IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 13, 2022, accepted May 30, 2022, date of publication June 6, 2022, date of current version June 9, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3180367

Blockchain-Based Identity Management Systems in Health IoT: A Systematic Review

BANDAR ALAMRI, KATIE CROWLEY, AND ITA RICHARDSON
Department of Computer Science and Information Systems (CSIS), Lero Science Foundation Ireland Research Centre for Software, Health Research Institute (HRI), University of Limerick, Limerick, V94 T9PX Ireland

Corresponding author: Bandar Alamri (bandar.alamri@ul.ie)

This work was supported in part by the Ministry of Education of Saudi Arabia, and in part by the Science Foundation Ireland Research Centre for Software (www.lero.ie).

ABSTRACT Identity and Access Management (IAM) systems are crucial for any information system, such as healthcare information systems. Health IoT (HIoT) applications are targeted by attackers due to the high-volume and sensitivity of health data. Thus, IAM systems for HIoT need to be built with high standards and based on reliable frameworks. Blockchain (BC) is an emerging technology widely used for developing decentralized IAM solutions. Although, the integration of BC in HIoT for proposing IAM solutions has gained recent attention, BC is an evolving technology and needs to be studied carefully before using it for IAM solutions in HIoT applications. A systematic literature review was conducted on the BC-based IAM systems in HIoT applications to investigate the security aspect. Twenty-four studies that satisfied the inclusion criteria and passed the quality assessment were included in this review. We studied BC-based solutions in HIoT applications to explore the IAM system architecture, security requirements and threats. We summarized the main components and technologies in typical BC-based IAM systems and the layered architecture of the BC-based IAM system in HIoT. Accordingly, the security threats and requirements were summarized. Our systematic review shows that there is a lack of a comprehensive security framework, risk assessments, and security and functional performance evaluation metrics in BC-based IAM in HIoT applications.

INDEX TERMS Access control, blockchain, e-Health, health IoT, identity management, security, systematic literature review.

I. INTRODUCTION

E-Health is defined by the World Health Organisation (WHO) as the utilization of information and communication technology (ICT) in the health domain [1]. E-Health involves sub-domains like Electronic Health Records (EHR), Patient Health Records (PHR), and Mobile Health (m-Health). Health IoT (HIoT) technology is broadly used in e-Health fields. It is used in healthcare in different applications, such as health monitoring systems, real-time data, EHR, wearables, and many other applications [1]. HIoT is one of the targeted domains by attackers for its complexity, and the high sensitivity of data [2]. Thus, applying Privacy-Enhancing Technologies (PET) in HIoT-based systems is imperative. According to Cha *et al.* [3], there are seven different categories of PET, including personal data protection, control over data, and anonymous authorization. Identity and Access Management (IAM) systems (also referred to in the literature as ''identity management'') are deemed to be the primary safeguard for the access of any information system [4]. Therefore, using state-of-the-art technologies that have the potential to comply with data protection regulations, such as General Data Protection Regulations (GDPR), is paramount to enhancing data privacy and security. Ismail *et al.* [5], in a scoping review, studied the requirements of health data management systems in healthcare. They concluded that healthcare systems users need to be allowed to manage their data themselves, in accordance with GDPR. This study showed the transformation from traditionally using paper to record data to healthcare management systems, gradually moving through different stages that involve using emerging technologies like IoT, cloud and blockchain (BC). Such an evolution increases the importance of having functional, reliable, and secure IAM systems. The role of IAM systems involves using information security frameworks and technologies developed to provide secure access for legitimate users to the

The associate editor coordinating the review of this manuscript and approving it for publication was Mehdi Sookhak.

data assets. The significance of IAM in HIoT applications is high because of the kind and amount of data that HIoTs entail. Systems that are based on HIoT need to be studied carefully, as the system architecture differs from other typical systems [6].

BC technology was first invented in 2008 by Satoshi Nakamoto [7]. In 2013, BC 2.0 started by launching Ethereum BC and Smart Contracts. At that stage, BC was only used for financial applications. In 2017, there was a considerable rise in conducting research on BC technologies like Ethereum and Hyperledger in different domains like healthcare and for different purposes like IAM systems [8]. BC attracted researchers' attention to harness its advantages to develop decentralized IAM systems for HIoT applications. However, there is still a need for research on the standardization of this emerging technology and the security requirements for BC-based IAM of HIoT applications [9].

Our study, presented in this paper, has reviewed relevant primary studies proposing IAM solutions based on BC in HIoT applications. The aim is to explore the security threats and requirements, which are related to BC-based IAM systems in HIoT applications. Results from this systematic literature review will play a notable role in designing a security framework to be used as a guideline for developers and researchers who strive to harness BC for developing a decentralized IAM for HIoT.

The structure of the rest of this paper is as follows: Section II covers the background, Section III addresses the related works, Section IV describes the research methodology, Section V presents the analysis of the results, Section VI includes the discussion, limitations and future direction are covered in SectionVII, and Section VIII covers the article conclusion.

II. BACKGROUND

A. IDENTITY AND ACCESS MANAGEMENT

IAM systems are crucial for the security of data in IoT applications [4]. IAM can be defined as a security system used for managing the life-cycle of digital identities to ensure that only authenticated identities can be authorized to access data assets in a system. An IAM system consists of two primary operations. The first is authentication (AuthN), a process which verifies identity, thus preventing malicious access to a system. AuthN ensures that a claim of identity ownership using either digital (e.g., public-key cryptography) or physical (e.g., biometrics) authentication methods. The second is authorization (AuthZ), a process ensuring that only legitimate users can access specific data assets using access control mechanisms. After authenticating an identity, there is a need to control the access to process data. The AuthZ operation is responsible for denying or granting user access to data, which is achieved by first defining policies (set of rules) and then using and applying access control methods [10].

There are five access control models that manage user access rights to data in traditional IAM: mandatory access control, discretionary access control, role-based access control, attribute-based access control, and capacity-based access control. Based on these models, rights are given to identities or users according to their roles and attributes. There are a number of access management standards used to fulfil the access control AuthZ and AuthN processes, such as OpenID-Connect, open authorization, security assertion markup language, and extensible access control markup language [11].

Based on these two operations, IAM guarantees secure access to systems. Identities are managed in the whole life-cycle of the IAM system based on the IAM model category. There are four IAM models: 1) isolated, 2) centralized, 3) federated, and 4) user-centric (e.g., self-sovereign which is a BC-based IAM model) [12].

There are a number of digital identity standards and data protection laws which strive to organize the process of IAM. For example, ISO 27001 is an international standard for maintaining Information Security Management Systems (ISMS) in organizations. It focuses on providing the required framework for the implementation, enhancement, and maintenance of information security management systems. It involves a variety of aspects, such as data asset management, access control, change management, and business continuity. At the same time, ISO9798 focuses more on AuthN techniques in the ISMS [13].

GDPR, is the EU standard that focuses on user data protection regulations for organizations that deal with EU residents' data. GDPR includes eight fundamental rights for the data subject: 1) the right to access data, 2) the right to be forgotten, 3) the right to restrict data processing, 4) the right to be informed, 5) the right to object, 6) the right to data portability, 7) rights related to automated decision-making, and 8) the right to rectification [14].

Recently, BC has been used widely for proposing IAM systems, which are based on two IAM models, Self-Sovereign Identity (SSI) and decentralized trusted identity [15]. According to Taylor *et al.* [16], in a systematic review conducted on using BC for security purposes, 45 percent of studies focused on IoT applications for AuthN purposes. IAM plays a role in managing data in IoT and cloud-based applications to ensure secure access to data assets. Although there are standards and best practices that need to be followed to develop secure IAM systems, centralization is still a critical issue in cloud-based systems [10]. The concept of IAM is different for IoT-based systems than other systems, because, in IoT, identities are not only users. There are subjects or "things" that need to be managed in order to secure access to data. Using different emerging technologies like cloud computing, IoT, and BC in developing information systems causes some IAM systems to be outdated for reasons, such as overheat rate, scalability, and data privacy. As a result, IAM systems are transforming to account for these changes [17].

B. HEALTH IoT APPLICATIONS

E-Health is an umbrella for various systems, such as EHR, PHR, and m-Health applications. It has many definitions in

the literature. However, it is agreed that it is an integration of information and communication technologies to improve healthcare services [18]. The term e-Health was coined in 1999-2000 with the beginning of "the Internet bubble." At that time, it covered a few ICT technologies. However, with the revolution of digital technologies, technologies like cloud computing, HIoT, and Big Data can be used and play a significant role in improving e-Health services [1]. E-Health aims to provide digital and smart health services that are economical, secure, and efficient. E-Health positively impacts not only individuals but also nations. It can play an influential role in facilitating receiving health services in developing countries by utilizing HIoT technologies [19].

Although HIoT has revolutionized healthcare services, HIoT comes with drawbacks as they are resource-constrained in memory, performance, and computational power, which increases the complexity, and security concerns of HIoT applications. HIoT architecture characteristics need to be considered in HIoT applications in order to build secure applications [20]. There are four layers in HIoT systems: HIoT device, networking, cloud computing technologies, and application layer. In the HIoT device layer, the HIoT device is connected to the HIoT user. The networking layer is responsible for connecting the sensor data to the cloud layer where data is processed using WiFi or other communication technologies. The application layer is where the data is presented to the health system stakeholders, such as patients and healthcare providers. Health data is transmitted through these layers, and so it is vulnerable to data breaches and security attacks [21]. HIoT system architecture is shown in Figure1.

HIoT devices are widely used in the healthcare domain. The taxonomy of HIoT is shown in Figure 2. There are four main types of HIoT: health and well-being sensors, diagnosis sensors, prognostic sensors, and assisting sensors. There are various sub-types of these four branches. These devices are used for different purposes, such as for collecting parameters like blood pressure, heart rate, and blood glucose. Some of these HIoT devices are used in hospitals; patients can use others from their homes [1]. HIoT devices are connected through the Internet to servers where data are stored, analyzed and accessed by healthcare stakeholders based on the privileges given in the IAM system. Although HIoT is similar to IoT in terms of architecture, they are different in terms of characteristics. HIoT differs from generic IoT based on the health environment needs in characteristics like the device power consumption, network bandwidth, device mobility, network protocol used, memory, security, and cryptography technologies [21].

C. BLOCKCHAIN

BC is defined as a distributed digital database shared between a number of network participants based on cryptography and consensus mechanisms and protocols. Characteristics such as decentralization, anonymity, immutability, transparency, and audibility distinguish it from other technologies and paradigms. The first application that was based on BC was Bitcoin, which was initially pioneered when Satoshi Nakamoto published a white paper in 2008 titled "Bitcoin: A Peer-to-Peer Electronic Cash System." The paper described how it would be possible to transfer money from one user to another without a third party using a cryptographic mechanism to fulfil this task. After one year, an open-source software implementing Bitcoin was launched [7].

Although BC is now used outside of financial applications where digital transactions are exchanged, its core technology is very much related to Bitcoin and cryptocurrency concepts. The Bitcoin decentralized payment system is based on a cryptographic proof mechanism instead of relying on trusted third parties. This mechanism uses a public/private key AuthN process for validation. After the transaction is shared with all other nodes in the network and gets validated, it is added to the public ledger. There are two steps to validate such a transaction; first, to ensure the sender owns the cryptocurrency and second, to ensure that the sender has a sufficient balance in their account. In order to avoid duplication in spending cryptocurrencies, there needs to be a mechanism that helps Bitcoin to organize and ensure this process. To solve this issue, Bitcoin made use of the concept of BCs where a group of chains are connected with each other by hashes creating the BC network. Every block has a group of transactions that are meant to be added to the network at the same time. However, there is still a need for a mechanism in charge of organizing the process of mining the blocks in a timely manner. From here, the role of Proof-of-Work (PoW) consensus mechanism starts. PoW is based on a mathematical puzzle where nodes are tested by other nodes to be allowed to add their transactions in the right order in a process called mining [22].

