access policies to ensure privacy in healthcare.

The motivation for the proposed work is elucidated by the use case scenario illustrated in Fig. 1. The usage of digital healthcare IoT systems presents a significant challenge in identifying the user of the device and the entity accessing confidential healthcare information [25]. With the ongoing pandemic, remote monitoring using medical sensor devices and digital healthcare systems has become increasingly prevalent. The wearable sensor device automates the collection, storage, and analysis of medical data, aiding in the diagnosis process [26]. The medical sensor device connected to the patient could be owned by either the patient or the hospital where the patient receives healthcare services. Access policies regulate access to medical sensor data and digital health records. Multiple stakeholders may have an interest in accessing this data, including consulting doctors, nurses, referred doctors, healthcare research institutes, and governmental agencies. Consider the following scenario: Nurses, Doctors 1 and 2, work at Healthcare Service Provider 1, while Doctor 3 works at Healthcare Service Provider 2. A patient is consulting Doctor 1, an orthopedic surgeon, and also regularly seeing Doctor 2, a psychiatrist. A nurse is assigned to the same ward as the patient. In a digital healthcare system, several concerns arise:

- Identity establishment: To establish trust in participants'/ stakeholders' identities in the healthcare ecosystem.
- Credential/key management: Owner-centric key management system.
- Access Management: To safeguard data privacy, it is imperative that Doctor 1 is granted access solely to the ortho database. The stakeholders' access levels must be determined based on their respective roles, and different levels of access permission must be defined for Doctor 1 and the nurse, as per our use case scenario. Policies must define Doctor 3's access rights to the patient data when the patient is referred to him. Since various patients use the Medical sensor device at different times, it is crucial to consider the context when deciding on access. To ensure patient privacy in all the above scenarios, the proposed work incorporates a hybrid model that considers stakeholders' roles, attributes, and owner consent when defining access policies. Moreover, access to the system must be restricted when an unauthorized user tries to gain access, as is the case with medical device hacking [27], which poses a grave threat to human life.

1.1. Contribution

The research work leverages emerging concepts such as decentralized identifiers (DID), verifiable credentials, zero-knowledge proofs, and blockchain technology to tackle challenges associated with identity establishment, user privacy, and decentralized key management and security threats in the healthcare domain without compromising data security. The proposed work makes significant contributions in the following areas:

- The proposed approach aims to bolster user privacy and dynamic access control within the healthcare sector by establishing a mapping between verifiable credentials and derived credentials. Verifiable credentials consist of claims regarding the user's identity, and our proposed work involves amalgamating these claims from diverse user-verifiable credentials to create a codeword based on their combinations. The resulting collection of claims, distinguished by a unique codeword, is referred to as derived credentials. Notably, the integrity and authenticity of these claims are collectively substantiated through compound proof, a cryptographic demonstration that underscores the legitimacy of claims originating from multiple verifiable credentials. Moreover, the proposed approach advances the reliability of identity by introducing trust score computation, this trust score offers a tangible metric of trustworthiness within the healthcare identity framework, thereby strengthening the very foundation on which identities rest.
- The proposed research introduces a novel decentralized key recovery algorithm tailored for stakeholders in the healthcare domain. This algorithm incorporates concepts including Shamir secret key sharing, Lagrange interpolation, and induced PIN-based diffusion to distribute private keys among a designated group of users. Moreover, to authenticate the user during the recovery phase, the proposed work employs a commit and reveal scheme utilizing Pedersen's commitment. The novelty of the algorithm lies in the PIN-based diffusion performed where the key owner using the PIN can authenticate themselves at different trustees which eases the process of recovery where the user needs to remember only their PIN while recovering.
  In the existing social recovery method the user needs to either rely on the third party for the recovery [28] or using the social recovery has to authenticate themselves using the digital signature/ password [29,30] and a separate public, the private key is maintained for each trustee, hence to recover one key the user has to manage multiple keys which is cumbersome. The proposed approach ensures user-friendly, robust, and secure key recovery while maintaining the decentralized nature of the system.
- The proposed model harnesses the modularization capability of the Fabric blockchain to enable effective isolation and confidentiality in communication. Additionally, it leverages smart contracts to implement fine-grained attribute access policies specifically designed to address the unique requirements of the healthcare domain. Importantly, these policies ensure data privacy remains a top priority, safeguarding sensitive information within the healthcare ecosystem.
- The proposed framework's security is verified through a comprehensive threat modeling and security analysis. The threat model is constructed using the Owasp Dragon tool. The threat modeling, mitigation strategies, and security analysis ensure its resilience to potential threats and instill confidence in its application.

The remainder of the paper is organized as follows: Section 2 describes related work undertaken within the healthcare system to manage identity and access. In Section 3, the methodology proposed for identity establishment and access management in the healthcare system is described, followed by the implementation and result in Section 4, and Section 5 covers the security analysis followed by a conclusion.

2. Literature review

This section examines related work in the field of healthcare with or without the use of the SSI ecosystem and recent research in the area of key recovery and access management.

In a centralized healthcare identity management system, the patient is dependent on the service provider to verify their identity, resulting in minimal control or authority over their personal data. To address this limitation, various authentication methods have been proposed, including OTP or biometric-based authentication [31], two-factor authentication [32], and three-factor-based authentications [33], aiming to identify stakeholders and enhance security measures.

Centralized identity management systems require centralized identity providers to issue identities and maintain the trust factor associated with those identities. These additional factors of authentication are not sufficient to eliminate identity theft, masquerading, and phishing attacks.

MedRec, an Ethereum-based decentralized healthcare record system [34], faces challenges such as stakeholders bearing the computation costs for proof-of-work consensus and the lack of a patient-centric approach to record handling. To address these issues, a study [35] proposed an authentication mechanism to identify patients within the hospital network. However, this approach relies on the participation of multiple stakeholders to validate transactions and incurs costs per transaction due to its reliance on a public blockchain.

In the work presented in [36], the primary focus of this work was on validating the vaccination certificate, where the identity of individuals is established through the creation of an account on uport and manual verification of their physical ID once the vaccination is completed or their test result is available. The vaccination certificate is represented in the form of a QR code, which is digitally signed by the healthcare service provider and then approved by the holder through a counter signature. This process ensures the authenticity of both the certificate holder and the issuer. In the event of the user losing the key to their wallet, they rely on uport for recovery. In the proposed work, the key recovery process is centered around the user and has been designed to simplify the recovery procedure.

In the healthcare system presented by [37], stakeholder identities are linked to their respective Ethereum addresses. COVID-19 records are securely encrypted and stored in the cloud. To access these records, requestors must provide specific attributes to the service provider. The service provider then grants the requestor an intermediate parameter and private key, which enables them to access and decrypt the records. However, successful decryption is only possible if the presented attributes match the access policy. To maintain data integrity and immutability, a blockchain is employed. It serves as an immutable ledger for patient and hospital identifiers, public keys, and revocation statuses. To further enhance the security of these frameworks [36,37], the proposed work aims to authenticate the healthcare provider's identity using a compound proof generated from the claims made using credentials from multiple issuers. This additional layer of verification strengthens the overall system's integrity. Additionally, the research introduces a novel approach for key recovery, focusing on a user-centric PIN-based social recovery method, which adds an extra layer of protection and convenience for users while ensuring a reliable and user-friendly experience for individuals.

The work presented in [7] introduces a blockchain-based framework for sharing clinical data. This architecture utilizes public key cryptography to verify users' identities. The user's public key is stored in an immutable ledger on the blockchain, establishing their identity, while the corresponding private key is employed for authentication purposes. To enable data sharing, a temporary pointer to the data is stored on the blockchain. When sharing the data, it is encrypted using the requester's public key and digitally signed by the clinician, ensuring authentication. However, a limitation of this approach is that only clinicians can initiate data sharing, leading to a lack of user control. To enhance trust

Table 1
Literature pertaining to identity establishment.

Paper/ Parameter	Blockchain	SSI	Authentication	Ease	ZKP	Single proof	Compound proof	Privacy	Integrity
[31]	×	×	3rd party IDP	~	×	×	×	×	×
[32]	×	×	Physical ID+ Password+ Smart card	×	×	×	×	×	×
[33]	×	×	Physical ID+ Password+ Biometric	×	×	×	×	×	×
[34]	Public	~	Public key+ SSN+ Blockchain account address	✓	✓	✓	✓	~	✓
[35]	Public	~	Account address	✓	×	×	×	~	✓
[36]	Private	✓	Physical ID+ Blockchain account address	✓	✓	✓	×	✓	✓
[37]	Private	~	Password+ Blockchain account address	✓	×	✓	×	~	✓
[38]	Permissioned	×	Password+ Biometric	×	×	✓	×	✓	✓
[39]	×	×	Credential provided during registration	✓	×	×	×	~	×
[7]	Public	×	Public key cryptography	~	×	×	×	✓	✓
[12]	Public permissioned	×	MAM	~	×	×	×	~	✓
Proposed work	Permissioned	✓	VC based	✓	✓	✓	✓	✓	✓

~ represents partially considered.

in user identity, the inclusion of verifiable attributes of the user could be considered. The work [12] illustrates a method for ensuring secure access to healthcare activity data. This method leverages the Masked Authenticated Messaging extension module protocol, which is backed by IOTA's distributed ledger capability. Enhancing trust in the authentication process could be achieved through the incorporation of verifiable credentials. These credentials enable cryptographic verification of each claim made by a user.

Most of the research work is focused on patient-centric access. The Ayushman Bharat Digital Mission (ABDM) was launched by the Ministry of Health and Family Welfare in India [3,40]. ABDM assigns a unique identifier called an ABDM number to each patient. During registration, a link to download a Personal Health Record (PHR) is sent to the mobile device. The user can access their health records via the PHR app and give consent to share records. The doctor is identified by the record stored in the ABDM directory. In ABDM, doctors' credential verification is done manually. Medilinker is a patient-centric SSI model [9]. Patients can present their government-issued ID at the clinic for their first verifiable healthcare ID. With the obtained healthcare ID, the patient's demographic information can be verified at any clinic. Medilinker allows the patient to give consent to what data they wish to share with the requestor. The proposed work could improve Medilinker further by involving various stakeholders in the healthcare domain and providing verifiable identities for each stakeholder as well as further enhancing the controlled disclosure of information based on patient consent.

My Health Record by the Australian government provides secure online health records [5]. Users can manage their health information through My Health Record. Patients control who has access to their information. Healthcare professionals registered with My Health Record can access a patient's records. Trust in the identity of stakeholders could be a major concern in ABDM, Medilinker, and My Health Records.

A scheme for user authentication and identity management is presented in [38] using SSI. Biometric information is used to establish a user's identity. Healthcare systems must protect the privacy of their users. Researchers conducted a survey to investigate the potential of blockchain technology to manage identity in patient health records [8]. The survey aims to explore the benefits of integrating centralized and decentralized systems and how SSI-based systems could enhance privacy within the healthcare industry. In the work [41], a proxy re-encryption method is employed to delegate authority using a smart contract and digital signature. It is noted that role-based access control is defined in the work [39], however, identity management and privacy issues related to user identity and healthcare data are not addressed.

Inefficient referral systems lead to a delay in patient care and ineffective service usage of doctors and hospitals as mentioned in work [46]. In a study conducted at the University Hospital of Southern California in Denmark, referral practices were examined and found to be inefficient as shown in work [47]. The organizational structure and the types of care provided play a role and further investigation is needed to facilitate the process and better utilize the resources.

