Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.066579

REVIEW

Security Challenges and Analysis Tools in Internet of Health Things: A Comprehensive Review

Enas W. Abood[1], Ali A. Yassin[2,*], Zaid Ameen Abduljabbar[2,3,4,*], Vincent Omollo Nyangaresi[5,6], Iman Qays Abduljaleel[2], Abdulla J. Y. Aldarwish[2] and Husam A. Neamah[7,8]

[1]Department of Mathematics, College of Science, University of Basrah, Basrah, 61004, Iraq
[2]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, 61004, Iraq
[3]Department of Business Management, Al-Imam University College, Balad, 34011, Iraq
[4]Shenzhen Institute, Huazhong University of Science and Technology, Shenzhen, 518000, China
[5]Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Bondo, 40601, Kenya
[6]Department of Applied Electronics, Saveetha School of Engineering, SIMATS, Chennai, 602105, Tamil Nadu, India
[7]Department of Electrical Engineering and Mechatronics, Faculty of Engineering, University of Debrecen, Otemeto u.4-5, Debrecen, 4028, Hungary
[8]College of Engineering, National University of Science and Technology, Dhi Qar, 64001, Iraq

*Corresponding Authors: Ali A. Yassin. Email: ali.yassin@uobasrah.edu.iq;
Zaid Ameen Abduljabbar. Email: zaid.ameen@uobasrah.edu.iq

Received: 11 April 2025; Accepted: 28 July 2025; Published: 23 September 2025

ABSTRACT: The digital revolution era has impacted various domains, including healthcare, where digital technology enables access to and control of medical information, remote patient monitoring, and enhanced clinical support based on the Internet of Health Things (IoHTs). However, data privacy and security, data management, and scalability present challenges to widespread adoption. This paper presents a comprehensive literature review that examines the authentication mechanisms utilized within IoHT, highlighting their critical roles in ensuring secure data exchange and patient privacy. This includes various authentication technologies and strategies, such as biometric and multi-factor authentication, as well as the influence of emerging technologies like blockchain, fog computing, and Artificial Intelligence (AI). The findings indicate that emerging technologies offer hope for the future of IoHT security, promising to address key challenges such as scalability, integrity, privacy and other security requirements. With this systematic review, healthcare providers, decision makers, scientists and researchers are empowered to confidently evaluate the applicability of IoT in healthcare, shaping the future of this field.

KEYWORDS: Internet of health things; authentication; privacy; fog-computing; blockchain; AI

1 Introduction

Over the past three decades, the Healthcare System (HCS) has undergone extensive changes and improvements globally [1]. However, the healthcare sector faces numerous challenges, including continuous population growth, behavioral changes, shifting lifestyles, and a range of chronic and infectious diseases. These challenges have necessitated the design of advanced technological implementations and systems that monitor, measure, forward and disseminate health-related data to the relevant stakeholders. This has been demonstrated to help meet the needs of patients, families, and service providers [2].

The HCS framework is a testament to the value of collaboration among diverse group of people, institutions and information communication technology resources to address medical needs and services. While HCSs vary and differ across countries and cultures, they still share fundamental components: the human and physical resources [3]. The human component encompasses various roles, including system supervisors, service providers, and employees responsible for feeding the system with data, analysis, and maintenance, among others. This component also includes users who have the authority to browse, read, modify, and work on data as patients, doctors, or medical technicians [4]. Meanwhile, the physical component comprises peripheral devices, such as sensors, wearable devices, radiology equipment, analytical instruments, and others, which provide feedback to the system regarding the patient's condition, diagnosis, and medical treatment [5]. Cloud computing represents one such physical resource, where numerous devices support diverse functions such as transferring and controlling data among components [6]. The cloud systems are characterized by local or global servers, peripheral computers for browsing and access, as well as mobile devices for users or doctors to interact with and utilize the system's functionality [7,8].

The Internet of Things (IoT) has become a crucial component in the success of various services across multiple fields related to networked information systems [9]. IoT comprises physical objects or 'things' embedded with sensors, software, and other technologies that enable data exchange and interconnection of entities (people and devices) over the Internet [10]. These connected "things" can be industrial elements, sensors, household items, or mobiles. Basically, IoT components are responsible for collecting and sharing data, allowing smart and highly efficient operations and decision-making across various sectors, such as smart cities, commerce, healthcare and educational systems [11]. As explained in [12], healthcare is one of the common applications of IoT, as healthcare data requires high regulatory and security strategies [12].

The traditional HCS was built based on the IoT architecture, referred to as the Internet of Health Things (IoHT) [13] or Internet of Medical Things IoMT [6], based on how systems react to data. Basically, IoHT is a system to monitor and alert, while IoMT is a system to monitor and treat [14,15]. Fig. 1 illustrates the main elements of a typical IoHT system.

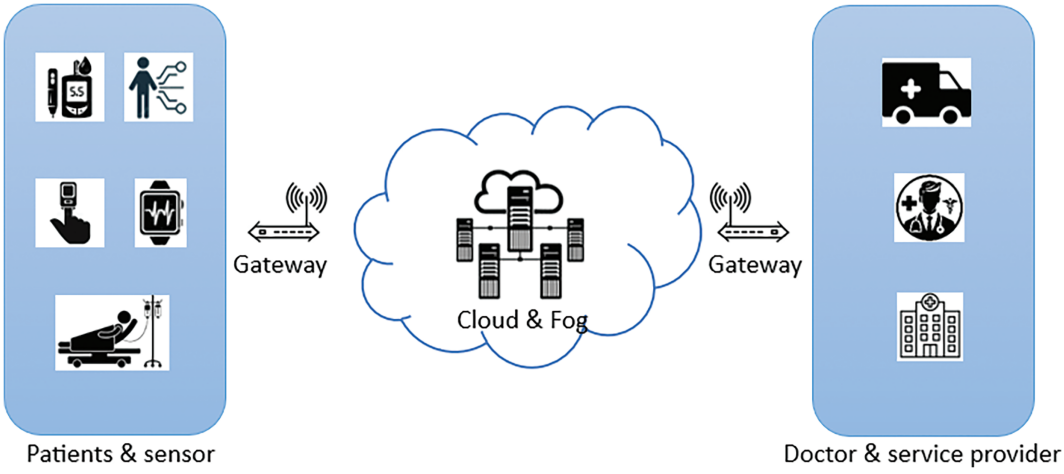

Figure 1: IoHT system

Medical devices in IoHT are designed to collect and analyze a wide range of data. These devices connect to sensors that track patient physiological data such as blood pressure, sugar, heart rate, and body temperature. Additionally, data on other activities unrelated to diseases, such as sleep patterns or walking can be monitored and collected [12,16]. Furthermore, IoHT devices have implicit algorithms for

analysis, decision-making, and writing reports. This helps enhance medical care and support the healthcare systems even in the absence of medical staff [17,18]. This advancement has played a crucial role in managing chronic diseases such as diabetes and heart disease. As such, IoHT provides assurance about the potential of technology in improving the healthcare sector [19].

With the increasing number of connected devices, systems, and the diversity of data and connected networks, the IoHT continues to evolve and mature. However, this technological development comes with various risks and challenges arising from the amount of data processed and transmitted via different networks. Such risks include healthcare data leakages, modifications, integrity violation, and unauthorized access [20,21]. For instance, a report by Censys reveals that nearly 14,004 unique IP addresses threaten healthcare devices and data systems on the public internet, exposing them to the risk of unauthorized access, with potentially many more devices remaining invisible. Meanwhile, the FBI's 2023 Internet Crime Report identifies the Healthcare and Public Health sector as the primary targets for ransomware attacks [22]. Another concern in IoHT is data sharing, ownership, and protection from unauthorized access and host–provider intrusion. Therefore, strict regulatory and security strategies are required [12]. As such, researchers and practitioners have been exploring and developing many technologies to mitigate these risks, including cyber and physical attacks [23,24].

In IoHT, authentication is the primary and most critical line of defense for safeguarding exchanged data. In an IoHT environment, effective authentication and access management are essential due to the volume and sensitivity of healthcare data and applications. In addition, robust security protection is required due to the critical role these systems play in patient care, which remains vulnerable to various cyber threats [25]. Some of the well-known malicious attacks in IoHT include Denial of Service (DoS), Man-In-The-Middle (MITM) [26], malware infections, spoofing, replay, phishing, and insider attacks [27]. Therefore, there is need to implement and evaluate robust authentication techniques so as to ensure the secure management of IoT devices [28]. Consequently, numerous security techniques, algorithms, models, frameworks, protocols, and methods have been presented in literature [29].

Ideal authentication systems for IoT must help preserve integrity, privacy, and availability [30]. In addition, other features such as confidentiality, key agreement, scalability, and password change, are required to ensure comprehensive security [31]. Although traditional password-based authentication is simple, cost-effective, and does not require extra devices or tokens, it poses significant security challenges. For instance, passwords are easy to hack, and can be obtained through conventional eavesdropping and fraudulent methods [16,20]. Meanwhile, the hacked account risks differ based on the role played by the authenticated user. For example, a patient exposing data faces a lower risk than a doctor or employee with authority to access and modify that data [32].

Apart from password-based solutions, several biometric authentication methods have been proposed to protect medical information and securely manage data flows [33]. In biometric authentication, unique physical characteristics of individuals are utilized for identification and security [34]. To achieve this, many biometric features are deployed, ranging from fingerprints, facial, voice, iris, to palms [35,36]. These methods are considered highly secure due to the unique traits of the individual entities that cannot be easily cloned [34,37]. In addition, these methods provide user-friendly authentication, reducing the risk of stealing or replicating passwords. As explained in [34], biometric traits enhance security by applying multi-factor authentication. In spite of all the advantages, biometric authentication suffers from privacy concerns since the entities involved give their bio information. In addition, biometric authentication systems are costly and can experience recognition failure, as well as potential inaccuracies such as false positives or false negatives [31].

Artificial intelligence (AI) learning mechanisms play a vital role in developing and implementing advanced authentication systems to detect hacking or attacks. In addition, AI helps create approaches or applications that monitor and evaluate any processes or indicators related to any access by intruders, determine its severity, and establish whether it is acceptable or not [38]. The most well-known AI learning architectures are deep learning (DL) methods and machine learning (ML) algorithms [39]. In a nutshell, AI systems can observe and learn from user behavior over time and repeated attempts, providing continuous real-time authentication, immediately detecting anomalies and suspicious activities [40]. However, it's crucial to note that AI can also be utilized as an attack vector to enhance the effectiveness and sophistication of cyberattacks. This potential underscores the urgency of developing robust security measures, as AI can leverage its capabilities to deceive targets and manipulate automated phishing attacks [41], malware Development, as well as brute force attacks. This is accomplished by the prediction of likely passwords based on user behavior and common patterns, as well as exploiting network weaknesses more efficiently and effectively [42]. However, these AI systems may suffer from complexity, misidentification, training data quality dependency, and cost-related issues [40,43].