Ethereum BC and Smart Contracts were launched in 2013, paving the way for using BC in non-financial applications. In more recent years, the attention of developers and researchers shifted to propose applications based on BC in different domains. Recently, some big technology companies like Microsoft and IBM have offered BC as a service [23]. There are two main categories of BC: (a) public or permissionless BC and (b) private, or permissioned BC. A hybrid of public and private BCs is the consortium BC. There are a number of BC platforms besides Bitcoin and Ethereum; the Hyperledger Fabric BC is one of the most attractive BC platforms recently used for non-financial applications [24]. On the other hand, there are other distributed-ledger technologies like IOTA, which is similar to BC technology but different in that it is based on the Tangle data structure rather than blocks and uses a different validation process to add new transactions. IOTA is an evolving peer-to-peer network based on consensus protocols, which has potential benefits in IoT applications. However, it is under development and does not support Smart Contract at the moment [25].

BC is a disruptive technology that, for its profound benefits, is widely used in different domains and applications. The trend shows that it attracted researchers' attention after its platforms became available beyond financial and cryptocurrency applications. According to Zou *et al.* [8], since 2017,

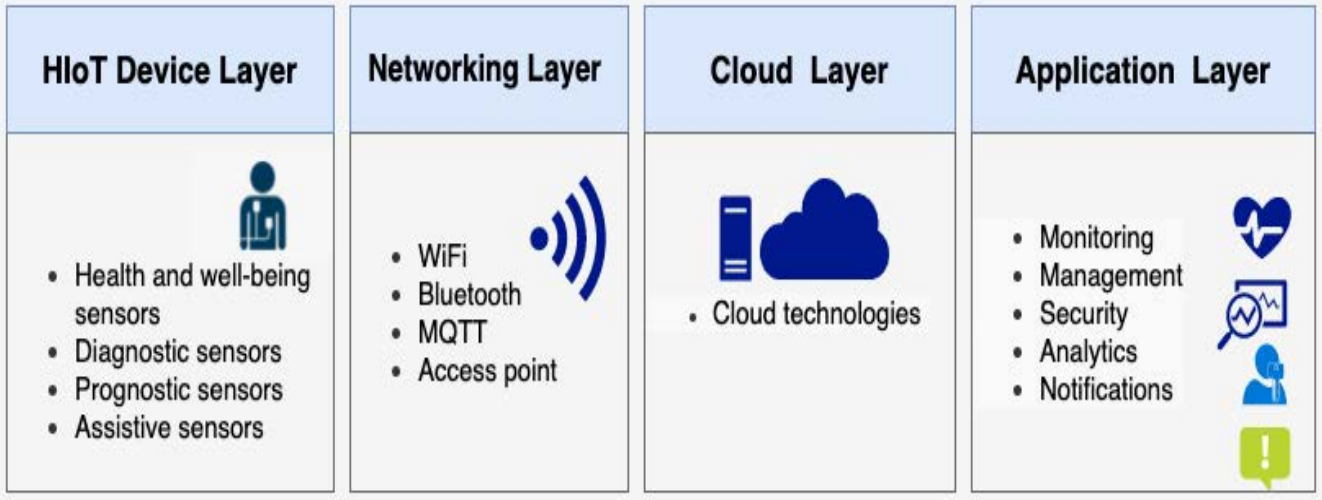


FIGURE 1. HIoT system layers.

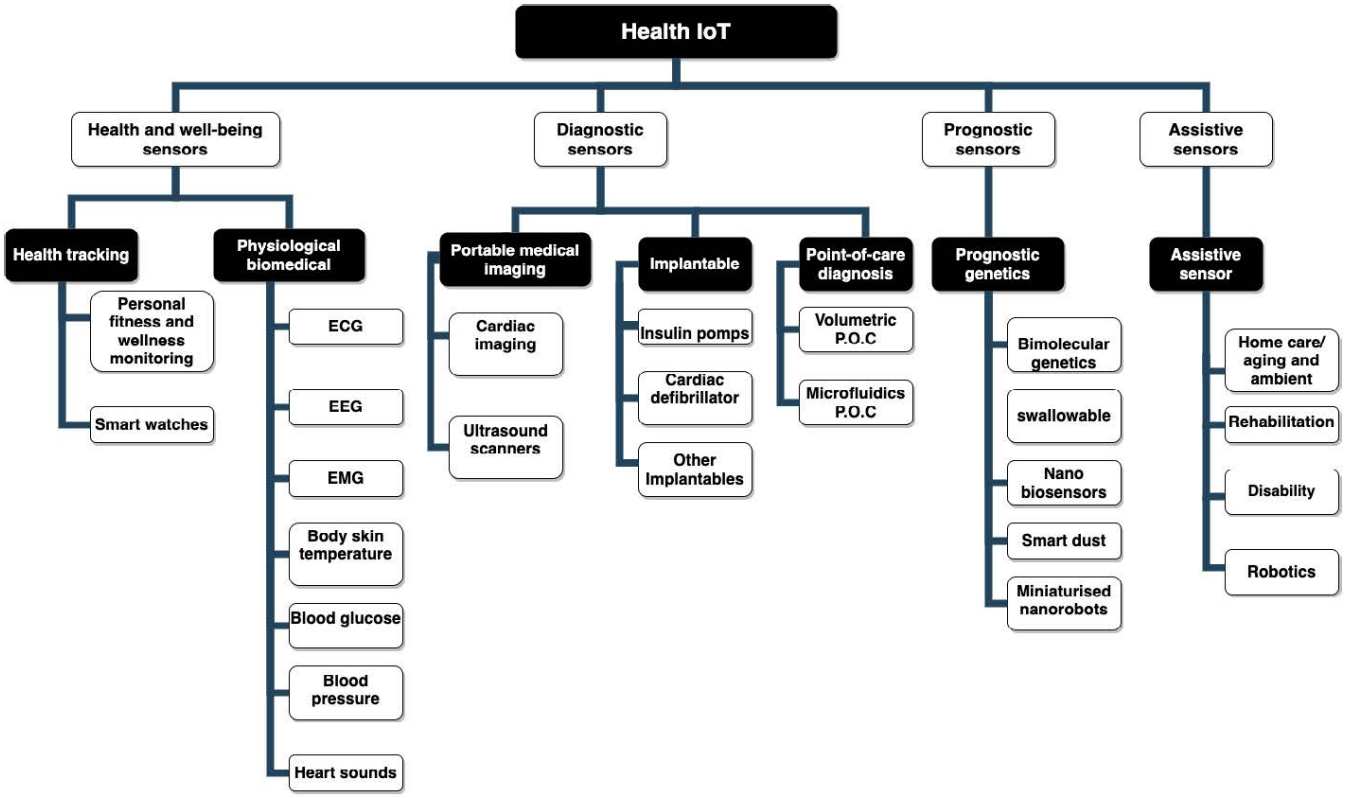


FIGURE 2. HIoT taxonomy.

the application of BC in different domains like healthcare and IoT has increased dramatically. In particular, applications of BC in the healthcare domain are increasing significantly because it is stated to be a better choice for managing sensitive data [26]. However, there is still a shortage of studies which address the challenges around BC [27].

According to Wang *et al.* [28], as the number of BC application studies is rising, the number of attacks on BC-based applications are also increasing, leading to a huge economic loss. These attack incidents are categorized based on the BC layers, (the application layer, smart contract layer, incentive layer, consensus layer, network layer, and data layer).

III. RELATED WORKS

The considerations of IAM and the complexity of BC and HIoT applications stated in the previous sections motivated a number of secondary studies on IAM in general and SSI in particular for IoT applications, e-Health applications, and other domains. These studies cover IAM mechanisms, BC-based IAM opportunities, solutions, issues, and future directions. Some studies focus on a particular aspect of IAM,

(i.e., AuthN or AuthZ) for a specific application, like IoT or industrial IoT. Others focus on specific healthcare applications like EHR, as discussed in the following paragraphs.

Indu *et al.* [10], conducted a comprehensive study on IAM mechanisms and models in cloud environments. In addition, security analyses have been conducted on a number of mainstream IAM attacks, such as a man-in-the-middle attacks, insider attacks, replay attacks, and session/cookie attacks. Cremonezi *et al.* [17], conducted a survey study on conventional IAM systems covering AuthN, AuthZ operations, and IAM models in IoT environments, where the IoT system architecture and characteristics are considered. Other researchers have conducted studies on the AuthZ part of IAM for IoT. For example, Qiu *et al.* [29], analyzed the challenges and issues of access control in IoT environments and proposed conceptual and technical guidelines to open the door to developers and researchers for building reliable access control solutions. Ouaddah *et al.* [4], proposed a framework to evaluate the proposed AuthZ mechanisms for IoT systems. Ravidas *et al.* [30], analyzed AuthZ issues found by previous surveys and tested the current access control solutions against them. The researchers then proposed a requirement framework and guidelines for building an access control mechanism tailored to chosen IoT applications.

A number of studies have investigated using BC to develop IAM solutions. Kuperberg [31], conducted a survey study on the functional and non-functional requirements for BC-based IAM. The requirements and considerations included data protection laws and BC pitfalls, such as overhead aspects and standards. The study did not focus on specific applications or domains. However, it developed 75 criteria to evaluate qualitative offerings, such as regulatory compliance in the BC-based IAM solutions in general. Liu *et al.* [32], reviewed the existing BC-based identity management systems, focusing on three: Sovrin, uPort, and ShoCard BC-based IAM systems. They reviewed these three systems and the AuthN, privacy, and trust related works.

Decentralized access control mechanisms for IoT that are based on BC are surveyed by Butun and Osterberg [33]. In this study, varied AuthZ, AuthN, and revocation mechanisms in permissioned and permissionless BC-based systems from proposed solutions were studied. The researchers concluded that there are specific requirements that should be considered when using peer-to-peer networks for access control solutions in IoT applications. They stated that permissioned BC is the best option for IoT security, which should involve specific mechanisms in the main three operations; AuthN, AuthZ, and revocation. The authors also concluded that cost, performance, and scalability are challenges that need to be considered in order to build a reliable BC-based IAM for IoT applications. Zhu and Badr in a similar study [12], explored the IAM system requirements in some proposed solutions using BC with more focus on IAM challenges in IoT applications.

Regarding BC-based IAM systems in the healthcare domain, Houtan *et al.* [9], conducted a survey study on BC-based Patient Identity Management Systems, i.e., SSI in EHRs. Authors in this study compared different BC-based applications in Personal Health Records and EHR against a set of criteria. The vast majority of these applications do not consider IoT in their architecture. Bouras *et al.* in another survey study [34], compared different BC-based IAM models against the IAM systems' seven laws, which are proposed by Cameron [35]. Based on an e-Health application scenario that involves healthcare regulators, healthcare providers, industry representatives, and healthcare consumers, they proposed a performance evaluation metrics for BC-based IAM. Mamdouh *et al.* in another study [21], conducted a survey on AuthN mechanisms for HIoT that are based on BC technology and Physical Unclonable Function (PUF) (i.e., a mechanism used for HIoT device AuthN). This study concentrated on security threats in all HIoT system layers. The researchers concluded that as HIoT are different from general IoT systems, and that these differences need to be considered when proposing any AuthN mechanisms. According to these studies, the current proposed applications are in beta or test stages and not ready to be developed in real-life applications. They concluded that there is still a shortage in standardization studies for using BC in HIoT applications for providing BC-based IAM systems. Therefore, our work contributes to this research direction and stands out from other studies in three aspects: 1) focusing on HIoT applications, 2) conducting a systematic review to get a better understanding of the security requirements for BC-based IAM in HIoT and to explore security threats, and 3) covering all proposed solutions concerning AuthN and AuthZ aspects.