Table 1, compares the proposed work with recent work in identity establishment, taking into consideration factors such as blockchain platform use, self-sovereign identity (SSI), authentication mechanism, ease of use, Zero Knowledge Proofs (ZKPs) of the claims made by the user, single and compound cryptographic proofs, identity and data privacy and integrity of data. According to the table, × stands for not covered, and ~ stands for partially done.

The privacy of user identity is a crucial concern in sharing information. In the work [19,48], the focus is on session data privacy rather than user identity. To address this issue, [17] proposes an attribute-based scheme that discloses information only to users who satisfy attribute predicates. In the smart city environment, [20] uses Unicode generated through user attributes as a privacy measure for user identity. However, further improvements can be made by incorporating a codeword, as proposed in the SSI-based models presented in [18,22], to enhance access control and trust in the system. The paper referenced as [49] introduces a blockchain-based identity solution that incorporates provable claims and enables Zero-knowledge proofs. However, the paper lacks in-depth information about the management of these credentials. The work discussed in [28] presents two key recovery mechanisms. The first scheme is a multi-agent-based key recovery, and the second scheme is a collusion-resistant proxy encryption scheme. In both schemes, users are required to depend on a third party for key recovery services.

The work in [22] proposes a guardianship model for key recovery, where users rely entirely on a third party for key recovery. However, the mechanism to recover the key if it is lost is not taken into consideration in [17,20,21,48], and [22].

Table 2
Key recovery process in the existing IDM system.

SL	IDM	Recovery process	Observations
1	[42]	1. Using Shamir Secret Sharing (SSS) scheme split, encrypt and share the private key with recovery delegates. 2. When the device/key is lost, generate a temporary encryption key pair on a new device. 3. The delegate contact DID document using a temporary public key. 4. Encrypt the key share using the temporary public key and share it with the user.	1. Dependency on the thirdparty. 2. Ease of use. 3. Limits user-centric IDM.
2	[43]	1. It employs a three-factor recovery strategy. 2. A user must have access to their mobile number, email account, phrase, and scanned document. 3. A service provider can retrieve the unique salt value after the user provides proof that he or she has access to the above assets. 4. The user's new device will be provided with information allowing it to retrieve their identity information.	
3	[44]	1. Using another registered device, revoke the permissions of the lost device. 2. Revoke all private keys associated with the device. 3. The registered device will become the primary device.	
4	[45]	1. If a phone is lost, the permissions can be revoked using a centralized keyshare server. 2. The expiration date for credentials will be short.	

*IDM= Identity Management, SP= Service Provider.

Table 3
Literature pertaining to access control.

Paper	Blockchain	Fine grained access	Use centric	IoT	Privacy
[50]	×	×	×	✓	✓
[51]	×	✓	×	×	✓
[52]	✓	✓	×	✓	✓
[53]	✓	✓	×	✓	~
[54]	✓	✓	×	✓	~
[55]	✓	✓	×	✓	✓
[56]	×	✓	×	✓	~
Proposed work	✓	✓	✓	✓	✓

~ represents partially considered.

The work presented in [29,30] introduces a key recovery algorithm based on the Shamir secret sharing scheme. In the work [29] approach, the need for reliance on a third party is eliminated. Instead, the user can divide the key into shares, and for each share, a pair of public and private keys is generated. The key owner then digitally signs each share and encrypts them using the public keys of each key escrow. During the recovery phase, Lagrange interpolation is employed to retrieve the original key.

In this scheme, to recover the key, the user would traditionally need to manage several sets of temporary keys for digital signatures, which can be cumbersome. In [30], the user generates the password for each share which is again difficult to remember. However, the proposed approach in this work utilizes PIN-based induced diffusion to streamline the process of social key recovery, making it more user-friendly.

Table 2 summarizes a popular existing identity management system, its key recovery process, and its observations.

Access control systems play a crucial role in providing controlled access to data based on policy constraints defined for access, regardless of identity or device. Inadequate policies in such systems have led to security breaches in more than 150,000 IoT devices [18,57,58].

Polymorphic encryption was employed in [50] to ensure data integrity and authenticate entities in an E-Healthcare system. However, the study lacked a fine-grained and user-centric access control mechanism. In contrast, a fine-grained access control system was proposed in [51] for an E-Healthcare cloud system, but the work did not focus on user-centricity.

In [52], an access control system was designed without using access control lists or user roles. Access decisions were made based on the attributes that the requestor possesses, although the use of the AES 128 algorithm resulted in significant overhead.

Blockchain technology was utilized to extend organization-based access control in [53], but the work did not support access policies at a granular level. In contrast, a fine-grained access control mechanism for IoT ecosystems based on smart contracts was proposed in [54] using private permissioned Hyperledger Fabric blockchains. However, the work utilized a Kafka service for ordering transactions, which is slower than the Raft ordering service.

An access control system was proposed in [55] using the Raft protocol for ordering services and ABAC for fine-grained access management. However, the work did not allow controlled ownership in which data owners can decide which attributes to reveal and when to apply Zero Knowledge Proof(ZKP).

Table 3 summarizes recent work in access control systems, including the proposed work. The table compares parameters such as the blockchain platform used, granular access control to data owners, IoT devices, and identity and data privacy protection.

3. Methodology

This section presents a healthcare model based on self-sovereign identity (SSI). The primary objective is to offer an overview of the SSI-based healthcare ecosystem, accompanied by a comprehensive framework for building trust in health identity and preserving data privacy. To achieve this, smart contracts are utilized to define access policies tailored to each stakeholder involved. Furthermore, a decentralized key recovery mechanism is introduced, which ensures secure and reliable key retrieval.

3.1. Identity establishment

To demonstrate commitment to trustworthiness and compliance with data protection regulations, the proposed work is based on an alpha version 2 prototype for the United Kingdom digital identity and trust framework [59]. The healthcare trust frameworks, as depicted in Fig. 2, could be overseen by government regulation agencies, quality compliance regulators, and medical councils to monitor compliance, performance, and scheme management. The scheme owner is

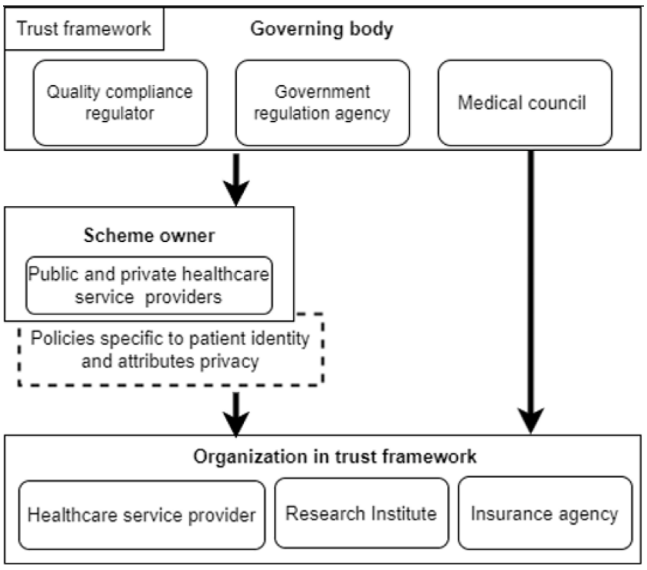

Fig. 2. Trust framework for healthcare ecosystem.

comprised of both public and private healthcare providers who must agree to standard digital identity and attribute rules. The contractual agreement can be used to establish liability between service providers. Research institutes, healthcare providers, and insurance agencies may participate in the trust framework for healthcare.

The identity service in the proposed healthcare system is based on self-sovereign identity (SSI) created by the Aries-Askar wallet, which is designed to be used by Hyperledger Aries agents. The Hyperledger Aries toolkit is primarily used to manage cryptographically verifiable credentials. According to the proposed healthcare system, attribute service providers are essentially issuers as mentioned in Table 4, who issue credentials containing evidence of different claims relating to the user's identity to the user.

In the proposed healthcare system, orchestration service providers are healthcare providers, whose role is to ensure secure data sharing within the healthcare trust framework. Healthcare service providers use decentralized ledger services such as Hyperledger Indy and Hyperledger Fabric to manage identity and medical data transactions respectively. Two separate ledgers are used to ensure user privacy.

A scheme owner manages access control, and granular rules are defined that include user consent as an attribute before accepting any access request from the parties relying on the scheme. The scheme owner is responsible for overseeing the entire healthcare trust framework, including compliance with regulations, performance, and scheme management. The proposed healthcare system aims to promote trust in healthcare by ensuring the security and privacy of users' medical data through the use of SSI, decentralized ledger services, and access control mechanisms.

The system architecture proposed for the healthcare identity framework utilizes decentralized ledger services such as Hyperledger Indy and Hyperledger Fabric to oversee identity and medical data transactions. Within this framework, each credential issuer adheres to a specific schema for issuing credentials. This schema encompasses essential details about the credentials, including the issuance date, authority, validity period, issuer's signature, and the issuer's decentralized identifier (DID). Additionally, the schema incorporates attributes that serve as the foundation for claims made within the credentials. To ensure security and efficiency, the verifiable credentials are signed using the ED25519 public key signature scheme, known for its swift signing and verification processes, compact signature size, and robust security measures.

Data owners have the capability to issue temporary credentials as tokens of consent, granting access to their data. With these credentials, owners have control over which attributes are disclosed and can employ Zero Knowledge Proof protocols to convey information without revealing sensitive details. To facilitate the verification process of these credentials, the permissioned blockchain platform, Hyperledger Indy, is utilized. It stores the credentials, schemas, and decentralized identifiers (DIDs) of both issuers and patients. Additionally, the blockchain maintains a credential revocation list, ensuring information regarding revoked credentials is readily available. Verifiable credentials can be stored securely in wallet software, such as Askar, on the owner's mobile device. Alternatively, they can be managed by the cloud agent Aries Cloud Agent (ACA) on behalf of the owner, providing flexibility in storage and management options.

The proposed framework empowers credential holders, like Dr. Stacy, to have control over attribute disclosure from the credentials issued by entities such as NMC, SPMEA, and the data owner as shown in Fig. 3. With this control, the holder can determine the appropriate instances to employ Zero Knowledge Proof protocols, ensuring cryptographic proof for all claims made. The framework allows the selection of individual claims from a single credential or a combination of claims from multiple credentials, enabling the presentation of a single or compound proof to the verifier, thus substantiating the claims effectively.

$$\begin{matrix} y = x^z \\ z = log_x y \end{matrix} \quad \text{Discrete Logarithm Problem} \tag{1}$$

$$c = a^m \quad \text{Pedersen commit} \tag{2}$$

In the proposed work, each credential comprises multiple claims. To sign these credentials with multiple claims, the Camenisch-Lysyanskaya (CL) signature scheme is employed. The CL signature scheme is rooted in the Discrete Logarithm Problem and Pedersen Commitment, denoted by Eqs. (1) and (2) respectively. In these equations, 'y', 'z', and 'a' represent members of a large discrete group. Eq. (2) showcases the commitment 'c' for the message 'm', initially transmitted to the receiver, and subsequently revealed for verification at a later stage. The adoption of CL signature schemes ensures selective disclosure of attribute values, maintaining the privacy of the credential holder.