Essentially, IoHT systems must be available anytime and anywhere, ensuring easy accessibility and user-friendliness [44]. To the greatest extent possible, IoHT systems should remain effective even during crises or outages and operate seamlessly across different devices and platforms. To achieve this, it is necessary to adopt decentralization in the design of IoHT [45]. Recently, a decentralized and distributed ledger technology, referred to as Blockchain (BC), has been developed. This technology plays a crucial role in preventing unauthorized access and data breaches through cryptographic techniques [46]. It is utilized in authentication through transaction verification, presenting unalterable and trustable authentication technique [47]. In addition, Blockchain uses cryptography to ensure that only authorized users can access or manipulate authentication information, providing a reassuring layer of security [48].

Another decentralized computing infrastructure is Fog Computing (FC), which increases the utility of network edges by allowing them to implement data operations (process, store, analysis) instead of depending on centralized cloud servers [49]. FC is effective in enhancing authentication for IoHT systems through the reduction of authentication time. It also offers real-time verification with multi-layered security such as local firewalls and intrusion detection systems [50]. Furthermore, FC contributes to scalability by facilitating the addition of nodes and terminals whilst maintaining system consistency and performance. As explained in [51], FC supports Multi-Factor Authentication (MFA) through the incorporation of authentication at various system layers [51].

The main contributions of this paper are illustrated as follows:

1. Providing a comprehensive and chronological literature review of authentication techniques to understand the evolution of security in IoHT systems.
2. The analysis of common authentication methods and security requirements, along with the integration of traditional and AI techniques, is a significant aspect of this research. This integration holds the potential for improved threat detection in IoHT systems. Examining how FC and BC are utilized to enhance the security requirements of the IoHT environment, focusing on authentication mechanisms.
3. This paper helps bring out the transformative potential of AI-based tools that offer semantic robustness in addressing security challenges in the IoHT environment.
4. Discussing security vulnerabilities, their detection and corresponding countermeasures using ML and DL algorithms and BC techniques.
5. Providing an overview of the formal tools and testing methodologies for analyzing security protocols.
6. Finally, we discuss several studies that combined various models and methods to strengthen privacy and safety, identifying critical security gaps.

The rest of the article is organized as follows: Section 3 discusses the IoHT system model, including architecture, security requirements, threats and solutions. Sections 4 and 5 describe various IoHT security tools and security analysis tools, respectively. On the other hand, Section 6 provides a review of related works in IoHT. In contrast, Section 8 highlights future concerns that should be considered in the development of IoHT systems, underscoring the need for further research and development in this area. Finally, Section 9 concludes the paper.

2 Data Collection Procedure

A systematic literature search was conducted in Google Scholar, Scopus and IEEE Library, adhering to the guidelines of Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA), a widely accepted framework for conducting systematic reviews. To ensure comprehensive coverage of the relevant research landscape, the search terms included "Internet of Things", "IOT", "IOHT", "IOMT", "IODT", and to further refine the search, the terms "Blockchain", "IPFS", and fog computing were also incorporated in combination with "Healthcare system". Additionally, inclusion criteria were English language articles published in reputable journals, available in full text, and published in the period (2005–2025) to capture both the early development and more recent advancements in the field. Following the initial search based on the inclusion criteria, a total of 974 articles were swiftly and efficiently filtered by title and abstract with irrelevant papers promptly excluded ensuring a streamlined and time-efficient process.

Duplicate articles were also filtered to finally yield 183 articles, which were deemed the most relevant and comprehensive for the study. Notably, 39 articles of the final chosen articles were IoHT-relevant systematic reviews and survey articles. Fig. 2 shows the PRISMA flowchart outlining search and inclusion criteria.

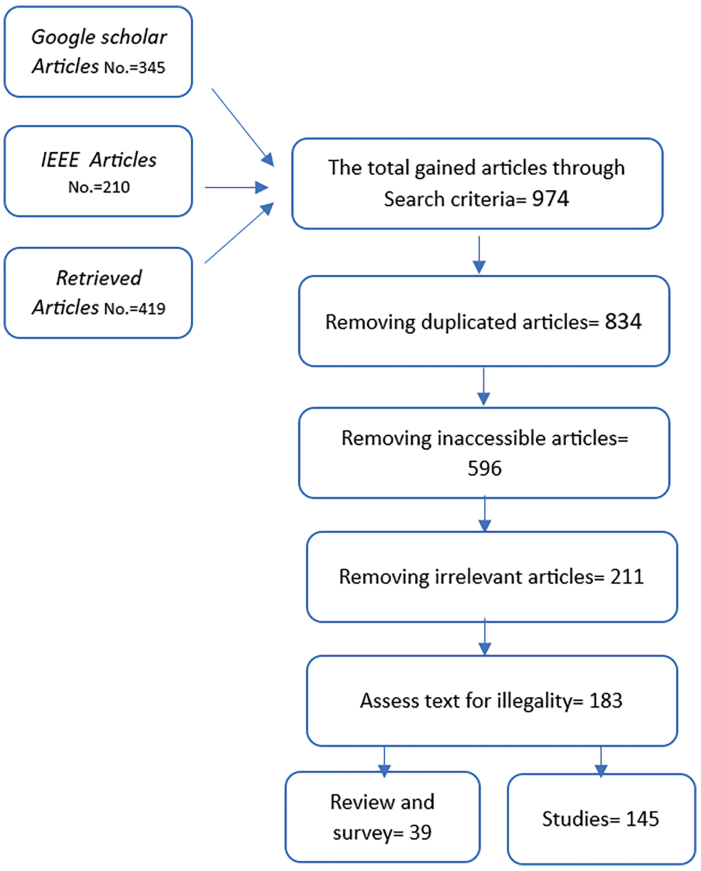

Figure 2: PRISMA flow chart

The resulting research articles in this review were selected based on a classification framework that includes the types of authentications, the technology used, the application, and the assessed risks shown in Table 1.

Table 1: Classification framework for IoHT studies

Category	Subcategory/Specifics	Description/Examples
Types of authentications	Password authentication, factor-based (single, multi), factor types (biometrics, password), Device-based, Token-based, Digital certificates.	How to authenticate between users or devices in a way that ensures secure access to systems or data.
Technology used	Cloud computing, Fog computing, Centralization (blockchain, IPFS), AI/ML algorithms.	The hardware and software technologies incorporated in the system.
Application	Remote patient monitoring, Chronic disease management, WBAN, Telemedicine.	The use case or health service that the system addresses.
Evaluated risks	Security requirements and goals (privacy, integrity, confidentiality, authenticity and authority) and Security threats (hacking, eavesdropping, Tampering and others).	Security concerns and threats studied and evaluated.

3 System Model

The IoHT system model comprises of a set of interconnected devices and heterogeneous technologies that manage and analyze patient and healthcare data. This ranges from physical components such as measuring devices and sensors, to software components for collection, analysis and monitoring, along with their connective entities to cloud platforms to facilitate the sharing process [52].

3.1 IoHT Model Architecture

System architecture refers to the high-level organization of system elements and the interconnections between them [53]. There are unified standards for the general architecture of the IoTs, consisting of either 3, 4 or 7 layers [54] as described below.

According to [1], the three-layers model is the basic IoHT model consisting of the perception layer (works on sensors, gadgets, and other devices), network layer (maintains the connectivity between IoT contents), and the application (the user interaction interface). On the other hand, the four-layers model [55,56] comprises of the sensing layer (sensors in IoT device), network layer (communication channel), data processing layer (the main data processing unit), and the application layer (user interface). As explained in [57,58], the seven-layers model is made up of the collaboration and processes layer (humans and business processes), application layer (user interface), data abstraction layer (data reconciling, semantics, completeness and integration), data accumulation layer (real-time data formatting for later use), edge (fog) computing layer (data analysis and transformation), connectivity layer (data communication networks), and the physical devices and controllers layer (actuators and gadgets).

Although the terms (IoT) and (IoHT) share the same general architecture, they differ in the applications of connected devices [59]. IoHT specifically focuses on healthcare applications and devices that monitor, sense vital indicators, and improve wellness of the patients. Such devices include wearables, such as smartwatches, and pressure measurement sensors. On the other hand, such applications include fitness and heart monitors [15]. According to [39], IoHT is a model of the internet of things specialized in

the healthcare sector. In IoHT, the seven-layered architecture provides a comprehensive framework that enhances the modularity of each layer by replacing or maintaining each layer individually. In addition, it provides adaptability and scalability to a certain extent by integrating new devices or techniques without disrupting existing functionalities, interoperability, and multiple levels of security. This serves to enhance efficiency in data collection and management, user experience, and flexibility, making it superior to simpler architectures [41]. Fig. 3 gives an illustration of this seven-layered architecture. In order to achieve adaptation and scalability, IoHTs are normally integrated with FC, as discussed in Section 4.2.

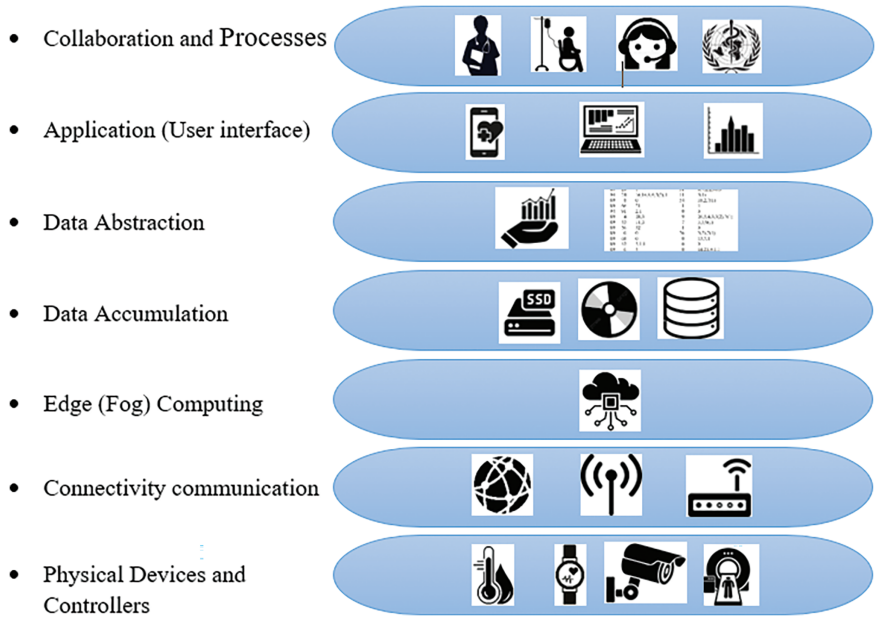

Figure 3: Seven-layers IoHT architecture

3.2 IoHT Security

The protection of data in the IoHT systems is a major focus in studies within the healthcare field. This is due to its critical role in upholding healthcare data privacy, reliability of individuals and devices in the healthcare sector, and the overall protection of the system. In most of the conventional IoHT sytems, medical data is stored in centralized storage systems [17]. However, this centralization leads to a single point of failure, privacy [36], and security concerns attributed to the single architecture deployed for storing and processing data [23].