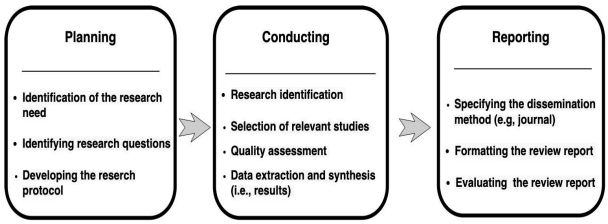


FIGURE 3. SLR main stages and associated steps.

IV. RESEARCH METHODOLOGY

This systematic review used a search based on the Preferred Reporting Items for Systemic Reviews and Meta-Analyses (PRISMA) standards across multi-disciplinary databases [36]. As the research is interdisciplinary, the procedures and guidelines for conducting systematic literature reviews in software engineering by Keele [37] and Kitchenham [38] were also used. To ensure that a wide range of literature was analyzed, a backward and forward snowballing approach was used [39]. Performing a systematic literature review involves three main stages: planning, conducting, and reporting, as shown in Figure 3.

A. RESEARCH NEED IDENTIFICATION

BC technologies are widely used to propose decentralized IAM solutions in varied HIoT applications. Some solutions

TABLE 1. Population, Intervention, Comparison and Outcome (PICO) criteria used in this study.

Criteria	The equivalent in our study
Population	HIoT applications.
Intervention	BC-based IAM systems.
Comparison	conventional IAM systems.
Outcome	Protection of identities' security and privacy in HIoT applications. Compliance with data protection regulations, such as GDPR and standards, such as ISO27001. Improvement the reliability of BC-based IAM in HIoT applications.

consider functional, but not non-functional requirements, for HIoT applications and BC limitations. Security requirements are not usually considered in the solutions. Some of the proposed solutions provide privacy preservation techniques and strive to comply with data regulations like GDPR. This systematic literature review aims to explore all the IAM solutions that are based on BC in HIoT applications in order to investigate the security threats and requirements in BC-based IAM in HIoT, thus providing a unified picture for designing a comprehensive security framework.

B. RESEARCH QUESTIONS

Based on the research aim and using the criteria structure recommended by Kitchenham [38] and Moher *et al.* [36], shown in Table 1, we defined three main research questions (RQs) as follows:

- Q1: What are the methods used to ensure BC-based IAM in HIoT applications?
- Q2: What are the architecture components and required technologies in BC-based IAM systems?
- Q3: What are the architecture of BC-based IAM in HIoT applications, security threats and requirements, and other considerations?

C. DEVELOPING THE RESEARCH PROTOCOL

The research protocol is a main aspect of any systematic literature review. The following processes are planned in the research protocol: (a) research identification, which involves selecting the relevant databases chosen to be surveyed, choosing search strings, and inclusion/exclusion process, (b) selection of relevant studies and (c) quality assessment process.

D. RESEARCH IDENTIFICATION

1) RESEARCH SOURCES

In order to find all studies related to our research questions, there were seven databases chosen to be surveyed, as shown in Table 2. These databases were checked to review all published primary studies on BC-based IAM for HIoT applications between 2016 (when BC started to be used beyond financial applications) and 2021. Databases were chosen based on the research domain, which involves software engineering and health informatics.

TABLE 2. Databases used in the systematic literature review.

Database	Website
ACM	https://dl.acm.org/
IEEE	https://ieeexplore.ieee.org/
JMRI	https://jmirpublications.com/
Pubmed	https://pubmed.ncbi.nlm.nih.gov/
ScienceDirect	https://www.sciencedirect.com/
Scopus	https://www.scopus.com/
Web of Science	https://www.webofscience.com/

2) SEARCH STRINGS

Initially, the terms "blockchain," "identity," "access," "health," and "IoT" were considered the main keywords. After that, keyword synonyms and related terms are defined. As IAM involves two main concepts, "authentication" and "authorization", these two keywords were considered as alternative keywords for "identity" and "access," so they were added to the keyword list. Also, "distributed-ledger" was used as an alternative for "blockchain." The backward and forward snowballing approach was used to find more related keywords to "blockchain" keyword and make sure all common alternative keywords are covered. Based on the two highest cited articles in BC-based IAM-related works, by Dunphy and Petitcolas [40], and Jacobovitz [41], it was discovered that the term "Self-Sovereign Identity" has been used recently to describe the BC-based IAM solutions, and it was therefore added to the keyword list. According to the above aforementioned definition of e-Health, which covers all ICT-based healthcare systems, and as our review study focuses on HIoT applications, we consider all studies covering IoT in healthcare fall under HIoT applications. Therefore, we checked databases for "health" and "medical" keywords with "IoT" keyword. The keywords and their alternatives used in our search process are as follows:

- Blockchain: "distributed-ledger," "self-sovereign."
- Identity: "access," "authentication," "authorization."
- Health: "medical."
- IoT.

As electronic databases allow the use of Boolean operators with keywords and their synonyms to conduct a sophisticated search to find the relevant articles, we used the strings shown in Table 3 with a number of selected databases (note, the structure of using Boolean operators can be different from one database to another).

3) INCLUSION/EXCLUSION CRITERIA

Table 4 shows the inclusion and exclusion criteria used in order to select only the relevant primary studies. All studies in the final list satisfied these criteria.

E. SELECTION OF RELEVANT STUDIES

The steps in Figure 4 depicts the article selection flowchart used in PRISMA standards. These steps were followed to select relevant studies. Initially, every database's relevant studies were added in a group using EndNote software. They were then combined into a library to exclude duplicates.

TABLE 3. Strings used in the chosen databases.

DBs	Strings
ACM	(blockchain OR distributed-ledger OR self-sovereign) AND (Identity OR authentication OR access OR authorization) AND (health OR medical) AND IoT
IEEE JMRI Pubmed Scopus Web-of science	(blockchain AND access AND health AND IoT) OR(blockchain AND identity AND health AND IoT) OR(blockchain AND authentication AND health AND IoT)OR(blockchain AND authorization AND health AND IoT)OR(blockchain AND access AND medical AND IoT)OR(blockchain AND identity AND medical AND IoT)(blockchain AND authorization AND medical AND IoT)OR (blockchain AND authentication AND medical AND IoT)OR (self-sovereign AND health AND IoT)OR (self-sovereign AND medical AND IoT)OR(distributed-ledger AND health AND IoT)OR (distributed-ledger AND medical AND IoT)
Science Direct	(blockchain access health IoT)OR(blockchain identity health IoT)OR(blockchain authentication health IoT)OR(blockchain authorization health IoT)OR(blockchain access medical IoT)OR(blockchain identity medical IoT)(blockchain authorization medical IoT)OR (blockchain authentication medical IoT)OR (self-sovereign health IoT)OR (distributed-ledger health IoT)

TABLE 4. Inclusion and exclusion criteria.

Inclusion criteria	Exclusion criteria
English-written studies	Studies written in other than English
Studies published between 2016-2021	Studies published before 2016
Primary studies	Secondary studies
BC-based IAM solutions	IAM solutions based on other than BC, including IOTA.
HIoT applications	Other e-Health applications do not include HIoT.

The number of records identified initially was 1493. The inclusion/exclusion criteria was applied. The first exclusion was based on the duplicate studies and reference types, which resulted in eliminating 341 records. Based on the screening of these studies, 1075 studies were excluded based on reading titles and abstracts. Secondary studies, concept papers, magazine articles, and studies outside the study scope were removed. The final step was to download and read the remaining 77 studies to assess them against the inclusion/exclusion and the quality assessment criteria.

F. QUALITY ASSESSMENT

According to Kitchenham [38], quality assessment is crucial to eliminate bias from chosen studies. The quality assessment criteria in Table 5 were used to make sure that all chosen primary studies addressed the research questions. In order to pass the quality assessment, the quality score for all checklist factors needed to be met with a score of 1.0. If a study did not get a 1.0 quality score in all quality assessment factors, it was then excluded. Uncompleted and theoretical studies, non-evaluated solutions, and studies that did not consider HIoT devices in the system architecture are excluded. Also, studies that did not include an implementation using BC technology were excluded. This process resulted in 24 studies that were included for further analysis and discussion.

V. RESULTS

The final list of included studies is shown in Table 6. Data from these studies were extracted, synthesized, and studied

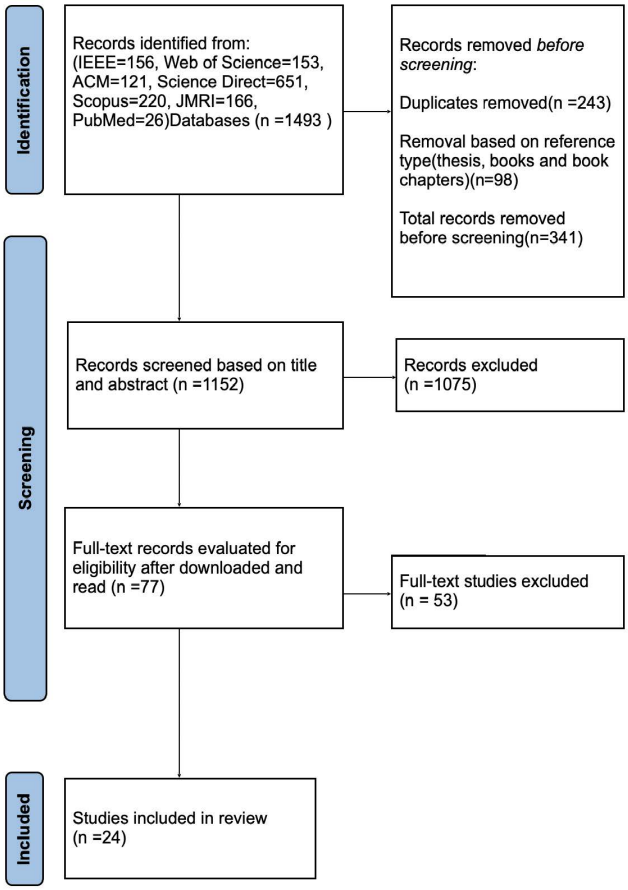


FIGURE 4. Article selection steps.

TABLE 5. Quality assessment criteria.

Quality assessment factor	Yes	No
Does the study address the research questions?	1.0	0.0
Is the IAM solution implemented using a BC platform?	1.0	0.0
Is HIoT considered in the system architecture?	1.0	0.0
Is the solution's performance evaluated?	1.0	0.0

critically in order to answer the three main research questions, determining research gaps and future direction.

BC technology has gained attention in recent years as a solution to provide decentralization in IAM systems, as shown in Figure 5. The figure shows there was an increase in studies on BC from 2018 to 2021. Data extracted from Table 6, which contains the final list of selected peer-reviewed conference and journal article studies, indicates that research studies about BC-based IAM for HIoT applications increased dramatically in last two years. Data in Table 7 shows the BC-based HIoT application details, including HIoT applications, proposed IAM methods, and BC technology details.

BC-based IAM solutions are proposed in eight different types of HIoT-based e-Health applications, as shown in Figure 6. E-Health applications covered are EHR, PHR, medical IoT device security and management, Distributed Health Systems (DHS), Data Sharing and Management Systems (DSMS), telehealth, m-Health, and Remote Patient Monitoring Systems (RPMS). There are different HIoT devices

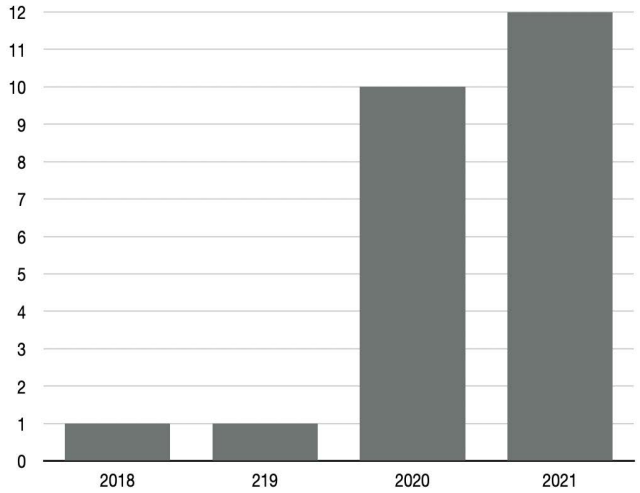


FIGURE 5. Trend of studies on BC-based IAM in HIoT applications. It indicates the number of studies per year.