3.2. Access control

In this work, an attribute is defined as a set of elements consisting of the subject, resource, permission, and context. The subject can have various attributes that define their identity. For instance, in the case of Dr. Stacy, attributes can include her name, qualifications, and the name of the clinic she owns. The resource denotes the specific type of data that the subject is attempting to access within the healthcare system. Examples of resources include patient health records or data collected by medical sensor devices. These resources may include information such as device ID, MAC address, owner's decentralized identifier (DID), heart rate, blood oxygen levels, blood pressure, medications, and more. The permission element signifies the specific read or write permissions granted to the holder for accessing the data. Lastly, the context element captures the duration of data accessibility and the event that triggered the request for access.

Once the credential holder has been authenticated with cryptographic proof, the next level of security in the proposed system is access management. Attribute-based access control (ABAC) mechanisms are employed, granting access based on specific attributes. These attributes may contain actual values or information derived through Zero Knowledge Proof (ZKP) protocols. ABAC consists of several functional points. The Policy Enforcement Point (PEP) interprets access requests and enforces the access decisions made by the Policy Decision Point (PDP). In this work, access control policies are derived from smart contracts and leverage information provided by the credential holder. The user

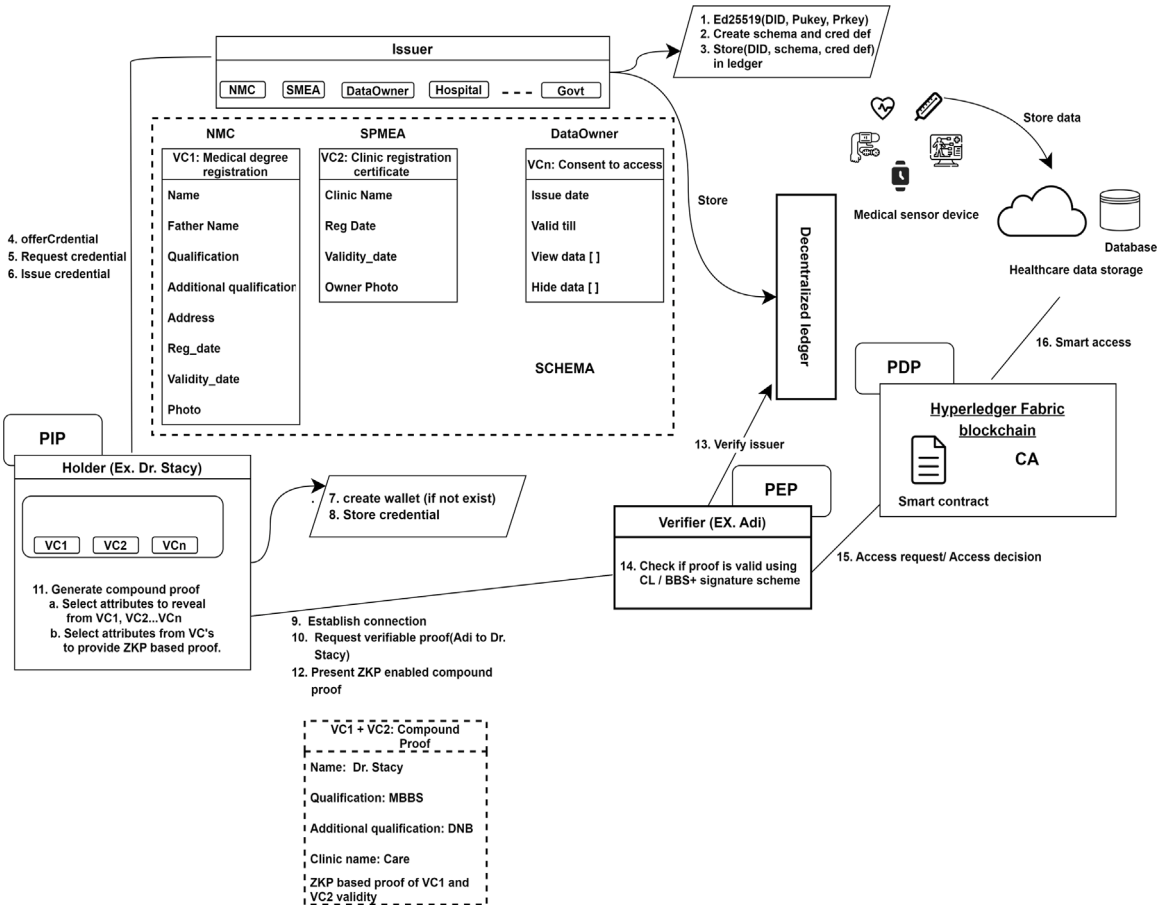

Fig. 3. System architecture for the proposed model.

Table 4
Representation of credentials.

SL.No	Credential	Issuer	Represents
1	Identity document VC	Government Authority	Demographics, identity and citizenship details.
2	Guardian VC	Legal authority	Temporary credential to manage health record.
3	Health history VC	Healthcare service provider,	Past medical history, allergies, family history, psychological illness and nutritional status of the patient.
4	Insurance VC	Insurance agency either government or private	Insurance plan and cover subscribed by the patient.
5	Hospital referral VC	Healthcare service provider	Patient's current medical condition and the type of medication and tests administered.
6	Hospital/clinic Bill VC	Healthcare provider	Medicare bill
7	Identity document VC	Government authority	Residence and citizenship details.
8	Education VC	Medical university	Medical qualification.
9	License VC	Designated authority	License needed to practice medicine or to setup a clinic or hospital.
10	Employment VC	Employer	Work status.
11	Illicit record check VC	Legal authority	Criminal background check status.
12	Patient consent VC	Patient	Patient consent to view their medical data
13	Quality compliance VC	Government recognized quality compliance authority	Quality compliance status of clinic/hospital.
14	Patient Bill Information VC	Patient	Patient's consent to view their medicare bill

wallet (Askar) or the cloud agent (Aries Cloud Agent) acts as the Policy Information Points (PIPs), contributing relevant data to the access control process. To ensure accountability, access requests are stored as transactions on the Hyperledger Fabric decentralized ledger using the RAFT service. This approach facilitates traceability and transparency in the access management process.

As an integral component of the proposed work, the modularization feature of Hyperledger Fabric is employed. This feature facilitates the

creation of separate channels, each with its own distinct set of chaincode containing smart contracts that define access policies. To enhance management, security, and reduce the number of policies/rules needed while maintaining robust access authorization, the following set of rules/policies have been identified:

- Role membership rule: This policy defines the required attributes that a user must possess to obtain membership in the role. It is represented as a boolean function that evaluates whether the rule is satisfied or not. If the rule is satisfied, the function returns '1'; otherwise, it returns '0'.
- Parameterization rule: Based on this policy, users are granted access to resources that align with the verified attributes they present.
- Class rule: The rule defines the specific attributes that a user must possess in order to be classified within a particular category.
- Context rule: Access decisions are made based on the user's access to resources within the given context. The decision to grant or reject access is determined by rules that consider the attributes of the user, the context, and the specific resource involved.
- Delegation rule: Delegation rules are classified into two categories: patients and healthcare providers. In situations where there is an emergency, a patient has the ability to designate an individual to manage their health records temporarily. However, for long-term delegation, distinct policies are necessary. On the other hand, in the case of healthcare service providers, delegation is associated with changes in management responsibilities.

Algorithm 1 Generate codeword

```
Generatecodeword(** details):
E=details[NrOfEntity]
Nr of entity: E
NrOfBits=Ceiling(E/2)
ESeq = append(0, NrOfBits)
for j ← 0 to E − 1 do
    Ecode[j]=ESeq
    ESeq=NextSeq(ESeq)
    C=details[j].length
    NrOfBits=Ceiling(C/2)
    CSeq = append(0, NrOfBits)
    for k ← 0 to C − 1 do
        C[j][K]=CSeq
        CSeq=NextSeq(CSeq)
        SC=details[j][K].length
        NrOfBits=Ceiling(SC/2)
        for m ← 0 to SC − 1 do
            C[j][K][m]=SCSeq
            SCSeq=NextSeq(SCSeq)
        end for
    end for
end for
```

Codewords are generated to represent the combination of claims used in presenting credentials. The algorithm utilized for codeword generation is outlined in Algorithm 1 and its structure is depicted in Fig. 4. The initial bits of the codeword indicate the type of entity involved, such as e1, e2, and e3, representing entities like doctors, healthcare service providers, etc. This is followed by the context and sub-context in which the verifiable credential (VC) is issued.

In cases where claims are derived from multiple contexts, the presented context codeword is a sequence of each context divided by an underscore. For instance, if the entity "doctor" has a codeword of 000, and claims are from three contexts (e.g., education (00), citizenship (01), and work details (11)), the resulting codeword will be 000_00_01_11.

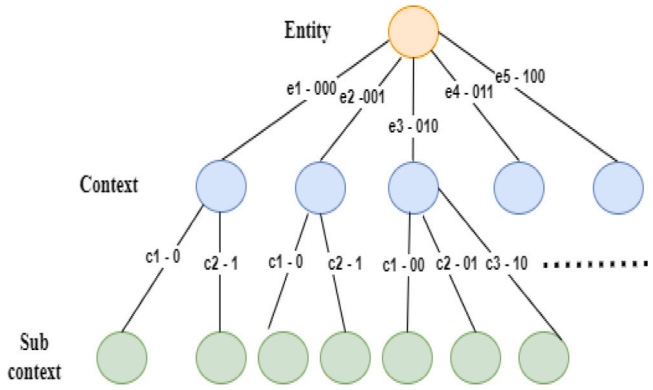

Fig. 4. Codeword generation structure.

The combination of the entity and context codeword forms a codeword for derived credentials (DC). A DC comprises claims derived from multiple VCs. By utilizing a codeword, the privacy of the entity is maintained as specific details are concealed within the codeword, simplifying the implementation of access control mechanisms.

The user/entity identity is given a trust score based on the VC issued by identity providers to improve the ecosystem's trust as the identity is established based on the claims made in the VC. A trust level is calculated to measure how trustworthy the entity is. In a given context, such as education, the accreditations attained by the education institute are compared to the standard accreditations set. Eq. (3) represents the trust score calculation used for the context. As shown in the equation, n represents the number of accreditations considered in the context, $A_i w$ represents the weight assigned to each accreditation where i is the accreditation sequence number and w is the weight assigned to it, and $IA_i w$ means the total weight given to all accreditations considered in the context.

$$AC_{score} = \sum_{i=1}^{n} \frac{A_{iw}}{IA_{iw}} * 100 \tag{3}$$

The Eq. (4) represents the trust score(ϕ) computation for the entity. When calculating the entity trust score, the context used to establish the identity is taken into account. For example, if the doctor is an entity, then citizenship, educational background, and work history are considered to establish identity. P_i denotes the percentage weightage assigned to each context in the equation, and m represents the number of contexts considered to establish identity.

$$\phi = \sum_{i=1}^{m} AC_{i,score} * P_i \tag{4}$$

To illustrate, trust scores are computed for demonstration purposes by assigning significance to each Verifiable Credential (VC), denoted as α_i. The standard VC count for an entity ranges from 1 to n, and the entity's VC possession ranges from 1 to m, where $m \leqslant n$. Eq. (5) indicates how the cumulative significance(Γ) is obtained for the standard VC given in Table 5. The weight for each VC(β_i) is calculated using Eq. (6) and the obtained values are represented in Table 5. Using the assigned weight for each Verifiable Credential (VC), trust scores based on VC significance($\tilde{\phi}$) are calculated, taking into account the quantity and nature of VCs held by the entity as shown in Eq. (7). This trust score mechanism helps to increase trust in the entity's identification and authenticity.

$$\Gamma = \sum_{i=1}^{n} \alpha_i \tag{5}$$

$$\beta_i = \frac{\alpha_i}{\sum_{i=1}^{n} \alpha_i} \tag{6}$$

Table 5
Table representing weight calculation for VC.