3.3 IoHT Security Requirements

The essential security requirements of IoHT include access control, integrity, confidentiality, non-repudiation, availability, forward secrecy, backward secrecy, and scalability [60]. Here, access control is divided into two concepts: mutual authentication and authorization [61]. As discussed in [62], mutual authentication is the process of reciprocally confirming system entities, users, or devices on both sides, thereby granting permission to access system resources [62]. On the other hand, authorization is a mechanism that regulates access permissions and controls network resources for authorised users or devices only. This authorization is based on various principles such as Role-based access control (RBAC), Attribute-based access control (ABAC), also known as policy-based access control (PBAC) or claims-based access control (CBAC). In RBAC, resource access is restricted based on a person's role within an organization [63]. It is based

on the levels of access that users have to the network. Therefore, access is granted based upon several factors, such as authority, responsibility, and job competency [61]. However, in ABAC, permissions are established and restricted according to specific positions, including department, location, managerial oversight, and time of day [63].

As discussed in [64], data integrity is crucial in ensuring data consistency, reliability, and accuracy, all of which are important for patient safety. In IoHT, several factors, such as human error, system failures and manipulation by cyber threats, can compromise data integrity. Therefore, various processes and controls are implemented to maintain data integrity, such as data validation, access controls, backups, error detection and correction techniques, and audits. On the other hand, non-repudiation ensures that entities cannot deny or dispute the legitimacy of any communication or transaction. It is considered as an important accountability tool in the occurrence of an attack [65]. With regard to confidentiality, its goal is to keep sensitive data secure and protected from unauthorized access [12], while availability guarantees accessibility of the services and data when required [33]. This implies keeping the system operable and usable at all times.

The authors in [66] have defined forward secrecy as the process of ensuring that each session has a unique and invulnerable key which cannot be re-used in the new session. On the other hand, backward secrecy ensures that if a long-time key used for all sessions has been compromised, the attacker cannot utilize it to decrypt previous messages or gain access to current or future communications [67]. Regarding scalability, the components of the system must seamlessly adapt and evolve with the dynamic evolution of communication systems [15]. In terms of key sizes, salability depends on the key block size and increases exponentially with the increase in block size [64]. To support anonymity, an individual's identity must be concealed and not revealed to others so as to render an individual unidentifiable. It is often sought for various reasons, such as protecting users, safeguarding the privacy of vulnerable individuals or maintaining personal security and safety [68]. On the flipside, anonymity can also be used to conceal illegal or unethical activities, which raises concerns about the potential misuse of anonymity [67].

As discussed in [69], decentralization guarantees that there is no dependency on central authorities, which strengthens the system's security and functionality by maintaining synchronised transactions. The distributed computational power simplifies the management and operation of the network. In addition, decentralization offers various features, such as data availability, responsibility, scalability, and mitigates single-point failure problems [70]. With regard to attacks prevention, the authors in [71] explain that devoid of security resistance mechanisms in IoHT, attacks will outweigh all the system's benefits. This can cause network capacity reduction, misrouting, latency, data disclosure, and other problems. The authors in [59] have explained that IoHT is susceptible to various types of attacks, such as spoofing, data altering, replay, Denial of Service (DoS), Sybil, node capture and many more, as discussed in Section 3.4.

3.4 IoHT Security Threats

The continuous development of the IoHT structure, integration of heterogeneous devices and technologies, and the criticality of healthcare data have made it a target of numerous cyber-attacks and threats. Therefore, they have been concerted efforts in developing security techniques to curb these threats and vulnerabilities, and hence maintain the security of the IoHT system [60]. The authors in [65] explain that the impact of vulnerabilities is more pronounced in authentication models based on centralized and traditional databases. In addition, the decentralized systems have also been subjected to security attacks that damage and breach sensitive data. In this regard, the IoHT system may be susceptible to the following cyber-attacks and threats:

- **Brute-force and dictionary attacks:** These are considered the simplest attacks on networks, requiring basic computer and software knowledge to gain unauthorized access to systems, accounts, or encrypted

data. In healthcare systems, the data includes patient, care and tracking, device management and treatment, and other network data and accounts. The attacker uses sophisticated devices and software to try out many possible combinations of passwords and accounts and try different encryption keys until they obtain the correct choice. Accounts with weak passwords and simple keys are easily hacked in these ways [60]. To withstand these attacks and reduce the likelihood of successful compromise, strong passwords should be combined, multi-factor authentication and secure password storage techniques [27].

- **Man-in-the-middle attacks:** MITM attacks are remotely carried out by intercepting the communication channel between two entities. In addition, authentication phase can be compromised, allowing snooping on or changing of the data being exchanged [72]. In the IoHT system, the attacker intercepts communication channels between legitimate components in the healthcare system (such as the patient, devices, healthcare service, or medical records) [52]. To face MITM attacks, employ strong encryption with valid certificates, mutual authentication, forward secrecy, and implement secure protocols and channels like HTTP [71].
- **An eavesdropping attack:** This refers to the unauthorized interception of patients' and healthcare data transmitted over the communication channels or the cloud. As discussed in [73], one of the facilitating factor for these attacks is the transmission of plain data using non-secure protocols. This attack may be used to collect or alter information, causing system failure. To eliminate such attacks, approaches that focus on detecting unauthorized interception of data are needed. Such approaches utilize ensemble learning methods that combine ML for detection and network breach monitoring [73].
- **Spoofing:** In this threat, attackers impersonate the identity of an authorized device or account to obtain data. Afterwards, adversaries can use network resources, or steal and sabotage them. This exposes violates the privacy of the patients and can lead to failure of the health system [74]. Several types of spoofing threats exist, including IP address spoofing, manipulation of DNS records, using hidden phones or numbers, or even using Media Access Control (MAC) in the case of local networks. According to [75], spoofing is usually overcome by using multi-factor authentication or secure protocols such as Dynamic Host Configuration Protocol (DHCP).
- **Distributed Denial-of-Service (DDoS) attacks:** These threats prevent legitimate IoHT users from accessing network resources by overwhelming the network with excessive requests, making it unavailable. These attacks are implemented by multiple entities trying to block access to a service for legitimate users [76]. Attackers may conceal or manipulate the service's IP address to prevent access or utilize various sources and devices to target a service provider, distracting it from serving its legitimate users [77]. DDoS defense requires layered strategies: immediate response, resilience, and long-term planning, such as limiting traffic from individual IP addresses sent to the server to prevent overload, blocking malicious traffic, and employing AI techniques to monitor service requests [64].
- **Sybil attacks:** These attacks aim to steal data using malware that impersonates a legitimate user. The Sybil node assumes multiple identities to simultaneously appear in various locations, which threatens data safety and the utilization of IoHT resources. In a nutshell, Sybil looks like many ordinary users but it is one masquerade node [71]. Cryptographic techniques, including key exchange, digital signatures, and an Asymmetric Proof-of-Work defense algorithm, can mitigate Sybil attacks by authenticating node identities and messages, preventing unauthorized nodes from joining the network [78].
- **Physical attacks:** These threats are carried out through direct attacks on IoHT devices. They can also destroy the infrastructure of the IoHT systems. These attacks intentionally tamper with the functionality of the devices connected to the network, sabotage them, and make them inoperable. As such, they take them out of service, losing or altering the data, potentially threatening the safety of patients, healthcare systems as well as disrupting its services [5]. Protection from these attacks is achieved by

providing physical protection for network devices, encrypting stored data, and integrating protection and tampering detection programs into the devices [71].

- **Botnet attacks:** It is a group of network devices infected with malware, commonly referred to as zombies. These devices are controlled by the attacker, who performs various activities such as stealing and changing data, launching a DDoS attack, and distributing malicious spam messages on email. These attacks are detected by monitoring traffic, observing abnormal patterns, and securing devices with authentication and strong passwords [79].
- **Node capture**: This attack gains access to a crucial node or group of nodes in the system to steal data stored on IoHT network devices [80], to protect against these attacks, it is preferable to employ robust encryption algorithms for stored data to prevent its content from being exposed by untrusted nodes [81].
- **Timing attack:** In this attack, the adversary analyzes the responding time of the devices and attempts to find vulnerabilities to be used in the hack, to eliminate timing attacks, constant-time algorithms should be implemented, utilizing blinding and cryptographic methods, and regular network monitoring and testing [82].
- **Malicious code attack:** These attacks are carried out by malicious programs called computer viruses, which are intended to damage or ruin internet devices and applications, defending against malicious code involves using security software like firewall, keeping them updated, restricting user permissions, securing networks and maintaining backups [83].
- **Impersonation attacks:** These threats involve a malicious adversary pretending to be a trusted entity to reveal sensitive information or transactions [67]. To stop impersonation attacks, employ multi-factor authentication and enforce strong, unique passwords, digital certificates, strong access controls, adding strategies of anomaly detection, secure communication, user education, and performing verification processes within the authentication protocol [84].
- **Replay attacks:** Here, adversaries capture and reuse valid authentication messages to gain unauthorized access, effectively halting replay attacks requires many strategies: exchanged data encryption and timestamping to ensure that each communication is unique and cannot be reused maliciously [85].
- **Hijacking attack:** In this type of attack, the adversaries try to steal or predict the session key of an authorized user to gain unauthorized access. Active hijacking attacks can manipulate or alter the client's connection. On the other hand, passive hijackers can only monitor or capture network traffic or information [86]. On the other hand, these attackers can be undermined using strong authentication with MFA, a strong password, and RBAC to restrict unauthorized access, as well as using secure session protocols and system monitoring strategies for anomalies [87].
- **51% attack:** Suppose an entity or group of malicious users control (s) over 50% of the BC or decentralized network. In that case, they will have the ability to alter the cryptocurrency blockchain. This can prevent access to new transaction confirmations, obstruct payment, or reverse non-confirmed transactions that were completed [88]. Some implementations may prevent 51% attacks like promoting decentralization, using resistant consensus algorithms (POS), implementing economic penalties, monitoring network distribution, and layer security measures [89].
- **Forgery attack:** In this attack, the adversary impersonates a legitimate entity to gain unauthorized access, allowing access and manipulating data [90]. This attack is typically accomplished through utilizing forged data or employing man-in-the-middle attack techniques. Fortunately, these attacks are often mitigated and thwarted using machine learning techniques [91]. Table 2 shows each layer of attack and the security requirements it violates.