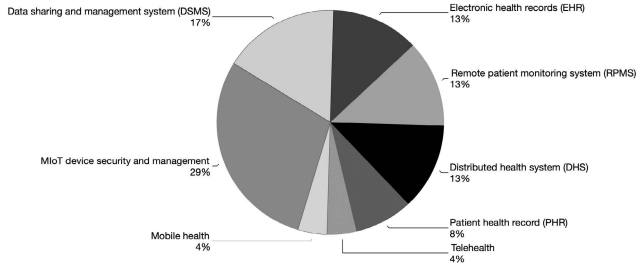


FIGURE 6. Types of HIoT-based e-Health applications covered in the studies.

covered, the majority of which are medical. Nineteen of the 24 studies (i.e., 79 percent) focused on medical IoT devices, such as physiological biomedical IoT devices that are used for reading vital signs. Two studies did not specify the HIoT device used. One study focused on a fitness wearable, one study focused on m-Health using smart devices, and one focused on implanted medical devices, as shown in Figure 7.

The results show that Ethereum and Hyperledger Fabric are the most used BC technologies. Figure 9 shows that 50 percent of the studies used Ethereum BC as a foundation for solutions, whereas 42 percent used Hyperledger Fabric. Four percent used Ripple BC with Ethereum BC in their solution and Hyperledger Indy was used in 4 percent. IAM systems includes two main operations, however, not all proposed solutions include these two operations together. As shown in Figure 8, 50 percent of the solutions include AuthN and AuthZ operations, 33 percent cover AuthZ only, and 17 percent cover AuthN only. The IAM system should include Identity Management (IdM) operation besides AuthN and AuthZ operations in order to manage identities, which should include a revocation process. Not all solutions have considered IdM operations including the revocation process, as shown in Table 8.

VI. DISCUSSION

BC technologies are used for proposing IAM systems in HIoT. BC should not be used individually to develop an

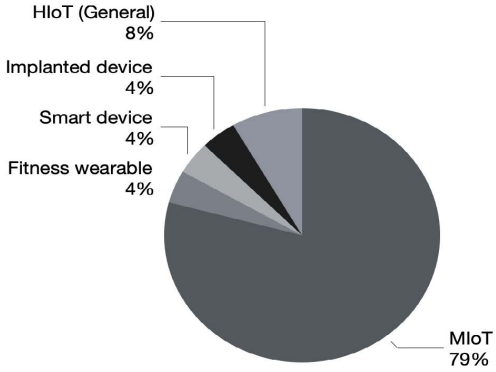


FIGURE 7. Types of HIoT devices considered in the studies.

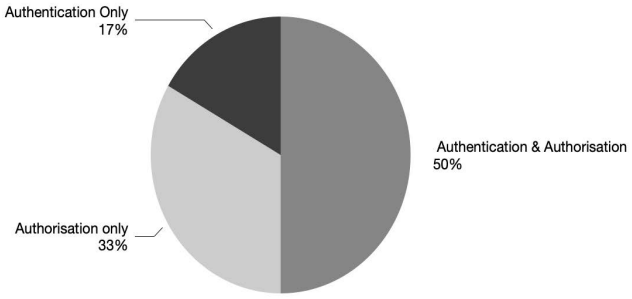


FIGURE 8. IAM mechanisms proposed.

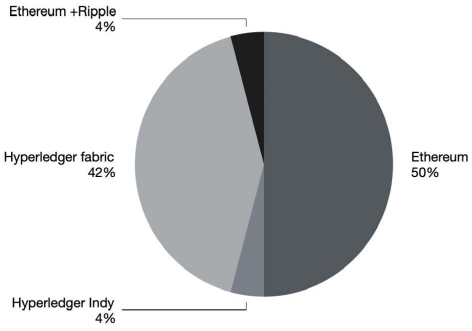


FIGURE 9. The BC technologies used.

IAM system. Thus, other technologies are utilized to store IAM systems' data and facilitate exchanging data between BC-based system layers and stakeholders. In this section we address the three main research questions, divided into three subsections.

A. ENSURING THE BC-BASED IAM IN HIoT APPLICATIONS

Solutions in the selected and reviewed studies can be divided into two categories: (1) IAM-focused studies in HIoT applications; (2) BC-based HIoT applications, which involve BC-based IAM systems. Both categories cover BC-based IAM systems for HIoT applications, however, the former is more focused on IAM aspects (AuthN and AuthZ), while the latter focuses on the BC-based proposed system and the IAM system is a part of the solution. Table 7 shows that studies in [42]–[48], focus on BC-based IAM for MIoT devices, while other studies [49]–[65], include IAM in BC-based solutions for different HIoT applications. Studies in, [47],

TABLE 6. The final list for included studies.

Study no.	Title	Author names	Year	Type	Publisher
S1	HealthBlock: A secure blockchain-based healthcare data management system	Zaabar et al.	2021	Article	Elsevier
S2	A blockchain-based eHealthcare system interoperating with WBANs	Wang et al.	2019	Article	Elsevier
S3	A Lightweight Authentication and Authorization Framework for Blockchain-Enabled IoT Network in Health-Informatics	Tahir	2020	Article	MDPI
S4	A decentralized framework for device authentication and data security in the next generation internet of medical things	Satamraju and Malarkodi	2021	Article	Elsevier
S5	Proof of Concept of Scalable Integration of Internet of Things and Blockchain in Healthcare	Satamraju and Malarkodi	2020	Article	MDPI
S6	Artificial intelligence-powered decentralized framework for Internet of Things in Health-care 4.0	Puri et al.	2021	Article	Wiley
S7	BEdgeHealth: A Decentralized Architecture for Edge-Based IoMT Networks Using Blockchain	Nguyen et al.	2021	Article	IEEE
S8	Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology	Kumar and Tripathi	2021	Article	Springer
S9	MedHypChain: A patient-centered interoperability hyperledger-based medical healthcare system: Regulation in COVID-19 pandemic	Kumar and Chand	2021	Article	Elsevier
S10	Trusted Remote Patient Monitoring Using Blockchain-Based Smart Contracts	Kazmi et al.	2020	Conference	Springer
S11	Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals	Jamil et al.	2020	Article	MDPI
S12	Multi-Access Edge Computing and Blockchain-based Secure Telehealth System Connected with 5G and IoT	Hewa et al.	2020	Conference	IEEE
S13	Protect Your Pacemaker: Blockchain based Authentication and Consented Authorization for Implanted Medical Devices	Gibson and Thamilarasu	2020	Article	Elsevier
S14	A user Authentication and Access Control Scheme for IoT-Based Healthcare Using Blockchain	Geetha and Balakrishnan	2021	Conference	IEEE
S15	Blockchain and SGX-Enabled Edge-Computing-Empowered Secure IoMT Data Analysis	Gao et al.	2021	Article	IEEE
S16	Healthcare and Fitness Data Management Using the IoT-Based Blockchain Platform	Frikha et al.	2021	Article	Hindawi
S17	SmartMedChain: A Blockchain-Based Privacy-Preserving Smart Healthcare Framework	Majdoubi et al.	2021	Article	Hindawi
S18	A blockchain-based preserving and sharing system for medical data privacy	Chen et al.	2021	Article	Elsevier
S19	Interoperability and Synchronization Management of Blockchain-Based Decentralized e-Health Systems	Biswas et al.	2020	Article	IEEE
S20	An anonymity communication protocol for security and privacy of clients in IoT-based mobile health transactions	Attarian and Hashemi	2021	Article	Elsevier
S21	DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems	Abou-Nassar et al.	2020	Article	IEEE
S22	Blockchain-based Ownership Management for Medical IoT (MIoT) Devices	Alblooshi et al.	2018	Conference	IEEE
S23	Blockchain for the Management of Internet of Things Devices in the Medical Industry	Akkaoui	2021	Article	IEEE
S24	EdgeMediChain:A Hybrid Edge Blockchain-Based Framework for Health Data Exchange	Akkaoui et al.	2020	Article	IEEE

[48], [63], [64], proposed AuthN solutions, while studies in [42], [43], [50], [54], [55], [58], [59], [65] proposed AuthZ solutions. The rest of the studies [44]–[46], [49], [51]–[53], [56], [57], [60]–[62] covered both AuthN and AuthZ solutions. A complete IAM system should involve AuthN and AuthZ operations, as well as covering the identity management (IdM) for the whole life-cycle of identities, from registration to deleting identity data when it is no longer belongs to a system. As shown in Table 8 there are sixteen studies among the reviewed studies that included IdM in the IAM system. Although, they covered registration and verification processes, only two studies [57], [60] covered the revocation process. The lack of the revocation process causes functional and security issues.

There are multiple HIoT-based e-Health applications covered in the 24 reviewed studies. In [49], [59], and [60], IAM solutions were proposed for HIoT-based EHRs, while in [50], [55], [56], IAM solutions were proposed for RPMS. In [53], [62], and [64], IAM solutions were proposed for DHS. IAM for MIoT device security and management were proposed in [42]–[48]. In [57], an IAM solution was proposed for a telehealth system, and in [63], an IAM solution was proposed for a m-Health system. In [52] and [61], IAM solutions were proposed for PHR and in [51], [54], [58], and [65], IAM solutions were proposed in DSMS.

B. ARCHITECTURE COMPONENTS AND REQUIRED TECHNOLOGIES IN BC-BASED IAM SYSTEMS

There are specific BC platforms used to implement the BC-based IAM systems in the HIoT applications. Ethereum and Hyperledger Fabric BC technologies are the most used solutions. The main reasons why these BC technologies were chosen are for the decentralization advantage. There are other advantages, such as immutability, transparency, and audibility, additionally, Smart Contracts, which are crucial for BC-based IAM systems. The permissioned access policy feature in the Hyperledger Fabric BC distinguishes it from Ethereum, which makes it more suitable for health information systems.

TABLE 7. BC-based HIoT application details.