Entity	Standard VC set	α_i	Γ	β_i
Doctor	Identity document(vc1)	4.01		0.179
	Medicine degree(vc2)	4.77		0.213
	License to practice(vc3)	4.82	22.34	0.215
	Illicit record check(vc4)	4.43		0.198
	Employment(vc5)	4.31		0.192
Patient	Identity document(vc1)	4.14		0.235
	Health history(vc2)	4.7	17.59	0.267
	Health insurance(vc3)	4.31		0.245
	Guardian(vc4)	4.44		0.252
Healthcare Service center	Registered(vc1)	4.62		0.327
	License to operate(vc2)	4.73	14.11	0.335
	Compliance with quality standards(vc3)	4.76		0.337
Research center	Registered(vc1)	4.56		0.328
	License to operate(vc2)	4.55	13.88	0.327
	Compliance with quality standards(vc3)	4.73		0.340
Insurance agency	Registered(vc1)	4.60		0.334
	License to operate(vc2)	4.50	13.77	0.326
	Compliance with quality standards(vc3)	4.67		0.339

$$\widetilde{\phi} = (\sum_{i=1}^{m} \beta_i) * 100 \tag{7}$$

As stated in the contribution section the proposed work focuses on decentralized key recovery. However, sharing private keys even over the secure channel is not safe; it is therefore recommended to use derived keys in place [60].

3.3. Key recovery

In Fig. 5, the sequence of the activities of entity registration is shown. An entity first installs a wallet application to store its verifiable credentials and private key in the SSI-based system. A user initiates the registration process by submitting mobile or email-based OTP or biometric data to the service agent or a combination of both. The service agent could be the service provider of the wallet. Following authentication, the service agent asks the user for the four-digit PIN in order to recover the key in the future. The registration process involves the service agent providing a private DID for communication. The entity generates a public and private key and a private DID to communicate with the service agent. It also provides DIDs for social trustees. According to the proposed system, trustees could be parents, siblings, or close friends. Trustees receive information about requests from service agents. Upon acceptance, the biometric data, email, mobile number, PIN, and trustees' DIDs will be encoded and stored off-chain by the service agent. A notification is sent to the entity about the trustee's acceptance. Afterward, the entity generates derived keys and sends each key along with the Pedersen commit to a different trustee.

SSI-based identity management systems store credentials in a wallet, and the owner can add new credentials to a wallet over time. Consequently, a wallet backup is necessary to restore the wallet content if the owner loses the wallet; hence, in the proposed system, the Algorithm 2 outlines the steps involved in sharing the wallet content. First, the wallet owner needs to encrypt the wallet content using the public key Pu_{RA} and divide it into N pieces. N represents the number of trustees to maintain the backup data. Then, before transmitting, the data is encrypted using the public key Pu_{Ai} of the trustee. Fig. 6 illustrates the flow of the proposed share wallet data algorithm.

Algorithm 3 shows the steps behind sharing the key with the trustees. In Fig. 5 the registration process is explained. Once the entity authenticates itself to the service agent using PIN and OTP or biometric data, the process of sharing the recovery key starts. Firstly the four-digit PIN is hashed with the SHA256 algorithm and XOR with the private key Pr_{RA}. The result of XOR is shifted left circularly(CLS) to improve the security level, where each digit of PIN represents the number of bytes

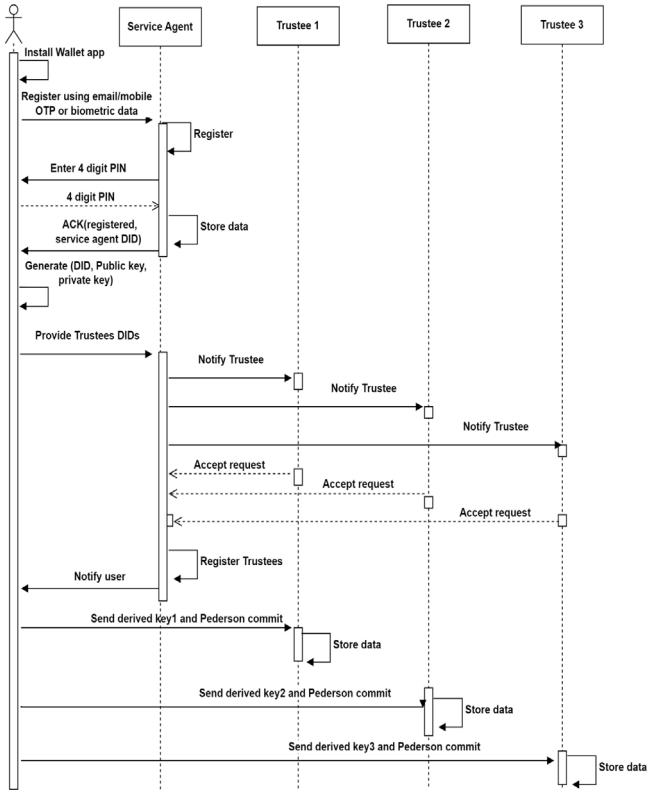

Fig. 5. Sequence diagram for entity registration.

Algorithm 2 Share wallet data

ECC equation $y^2 = x^3 + ax + b$
$(Pu_{RA}, Pr_{RA}) \leftarrow KeyGen$
Let $S_A = wallet(data)$
$C_A \leftarrow Encrypt(S_A, Pu_{RA})$
Input N
$(n_0, n_1, n_2, ..., n_{N-1}) = C_A/N$
for $i \leftarrow 0$ to $N-1$ **do**
  $P[i] \leftarrow n_i$
  $S_i \leftarrow Encrypt(P[i], Pu_{Ai})$
end for
Share $(S_0, S_1, S_2, ...S_{N-1})$ to trustee

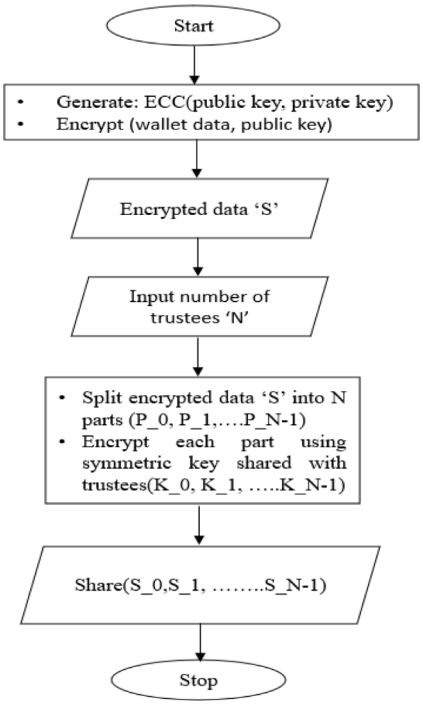

Fig. 6. Flowchart for the proposed share wallet data algorithm.

to be shifted, and after each shift, the first byte is toggled. The Shamir secret sharing algorithm is used where the output of CLS is stored in the initial coefficient C_0 of the chosen polynomial. Depending on the number of trustees, distinct y_i(secret) values are calculated. Finally, to authenticate the entity during key recovery, the Pedersen commit x is applied. The combination of encoded commits C_{mr} and y_i are sent to the trustees. The flowchart in Fig. 7 illustrates how a proposed share recovery key algorithm works.

The trustee-based key recovery mechanism is depicted in Fig. 8. Key recovery is initiated by contacting the service agent. The service agent authenticates the entity using the PIN and OTP or biometric data stored during registration. The service agent retrieves the entity's updated device ID and the trustee DID on successful authentication and notifies the trustees about key recovery. The trustee who wishes to engage in the key recovery process sends an authentication request. Through the sharing of the commit, the entity establishes itself. The participating trustee shares the derived key with the entity after successful authentication. It is then possible for the entity to regenerate the recovery key if the number of participating trustees exceeds the threshold value. The threshold value is determined by the polynomial degree selected during the key sharing process.

The Algorithm 4 represents the trustee-based key recovery process. By revealing the commit x, r to the trustee, the entity authenticates itself. Upon successful authentication, the trustee sends the derived key y_i to the entity, which then uses Lagrange interpolation to obtain the encoded recovery key. Circular right shift (CRS) is used on the encoded key based on the PIN sequence, and the first byte is toggled on each shift. To recover the key, CRS output is then XOR with the hash of the PIN.

The flowchart for the Algorithm 4 is presented in Fig. 9. This algorithm considers circular shift, toggle, and XOR operations, due to their reversible properties, which are essential for key recovery. In order to ensure the confidentiality of the key, hashing, and Langrage interpolation are used, while Pederson commit is used to authenticate the user at the time of key recovery.

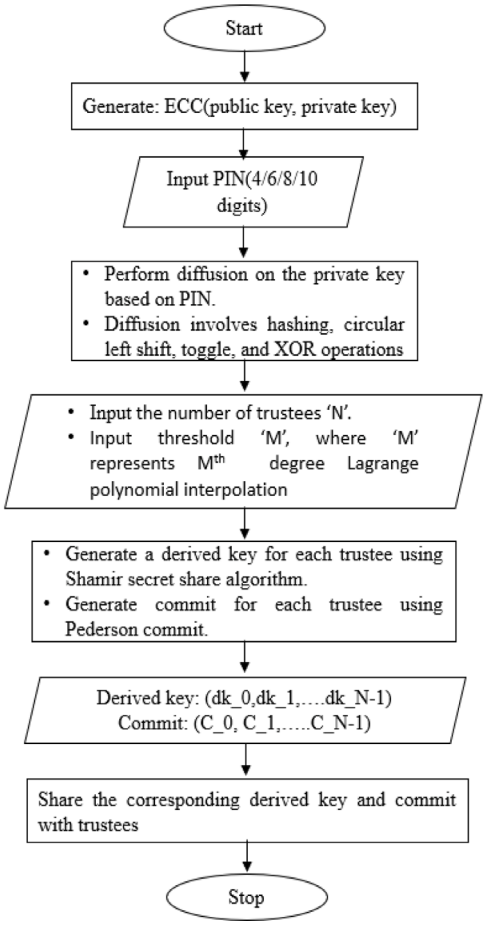

Fig. 7. Flowchart for the proposed share recovery key algorithm.

4. Implementation and result

The proposed work is executed on a Windows 11 system with 16 GB of RAM and an AMD Ryzen 7, 5800H processor. The infrastructure setup utilizes Ubuntu 18.04 as the operating system. To ensure portability, flexibility, and easy configuration of the docker containers, the von-network is operated using Docker images and docker-compose. Open-source software tools such as git bash, npm, and node are employed in this work. Git bash enables the execution of Linux commands within the Windows environment. The npm package manager and node framework are utilized as dependencies. The Hyperledger Aries toolkit is leveraged to interact with the Indy test network. Specifically, the Python version of the Aries Cloud Agent is employed to create schemas for issuers and manage end users' credentials. For privacy and performance reasons, Hyperledger Fabric, a permissioned private blockchain, is chosen over Ethereum. It provides enhanced data privacy and better overall performance for the proposed work.