Table 2: The attacks on every layer of the IoT

Layers	Attacks	Security threatens
Perception layer	Eavesdropping	Confidentiality
	Spoofing	Authentication
	Physical attacks	Confidentiality, integrity, and availability
	Node capture	Confidentiality, and availability
	Timing Attack	Authentication
	Forgery Attack	Authentication and confidentiality
Network layer	DDoS Attack	Availability
	MITM	Authentication, confidentiality and integrity
	Spoofing	Authentication
	Brute-force and dictionary attacks	Authentication and confidentiality
	Sybil Attack	Confidentiality, integrity, and availability
	Botnet attacks	Confidentiality, integrity, and availability
	51% attack	Integrity and security
Application layer	Brute-force and dictionary attacks	Authentication and confidentiality
	DDoS Attack	Availability
	MITM	Authentication, confidentiality and integrity
	Malicious code attack	Authentication, confidentiality and integrity
	Cross-site scripting	Authentication
	Replay attack	Authentication, confidentiality and integrity
	Hijacking Attack	Authentication, confidentiality and integrity
	51% attack	Integrity and security

3.5 IoHT Security Requirements Enforcement

Globally, the security, safety and privacy of healthcare systems are supervised by international organizations such as the US Food and Drug Administration (FDA) and the European Medicines Agency (EMA). These organizations establish the necessary laws and technologies to protect and secure data and devices for the entire healthcare system [92], in addition to expanding their roles to include supervision and evaluation of medical products. Moreover, these organizations supervise the development and deployment of health information systems to protect privacy and data security. On the same breadth, they prevent breaches which threaten the safety of the patient and the healthcare system [93].

Over the recent past, traditional solutions have been prevalent in detecting attacks, intrusions, and attempts to maliciously control access [45]. However, the dynamic and evolutionary nature of IoHT networks, coupled with their continuous complexity renders traditional methods such as password and email authentication insufficient [93]. These techniques are unable to handle the complexity, continuous evolution, and expansion of modern attack methods, as well as network complexity [94]. Fortunately, AI-based solutions, such as DL, ML and other technologies, have been presented to support such developments. These solutions are characterized by the ability to collect, analyze data and detect breaches as well as anomalies in real-time. This helps in developing responses to various cyber threats [95]. One of the most important security considerations in IoHT is access control, which is the basic mechanism for regulating

who or what is allowed to access network resources. Basically, access control ensures that only authorized entities can access the network and use its applications, data, devices, and other network components [16,96]. The basic tenets of access control include authentication, authorization and integrity.

1. *Authentication*

Authentication systems incorporate AI techniques to achieve high security standards and enhance privacy [37,97]. One of the common strategies for AI-based authentication is DL due to its ability to collect and analyze large amounts of data with complex patterns such as biometric, facial or behavioral patterns [98]. Another mechanism for access control is based on attributes, using federated deep learning (FDL). This technique allows multiple parties to train a model collaboratively while keeping their data decentralized. This helps get optimal access parameter threshold, producing high data privacy and integrity [20]. In addition, other ML techniques have an important role in IoHT authentication for enhancing security, improving utility and facilitating the management of healthcare devices [99,100]. These methods areas based on neural learning utilizing legitimate and malicious access data for training. The trained models help in detecting suspicious requests in authentication and access control processes [21]. Over the recent past, BC has been used as an authentication tool, owing to its characteristics such as decentralization, smart contracts (SCs), distributed ledgers and two keys crypto instead of traditional passwords [24]. Nevertheless, numerous security challenges have been identified in BC networks. To mitigate BC attacks, DL or ML techniques have been integrated with BC as a hybrid system with high protection features [101].

2. *Authorization*

Authorization is a process that typically follows authentication and is used to grant an individual or system permission to access network resources or perform actions within a system or network. This is achieved after verifying the identity of the user [102]. Authorization is crucial in specifying which resources a user can access and what actions they can perform. These actions include read, write, or execute files, based on predefined permissions and roles [1]. Some researchers have proposed secure SDN-based frameworks for healthcare systems to provide trusted services for patients using MAC addresses to control authorization for legitimate users [103]. Meanwhile, other researchers have developed access control mechanisms for healthcare data using symptom matching technology. These techniques are based on blind signatures which are used to maintain privacy and ensure that only authorized people engage in data exchange. In addition, some researchers have developed continuous authentication techniques to support access to authorized users [98]. To implement continuous authentication, IoHTs employ biometric factors, behavioral patterns, contextual or multiple factors, as well as ML and anomaly detection. The specific choice of continuous authentication mechanisms depends on the capabilities and security requirements of the system [104].

3. *Data integrity*

Data integrity in IoHT is important because it directly relates to patient health and the healthcare system. Integrity represents the accuracy, consistency, and reliability of data collected and exchanged across the healthcare system entities [105]. As such, numerous security solutions have emerged to protect data from changes and breaches. In addition to imposing many restrictions, other approaches include limiting IoHT use to authorized users, and providing updated firmware [106].

In spite of the above efforts, a number of attacks have emerged that threaten data integrity. Such risks include tampering, poisoning, and alteration. Consequently, much research efforts have been directed towards AI and decentralized techniques to find effective solutions [5]. For instance, authors in [107] have presented a decentralized AI healthcare system based on FDL to secure patient health record data and maintain its privacy as well as integrity. Other researchers have utilized BC technology to secure and protect

data integrity from potential security breaches. The attacks in BC are attributed to its distributed nature, as well as the inclusion of smart contracts and cryptographic technologies [21]. In addition, other researchers have adopted two-step authentication through the integration of BC with the cloud to offer two levels of protection: authentication and integrity [108].

4 IoHT Security Tools

This section presents some of the most common cryptographic primitives frequently deployed to offer protection in an IoHT environment.

4.1 Cryptographic Tools

- **Elliptic Curve Cryptography (ECC)**

ECC is one of the newest, strongest, and most secure encryption techniques compared with most encryption techniques [11]. This technique is also lightweight and hence enhances authentication speeds. It relies on elliptic curve for generation of security tokens. ECC uses standard point multiplication as a mathematical operation for encryption, and is considered a leap from classical encryption to modern encryption [109].

The elliptic curve is mathematically represented by the equation below.

$$y^2 = x^3 + ax + b$$

Let G be a point on the curve (generator point), which is used to produce a cyclic group of points [110]. These points lie on that elliptic curve and are generated by multiplying G by an integer $k \in \{1, 2, \ldots, N-1\}$, where N is the number of points on the curve. Therefore, these values are multiples of $G \rightarrow \{G, 2G, \ldots, (N-1)G\}$.

ECC is based on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP). This problem is very cumbersome and requires powerful computers to break solve. Basically, these computers need to expose k given the value of public key G [59,111]. Mathematically, ECC needs to find a scalar k that helps derive the following.

$$P = k * G$$

This multiplication process is used to generate asymmetric encryption keys where P is the public key value, while k represents the private key [112].

- **SHA-256**

SHA-256 is a cryptographic hash function developed by the National Security Agency (NSA) in the United States. It is designed to withstand various attacks. This function takes any value as input and converts it to a fixed hash length of 256 bits, which makes it resistant to data alteration attacks. As such, it upholds the integrity of the data and prevents it from being exposed. SHA-256 is fast and computationally inexpensive. The algorithm of this function works in several steps: first the data are divided into blocks of 512 bits. This is followed by the hash calculation step in which a series of logical and arithmetic operations are performed to expand and compress the blocks, ultimately producing a hash of 256 bits [113].

- **Shamir's Secret Sharing (SSS) Algorithm**

Secret sharing is a cryptographic technique for securely distributing pieces of private information called *shares* amongst a distributed group or network such that each group member receives only one share without

information about the original secret. The SSS algorithm is based on the property of polynomial interpolation over a finite field. The linear polynomial can be reconstructed by two or more points (i.e., shares S_1 and S_2). Consequently, the secret is disclosed by (0) = Secret. However, if we have only one share (S_1), it is impossible to reconstruct the linear polynomial and disclose the secret [114].

In general, any polynomial of degree $t-1$ can be obtained only by (s *hares* => t) where t is the number of shares required to reconstruct the secret. According to [20], the threshold (t) should be less than or equal to the total number of group members (n) who share the secret.

- **Advanced Encryption Standard (AES)**

AES is a symmetric encryption mechanism that uses a single key for encryption and decryption. Mathematically, AES encryption is expressed as follows.

$$C = E(K, P)$$

where P is the plaintext message and C is the resulting ciphertext. The system's security relies on the secrecy of the key K [115].

AES encryption involves several cryptographic operations that utilize a symmetric key. These operations include dividing data into 128-bit blocks, repeatedly applying substitution, permutation, and key-dependent operations. As explained in [79,115], the number of rounds varies with key size, with longer keys providing stronger encryption.

- **Bilinear Pairing (BP)**

This is an asymmetric cryptographic technique that involves using a mathematical principle referred to as bilinear mapping [116]. Mathematically, BP can be expressed as follows.

$$e : G_1 x G_2 \rightarrow G_T$$

where G_1 is additive, G_2 is multiplicative while G_T represents a multiplicative group [79].

The function e must satisfy the bilinear condition below:

$$E(P^a, Q^b) = e(P, Q)^{ab}$$

where $P \in G_1$, $Q \in G_2$, a and $b \in Z$.

BP has a wide application in cryptography. For instance, this technique has been deployed in attribute-based encryption (ABE) and short signatures [117].

- **Harmonic Cryptography (HC)**

HC is a modern cryptographic technique that unlike traditional methods relies on algebraic structures and cryptographic hashes. It offers an efficient alternative by using mathematical waveforms for encryption [118]. HC employs sinusoidal transformations to derive a dynamic keystream a process that is both efficient and effective. HC is designed to be robust with scaling factors derived from the key and a varying frequency per encryption cycle.

$$K(t) = \alpha \sin(\omega t + \theta) + \beta \cos(\omega t + \varnothing)$$

where α and β are scaling factors derived from the key ω is the frequency which is varying per encryption cycle. Both θ and $\varnothing$ are used to maximize entropy [119]. It encrypts data by transforming the cryptographic key into a numeric harmonic signature, applying sine and cosine transformations to the data, and XORing the result with the generated waveform [119]. HC withstands brute-force, statistical and quantum attacks [118].

4.2 Artificial Intelligent Tools

- **Machine Learning (ML)**

This is an artificial intelligence method that develops algorithms and statistical models which enable computers to analyze patterns and make decisions [21]. ML systems learn from data and make decisions based on their attributes and features [99]. This method relies on an extensive data set for training and learning, significantly enhancing performance. ML-based systems are characterized by their adaptability and self-improvement through feedback and training. Therefore, these systems are used in complex systems, such as image and speech recognition, natural language processing, autonomous vehicles, and detecting security breaches in IoT systems [120,121].

According to [122], there are several types of machine learning methods, some of which are described below.

- *Supervised learning*: In this form of learning, the model is trained using labeled data, and data features are extracted to train the model to predict outcomes.
- *Unsupervised learning*: In these models, the data is unlabeled and the model works to identify patterns and clusters without pre-specified information.
- *Reinforcement learning*: These models interact with the environment for learning, using feedback to strengthen the learning process.

However, it also faces significant limitations. These challenges stem from the unique characteristics of IoT environments, including computational Limitations such as processing power, making it difficult to implement complex ML algorithms effectively, and Energy Consumption, which is critical for battery-operated devices. More aspects like vulnerability to Attacks, such as cloning through Physical Unclonable Functions (PUFs) [122]. Inability to withstand newly arising attacks. Additionally, the training data may contain sensitive data that poses a privacy concern [21].