Study Number	Application	HIoT	BC IAM Mechanism	BC platform	Access policy	Consensus protocol
S1	EHR	HIoT(General)	AuthN and AuthZ	Hyperledger Fabric	Permissioned	PBFT
S2	RPMS	MIoT (WBAN)	AuthZ	Hyperledger Fabric	Permissioned	Solo
S3	DSMS	MIoT	AuthN and AuthZ	Ethereum	Permissionless	PoA
S4	MIoT security and management	MIoT	AuthZ	Ethereum	Permissionless	PoW
S5	MIoT security and management	MIoT	AuthZ	Ethereum	Permissionless	PoW
S6	PHR	MIoT	AuthN and AuthZ	Ethereum	Permissionless	PoW
S7	DHS	MIoT	AuthN and AuthZ	Hyperledger Fabric	Permissioned	PBFT
S8	MIoT security and management	MIoT	AuthN and AuthZ	Ethereum	Permissionless	PoW
S9	DSMS	MIoT	AuthZ	Hyperledger Fabric	Permissioned	PBFT
S10	RPMS	MIoT	AuthZ	Ethereum	Permissionless	PoW
S11	RPMS	MIoT	AuthN and AuthZ	Hyperledger Fabric	Permissioned	PBFT
S12	Telehealth	MIoT	AuthN and AuthZ	Hyperledger Fabric	Permissioned	PBFT
S13	MIoT device security and management	Implanted medical device	AuthN and AuthZ	Hyperledger Indy	Permissioned	RBTP
S14	DSMS	MIoT	AuthZ	Ethereum	Permissionless	PoW
S15	MIoT device security and management	MIoT	AuthN and AuthZ	Hyperledger Fabric	Permissioned	PBFT
S16	EHR	fitness Wearable	AuthZ	Ethereum	Permissionless	PoW
S17	EHR	MIoT	AuthN and AuthZ	Hyperledger Fabric	Permissioned	PBFT
S18	PHR	MIoT	AuthN and AuthZ	Hyperledger Fabric	Permissioned	Kafka
S19	DHS	MIoT	AuthN and AuthZ	Hyperledger Fabric	Permissioned	PBFT
S20	m-Health	Smart Device	AuthN	Ethereum	Permissionless	PoW
S21	DHS	HIoT (General)	AuthN	Ethereum and Ripple	Permissionless , Permissioned	PoW (Ethereum)
S22	MIoT device security and management	MIoT	AuthN	Ethereum	Permissionless	PoW
S23	MIoT device security and management	MIoT	AuthN	Ethereum	Permissionless	PoA
S24	DSMS	MIoT	AuthZ	Ethereum	Permissionless	PoW

BC-based IAM systems commonly consist of a number of technical components [66]. Table 9 shows an analysis of the main components and technologies proposed by the reviewed studies, which are summarized as follows:

- **Blockchain:** based on the reviewed studies, there are two different types of BC used for proposing IAM solutions: (1) Identity management BC, such as Indy Hyperledger, which was used in [45]. This type of BC is dedicated for IAM solutions; (2) Smart Contract-supported BC technologies, such as Hyperledger Fabric and Ethereum BC, which are the most used by the reviewed studies as shown in Table 9.
- **Off-chain Protocol:** as BC should not be used as a storage because of storage limitations and high-processing costs, offloading solutions proposed to allow scalability in the IAM system. InterPlanetary File System (IPFS) was the most used off-chain storage technology in the IAM solutions proposed in the reviewed studies. Nine out of 24 studies used IPFS system as an Off-chain protocol. Some studies used other Off-chain technologies such as CouchDB and Software Guard Extensions (SGX) as shown in Table 9.
- **Smart Contracts:** as shown in Table 9 SCs are used by all proposed IAM solutions mainly to build the IAM access control logic, which is applied using the BC technology.
- **Identity Wallet and Database:** applications and database technologies used in the BC-based IAM to allow users to manage identifiers and store identity credentials (i.e., key values) included in the BC. For example, in Hyperledger Fabric, LevelDB is used as an embedded database and CouchDB is used as an external database to store identity key values. Table 9 shows CouchDB technology used mostly in the solutions. There are other technologies were used for this purpose such as OrbitDB, mobile applications, Indy Plenum Repository.
- **User Profile Management Methods:** external protocols allow storing data in encrypted Off-chain storage that manage user profile data, such as settings and transaction history. For example, OrbitDB technology was used by [49] for this purpose.
- **Data Exchange Methods:** an identity's credentials are mostly exchanged between the technologies (e.g., BC, IPFS, and CouchDB) using data interchange format and model, such as JSON. JSON model technology was mostly used in solutions for exchanging data between the AIM system layers and components.

TABLE 8. Comparative analysis to the solution functional performance, security requirements, and other considerations.

Study	Crypto-currency	SC	Mining	HIoT Identity	IdM/Revocation	IdM model	Throughput	Latency	Security REQS/Other considerations
S1	No	Yes	No	Yes	Yes, without revocation	Trusted Identity	(RT=2500T/s) (TT=1200T/s)	(RL=220ms) (TL=2500ms)	Confidentiality, Availability, Integrity, Privacy,Traceability, and Scalability.
S2	No	Yes	No	No	No	NA	NA	TL=2350ms	Privacy and HIoT device security.
S3	Yes	Yes	Yes	Yes	Yes, without revocation	Trusted Identity	(RT=1045T/s) (TT=4304T/s)	NA	Confidentiality and HIoT device security.
S4	Yes	Yes	Yes	Yes	No	NA	NA	NA	privacy, Scalability, and HIoT device security.
S5	Yes	Yes	Yes	No	No	NA	NA	1.7 s	Integrity and Privacy.
S6	Yes	Yes	Yes	Yes	Yes, without revocation	Trusted Identity	TT=119T/s	9s	Privacy and HIoT device authentication
S7	No	Yes	No	No	Yes, without revocation	Trusted Identity	NA	1200 ms	Privacy and Service quality
S8	Yes	Yes	Yes	Yes	Yes, without revocation	Trusted Identity	NA	NA	Privacy and HIOT device security
S9	No	Yes	No	No	Yes, without revocation	Trusted Identity	(QT=441T/s) (IT=152T/s)	(QL=12s)(IL=12s)	Privacy, Interoperability and Scalability.
S10	Yes	Yes	Yes	No	No	NA	NA	NA	Privacy
S11	No	Yes	No	No	Yes, without revocation	Trusted Identity	56 T/s	(QL=850ms) (IL=3516ms)	Privacy, Integrity, Reliability, and Scalability.
S12	No	Yes	No	Yes	Yes, with revocation	Trusted Identity	NA	NC	Confidentiality, Integrity, and Privacy.
S13	No	No	No	No	Yes, without revocation	Trusted Identity	NA	RL=200ms	Medical device authentication.
S14	Yes	Yes	Yes	No	No	NA	NA	NA	Confidentiality, Integrity, and Availability.
S15	No	Yes	No	Yes	Yes, without revocation	Trusted Identity	RT=120T/s	NC	Authenticity, Confidentiality, and Integrity.
S16	Yes	Yes	Yes	No	No	NA	NA	NA	Privacy
S17	No	Yes	No	No	Yes, with revocation	Trusted Identity	39.6 T/s	1.34 s	Privacy, Accountability, Revocability and Scalability.
S18	No	Yes	No	No	Yes, without revocation	Trusted Identity	(AT=140)(QT=166)	NC	Privacy
S19	No	Yes	No	Yes	Yes, without revocation	Trusted Identity	NA	(TL 20ms)(QL 4ms)	Efficiency, Availability, Scalability, and Interoperability.
S20	Yes	Yes	Yes	No	Yes, without revocation	Trusted Identity	NA	<60ms/100kB	Confidentiality, Integrity, Privacy, Untraceably, and Unforgeability.
S21	Yes	Yes	Yes	No	Yes, without revocation	Trusted Identity	NA	NA	Confidentiality , Integrity, Privacy, and Interoperability.
S22	Yes	Yes	Yes	Yes	No	NA	NA	NA	Integrity, Availability, Accountability and HIoT device ownership management.
S23	Yes	Yes	Yes	Yes	No	NA	NA	28ms	Confidentiality, Integrity, Privacy, and Medical device management (certifiebility).
S24	Yes	Yes	Yes	Yes	Yes, without revocation	Trusted Identity	NC	8.924ms	Confidentiality, Integrity, Privacy, Transparency, Traceability, and HIoT device authenticity.

Acronyms: Requirements (REQS), Transaction Throughput(TT), Read Throughput(RT),Transaction Latency(TL), Read Latency(RL), Query Throughput(QT), Invoke Throughput (IT), Query Latency(QL), Invoke Latency(IL), second(s), millisecond(ms), T/s(transaction per second) and Adding Throughput (AT). Not all studies exposed their functional performance, thus they are indicated by Not Available (NA). A few studies exposed their performance in the figures, however, without giving exact numbers, thus they are indicated by Not clear (NC). In the IdM model column, (NA) means not applicable as either the study focused on AuthZ operation or it only focused on the HIoT device AuthN.

- **Applications and Libraries:** applications are used to allow users to use the IAM systems to manage their data and credentials. Libraries and Application Programming Interfaces (APIs) are used to allow integration between applications and facilitate exchanging data between the IAM roles, such as requester, issuer, verifier, and

TABLE 9. Analysis of the components and technologies used by reviewed studies in the BC-based IAM system.

Study	Blockchain	Off-chain	SC	Identity wallet and DB	User Profile Methods	Data Exchange	APIs and Libraries
S1	Fabric	IPFS	Yes	OrbitDB	OrbitDB	JSON	Restful API
S2	Fabric	NA	Yes	Internally	NA	NA	Restful API
S3	Ethereum	IPFS	Yes	NA	NA	NA	NA
S4	Ethereum	NA	Yes	NA	NA	JSON	API
S5	Ethereum	NA	Yes	NA	NA	NA	Python API
S6	Ethereum	NA	Yes	NA	NA	NA	NA
S7	Fabric	IPFS	Yes	NA	NA	NA	Mobile app
S8	Ethereum	IPFS	Yes	NA	NA	NA	API
S9	Fabric	NA	Yes	NA	NA	NA	API
S10	Ethereum	IPFS	Yes	NA	NA	NA	NA
S11	Fabric	CouchDB	Yes	NA	NA	JSON	Restful API
S12	Fabric	IPFS	Yes	CouchDB	NA	NA	Restful API
S13	Indy	NA	Yes	Plenum	NA	NA	NA
S14	Ethereum	NA	Yes	NA	NA	JSON	API
S15	Fabric	SGX	Yes	NA	NA	NA	NA
S16	Ethereum	NA	Yes	Mobile app	NA	NA	NA
S17	Fabric	IPFS	Yes	CouchDB	NA	NA	API
S18	Fabric	NA	Yes	CouchDB	NA	NA	Restful API
S19	Fabric	IPFS	Yes	CouchDB	NA	JSON	Restful API
S20	Ethereum	NA	Yes	NA	NA	NA	Web3 API
S21	Ethereum + Ripple	NA	Yes	NA	NA	JSON	NA
S22	Ethereum	NA	Yes	NA	NA	NA	NA
S23	Ethereum	NA	Yes	NA	NA	NA	NA
S24	Ethereum	IPFS	Yes	NA	NA	JSON	NA

relying party. Restful API was used commonly in the solutions.

Aforementioned components are essential to have a functional IAM system [66]. It is clear from Table 9 that Hyperledger Fabric-based IAM solutions reasonably include more components than Ethereum-based solutions. This gives credibility to Hyperledger Fabric BC in terms of the system orchestration.

C. BC-BASED IAM IN HIoT ARCHITECTURE, SECURITY AND OTHER CONSIDERATIONS

Studies are reviewed to identify the main architecture layers of BC-based IAM in HIoT applications. Table 10 shows the architecture layers proposed by the reviewed studies. The User, Application, BC, Off-chain, Connectivity, and HIoT layers are the main layers in order to develop a functional system. The inclusion of these layers in the solutions was varied and the names were used differently. However, The concluded layered architecture of BC-based IAM in HIoT applications which fulfills the functional goals of the system is shown and explained in Figure 10.

There are a number of security threats in permissioned (e.g., Hyperledger Fabric) and permissionless (e.g.,Ethereum) BC-based applications [67]–[69], whereas there are security threats in IAM systems in HIoT applications [21]. A combination of the aforementioned security threats is shown in Table 11. Reviewed studies are analyzed to summarize the security threats in the BC-based IAM in HIoT applications. The main security threats are classified by the layered architecture of BC-based IAM in HIoT applications

TABLE 10. Architecture components of BC-IAM in HIoT proposed by reviewed studies.