The proposed system utilizes Von-network, a Hyperledger Indy test network, which is used to store issuer DIDs, credential schema, and credential definitions which are then used for verification of the issuer. Transactions related to medical data access requests are stored in Hyperledger Fabric. Through the use of a separate ledger for managing identity and healthcare data access, better privacy is ensured for users. Fig. 12 illustrates the time required to establish the necessary infrastructure for identity management. It is observed that it takes 11.15 s to start von-Network, activate the Aries cloud agent in 5.08 s, publish the schema, and register the DID on the ledger in 8.95 s, 0.06 s to create invitations. This invitation is used to connect with other agents within the ecosystem. Once the infrastructure is set up, the issuer

Algorithm 3 Share Recovery Key

ECC equation $y^2 = x^3 + ax + b$
Public: p, q
$(Pu_{RA}, Pr_{RA}) \leftarrow KeyGen$
$Authenticate([PIN, OTP]/biometric)$
$H_A \leftarrow SHA256(PIN)$
$H'_A \leftarrow H_A$ XOR Pr_{RA}
PIN ← Input(4 digit passcode)
for $i \leftarrow 0$ to 4 **do**
  $d[i] \leftarrow extract(PIN)_i$
  $H_A \leftarrow CLS(H'_A, d[i])$
  $H'_A \leftarrow Toggle(H_A, 1)$
end for
Choose prime p
Input $n, k \in N, l \leq k, x_i, y_i \in Z/pZ, 1 \leq i \leq l$
x_i are pairwise distinct
Choose polynomial coefficients: C ∈ $(Z/pZ)[X]$ of degree ≤ k-1
$C_0 \leftarrow H'_A$
Generate polynomial C(X)
$C(X) = C_{k-1}x^{k-1} + C_{k-2}x^{k-2} + ... + C_2x^2 + C_1x + C_0$
Compute $y_i = C(i)$, $1 \leq i \leq n$
Select q such that q divides $p - 1$
g is a generator of multiplicative group Z_p^*
$a \leftarrow Hash(PIN)$
if $a \neq prime$ **then**
  $ChooseNearestPrime(a)$
end if
$h \leftarrow g^a \bmod p$
$r \leftarrow ChooseNearestPrime(HASH(PIN) \bmod q)$
Commit: $x \in Z_q$
$C_{mr} \leftarrow g^x h^r \bmod p$
Distribute C_{mr}, y_i to trusted entity

Algorithm 4 Decentralized key recovery

ECC equation $y^2 = x^3 + ax + b$
Public: p, q
$Compute(H_A, a, r)$
Reveal: x, r to receiver
Verify:
if then $C_{mr} = g^x h^r \ mod \ p$
  Collect: $y_i, k \leq i \leq n$
  Apply: Lagrange interpolation on y_i
  Compute: $C(0) = \sum_{i=1}^{k} y_i \prod_{j=1 i \neq j}^{k} \frac{x_j}{x_j - x_i}$
  $H'_A \leftarrow C_0$
  PIN ← Input(PIN)
  for $i \leftarrow 0$ to 4 **do**
    $d[i] \leftarrow Rextract(PIN)_i$
    $H_A \leftarrow Toggle(H'_A, 1)$
    $H'_A \leftarrow CRS(H_A, d[i])$
  end for
  $H_A \leftarrow SHA256(PIN)$
  $Pr_{RA} \leftarrow H_A$ XOR H'_A
end if

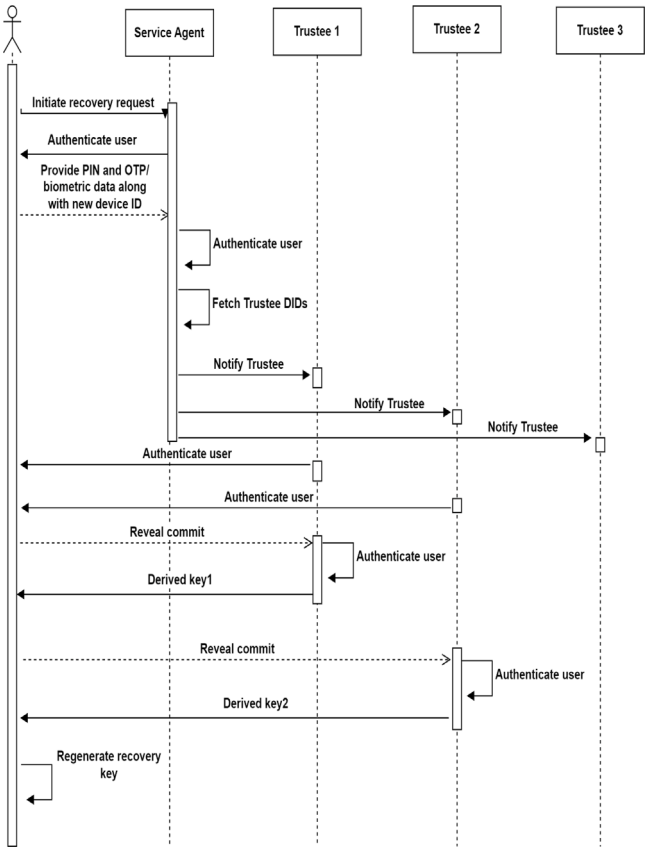

Fig. 8. Sequence diagram for key recovery.

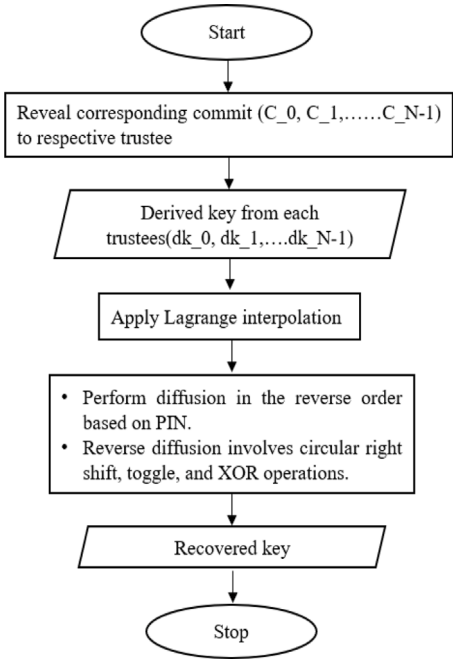

Fig. 9. Flowchart for the proposed decentralized key recovery algorithm.

agents can issue credentials to the requestor. The observed connection time is 0.2 s. After a successful connection, the issuer can issue a cryptographically verifiable credential comprising one or more claims. The issued credentials will have a validity period that could vary from a few hours to a lifetime. The time taken to issue such credentials is 0.7 s. The requestor can then use the acquired credentials to authenticate their identity. It is done by presenting proof containing claims from one credential or a compound cryptographic proof containing claims from multiple credentials. The observed time for single proof presentation and verification is 0.72 s and 0.82 s for compound proof presentation, as shown in Fig. 13. The attributes are selectively disclosed based on the preferences of the requestor/user/holder when providing the proof,

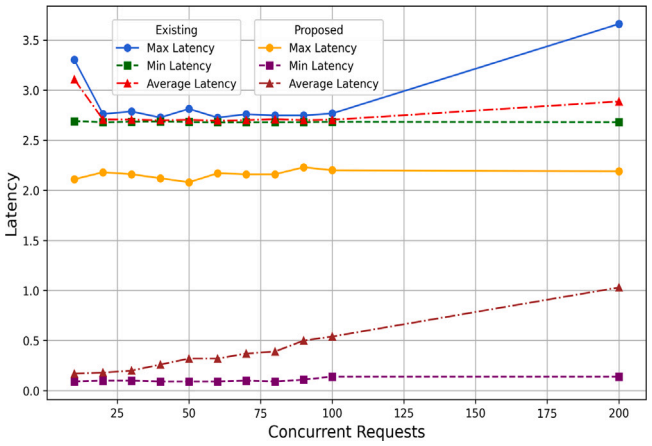

Fig. 10. Analyzing the performance of record insertion transactions in the proposed and existing systems.

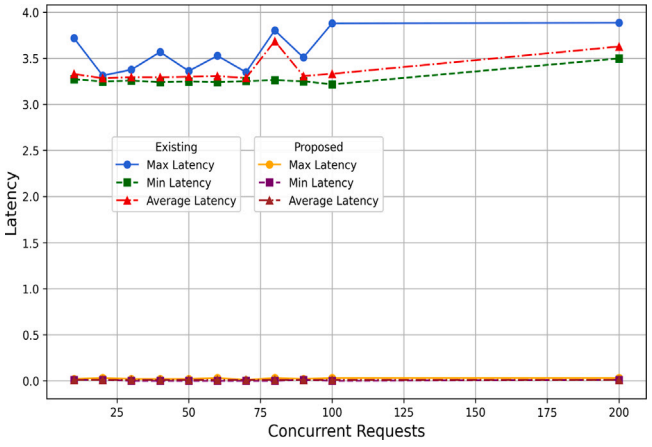

Fig. 11. Analyzing the performance of record access transactions in the proposed and existing systems.

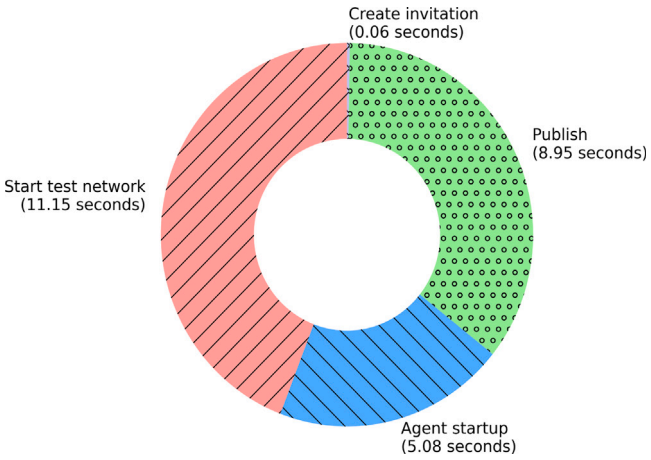

Fig. 12. Infrastructure setup (in seconds).

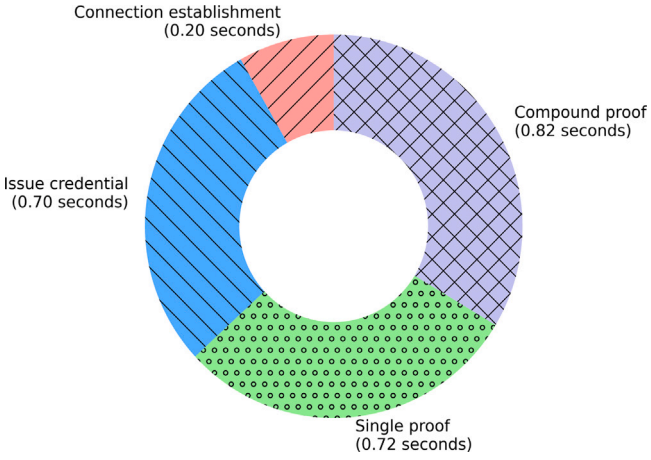

Fig. 13. Time taken to connect, issue and verify credential(in seconds).

and for a few of these selected attributes, the Zero Knowledge-based predicate method is used. The proposed project enhances ecosystem security through the integration of a dual-layer security approach. In the initial layer, verifiable credentials are employed to authenticate claims, while in the second layer, individuals seeking data access are required to possess an x.509 certificate issued by the organization's certificate authority. Unlike most existing approaches, which typically employ either verifiable credentials or x.509 certificates, our approach combines both for heightened security. The performance of the proposed work for access control management is analyzed by integrating the Hyperledger Caliper tool with Hyperledger Fabric. There are two organizations with two peers each, a RAFT ordering service is used the benchmark round is set to 4, the Transaction Per Second (TPS) is set to 50 during the test [54,55], and the transaction count varies from 10, 20, 30, …, 100, 200. The results of the average transaction send rate, latency, and CPU utilization are shown in Table 6. As shown in the table, the throughput for the send rate is quite good, the maximum CPU utilization is less than 13 percent, and the maximum latency is not more than 8.5 s.