- **Deep Learning (DL)**

This is a subset of ML used for modeling complex patterns in large data sets. It involves multi-layered neural networks that simulate the human brain and allow incremental learning [123]. DL requires a large amount of labeled data for training and is characterized by its ability to extract attributes from the data automatically. Although it yields highly accurate results, it faces some limitations, such as demanding significant computational resources, consuming time, and often requiring substantial energy, which negatively affect battery-operated devices. Furthermore, it is vulnerable to MITM and replay attacks [124].

- **Federated Deep Learning (FDL)**

This is an approach within ML that involves decentralized data storage. The training data remains on local devices (such as smartphones, and IoT devices). At the same time, the model is trained across these devices without transferring the data to a central server, which helps enhance privacy [19]. FDL is highly efficient in terms of communication cost because it only exchanges model updates. It is also scalable due to its distributed training nature. All these attributes render FDL suitable for IoHT applications where data privacy is a major concern [125].

However, FDL trust issues are worsened by diverse IoT devices, creating vulnerabilities. Decentralization causes authentication inefficiencies with cross-domain data exchanges, increasing latency and reducing throughput [95].

4.3 Supplementary Tools

- **Blockchain (BC)**

This is a new technology consisting of a decentralized distributed ledger used to store data as blocks [125]. These blocks form a digital list of ordered entries collected and arranged in an organized manner so that a cryptographic hash of the previous block is stored in the next block. This makes the blocks interconnected and thus immune to changes since any change in one block affect other connected blocks. Therefore, any node cannot individually manipulate or control data [126]. The records in BC are unchangeable for any type of data such as currency and medical [127]. The distributed architecture nature of BC, coupled with its decentralization protects the system from central point of failure problems [70]. Fig. 4 shows the blockchain connectivity.

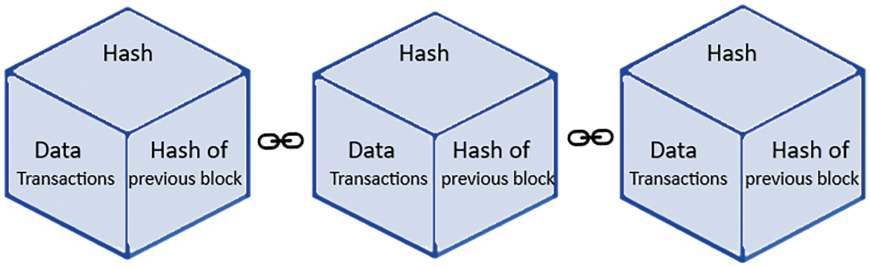

Figure 4: The BC connection mechanism

As explained in [69], the BC distributed ledger is a shared database for storing transactions that can only be accessed and modified by authorized team members. Additionally, Smart Contracts (SCs) are pre-defined with conditions (*if...then*) and are executed automatically when these conditions are met [128]. The BC also utilizes public key cryptography to ensure secure authentication and control access to data [129].

In spite of the several secure authentication schemes in IoHT, unauthorized access remains a threat to healthcare systems due to the human factors. Therefore, there are challenges in preserving confidentiality when dealing with authorized accounts and their transactions [69]. In addition, the decentralized structure of BC requires huge resources in terms of time, storage, and processing resources. This leads to a decrease in scalability, which is considered as one of the critical aspects in healthcare databases [1,130].

As explained in [131], there are three types of BC: public, private and Consortium BC. In public BC, anyone can reach the ledger and make data appending, while in private BC, the access needs to be authorized by the owner organization [131]. The third is Consortium BC, which supports both public and private ledger access. The consensus process can be controlled by multiple organizations rather than one [12,132]. A hybrid BC also exists, combining groups of the three types of BC for more flexibility in managing records and data. In the healthcare industry, the choice of BC type depends on the system requirements, as well as challenges for security, privacy, scalability and regulatory compliance [133].

In BC, a consensus algorithm is a hash-based mechanism used in distributed systems to ensure the effective agreement of all participants for data transmission. This algorithm is crucial for maintaining the integrity and reliability of blockchain networks and other decentralized systems [69]. Many types of consensus algorithms have been developed to determine the consensus propagation for data transactions among untrustworthy network node participants. According to [134], these consensus algorithms can be classified according to their implementations and characteristics.

***Proof of Work (PoW)*:** In this algorithm, participants (referred to as miners) need to solve complex mathematical problems to add new blocks to the BC. The first miner to solve the problem gets the right to

add the block and is rewarded with cryptocurrency [135]. In this environment, this implementation ensures that 51% attacks are kept at bay [88].

Proof of Stake (PoS): This algorithm allows nodes to create new blocks based on the number of coins they have and are aiming to stake as collateral [69].

Practical Byzantine Fault Tolerance (PBFT): This algorithm is designed to enhance the reliability and security of distributed systems. This is because it can tolerate a certain number of faulty nodes and still execute transactions even in the presence of faulty or malicious nodes [69].

Proof of Stake Velocity (PoSV): This algorithm combines elements of both PoS and the concept of velocity in economics. It aims to promote a more dynamic and engaged network by incentivizing the holding of coins and their active use in transactions [136].

- Smart Contract (SCs) are self-executing codes with the terms of an agreement for transaction regulation. They are used in blockchain networks to implement automated and trustless transactions without intermediaries when predefined conditions are met [109]. SCs offer transparency, security through cryptographic techniques, and efficiency in reducing transaction time and computational cost. Moreover, SCs are utilized within various applications, such as financial services, supply chain management, and decentralized applications (DApps) [137].

- **Fog Computing**

The FC is a paradigm for managing resources and data in decentralized and distributed computing environments; it is used to present computing resources over networks such as servers, data, and storage [138]. The general architecture of FC consists of edge devices, local servers, and gateways in addition to the cloud as shown in Fig. 5. This structure consists of three layers:

- **Things layer:** This layer contains connected devices that act as data inputs. Such devices may include sensors, wearable devices, Arduino, and actuators [138].
- **Fog layer:** This is the middle layer whose task is transferring data between data collectors (things layer) and the cloud. This layer includes network devices, internet gateways, local servers, and routers [137].
- **Cloud layer:** This is the third layer, which receives incoming data. Through its servers characterized by high processing, and storage capabilities, this layer analyses this data to facilitate decision making [139].

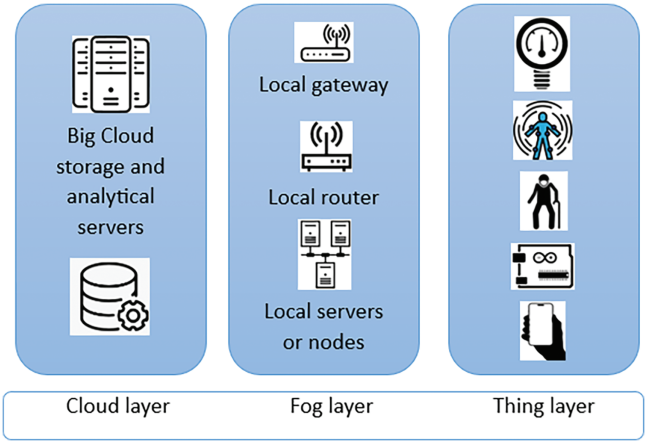

Figure 5: FC structure

As explained in [140], fog nodes are the basic physical infrastructure in FC. These nodes are categorised into two groups: resource-rich machines, and resource-poor devices. Resource-poor devices include routers,

switches, or access points. On the other hand, resource-rich machines include Cloudlets and IOx devices that are located at the edge of the network [141] They closely or directly interact with the user to enhance or provide resources, processing, and manage IoT applications [142].

FC offers unique advantages such as reduced latencies for data processing. This is particularly crucial for time-sensitive applications. Therefore, FC is ideal for the management of IoT systems [9,143]. FC's scalability, demonstrated by its ability to accommodate more nodes and be operable by multiple cloud and server providers [144], opens up possibilities for growth and expansion.

In healthcare systems, the things layer consists of devices that read vital signs and patient data which is then transferred to the cloud layer. In the cloud, the data can be stored, protected or analyzed to facilitate decision making during important medical and therapeutic emergencies [9]. The main drawback of FC is the complexity it presents during management and deployment. This is mainly due to its decentralized, distributed, and scalable nature [142].

4.4 Developer Tools

These tools include Interplanetary File System (IPFS), Ethereum, Ethereum Virtual Machine (EVM), Solidity, Node.js, Node Package Manager (NPM), Ganache, Truffle, and MetaMask. These tools are described in the sub-sections below.

- **The Interplanetary File System (IPFS):** This is a distributed system for storing files in a peer to peer version. It is based on content-addressing as a guide for requesting files [12]. This is done through its unique hashes generated cryptographically from the content of the file, instead of its address on the server [145]. These hashes can be considered as alternatives to the file contents [19]. The file storage mechanism is shown in Fig. 6.

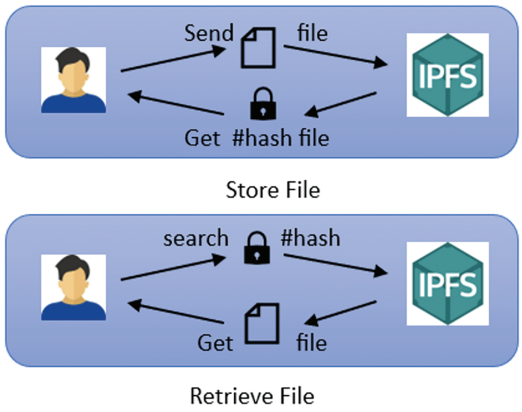

Figure 6: Storing files in IPFS

- **Ethereum:** This is an open-source decentralized platform that enables developers to build and deploy SCs and decentralized applications [146]. This platform is also used to execute fee payment, transactions on the network without intermediaries, digital assets management or management of items ownership. These programmable contracts can operate on three kinds of data storage: stack, temporary memory, and permanent storage (which is used for storing contracts after completion of computations) [147]. Any operation such as contract call, memory usage, or data retrieval is paid by Ethereum's cryptocurrency, ether [12].