Study No.	Architecture layers/Components
S1	Users, Decentralized application, BC, Off-chain, Connectivity, and HIoT.
S2	Stakeholders, BC, and HIoT.
S3	Users, BC, Off-chain, Gateway, and HIoT.
S4	Storage, Provision, and HIoT.
S5	Storage, Business, and Application.
S6	Rule-based AI system, Clinic, Hospital, and HIoT.
S7	Users, Off-chain, SC, Mobile edge computing, and Smart device.
S8	Users, BC, Off-chain, and HIoT.
S9	Users, Smart device, Gateway, BC, and Network.
S10	Users, BC, and Smart device.
S11	Application, BC, Network, and HIoT.
S12	Users, BC, Mobile edge computing, Cloud gateway, Off-chain, Communication, Application, and HIoT.
S13	Users, BC, and HIoT.
S14	Users, BC, and Gateway.
S15	BC, Cloud, Edge, and HIoT.
S16	Users, BC, Mobile app, Web app, and HIoT.
S17	Users, Storage, and Control.
S18	System management, Data collection, BC, Cloud, and Application.
S19	Users, BC, E-health system, Electronic medical record management system, and HIoT data servers
S20	N/A
S21	Users, BC, Cloud, Edge, application, and HIoT.
S22	Users, BC, and HIoT.
S23	Users, BC, and HIoT.
S24	User, BC, Off-chain, and Edge Mining layer.

as shown in Figure 10. The layered architecture and related security threats are summarized as follow:

- **User Layer:** this layer represents the stakeholders in the system who play functional roles, such as HIoT users, data consumers and system administrators. The identity

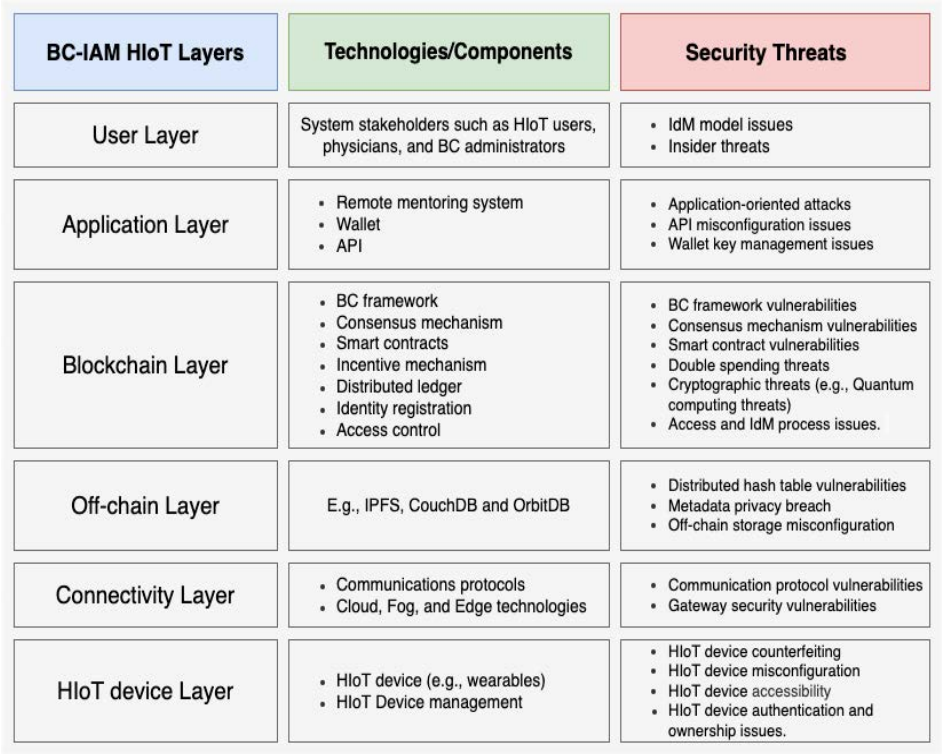


FIGURE 10. Layered architecture and security threats in BC-based IAM systems in HIoT applications.

TABLE 11. Security threats in BC and HIoT applications.

Asset	Security threats/Vulnerabilities/Attacks
Permissioned BC/ Permissionless BC	Contract Vulnerability, Framework Vulnerability, Dependency Vulnerability, Cryptographic Vulnerability, Denial of Service, Network Partitioning, Malicious Consensus Behavior, Consensus Configuration Manipulation, Identity Provider Compromise, Peer-to-Peer system vulnerabilities, Application oriented attacks, Sybil attack, Double spending attack, 51 percent attack, Deanonymization attack, Replay attack, SC reentrancy attack, Selfish mining attack, and Quantum computing threat.
HIoT	Spoofing, Eavesdropping, Accessibility, Counterfeiting, Hardware Threats, Tampering, Collisions, Jamming, Sybil attacks, Exhaustion attacks, Node failure and outage, Misconfiguration, interruption, DDoS, MIMA attacks, and Fabrication.

management governance model is at the core of any IAM system. As shown in Table 8, all solutions are based on trusted authority models in the proposed systems. Trusted authority model might lead to insider threat when these trusted identities misbehave and breach the rules.

- **Application Layer:** this layer includes user interfaces, remote monitoring systems, wallets, and APIs work on a Blockchain network. Reviewed studies provided BC-based IAM solutions and as the focus was on harnessing BC for this purpose, not all security threats are considered. Security threats in the application layer were not focused on in these studies, however, according to [69] and as summarized in Table 11, there are some attacks which target the application layer. Additionally, misconfiguration of technologies such as APIs and wallets that include metadata related to identities in the BC-based systems could lead to privacy breaches [66].
- **Blockchain Layer:** this layer is at the core of the IAM system. The BC layer components such as consensus mechanisms play a vital role in BC technology. Identity management systems rely on these mechanisms in order to manage identities' data. Thus, selecting the strongest and most secure consensus mechanisms protect identities' data security. Otherwise, they might be a source of security threats and vulnerabilities exploited by hackers by adding malicious transactions in the BC network. Studies such as [50] and [61], used alternate consensus mechanisms such as Solo and Kafka, which might impact the core of the system security when are exploited by hackers.

  BC layer can be targeted by some of attacks such as spoof attacks, sybil, substitution, Denial of Service (DoS), replay, and impersonation attacks [42].Thus, the use of countermeasures is vital to protect HIoT users' identity data. For example, in [61], the endorsement, sorting, and verification mechanism was used to prevent replay attacks in order to secure identity data. Moreover, attacks that are based on powerful processing computing, like Quantum, is another vital concern for all cryptography-based systems. Quantum has a promising futuristic application, which can be used by hackers to break encryption and cryptography-based systems easily [42]. As BC technologies are mainly based on

cryptography, this aspect needs to be considered as a threat and countermeasure solutions need to be taken into account for this long term concern.
The Smart Contract is another essential key player in any BC-based IAM system. Smart Contracts format the rules and policies of access control that are used in AuthN, and, if not programmed securely, might breach confidentiality. Smart Contracts have limited storage capability and should not be used beyond it. They are vulnerable to reentrancy attacks [53]. Evaluation tools and formal methods techniques can help to reduce the risk that might form vulnerable Smart Contracts. Moreover, Table 8 shows the solutions built using crypto-currency-based BC technologies such as Ethereum and Bitcoin. This kind of BCs is vulnerable to the double spending issue which is used by attacks such as 51 percent attack. Double spending breaches the integrity of the decentralized IAM system ledger. To tackle this security issue, studies like [50] used the MultiVersion Concurrency Control technique in the Hyperledger Fabric to eliminate double spending which exists in Ethereum and Bitcoin.

- **Off-chain Layer:** this layer is a complementary layer used to enhance the functionality of the BC-based system. Off-chain technologies are used to offload data from the BC network and to allow exchanging identity data between stakeholders and applications. Identity's data history and metadata are also stored Off-chain. Identity data should be stored securely to ensure integrity and privacy. In general, off-chain storage are less privacy-preserving than on-chain storage [66], thus security risks caused by using them need to be carefully studied. IPFS which relies on a distributed hash table was used widely in the solutions as an off-chain for storing data. Off-chain storage such as IPFS can cause security and privacy threats when it is misconfigured [70]. Similarly, privacy and security of other off-chain storage such as CouchDB which was used in [56], need to be considered in the BC-based IAM system.
- **Connectivity Layer:** the connectivity layer involves HIoT technologies, communications, and gateways used between layers in the system, such as cloud, fog, edge, Hypertext Transfer Protocol (HTTP), MQ Telemetry Transport (MQTT), and Constrained Application Protocol (CoAP). HIoT ecosystem is vulnerable to some attacks, such as Distributed Denial of Service (DDoS), Man-In-The-Meddle (MITM) attack [48], and it lacks standardized communication protocols [42].
- **HIoT device Layer:** this layer represents the HIoT device used in the system. HIoT devices as shown in Figure 2 are available in a wide range of forms. Medical IoT as shown in Figure 7 are the most HIoT devices used in the reviewed studies. AuthN of MIoT identities and ensuring HIoT ownership are crucial aspects in HIoT applications, as the number of counterfeited MIoT devices is rising. To tackle the counterfeiting of HIoT, HIoT AuthN and ownership issues, studies in [47], [48], and [65] covered the Medical IoT ownership issue and proposed proof-of-ownership solutions using Smart Contracts and Physical Unclonable Function (PUF) based AuthN mechanisms to tackle this security issue. Moreover, HIoT device layer is venerable to physical acces- sibility issues [42].

A number of non-functional requirements and considerations are discussed in the proposed solutions, such as confidentiality, integrity, availability, scalability, privacy, interoperability, trust, auditability, tracebility, unforgeability, relaibility, usability, service quality, and accountability as shown in Table8. Some of these considerations and requirements are related to IAM security, such as confidentiality, integrity, availability, privacy, unforgeability, and accountability. There are different concepts used to improve the quality of service, such as processing time, energy consumption, and memory usage in the IAM systems. For example, in [53], an offloading scheme was used to improve latency and decrease energy consumption. It is worth noting here that using solutions like this, which add additional layers in the system, open other security considerations in these new layers. Moreover, although, studies like [53], [62], [64], provided a distributed system between a number of hospitals and organizations for interoperability, it should be considered that they should use recommended interoperability standards like HL7/FHIR. HL7/FHIR standards recommend an understandable unified format for medical data to be exchanged, thus ensuring data availability.

Applying BC in HIoT is a complicated task. HIoT are resource-constrained devices that have specific standards and security requirements to work without faults and security breaches, so these aspects need to be carefully considered [53]. HIoT are prone to limitations like storage constraints, heterogeneity, privacy and security vulnerabilities, network complexity, and poor interoperability. BC also has limitations and security vulnerabilities [71]. Thus, data protection regulations like GDPR, health-related data protection standards like the US Health Insurance Portability and Accountability Act (HIPAA), and HIoT security requirements and threats [21], should be considered in the BC-based IAM HIoT applications. The proposed solutions strove to overcome and tackle some of these challenges. Although, the majority of studies did not consider the HIoT constraints, a number of studies built BC-based IAM systems with considerations to HIoT constraints. They mainly proposed additional hub layers between the BC layer and the HIoT layer to tackle the IAM operations. In [50] IEEE 802.15.6 WBAN security standards were used and the computation resource constrained issue was considered in HIoT by using multiple system layers. Researchers in [42] discussed the security challenges related to HIoT such as HIoT device heterogeneity, accessibility, lack of standardized communication protocols, and the vulnerability to attacks such as DDoS and data manipulations. Researchers in [43] discussed HIoT protocols, namely, MQTT and the need to lightweight AuthN solutions for the

resource constrained reasons and proposed BC-based solution considering this issue. Also, [56] separated the HIoT device from the BC system considering the computation and security resource constrained in the HIoT device. In [48] PUF AuthN mechanism used to tackle the computation limitation of HIoT devices. While in [65] BC-based IAM system was proposed with a consideration to the security and the limited computation resource capability in the HIoT device. Moreover, although not all studies consider HIoT identities, studies in [42], [44], [46]–[49], [51], [52], [57], [62], and [65], consider HIoT identities in the AuthN operation which is essential for HIoT device security, as shown in Table 8.