Figs. 10 and 11 present the latency comparison of the proposed work with the work presented in [54,61]. Fig. 10 illustrates a comparison of maximum, minimum, and average latency for the insert record transaction across varying concurrent user counts from 10 to 200. Similarly, Fig. 11 presents a latency comparison for the fetch record transaction. As depicted in the figures, the proposed approach outperforms existing methods.

In the proposed solution, transaction ordering is achieved through the Raft service, enabling multiple organizations to manage orders and define policies. These ordered transactions can become part of the subnetwork referred to as a channel, thereby supporting decentralized ordering services. In contrast, the Kafka ordering service relies on the third-party ZooKeeper and operates in a centralized manner.

In addition to establishing identity through compound proof for claims in verifiable credentials and implementing smart contract-based access policies for data within the Fabric network, the project also introduces a key recovery algorithm for wallet keys. Credentials for the proposed key recovery algorithm are stored in a JSON file in the wallet, so they must be encrypted before being shared with trustees. The x-axis of Fig. 14 represents the size/number of claims in the credentials, and the y-axis represents the time it takes to encrypt and decrypt them, which indicates that 64 claims can be encrypted and decrypted in less than 0.25 s. The proposed algorithm relies on trustees to recover keys, so a time estimate for encrypting/encoding the credentials to be shared with 'n' trustees is shown in Fig. 15, where 'n' is selected from 4, 6, 8 and 10. For encoding 10 trustees, the performance is approximately 1 s. A user must use a PIN in order to share a secret, Fig. 16 shows how long it takes to generate a hash code (SHA(256)), secret, and commit for an 'n' digit PIN, where 'n' can be 4, 6, 8, and 10. Fig. 17 shows the result of key recovery(Recovery) and commit reveal(E_secret) for 'n' digit PIN. The time taken to perform the proposed key share and recovery algorithm is less than 0.5 s (excluding encoding time). The key recovery method outlined in the research has distinct advantages over existing

Table 6
Performance metric generated using Caliper for Fabric.

	Send rate	Max latency (s)	Min latency (s)	Avg latency(s)	Throughput(TPS)	CPU% (max)	CPU% (avg)
Insert record	94.99	2.16	0.10	0.34	89.16	7.05	4.87
Query/access single record	429.34	0.02	0.002	0.01	429.13	12.22	7.95
Query/access multiple record	8.48	8.27	0.24	6.95	8.42	2.80	1.23

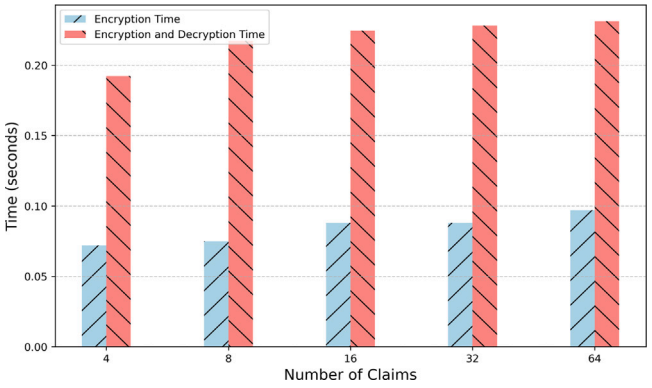

Fig. 14. Performance of encoding wallet data for 'n' number of claims.

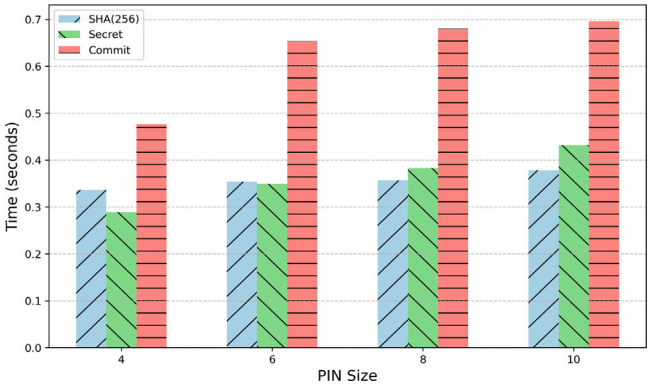

Fig. 16. Performance of the proposed key sharing algorithm.

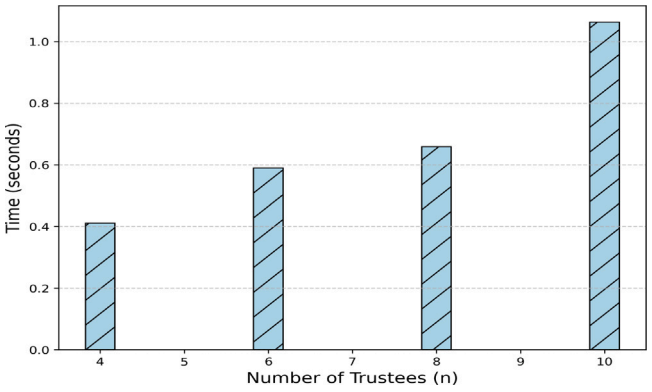

Fig. 15. Performance of encoding for 'n' number of trustees.

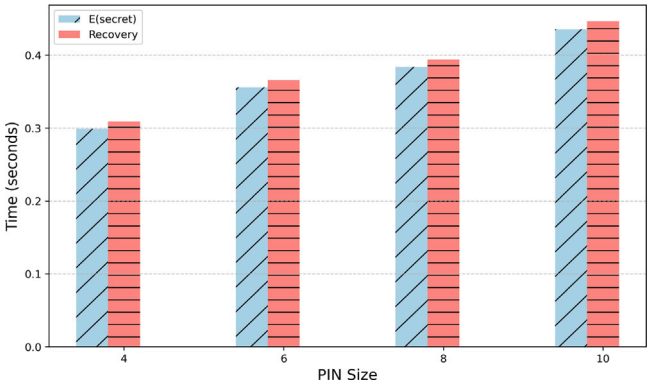

Fig. 17. Performance of the proposed key recovery algorithm.

approaches [22,28,43–45]. Unlike methods that depend on third parties for recovery, or those lacking a user-centric approach, or the somewhat cumbersome social recovery method employed by the work presented in [29,42], the proposed approach offers a streamlined solution. In this approach, the Pederson commitment is used to authenticate the user, simplifying the key recovery process for end-users who only need to remember a PIN, ensuring an easier and more user-friendly experience without relying on the third party for the key recovery process.

5. Security analysis

The proposed algorithm is verified for secrecy and security breaches using the threat model designed using the modeling tool OWASP threat dragon [62,63].

In the envisioned healthcare ecosystem, a comprehensive threat model, illustrated in Fig. 18, has been devised to safeguard the confidentiality and accuracy of sensitive healthcare information and stakeholder identities. The involved parties, including doctors, patients, hospitals, government agencies, insurance companies, and research institutes, utilize verifiable credentials obtained from a trusted authority. The computation of a trust store further enhances the credibility of the identity.

For a more detailed insight, refer to Table 7, which outlines the primary threat actor like a credential forger, external attackers, and insiders with malicious intent followed by the principal threat categories like spoofing, tampering, information disclosure, and elevation of privilege and their impact on the healthcare ecosystem are recognized within the proposed framework and the corresponding strategies enacted to mitigate these potential risks. Table 8 displays symbols along with their corresponding descriptions. These symbols are utilized in Eqs. (8)–(19).

Mitigation Strategy:

- Authentication: In order to address impersonation and prevent unauthorized access, the authentication process relies on the presentation of claims in the form of verifiable credentials. These credentials are digitally signed by both the trusted issuer and the credential owner, ensuring their authenticity. In the event of key recovery, the proposed work employs a PIN-based Pedersen commitment scheme to authenticate the user. During recovery, the user is required to disclose the committed message associated with the derived key share. This layered approach ensures a

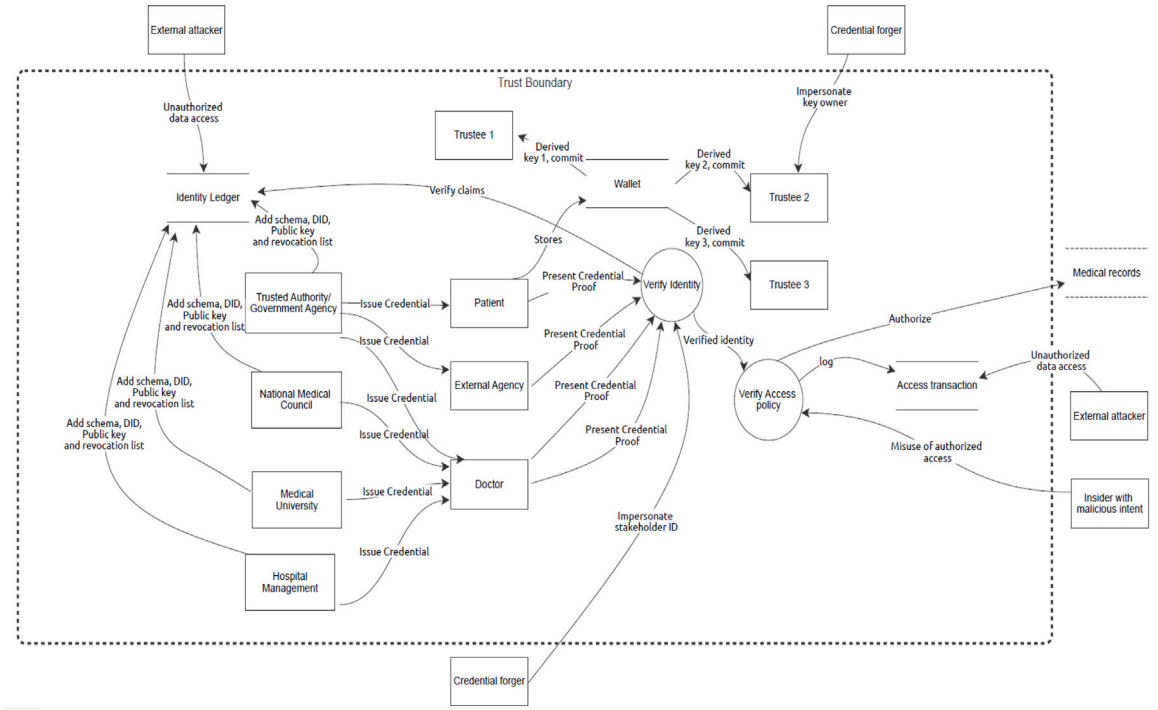

Fig. 18. Threat model for the proposed model.

Table 7
Threat mapping and mitigation strategy for the proposed work.