- **Ethereum Virtual Machine (EVM):** This is presented by Ethereum on the BC to provide a suitable decentralized execution environment for SCs across all Ethereum nodes. A VM's essential ability is to encapsulate the entire network and operate as a supercomputer to solve any computational tasks. EVM uses "gas" as currency to account for the computational effort required for executing various operations [148,149].
- **Solidity:** This is an object-oriented highly effective programming language built for EVM. It is deployed for writing and developing smart contracts. It easily creates contracts for various uses, such as voting, blind auctions, multi-signature wallets, and other functions [150]. Solidity software is based on programming languages such as Python, JavaScript, and C++, with the ability to support libraries, inheritance, and user-defined types [151].
- **Node.js:** This is an open-source runtime environment built on the JavaScript V8 engine. This tool is used to build high-performance and scalable applications. It efficiently works with heavy I/O applications and can simultaneously handle multiple tasks [152]. Moreover, Node.js is fast and efficient in building real-time applications, which renders it highly popular. As explained in [153], it is flexible and can run on different operating systems such as Windows, Linux, and Mac.
- **Node Package Manager (NPM):** This tool allows users to install and use different versions of a package whilst running a single execution. Node.js has a vast ecosystem of libraries and frameworks for managing several dependencies. These extensive libraries and functions help developers in building professional applications easily [154]. According to [153], over 2.1 million packages are listed in the NPM registry.
- **Ganache:** This is an Ethereum development tool that enables developers to deploy, manage, and test SCs [155]. It is used to simulate the Ethereum BC, allowing for complete control during examination and testing. All transactions are instantly mined. This results in not only fast but also efficient testing and development, devoid of confirmation. As explained in [156], Ganache provides pre-funded Ethereum accounts to facilitate the work of developers. Fig. 7 presents Ganache user-interface.

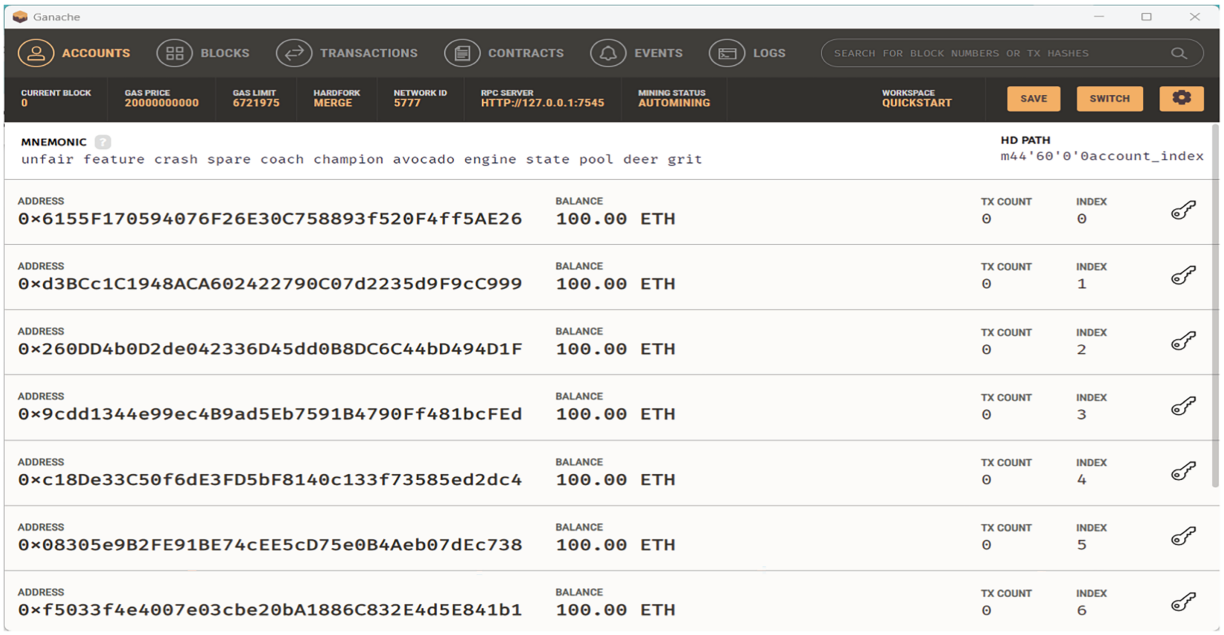

Figure 7: Ganache user-interface

- **Truffle:** This is a framework that integrates with Ganache to develop, manage, deploy, and scale SCs on Ethereum through its comprehensive environment [157]. Fig. 8 presents the Truffle framework.

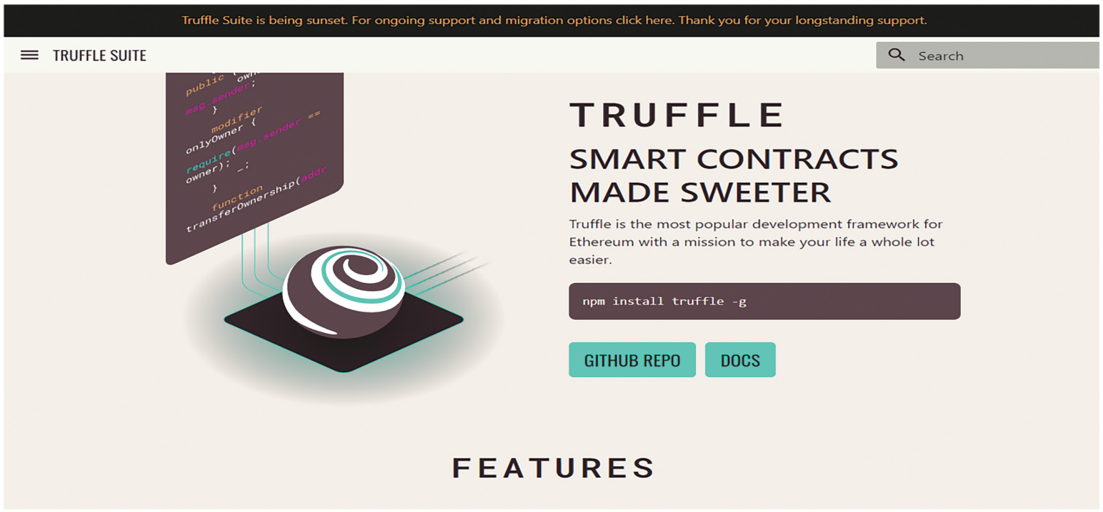

Figure 8: Truffle framework

- **MetaMask:** This is an extension that can be added to the browser to serve as a cryptocurrency wallet and a gateway to the Ethereum BC. This extension enables users to store and manage their Ethereum-based assets. It also facilitates interaction with DApps through a user-friendly interface, as depicted in Fig. 9. This facilitates easy manipulation of accounts and provides a secure environment for transactions [158].

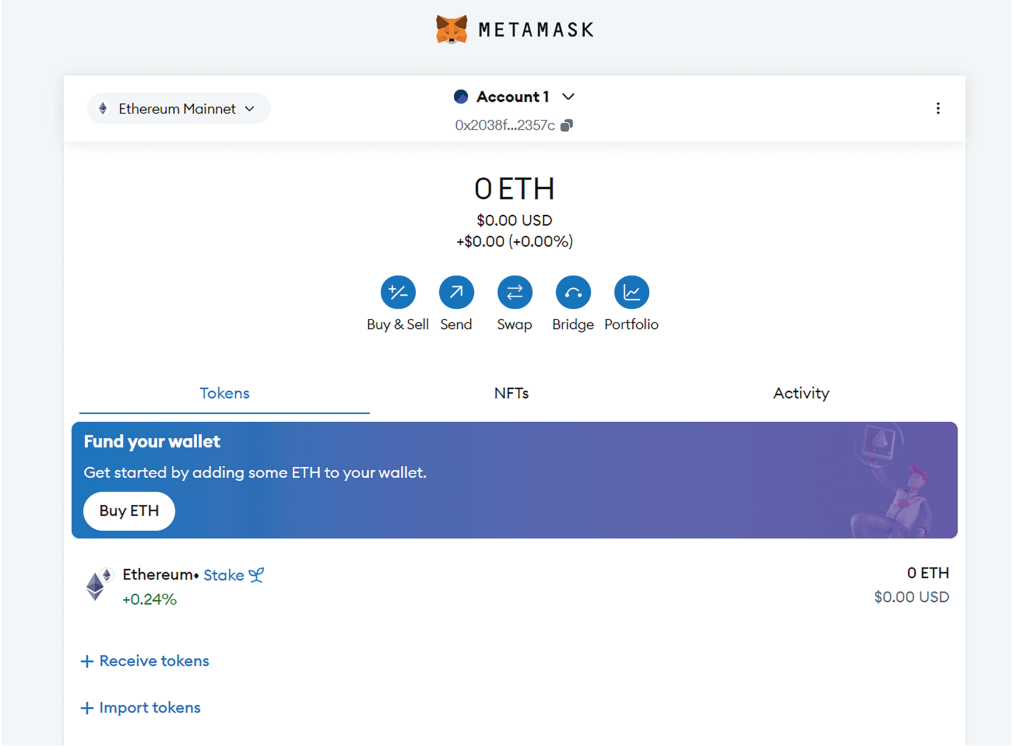

Figure 9: MetaMask cryptocurrency wallet

5 Security Analysis Tools

In this section, various security analysis tools are described. They include Scyther, AVISPA, ProVerif, Burrows-Abadi-Needham (BAN) logic analysis, Real-or-Random (ROR), Interrogator, Naval Research Laboratory NRL protocol analyzer, and Murphy analyzer as detailed in the sub-sections that follow.

- **Scyther:** This is a tool for large-scale protocol verification tests. As shown in Fig. 10, it offers a user interface, command-line and scripting interfaces functionality [8]. It has numerous salient characteristics and high performance. For instance, it allows termination of correct proof sessions for protocols with unlimited trials. Unlike other tools, Scyther analyzes the protocol, produces its behavior, and describes the class of the attack. Finally, this tool facilitates multi-protocol analysis with parallel composition of sub-protocols [159].