Although the majority of the studies considered the privacy aspect, data protection regulations like GDPR and HIPAA are barely considered in the the solutions. Security and privacy requirements should be based on standards and regulations. The minimum privacy that can be provided is to develop a concrete access management system. Patients should control access to their medical data, but should not be able to edit them. When accessing data, privacy of data should be preserved, which includes personal information like name, address, phone number. Privacy techniques should preserve and not sacrifice data integrity. Additionally, HIoT user privacy should be preserved while sharing, uploading and auditing data. Examples of privacy preserving mechanisms that can be proposed for preserving medical data privacy are deferential privacy and K-anonymity [72]. Access control can preserve privacy to some extent. However, studies in [61], [63], and [47], proceeded to comply with HIPAA and GDPR regulations by proposing additional privacy mechanisms, i.e., pseudo-identity, zero-knowledge-based anonymity, and pseudo-identity mechanisms, respectively.

The limitations of the BC technologies need to be considered before adopting them. Not all BC technologies can satisfy non-financial applications, as cryptocurrency is still the core substance of the majority of BC technologies, except the few as shown in Table8. The results showed that the most used BC technology is Ethereum [42]–[44], [47], [48], [51], [52], [55], [58], [59], [63]–[65], which is a cryptocurrency-based permissionless peer-to-peer network, followed by Hyperleger Fabric [46], [49], [50], [53], [54], [56], [57], [60]–[62], which is a permissioned BC technology. In permissioned BCs, only chosen and known participants can access data, whereas in permissionless BCs, all participants in the network can access data. According to Braunstein [73], permissioned BCs are the most appropriate BC technologies for healthcare applications where the participant identities should be known to one another.

Another critical consideration that impacts the security and functionality of BC-based IAM systems is the consensus mechanism used in the BC. The consensus mechanism in Ethereum BC is PoW, which is based on a mining mechanism used in order to add new blocks to the chain. On the other hand, the consensus mechanism used in Hyperledger Fabric is Practical Byzantine Fault Tolerance (PBFT). In PBFT, an agreement is made between the participants in the network based on a specific number of bad nodes that can be tolerated. There are two main disadvantages to mechanisms like PoW that are based on cryptocurrency. First, they require mining, which takes considerable time to process new data and this does not satisfy the fast transmission that HIoT applications need. Second, they are based on the cryptocurrency concept, which might be costly in high-volume data systems like HIoT applications. On the other hand, a study conducted by Nguyen *et al.* [74], demonstrated that using PBFT can cause a delay in transmitting data in critical infrastructure systems. To eliminate these pitfalls, some developers use alternate consensus mechanisms [50], [61], which can allow malicious transactions to be mined in the BC network. This aspect should be considered when developing IAM BC-based solutions for HIoT.

Smart Contracts, which are programmable rules and polices used to provide AuthZ and access control in IAM systems, were used in all reviewed studies as shown in Table 8. Smart Contracts are used to implement the logic of the access control, which is then guaranteed by the BC technology. There are different programming languages used to program Smart Contracts, such as Solidity in Ethereum and Go and JavaScript in Hyperledger Fabric. According to Wang *et al.* [28], some of Smart Contracts programs are vulnerable to security attacks for bugs in the programs. Thus, choosing the best programming language and using evaluation tools to check Smart Contracts before using them in the BC are paramount.

The main advantage in using BC is the ability to eliminate the dependency on a single trusted third party. Although BC can provide two identity management models, SSI and decentralized trusted identity, the results show that all studies that proposed identity management adopted the decentralized trusted identity model as shown in Table 8.

Although a number of studies showed encouraging results based on the performance evaluations conducted in the studies, it is noticed that there are two critical points in the evaluation process: 1) the proposed solutions were mostly compared with other solutions based on other BC solutions. It is true that this might give an indication of the performance evaluation of the application, however, this does not mean the solution satisfies the IAM for HIoT security requirements, as these requirements are not considered fully in the first place in these BC applications, 2) there are no agreed metrics to evaluate the solution performance. Table8 shows a comparative analysis showing the functional performance, security requirements, and other considerations in the reviewed studies. The throughput and latency proprieties are used in the studies to evaluate the solution performance, however, the evaluation factors and units (e.g., Query, Read, Adding, Invoke, ms, and s) are different from study to study and from BC platform to another platform (e.g., Hyperledger Fabric and Ethereum). Moreover, the security aspect was not evaluated by the majority of studies. Hyperledger fabric-based solutions seemed more evaluated systematically than Ethereum-based studies as they use Hyperledger Caliper as a benchmark tool

to measure the application performance. However, both lack a systematic security-based evaluation.

D. ADDITIONAL POINT

Brogan *et al.* [25] and Zheng *et al.* [75], proposed IAM solutions based on IOTA Distributed Ledger Technology (DLT) for HIoT applications, which is different than BC technology. IOTA is another kind of DLT. It has a different data structure. IOTA has potential as a decentralized technology for IAM solutions, however, it is in early stages. It is a worthwhile topic to be studied and considered as a solution for IAM in HIoT, particularly, as it is suitable for IoT-based systems.

VII. LIMITATIONS AND FUTURE DIRECTION

Although this literature review study followed a systematic approach to ensure accuracy and eliminate bias, there are some limitations worth noting: 1) this study focused on studies written in the English language between 2016 and 2021, 2) the functional performance of the solutions was not investigated in detail as our study focused on the security aspect, however, it was covered to gain insights about the evaluation metrics used, 3) this study focused on BC applications, other DLT applications like IOTA are out of the study scope, and 4) according to other review studies that cover different parts of the BC-IAM in HIoT, security requirements and threats which are identified do not cover all security requirements and threats in BC-Based IAM in HIoT.

As noted in our study, a unified security framework for BC-based IAM solutions for HIoT applications is required. Moreover, there is a lack of security risk assessments for BC-based IAM systems in HIoT applications. BC-based IAM solutions for HIoT need to be evaluated based on ISMS standards like ISO 27001, and to comply with data protection regulations like GDPR and HIPAA. Future work will address the development of a comprehensive security framework for BC-based IAM systems in HIoT applications.

VIII. CONCLUSION

BC-based IAM solutions for HIoT applications were evaluated in this systematic literature review. A total of 24 peer-reviewed studies were investigated to explore the security aspect of the BC-based IAM solutions in HIoT applications to examine the security requirements and threats related to BC-based IAM systems in HIoT. Security, functional, and non-functional aspects of BC-based IAM were discussed, main architecture components and technologies, and the architecture of BC-based IAM systems in HIoT and related security threats were summarized. We outlined that there are some security and functional considerations that need to be considered in the chosen BC solution before implementation. In addition, the functional and security evaluation aspects of BC-based IAM systems require further investigation.

REFERENCES

[1] R. S. Istepanian and B. Woodward, *M-Health: Fundamentals and Applications*. Hoboken, NJ, USA: Wiley, 2016.

[2] S. M. Riazul Islam, D. Kwak, M. Humaun Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[3] S.-C. Cha, T.-Y. Hsu, Y. Xiang, and K.-H. Yeh, "Privacy enhancing technologies in the Internet of Things: Perspectives and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2159–2187, Apr. 2019.

[4] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access control in the Internet of Things: Big challenges and new opportunities," *Comput. Netw.*, vol. 112, pp. 237–262, Jan. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128616303735

[5] L. Ismail, H. Materwala, A. P. Karduck, and A. Adem, "Requirements of health data management systems for biomedical care and research: Scoping review," *J. Med. Internet Res.*, vol. 22, no. 7, Jul. 2020, Art. no. e17508. [Online]. Available: https://www.jmir.org/2020/7/e17508

[6] D. Anand and V. Khemchandani, "Identity and access management systems," in *Security and Privacy of Electronic Healthcare Records: Concepts, Paradigms and Solutions*. London, U.K.: The Institution of Engineering and Technology, 2019, p. 61.

[7] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Appl. Innov.*, vol. 2, nos. 6–10, p. 71, 2016. [Online]. Available: https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf

[8] Y. Zou, T. Meng, P. Zhang, W. Zhang, and H. Li, "Focus on blockchain: A comprehensive survey on academic and application," *IEEE Access*, vol. 8, pp. 187182–187201, 2020.

[9] B. Houtan, A. S. Hafid, and D. Makrakis, "A survey on blockchain-based self-sovereign patient identity in healthcare," *IEEE Access*, vol. 8, pp. 90478–90494, 2020.

[10] I. Indu, P. M. R. Anand, and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges," *Eng. Sci. Technol., Int. J.*, vol. 21, no. 4, pp. 574–588, Aug. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2215098617316750

[11] S. V. Sudarsan, O. Schelén, and U. Bodin, "Survey on delegated and self-contained authorization techniques in CPS and IoT," *IEEE Access*, vol. 9, pp. 98169–98184, 2021.

[12] X. Zhu and Y. Badr, "Identity management systems for the Internet of Things: A survey towards blockchain solutions," *Sensors*, vol. 18, no. 12, p. 4215, Dec. 2018. [Online]. Available: https://www.mdpi.com/1424-8220/18/12/4215

[13] L. Florio, *The Dark Side of Things*. Cham, Switzerland: Springer, 2019, pp. 107–117, doi: 10.1007/978-3-030-15705-0_8.

[14] *EU General Data Protection Regulation (GDPR)—An Implementation and Compliance Guide*, IT Governance, Ely, U.K., 2017. [Online]. Available: https://www.itgovernanceusa.com/download/EU-GDPR-Implementation-and-Compliance-Guide.pdf

[15] W. L. Sim, H. N. Chua, and M. Tahir, "Blockchain for identity management: The implications to personal data protection," in *Proc. IEEE Conf. Appl., Inf. Netw. Secur. (AINS)*, Nov. 2019, pp. 30–35. [Online]. Available: https://ieeexplore.ieee.org/document/8968708

[16] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K.-R. Choo, "A systematic literature review of blockchain cyber security," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 147–156, May 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352864818301536

[17] B. Cremonezi, A. Vieira, J. A. Nacif, and M. Nogueira, "Survey on identity and access management for Internet of Things," Federal Univ. Parana, Brazil, Tech. Rep., 2020. [Online]. Available: https://assets.researchsquare.com/files/rs-66793/v1_covered.pdf?c=1631840523

[18] C. Butpheng, K.-H. Yeh, and H. Xiong, "Security and privacy in IoT-cloud-based e-health systems—A comprehensive review," *Symmetry*, vol. 12, no. 7, p. 1191, Jul. 2020. [Online]. Available: https://www.mdpi.com/2073-8994/12/7/1191

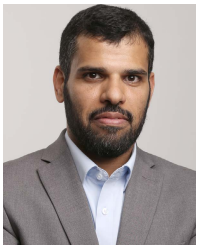
[19] *From Innovation to Implementation: eHealth in the WHO European Region*, World Health Org., Regional Office Eur., Geneva, Switzerland, 2016. [Online]. Available: https://apps.who.int/iris/bitstream/handle/10665/326317/9789289051378-eng.pdf

[20] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Future Generat. Comput. Syst.*, vol. 78, pp. 659–676, Jan. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X17307677

[21] M. Mamdouh, A. I. Awad, A. A. M. Khalaf, and H. F. A. Hamed, "Authentication and identity management of IoHT devices: Achievements, challenges, and future directions," *Comput. Secur.*, vol. 111, Dec. 2021, Art. no. 102491. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404821003151