Threat actor	Category	Threat	Impact	Mitigation strategy
Credential Forger	Spoofing	Impersonation of stakeholder identity	1. Unauthorized access to healthcare data 2. Unauthorized access to derived key	1. Authentication using VC 2. Credential proof contains digital signature of owner and issuer 3. Commit is used to authenticate user during key recovery
External attacker	Tampering	Data manipulation	1. Tampering VC schema 2. Tampering healthcare access transaction	Blockchain based integrity check
	Information disclosure	1. Unauthorized data access 2. Compromised key recovery	1. Exposure to sensitive healthcare data 2. Exposure to sensitive identity data 3. Exposure to wallet key	1. Encryption of data 2. Smart contract based access policy 3. Zero knowledge-based data sharing 4. Shamir secret share and PIN based social recovery
Insider with malicious intent	Elevation of Privilege	Unauthorized Escalation	Unauthorized access to sensitive data	Smart contract policy based on role and attribute access control

Table 8
Symbol and their description.

Symbol	Description
$\bar{C}$	The collection of credentials owned by the holder
$\{VC_1, VC_2, VC_3 ... VC_n\}$	Verifiable credential issued by issuer 1, issuer 2, ….issuer n
$(c_1{}^1, c_2{}^1, c_3{}^1 ... c_m{}^1)$	Denotes an assertion within the verifiable credentials issued by Issuer 1
DS_1	Represents issuer 1 digital signature
SK_1	Represents issuer 1 private key
$\mathbb{P}(c_1{}^1)$	Represents proof of claim $c_1{}^1$
$\widetilde{SK}$	Represents the owner's private key
$\widetilde{DS}$	Denotes the owner's digital signature
VP	Verifiable presentation containing proof of claims from different verifiable credentials
DS_2	Represents issuer 2 digital signature
$H(b_n)$	Hash of nth block
$Prev\_Hash_{n-1}$	Hash of $n-1^{th}$ block
Tr_n	nth block transactions
η_n	Nounce of nth block
CL_{expiry}	Clinic License expiry date
C_{date}	Current date
$\{r_1, r_2, r_3, \ldots..\}$	Represents role membership requirements
$\{p_1, p_2, p_3, \ldots.\}$	Represent policies to grant access to the resources
$\{cl_1, cl_2, cl_3, \ldots.\}$	The rule specifies the attributes that a user must have to be part of a specific class
$\{ct_1, ct_2, ct_3, \ldots.\}$	Establishes a rule for accessing a resource within a provided context

secure and reliable authentication process.

$$\bar{C} = \{VC_1, VC_2, VC_3 ... VC_n\} \tag{8}$$

where n represents the number of VCs

$$VC_1 = \{({c_1}^1, {c_2}^1, {c_3}^1 ... {c_m}^1), DS_1\} \tag{9}$$

where m represents the number of claims

$$DS_1 = \{Encrypt({c_1}^1, {c_2}^1, {c_3}^1 ... {c_m}^1), SK_1\} \tag{10}$$

$$\widetilde{DS} = \{Encrypt(\mathbb{P}({c_1}^1), \mathbb{P}({c_3}^1), \mathbb{P}({c_3}^2)), \widetilde{SK}\} \tag{11}$$

$$VP = \{(\mathbb{P}({c_1}^1), \mathbb{P}({c_3}^1), \mathbb{P}({c_3}^2)), \widetilde{DS}, DS_1, DS_2\} \tag{12}$$

As depicted in Algorithm 3, $\{C_{mr} \leftarrow g^x h^r \mod p\}$ symbolizes the act of committing and disseminating the commit C_{mr} and the resulting derived key y_i to a trusted entity as part of the key sharing process. Here, i signifies the identifier of the trustee. The strength of this commitment relies on the discrete logarithm problem.

- Integrity: To guarantee the integrity of both verifiable credentials and healthcare data access transactions, the proposed work relies on an immutable ledger. Hyperledger Indy is utilized for managing identity credentials, while Hyperledger Fabric is employed to oversee access transactions. This ensures a secure and tamper-proof environment for maintaining the integrity of crucial data and transactions.

$$H(b_n) = Hash(Prev\_Hash_{n-1} + Tr_n + \eta_n) \tag{13}$$

- Minimal Data Disclosure and Confidentiality: When verifying credentials, the proposed work implements predicate-based Zero Knowledge Proofs(ZKP) using CL signature scheme [64]. This approach allows for conveying sensitive information without actual data exposure. As an example, individuals have the ability to provide assertions regarding their clinic license status while safeguarding specific particulars. To establish a predicate-based Zero-Knowledge Proof (ZKP) concerning clinic license status, the software agent employed by the clinician undertakes the following steps: It selects a random value p, computes g^p, and determines $h^{CL_{expiry}}$ where g and h denote the group generators. Subsequently, the agent shares the values g^p and $h^{CL_{expiry}}$ with the verifier. The clinician's software agent then crafts a signature $\widetilde{s}$ using the private key SK. The verifier's task involves validating if $g^{\widetilde{s}}.PK^{CL_{expiry}}$ confirms the commitment, alongside confirming the stipulation $CL_{expiry} > C_{date}$. Importantly, data remains encrypted during transmission, and credentials are further encrypted and securely maintained within the wallet via the utilization of the private key SK.
  To enhance confidentiality, the work employs a combination of Shamir's Secret Sharing and PIN-based diffusion techniques to derive keys as shown in algorithm 3 and 4. Table 9 presents the comprehensive analysis of the proposed algorithms 3 and 4. This approach safeguards the confidentiality of keys, ensuring secure access. Additionally, fine-grained access policies are defined to regulate data access. Only users who meet specific access criteria are permitted to access the data, reinforcing confidentiality and minimizing unnecessary data exposure.

$$Role_{rule} = \{r_1, r_2, r_3 .....\} \tag{14}$$

$$Parameterization_{rule} = \{p_1, p_2, p_3 .....\} \tag{15}$$

$$Class_{rule} = \{cl_1, cl_2, cl_3 .....\} \tag{16}$$

$$Context_{rule} = \{ct_1, ct_2, ct_3 .....\} \tag{17}$$

$$Data_{attr} = \{d_1, d_2, d_3 .....\} \tag{18}$$

$$D_{min} = \{\{d_1, d_3, d_6\} | \{r_1 \Lambda \{p_2 \Lambda p_3\} \Lambda cl_1 \Lambda \{ct_2 \| ct_3\}\}\} \tag{19}$$

Referring to the illustration provided in Eq. (19), the access requester obtains permission to access the data attributes d_1, d_2, d_3 solely if certain conditions are met.
These conditions encompass fulfilling the membership requirement for the role r_1 adhering to the parameterization stipulations p_2, p_3, being a member of class $c1_1$, and satisfying either context rule ct_2 or ct_3. This meticulous arrangement ensures that the principle of data minimization is upheld.

- Preventing Unauthorized Privilege Elevation: While user identity is authenticated through credentials, access to requested data is subject to adherence to the policies specified in the smart contract. This ensures that even with authenticated credentials, users must fulfill contract-defined criteria to gain access, effectively preventing unauthorized privilege elevation.

Conclusion

The Identity Resilience and key recovery-enabled framework is specifically tailored to the healthcare sector, aiming to foster trust, uphold privacy standards, and ensure the secure handling of sensitive healthcare data through the implementation of a self-sovereign identity framework. This framework empowers individuals by placing control over their data in their hands. By incorporating digital technologies such as verifiable credentials, smart contracts, and blockchain technology, the system brings notable benefits to healthcare. The crucial aspect of trust in identity verification is imbibed into the framework. The fine-grained access control enabled by the system ensures robust privacy protection for healthcare users, safeguarding their sensitive data. The proposed owner-centric identity management ensures the security of users' credentials. This not only enhances data security but also simplifies the recovery process in case of loss or compromise, without relying on any third party for recovery assistance. The ecosystem is validated for security breaches and is capable of safeguarding sensitive identity and healthcare information. By enforcing controlled and authorized access, the system contributes to maintaining the privacy and confidentiality of healthcare information. Moreover, the framework incorporates selective disclosure of attributes and predicate-based zero-knowledge proof, which significantly enhances privacy protection measures. This advancement ensures that only necessary information is shared, preserving the privacy of individuals while enabling the exchange of relevant healthcare data.

CRediT authorship contribution statement

Chetana Pujari: Conceptualization, Methodology, Software, Writing – original draft. **Balachandra Muniyal:** Conceptualization, Review draft preparation. **Chandrakala C. B:** Conceptualization, Review draft preparation. **Anirudha Rao:** Software. **Vasudeva Sadiname:** Conceptualization. **Muttukrishnan Rajarajan:** Conceptualization, Review draft preparation.

Declaration of competing interest

None Declared.

Table 9
Comprehensive analysis of the proposed Key recovery algorithm.

Description	Security measures & rationale	Analysis
PIN Complexity	Enhanced security through increased PIN digits, thwarting brute force attacks	4-digit PIN: 10,000 possible combinations
SHA-256 Hashing	Robust collision and preimage resistance, safeguarding hash integrity	Hash length: 256 bits
	Collisions unlikely due to immense search space	Number of attempts needed for 50% collision chance: ~2^128
XOR & Iterations	Multi-layered obfuscation, ECC private key prerequisite for reverse-engineering	ECC key length: 256 bits
Shamir Secret Sharing with AES	Preventing unauthorized key recovery through threshold-based distribution of encrypted shares	Threshold: 5 shares, requiring 5 shares for ECC private key recovery and AES encryption enhances confidentiality
Langrange Interpolation	Secure ECC key reconstruction, enforcing share threshold	Share threshold: 5 shares
	Prevents key reconstruction with fewer shares, enhancing security	Minimum shares required for ECC private key reconstruction
Pedersen Commitment(PIN based) & Secure Hash	Concealing shared key values	Encrypted the shared derived key using AES
	Hides share values, preventing leakage during distribution	
	Resistance to discrete logarithm problems adds complexity to attacks	Attacker faces discrete log difficulty in breaking PIN based commitment

References

[1] Medical_board_of_Australia, Unqualified medical intern at Bankstown hospital convicted, 2022, https://www.medicalboard.gov.au/News/22-01-20--Fake-Bankstown-doc-convicted.aspx, [Online: Accessed on 16 June 2022].

[2] AP_news, Fake doctor signed 600 patients' medical pot paperwork, 2020, https://apnews.com/article/health-c29aafe8a675a842f2824a89ae85e299, [Online: Accessed on 04 April 2022].

[3] ABDM, e-hospital is ayushman bharat digital mission(ABDM) compliant, 2022, https://ehospital.nic.in/ehospitalsso/, [Online: Accessed on 15 April 2022].

[4] NHS, NHS services, 2022, https://www.nhs.uk/nhs-services/, [Online: Accessed on 05 May 2022].

[5] Australian_Government, Getting started with digital health, 2022, https://www.servicesaustralia.gov.au/getting-started-with-digital-health?context=20, [Online: Accessed on 05 April 2022].

[6] Department_of_commerce_USA, Health IT, 2022, https://www.trade.gov/country-commercial-guides/japan-health-it, [Online: Accessed on 06 April 2022].

[7] Peng Zhang, Jules White, Douglas C. Schmidt, Gunther Lenz, S. Trent Rosenbloom, FHIRChain: Applying blockchain to securely and scalably share clinical data, Comput. Struct. Biotechnol. J. 16 (2018) 267–278.

[8] Bahar Houtan, et al., A survey on blockchain-based self-sovereign patient identity in healthcare, IEEE Access 8 (2020) 90478–90494.

[9] D.T. Harrell, Technical design and development of a self-sovereign identity management platform for patient-centric healthcare using blockchain technology, Blockchain Healthc. Today 5 (2022).

[10] J. Andrew, Deva Priya Isravel, K. Martin Sagayam, Bharat Bhushan, Yuichi Sei, Jennifer Eunice, Blockchain for healthcare systems: Architecture, security challenges, trends and future directions, J. Netw. Comput. Appl. 215 (2023) 103633.