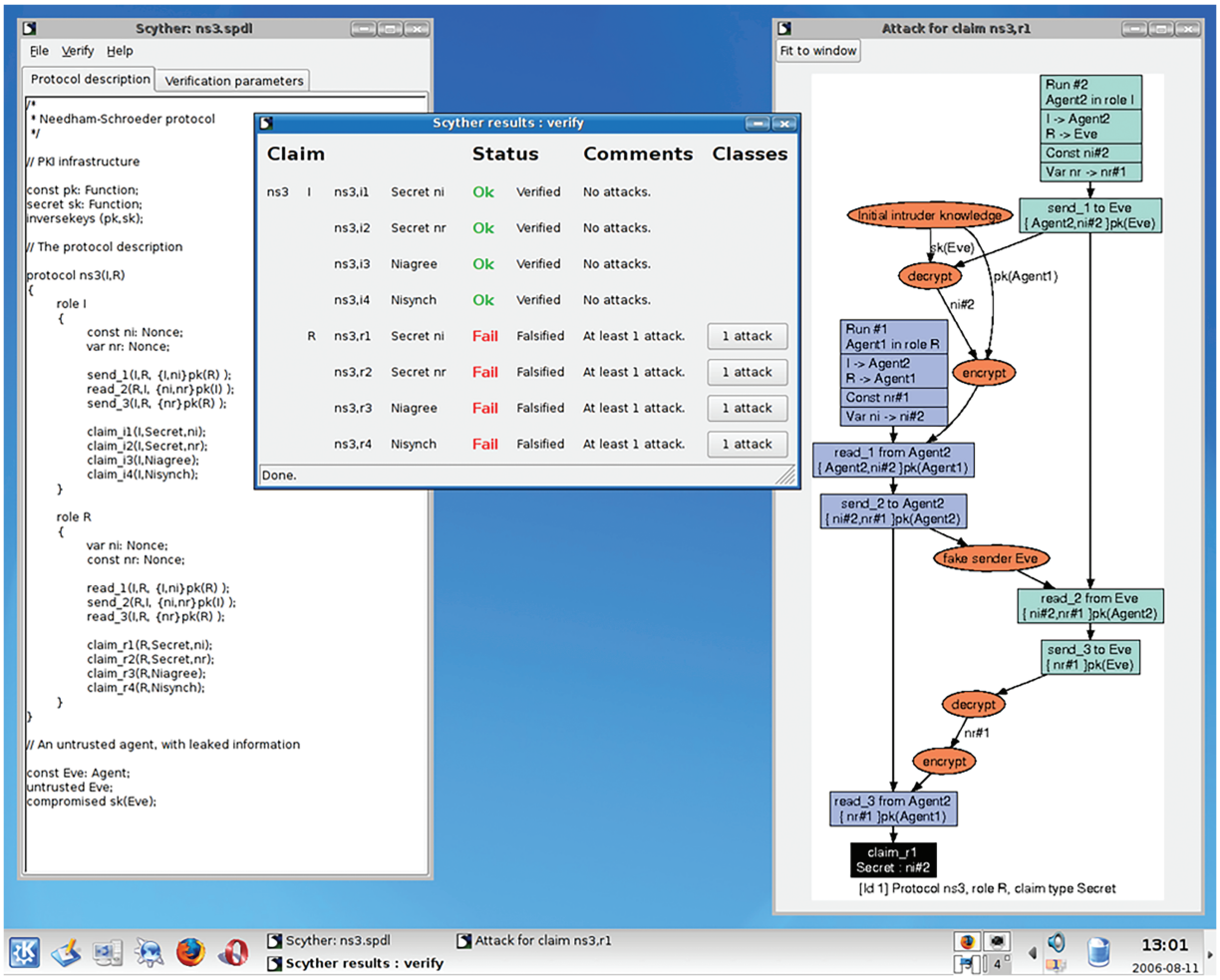

Figure 10: Scyther user-interface

As in [160], Device X's authentication and voice protocols were modeled using the Scyther Tool with protocol MSC compilation. In authentication, MSA and MSB initiated device registration, while in voice, only MSA initiated communication. Scyther Tool verified Device X's authentication protocol model. Scyther Tool analysis involves interpreting test results to assess protocol conditions and analyzing attack patterns that violate security claims. Fig. 10 provides a summary of verification results.

- **AVISPA:** This is a tool designed to validate and verify internet security-sensitive protocols and applications. It enables users to formally define safety properties and specifications. It then uses an extensive set of libraries to perform evaluations. AVISPA employs the High-Level Protocol Specification Language (HLPSL) for specifying protocols, allowing for comprehensive analysis and verification of security measures [161]. Fig. 11 shows the AVISPA tool interface.

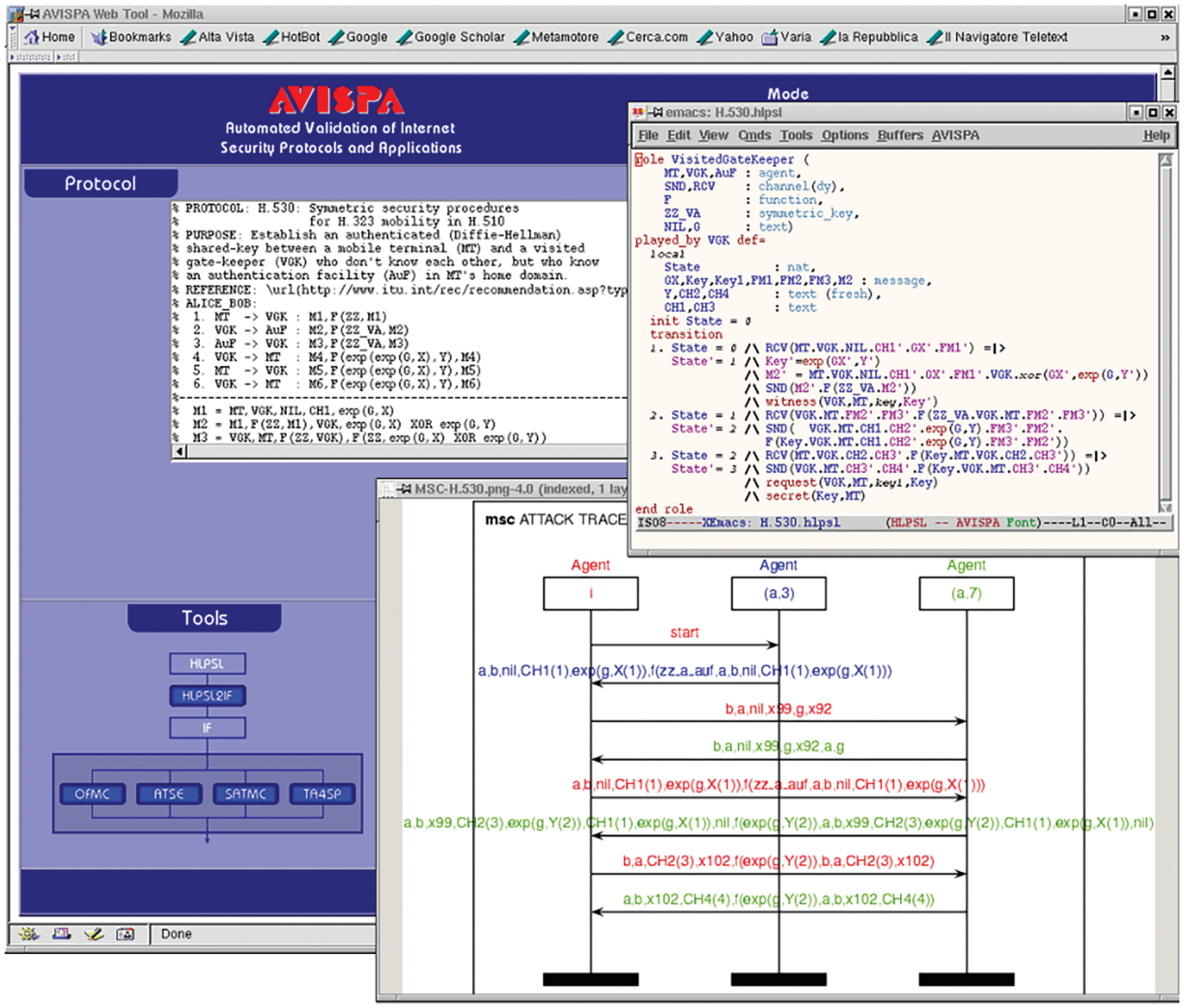

Figure 11: AVISPA security verification tool

- **ProVerif:** This is a formal tool designed to verify and analyze cryptographic protocols. It provides a precise framework to ensure protocols meet various security properties such as confidentiality, authenticity, and integrity. This tool can be modeled to check for potential vulnerabilities devoid of expertise. It has a simple and concise presentation language to represent and analyze complex protocols without the need for manually proving security properties [157]. The tool, shown in Fig. 12, can analyze symmetric and asymmetric cryptographic protocols while providing a vulnerability detection feature to debug and improve the protocol [159].

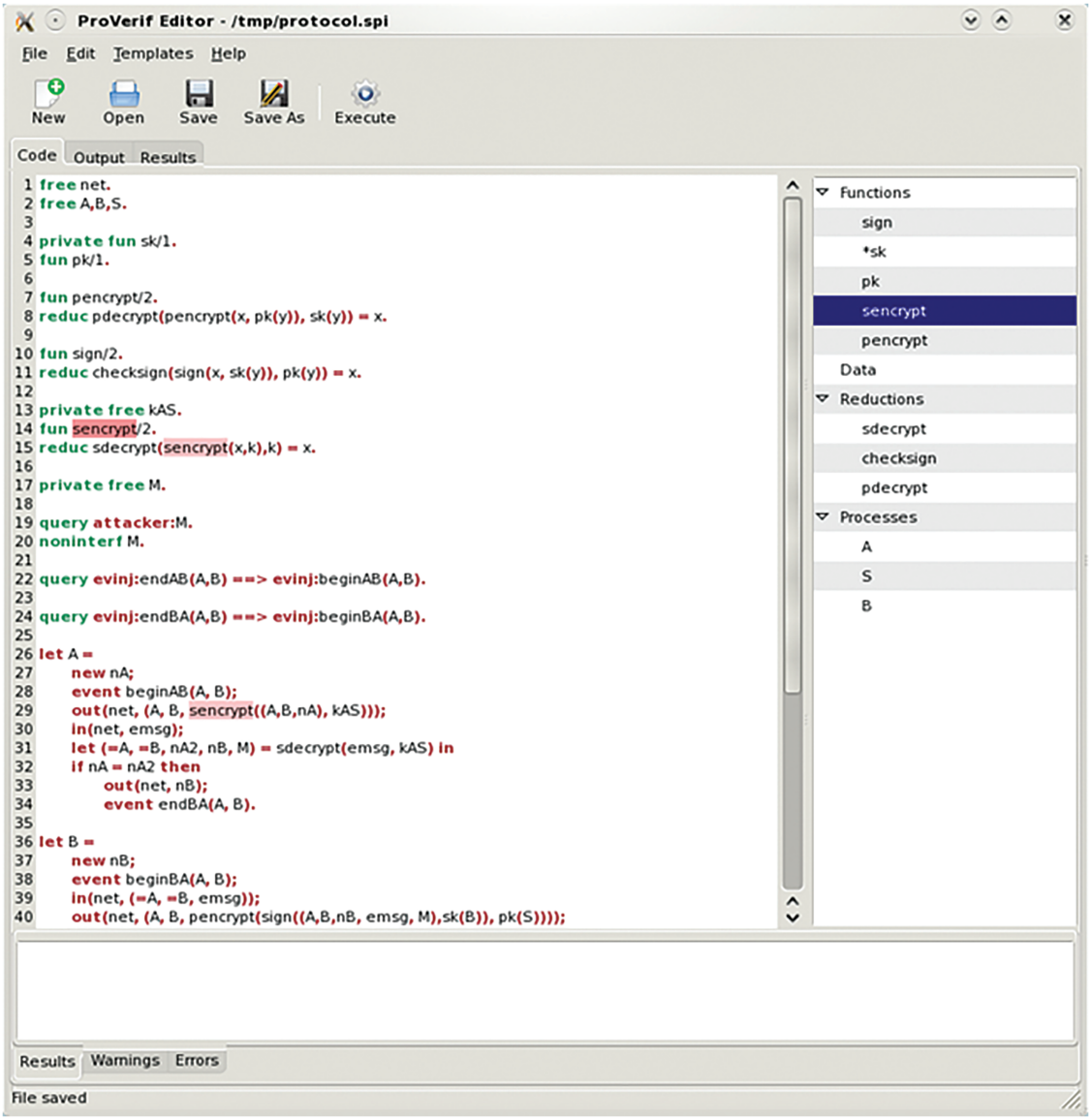

Figure 12: ProVerif formal verification tool

- **Burrows-Abadi-Needham (BAN) Logic Analysis:** This is a formal analysis mechanism to prove the security and viability of new protocols. It uses primitives and inference rules to describe crypto-system principles [162]. This mechanism follows three reasoning steps. Firstly, the description of the authentication protocol is logically expressed and initialized. Secondly, the exchanged messages of the authentication protocol are converted into BAN logic language, and unrelated phrases are eliminated. Thirdly, using the inference rules and based on the idealized model, the proposed protocol is traced and proven whether it accomplishes the security goals or not [67].
- **Real-or-Random (ROR):** This security analysis tool evaluates cryptographic protocol security, especially protocols that establish session keys and mutual authentication. It compares the protocol's output to a random model. This analysis emphasizes on privacy preservation and the strength of security definitions applied to specific schemes [163]. Moreover, this analysis works on the probability of whether an adversary can distinguish between real protocol messages and random messages. Basically, the protocol

is regarded secure if the adversary is unable to carry out this distinction. ROR can define both adversary capabilities and security properties such as mutual authentication or forward secrecy. This helps in the identification of potential vulnerabilities, ensuring the security of the entire system [164].