[22] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, 3rd Quart., 2016.
[23] R. Colomo-Palacios, M. Sánchez-Gordón, and D. Arias-Aranda, "A critical review on blockchain assessment initiatives: A technology evolution viewpoint," *J. Softw., Evol. Process.*, vol. 32, no. 11, p. e2272, Nov. 2020. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/smr.2272
[24] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.
[25] J. Brogan, I. Baskaran, and N. Ramachandran, "Authenticating health activity data using distributed ledger technologies," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 257–266, Jan. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2001037018300345
[26] A. Tandon, A. Dhir, A. K. M. N. Islam, and M. Mäntymäki, "Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda," *Comput. Ind.*, vol. 122, Nov. 2020, Art. no. 103290. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0166361520305248
[27] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Jun. 2017, pp. 557–564.
[28] H. Wang, Y. Wang, Z. Cao, Z. Li, and G. Xiong, "An overview of blockchain security analysis," in *Cyber Security*, X. Yun, W. Wen, B. Lang, H. Yan, L. Ding, J. Li, and Y. Zhou, Eds. Singapore: Springer, 2019, pp. 55–72.
[29] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, "A survey on access control in the age of Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 4682–4696, Jun. 2020.
[30] S. Ravidas, A. Lekidis, F. Paci, and N. Zannone, "Access control in Internet-of-Things: A survey," *J. Netw. Comput. Appl.*, vol. 144, pp. 79–101, Oct. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S108480451930222X
[31] M. Kuperberg, "Blockchain-based identity management: A survey from the enterprise and ecosystem perspective," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1008–1027, Nov. 2020.
[32] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Blockchain-based identity management systems: A review," *J. Netw. Comput. Appl.*, vol. 166, Sep. 2020, Art. no. 102731. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804520302058
[33] I. Butun and P. Österberg, "A review of distributed access control for blockchain systems towards securing the Internet of Things," *IEEE Access*, vol. 9, pp. 5428–5441, 2021.
[34] M. A. Bouras, Q. Lu, F. Zhang, Y. Wan, T. Zhang, and H. Ning, "Distributed ledger technology for eHealth identity privacy: State of the art and future perspective," *Sensors*, vol. 20, no. 2, p. 483, Jan. 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/2/483
[35] K. Cameron. (2005). The Laws of Identity. Microsoft Corp. [Online]. Available: https://docs.microsoft.com/en-us/previous-versions/dotnet/articles/ms996456(v=msdn.10)
[36] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *Int. J. Surg.*, vol. 8, no. 5, pp. 336–341, 2010. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1743919110000403
[37] S. Keele, "Guidelines for performing systematic literature reviews in software engineering," Technical report, Ver. 2.3 EBSE Technical Report. EBSE, Tech. Rep., 2007.
[38] B. Kitchenham, "Procedures for performing systematic reviews," Keele Univ., Keele, U.K., Tech. Rep., TR/SE-0401, 2004.
[39] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proc. 18th Int. Conf. Eval. Assessment Softw. Eng.*, 2014, pp. 1–10. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/2601248.2601268
[40] P. Dunphy and F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security Privacy*, vol. 16, no. 4, pp. 20–29, Jul./Aug. 2018.
[41] O. Jacobovitz, "Blockchain for identity management," Dept. Comput. Sci., Lynne William Frankel Center Comput. Sci., Negev, Israel, Tech. Rep. 16-02, 2016. [Online]. Available: https://www.cs.bgu.ac.il/~/TechnicalReports/2016/16-02.pdf
[42] K. P. Satamraju and B. Malarkodi, "A decentralized framework for device authentication and data security in the next generation internet of medical things," *Comput. Commun.*, vol. 180, pp. 146–160, Dec. 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366421003492
[43] K. P. Satamraju and M. B, "Proof of concept of scalable integration of Internet of Things and blockchain in healthcare," *Sensors*, vol. 20, no. 5, p. 1389, Mar. 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/5/1389
[44] R. Kumar and R. Tripathi, "Towards design and implementation of security and privacy framework for internet of medical things (IoMT) by leveraging blockchain and IPFS technology," *J. Supercomput.*, vol. 77, no. 8, pp. 7916–7955, Aug. 2021.
[45] A. Gibson and G. Thamilarasu, "Protect your pacemaker: Blockchain based authentication and consented authorization for implanted medical devices," *Proc. Comput. Sci.*, vol. 171, pp. 847–856, Jan. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050920310632
[46] Y. Gao, H. Lin, Y. Chen, and Y. Liu, "Blockchain and SGX-enabled edge-computing-empowered secure IoMT data analysis," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15785–15795, Nov. 2021.
[47] M. Alblooshi, K. Salah, and Y. Alhammadi, "Blockchain-based ownership management for medical IoT (MIoT) devices," in *Proc. Int. Conf. Innov. Inf. Technol. (IIT)*, Nov. 2018, pp. 151–156.
[48] R. Akkaoui, "Blockchain for the management of Internet of Things devices in the medical industry," *IEEE Trans. Eng. Manag.*, early access, Jul. 29, 2021, doi: 10.1109/TEM.2021.3097117.
[49] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "HealthBlock: A secure blockchain-based healthcare data management system," *Comput. Netw.*, vol. 200, Dec. 2021, Art. no. 108500. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128621004382
[50] J. Wang, K. Han, A. Alexandridis, Z. Chen, Z. Zilic, Y. Pang, G. Jeon, and F. Piccialli, "A blockchain-based eHealthcare system interoperating with WBANs," *Future Gener. Comput. Syst.*, vol. 110, pp. 675–685, Sep. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X19321247
[51] M. Tahir, M. Sardaraz, S. Muhammad, and M. Saud Khan, "A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics," *Sustainability*, vol. 12, no. 17, p. 6960, Aug. 2020. [Online]. Available: https://www.mdpi.com/2071-1050/12/17/6960
[52] V. Puri, A. Kataria, and V. Sharma, "Artificial intelligence-powered decentralized framework for Internet of Things in healthcare 4.0," *Trans. Emerg. Telecommun. Technol.*, Mar. 2021, Art. no. e4245. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4245
[53] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "BEdgeHealth: A decentralized architecture for edge-based IoMT networks using blockchain," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11743–11757, Jul. 2021.
[54] M. Kumar and S. Chand, "MedHypChain: A patient-centered interoperability hyperledger-based medical healthcare system: Regulation in COVID-19 pandemic," *J. Netw. Comput. Appl.*, vol. 179, Apr. 2021, Art. no. 102975. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804521000023
[55] H. S. Z. Kazmi, F. Nazeer, S. Mubarak, S. Hameed, A. Basharat, and N. Javaid, "Trusted remote patient monitoring using blockchain-based smart contracts," in *Proc. Adv. Broad-Band Wireless Comput., Commun. Appl.*, L. Barolli, P. Hellinckx, and T. Enokido, Eds. Cham, Switzerland: Springer, 2020, pp. 765–776.
[56] F. Jamil, S. Ahmad, N. Iqbal, and D.-H. Kim, "Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals," *Sensors*, vol. 20, no. 8, p. 2195, Apr. 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/8/2195
[57] T. Hewa, A. Braeken, M. Ylianttila, and M. Liyanage, "Multi-access edge computing and blockchain-based secure telehealth system connected with 5G and IoT," in *Proc. IEEE Global Commun. Conf.*, Dec. 2020, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9348125
[58] V. Geetha and B. Balakrishnan, "A user authentication and access control scheme for IoT-based healthcare using blockchain," in *Proc. 12th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, Jul. 2021, pp. 1–7. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9579992

[59] T. Frikha, A. Chaari, F. Chaabane, O. Cheikhrouhou, and A. Zaguia, "Healthcare and fitness data management using the IoT-based blockchain platform," *J. Healthcare Eng.*, vol. 2021, pp. 1–12, Jul. 2021.
[60] D. El Majdoubi, H. El Bakkali, and S. Sadki, "SmartMedChain: A blockchain-based privacy-preserving smart healthcare framework," *J. Healthcare Eng.*, vol. 2021, pp. 1–19, Nov. 2021.
[61] Z. Chen, W. Xu, B. Wang, and H. Yu, "A blockchain-based preserving and sharing system for medical data privacy," *Future Gener. Comput. Syst.*, vol. 124, pp. 338–350, Nov. 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X21001734
[62] S. Biswas, K. Sharif, F. Li, Z. Latif, S. S. Kanhere, and S. P. Mohanty, "Interoperability and synchronization management of blockchain-based decentralized e-Health systems," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1363–1376, Nov. 2020.
[63] R. Attarian and S. Hashemi, "An anonymity communication protocol for security and privacy of clients in IoT-based mobile health transactions," *Comput. Netw.*, vol. 190, May 2021, Art. no. 107976. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128621001079
[64] E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O.-Y. Song, A. K. Bashir, and A. A. A. El-Latif, "DITrust chain: Towards blockchain-based trust models for sustainable healthcare IoT systems," *IEEE Access*, vol. 8, pp. 111223–111238, 2020.
[65] R. Akkaoui, X. Hei, and W. Cheng, "EdgeMediChain: A hybrid edge blockchain-based framework for health data exchange," *IEEE Access*, vol. 8, pp. 113467–113486, 2020.
[66] L. Lesavre, P. Varin, P. Mell, M. Davidson, and J. Shook, "A taxonomic approach to understanding emerging blockchain identity management systems," 2019, *arXiv:1908.00929*.
[67] B. Putz and G. Pernul, "Detecting blockchain security threats," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Nov. 2020, pp. 313–320.
[68] E. Zamani, Y. He, and M. Phillips, "On the security risks of the blockchain," *J. Comput. Inf. Syst.*, vol. 60, no. 6, pp. 495–506, Nov. 2020.
[69] M. Iqbal and R. Matulevičius, "Blockchain-based application security risks: A systematic literature review," in *Proc. Adv. Inf. Syst. Eng. Workshops*, H. A. Proper and J. Stirna, Eds. Cham, Switzerland: Springer, 2019, pp. 176–188.
[70] L. Balduf, S. Henningsen, M. Florian, S. Rust, and B. Scheuermann, "Monitoring data requests in decentralized data storage systems: A case study of IPFS," 2021, *arXiv:2104.09202*.
[71] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.
[72] Y. Chen, L. Meng, H. Zhou, and G. Xue, "A blockchain-based medical data sharing mechanism with attribute-based access control and privacy protection," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–8, Jul. 2021, doi: 10.1155/2021/6685762.
[73] M. L. Braunstein, *Health Informatics on FHIR: How HL7's New API is Transforming Healthcare*. Cham, Switzerland: Springer, 2018, doi: 10.1007/978-3-319-93414-3.
[74] T. S. L. Nguyen, G. Jourjon, M. Potop-Butucaru, and K. L. Thai, "Impact of network delays on hyperledger fabric," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2019, pp. 222–227, doi: 10.1109/INFCOMW.2019.8845168.
[75] X. Zheng, S. Sun, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Meré, "Accelerating health data sharing: A solution based on the Internet of Things and distributed ledger technologies," *J. Med. Internet Res.*, vol. 21, no. 6, Jun. 2019, Art. no. e13583. [Online]. Available: https://www.jmir.org/2019/6/e13583/



BANDAR ALAMRI received the B.S. degree from Taibah University, Medina, Saudi Arabia, and the M.S. degree from the University of Bedfordshire, Luton, U.K., all in computer science. He is currently pursuing the Ph.D. degree in computer science at the University of Limerick, Ireland. His research interests include studying the security of blockchain, and using blockchain in identity and access management systems in the internet of things and e-Health applications.

KATIE CROWLEY received the B.Sc. degree in computer science from University College Cork, the M.Sc. degree in computer science from the University of Limerick, and the Ph.D. degree from University College Cork. She is a Lecturer and a Researcher with the Department of Computer Science and Information Systems, University of Limerick. She is a member of Lero—the SFI Research Centre for Software, and the Health Research Institute. She is currently the Course Director for the master's program in health informatics. Her research interests include affective computing, human computer interaction, and health information technology.

ITA RICHARDSON is a Professor of software quality with the University of Limerick, and the Principal Investigator at Lero—the Science Foundation Ireland Research Centre for Software. She has supervised 20 Ph.D. students to completion and has over 200 publications, many of which focus on digital health and regulation in healthcare software. She has received research funding from SFI, European Union, Irish Research Council, Enterprise Ireland, and many companies, including De Puy and IBM.