[11] Andreas Holzinger, Anna Saranti, Anne-Christin Hauschild, Jacqueline Beinecke, Dominik Heider, Richard Roettger, Heimo Mueller, Jan Baumbach, Bastian Pfeifer, Human-in-the-loop integration with domain-knowledge graphs for explainable federated deep learning, in: Lecture Notes in Computer Science (LNCS), 14065, Springer, 2023, pp. 45–64.

[12] James Brogan, Immanuel Baskaran, Navin Ramachandran, Authenticating health activity data using distributed ledger technologies, Comput. Struct. Biotechnol. J. 16 (2018) 257–266.

[13] Alexandre Siqueira, Arlindo Flavio Da Conceição, Vladimir Rocha, Blockchains and self-sovereign identities applied to healthcare solutions: A systematic review, 2021, CoRR arXiv:2104.12298.

[14] Hussain Seh Adil, et al., Healthcare data breaches: Insights and implications, Healthcare (Basel) 8 (2) (2020).

[15] Andreas Holzinger, Matthias Dehmer, Frank Emmert-Streib, Rita Cucchiara, Isabelle Augenstein, Javier Del Ser, Wojciech Samek, Igor Jurisica, Natalia Díaz-Rodríguez, Information fusion as an integrative cross-cutting enabler to achieve robust, explainable, and trustworthy medical artificial intelligence, Inf. Fusion 79 (2022) 263–278.

[16] Trust_Over_IP_Foudation, The trust over ip model, 2022, https://trustoverip.org/, [Online: Accessed on 08 May 2022].

[17] Yogachandran Rahulamathavan, et al., Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption, in: 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2017, pp. 1–6, http://dx.doi.org/10.1109/ANTS.2017.8384164.

[18] Rafael Belchior, et al., SSIBAC: Self-sovereign identity based access control, in: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020, pp. 1935–1943, http://dx.doi.org/10.1109/TrustCom50675.2020.00264.

[19] Sudip Misra, et al., Blockchain at the edge: Performance of resource-constrained IoT networks, IEEE Trans. Parallel Distrib. Syst. 32 (1) (2021) 174–183.

[20] Kwame Omono Asamoah, et al., Zero-chain: A blockchain-based identity for digital city operating system, IEEE Internet Things J. 7 (10) (2020) 10336–10346.

[21] Malik Sidra, et al., TradeChain: Decoupling traceability and identity inblockchain enabled supply chains, 2021, CoRR arXiv:2105.11217.

[22] Fennie Wang, Primavera De Filippi, Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion, Front. Blockchain 2 (28) (2020).

[23] Michael Kuperberg, Blockchain-based identity management: A survey from the enterprise and ecosystem perspective, IEEE Trans. Eng. Manage. 67 (4) (2020) 1008–1027.

[24] Jayasree Sengupta, Sushmita Ruj, Sipra Das Bit, A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT, J. Netw. Comput. Appl. 149 (2020) 102481.

[25] Shantanu Pal, Internet of Things and Access Control, Springer Nature, 2021.

[26] Georgios Keramidas, Nikolaos Voros, Michael Hübner, Components and Services for IoT Platforms Paving the Way for IoT Standards, Springer International Publishing, Switzerland, 2017.

[27] Threatscape, MEDJACK.4 Medical Device Hijacking, 2022, https://www.threatscape.com/trapx-medjack-medical-device-hijacking/, [Online: Accessed on 26 May 2022].

[28] Taehoon Kim, Wonbin Kim, Daehee Seo, Imyeong Lee, Secure encapsulation schemes using key recovery system in iomt environments, Sensors 21 (10) (2021).

[29] Reza Soltani, Uyen Trang Nguyen, Aijun An, Practical key recovery model for self-sovereign identity based digital wallets, in: 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), 2019, pp. 320–325, http://dx.doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00066.

[30] Gyeong-Jin Ra, Chang-Hyun Roh, Im-Yeong Lee, A key recovery system based on password-protected secret sharing in a permissioned blockchain, Comput., Mater. Continua 65 (1) (2020) 153–170.

[31] I. Indu, et al., Identity and access management in cloud environment: Mechanisms and challenges, Eng. Sci. Technol., Int. J. 21 (2018) 574–588.

[32] Chaturvedi Ankita, et al., An enhanced dynamic ID-based authentication scheme for telecare medical information systems, J. King Saud Univ. - Comput. Inf. Sci. 29 (2017) 54–62.

[33] Km Renuka, Saru Kumari, Xiong Li, Design of a secure three-factor authentication scheme for smart healthcare, J. Med. Syst. (2019).

[34] Asaph Azaria, et al., MedRec: Using blockchain for medical data access and permission management, in: 2016 2nd International Conference on Open and Big Data (OBD), 2016, pp. 25–30, http://dx.doi.org/10.1109/OBD.2016.11.

[35] Abbas Yazdinejad, et al., Decentralized authentication of distributed patients in hospital networks using blockchain, IEEE J. Biomed. Health Inform. 24 (2020) 2146–2156.

[36] A. Abid, S. Cheikhrouhou, S. Kallel, M. Jmaiel, Novidchain: Blockchain- based privacy-preserving platform for covid-19 test/vaccine certificates, Softw. Pract. Exp. 52 (2021) 1–27.

[37] Liang Tan, et al., Towards secure and privacy-preserving data sharing for COVID-19 medical records: A blockchain-empowered approach, IEEE Trans. Netw. Sci. Eng. 9 (2022) 271–281.

[38] Xinyin Xiang, Mingyu Wang, Weiguo Fan, A permissioned blockchain-based identity management and user authentication scheme for E-health systems, IEEE Access 8 (2020) 171771–171783.

[39] Dimitrios Xanthidis, Ourania Koutzampasopoulou Xanthidou, A proposed framework for developing an electronic medical record system, J. Glob. Inf. Manag. 29 (2019).
[40] ABDM, ABDM sandbox environment, 2022, https://sandbox.abdm.gov.in/, [Online: Accessed on 17 July 2022].
[41] Ray Hylock, Xiaoming Zeng, HealthChain: Patient-centered health records and exchange via blockchain, J. Med. Int. Res. 21 (2019).
[42] Uport, Simple ID (muPort), https://developer.uport.me/muport-core-js/guides/simple-id, [Online: Accessed on 08 May 2022].
[43] ShoCard, Mobile identity: What if I lose my phone?, 2018, https://medium.com/shocard/mobile-identity-what-if-i-lose-my-phone-5acf5a8af7c6, [Online: Accessed on 25 July 2022].
[44] ShoCard, Daniel hardman, 2019, https://sovrin.org/wp-content/uploads/2019/03/What-if-someone-steals-my-phone-040319.pdf, [Online: Accessed on 23 June 2022].
[45] Tim Janssen, Implementing SSI: Comparing uport, sovrin and IRMA, 2020, https://info.vismaconnect.nl/blog/different-approaches-ssi, [Online: Accessed on 25 July 2022].
[46] V. Nabelsi, A. Lévesque-Chouinard, C. Liddy, M. Dumas Pilon, Improving the referral process, timeliness, effectiveness, and equity of access to specialist medical services through electronic consultation: Pilot study, JMIR Med. Inform. 7 (2007).
[47] M. Safi, R. Clay-Williams, B.R. Thude, J. Vaisman, F. Brandt, Today's referral is tomorrow's repeat patient: referrals to and between medical outpatient clinics in a hospital, BMC Health Serv. Res. 22 (2022).
[48] Jie Xu, Kaiping Xue, Hangyu Tian, Jianan Hong, David S.L. Wei, Peilin Hong, An identity management and authentication scheme based on redactable blockchain for mobile networks, IEEE Trans. Veh. Technol. 69 (6) (2020) 6688–6698–75326.
[49] Quinten Stokkink, Johan Pouwelse, Deployment of a blockchain-based self-sovereign identity, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1336–1342, http://dx.doi.org/10.1109/Cybermatics_2018.2018.00230.
[50] Amitesh Singh Rajput, Balasubramanian Raman, Privacy-preserving distribution and access control of personalized healthcare data, IEEE Trans. Ind. Inform. 18 (2022) 5584–5591.
[51] Wei Zhang, Yaping Lin, Jie Wu, Ting Zhou, Inference attack-resistant E-healthcare cloud system with fine-grained access control, IEEE Trans. Serv. Comput. 14 (2021) 167–178.
[52] Sheng Ding, Jin Cao, Chen Li, Kai Fan, Hui Li, A novel attribute-based access control scheme using blockchain for IoT, IEEE Access 7 (2019) 38431–38441.
[53] Aafaf Ouaddah, Anas Abou Elkalam, Abdellah Ait Ouahman, FairAccess: a new Blockchain-based access control framework for the Internet of Things, Secur. Commun. Netw. 9 (2016) 5943–5964.
[54] Han Liu, Dezhi Han, Dun Li, Fabric-iot: A blockchain-based access control system in IoT, IEEE Access 8 (2020) 18207–18218.
[55] Elham A. Shammar, Ammar T. Zahary, Asma A. Al-Shargabi, An attribute-based access control model for internet of things using hyperledger fabric blockchain, Wirel. Commun. Mob. Comput. (2022).
[56] Seham Alnefaie, Asma Cherif, Suhair Alshehri, Towards a distributed access control model for IoT in healthcare, in: 2019 2nd International Conference on Computer Applications and Information Security (ICCAIS), 2019, pp. 1–6, http://dx.doi.org/10.1109/CAIS.2019.8769462.
[57] Otto Julio Ahlert Pinno, André Grégio, Luis C.E. Bona, ControlChain: Blockchain as a central enabler for access control authorizations in the IoT, in: GLOBECOM 2017 - 2017 IEEE Global Communications Conference, 2017, pp. 1–6, http://dx.doi.org/10.1109/GLOCOM.2017.8254521.
[58] Yan Zhang, Bing Li, Ben Liu, Jiaxin Wu, Yazhou Wang, Xia Yang, An attribute-based collaborative access control scheme using blockchain for IoT devices, Electronics (2020).
[59] GOV.UK, UK digital identity and attributes trust framework - alpha version 2, 2021, https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version, [Online: Accessed on 25 July 2022].
[60] Drummond Reed, Jason Law, Daniel Hardman, Mike Lodder, DKMS (decentralized key management system) design and architecture V3, 2018, https://github.com/hyperledger/indy-sdk/blob/master/docs/design/005-dkms/DKMS, [Online: Accessed on 23 April 2023].
[61] Fabric-iot is a blockchain based decentralized access control system in IoT, 2021, https://github.com/newham/fabric-iot/tree/bc73b8eed37b5967072943752237b85a38c4617e, [Online: Accessed on 15 Agust 2023].
[62] Zhenpeng Shi, Kalman Graffi, David Starobinski, Nikolay Matyunin, Threat modeling tools: A taxonomy, IEEE Security & Privacy 20 (4) (2022) 29–39.
[63] Daniele Granata, Massimiliano Rak, Giovanni Salzillo, Automated threat modeling approaches: Comparison of open source tools, in: International Conference on the Quality of Information and Communications Technology, Springer, 2022, pp. 250–265.
[64] Jan Camenisch, Anna Lysyanskaya, Signature schemes and anonymous credentials from bilinear maps, in: Matt Franklin (Ed.), Advances in Cryptology – CRYPTO 2004, Springer Berlin Heidelberg, Berlin, Heidelberg, 2004, pp. 56–72.