- **Interrogator:** This is a Prolog program with a GUI interface designed and controlled by LISP to determine vulnerabilities and observe key distribution flow within text-defined security protocols. The system has a tool that displays a simulation of the attacker's movement, tracks any changes made, and shows them as pop-up messages [165]. Additionally, the system looks for message modification attacks that undermine the protocol objective [166]. The Interrogator code in Fig. 13 checks for common vulnerabilities based on predefined rules.

```
% Define some basic protocol rules
vulnerability(insecure_key_distribution).
vulnerability(weak_encryption).
vulnerability(lack_of_authentication).

% Define a protocol
protocol(my_protocol) :-
    uses(insecure_key_distribution),
    uses(weak_encryption).

% Check for vulnerabilities in the protocol
check_vulnerabilities(Protocol) :-
    protocol(Protocol),
    findall(Vuln, vulnerability(Vuln), Vulnerabilities),
    write('Vulnerabilities found in '), write(Protocol), write(': '), nl,
    print_vulnerabilities(Vulnerabilities).
```

Figure 13: Interrogator interface

- **Naval Research Laboratory NRL Protocol Analyzer:** This tool is developed by the U.S. NRL, and used to analyze and debug network protocols. The analyser is implemented in Prolog programming language, and is designed to run on platforms that support Prolog environments [167]. The NRL supports a wide range of protocols, analyzes communication across different network layers, observes the flow of data and traffic, and is able to identify anomalies or bottlenecks in communication [166].
- **Murphy Analyzer:** This is a tool for analyzing network protocols and provides performance and reliability assessments. It focuses on error detection and correction, network performance, and efficiency. Moreover, it handles data reliability by evaluating data error and loss [166].

6 Related Works

6.1 Cryptographic Models

Numerous studies have presented authentication protocols for the IoHT, based on a variety of elements, such as the network server, the encryption algorithm used and the number of authentication factors. These studies focused on both external and internal attacks on the network. According to [108], attackers within the network are more dangerous than external attackers. In this respect, Feng et al. (2019) have proposed a lightweight authentication system that strikes a perfect balance between security and performance in electronic health record (EHR) systems. This protocol is a secure two-party authentication based on holomorphic encryption. It is devoid of a trusted third party to recover the original private key, but guarantees that only authorized users can collaboratively access and manage data. This protocol is shown to enhance

security and efficiency [168]. On the other hand, Oliveira et al. (2021) introduced the AC-AC protocol, a dynamic revocable access control system designed for healthcare teams to access encrypted electronic medical records (EMR) during emergencies. This protocol grants real-time access rights during critical care situations while maintaining patient privacy and data security. The system utilizes a hybrid encryption approach combining Dynamic index-based Symmetric Searchable Encryption (DSSE) and Attribute-Based Encryption (ABE) with less time consumption for access operations [16]. Yadav et al. (2023) introduced a lightweight dual-factor authentication protocols for WLAN-connected IoT. Their protocol is built on Extensible Authentication Protocol (EAP) encryption algorithms, random numbers, hash functions, and a combination of symmetric-key, public-key, and hash-based cryptography. The EAP is utilized to boost data security, and the protocol is shown to incur less time consumption and is highly scalable [62]. Wu et al. (2023) proposed a lightweight enhanced authentication and key agreement (AKA) protocol for the IoHT environment that aims to ensure data transmission security and protect user privacy. The proposed protocol facilitates the establishment of session keys between doctors and network nodes [169]. However, it is shown to be vulnerable to threats, such as privileged insider IP attacks. To effectively verify, identify, and authenticate IoT devices in a fog computing environment, Britto et al. (2024) developed a security model that combines machine learning and hybrid mathematical encryption techniques of Elliptic Curve Cryptography (ECC) and Proxy Re-encryption (PR) with Enhanced Salp Swarm Algorithm (ESSA). The proposed model is shown to be capable of detecting and predicting system vulnerabilities in the IoHT environment. In addition, its security and performance analyses demonstrates its effectiveness in improving performance metrics such as energy consumption, throughput, response time, execution time, processing time, packet error rate, reliability, and verification time compared to traditional cryptographic algorithms. However, the system's formal or informal security analyses are not carried out [121].

6.2 Biometric-Based Models

To transform patient identification in a healthcare system, Janelle et al. (2020) proposed an authentication technique based on biometrics. This technique combines periocular biometrics and an electronic master patient index during the authentication process. According to [37], this system has the potential to significantly enhance human identification in IoHTs [37]. To authenticate individuals in a healthcare system, Manjula Devi et al. (2022) have introduced a retina-based efficient biometric identification system, named ARBAS (ANFIS-based Retina Biometric Authentication System). The system utilized the VARIA database, which contains retinal images collected from various persons. This scheme comprises two main phases: enrollment and authentication. During the enrollment phase, retinal images are scanned, and the biometric patterns are derived and stored. On the other hand, the authentication involves scanning a user's retina and comparing the extracted pattern to the stored data. The results showed that it achieved a False Rejection Rate (FRR) of 2.78% and a False Acceptance Rate (FAR) of 2.94%. These results highlight its potential to significantly improve security in the healthcare sector [34].

6.3 Blockchain-Based Model

To maintain authorized access to data, Jaiman et al. (2020) have introduced an Ethereum BC-based consent model designed for health data-sharing platforms. This model introduces the Data Use Ontology (DUO) and Automatable Discovery and Access Matrix (ADA-M). The proposed model enhances accountability, flexibility, and personalization in data access requests through SCs whilst ensuring compliance with GDPR. However, the scalability and data privacy are not considered [66]. On the other hand, Ray (2021) proposed a novel system for an e-healthcare application, which involves a BC-lightweight IoT node-based system with an enhanced Simplified Payment Verification (SPV) process. However, this technique employs

the Bloom filter which brings scalability issues. In addition, this system has high false positives, and needed special hardware to be implemented [170]. Alnuaimi et al. (2022) proposed a healthcare model based on private Ethereum that utilized off-chain storage IPFS for image storage. For traceability and trustworthiness, the model used two SCs for registration and approval. Unfortunately, the system is unable to resist DoS attacks. In addition, it incurs high computational costs, and supports limited privacy and scalability [171].

To support remote chronic disease patients who need regular monitoring, Azbeg et al. (2022) proposed a BlockMedCare healthcare system which is based on the Ethereum BC and IPFS [12]. The system considered three main requirements: security, scalability, and processing time. The security is ensured through an encryption proxy, while scalability is achieved by utilizing an off-chain database based on IPFS. In this scheme, Ethereum is used to reduce execution time. However, the data reliability and validity were neglected in this method [12]. Luis et al. (2023) have developed a BC technology-enabled technique for medical records exchange. They utilized the Ethereum BC platform to provide a better healthcare service and minimize costs. In this technique, BC offers privacy, security, and availability. However, this approach cannot withstand 51% attacks [172].

To secure electronic health records (EHRs), enhance data integrity, and improve patient privacy, Agha (2023) has introduced BC technology-based decentralized framework. This system deploys sensors for real-time monitoring and is shown to enhance health information management. In this approach, patients have full control of their personal healthcare data. In addition, the usage of SCs offer more efficiency and reduce costs. However, the system suffers from limited scalability and presents some difficulties during its integration with existing systems. In addition, it fails to withstand DDoS and MITM attacks [173].

Norah et al. (2024) proposed group authentication for the IoMT framework. In addition, they introduced fog computing for maintaining scalability, enhancing efficiency and overcoming high costs associated with the decentralized BC technology. Nonetheless, the framework incurs high communication costs due to the large number of devices that need to be verified by a single entity [11]. To enhance authentication, security and efficiency in IoHT systems, Muwafaq et al. (2024) have developed a system based on the Bloom filter, Firebase framework and BC. In this scheme, the Bloom filter mainly reduces the authentication time, Firebase manages real-time synchronization, while the BC preserves data security and integrity. Despite the widespread use of the Bloom filter, it is costly due to its hardware requirements and the potential for high false positives [131].

6.4 DL-Based Models

On the other hand, Lin et al. (2023) have presented a novel technique for managing large volumes of medical data through an attribute-based secure access control mechanism (SACM) for IoT-enabled healthcare. The proposed mechanism is based on FDL and utilizes graph convolutional networks to establish a relationship between users' social attributes and their trustworthiness. In so doing, it helps control access to sensitive medical data. The system provided good access control accuracy and maintained data integrity and privacy. However, it has long latencies and malicious participants can manipulate or alter data [20].

6.5 CC-Based Models

Qadir et al. (2023) have presented an authentication and access control model for secure and efficient data sharing among healthcare providers. The proposed framework is based on Security Secret Key Provider (SSKP) technology for access control as well as managing and securing personal health records. However, authentication takes a long time [174]. To solve the problem of third parties-induced vulnerabilities, Ussatova et al. (2023) have developed an enhanced two-step authentication scheme. This approach combines cloud technology and BC to secure medical data access. The practical implementation and analysis demonstrate

the efficiency of biometric login. Still, their solution has some limitations as the encryption key generation is not fully defined and the key formation method is limited, and the limited fingerprint database reduces accuracy [108]. On the other hand, Abbas AI et al. (2024) have developed a robust fuzzy-based method for enhancing security in cloud-enabled healthcare systems. This ECC-based technique achieves good results in terms of communication cost, mutual authentication, and data integrity. However, it might not protect against cyber-attacks such as replay attacks, de-synchronization and spoofing [175].

6.6 Review and Survey Studies

Tance et al. (2023) have presented a review paper evaluating recent solutions in the field of authentication in healthcare systems. In addition, the authors describe the latest technologies integrated into IoHT, the applications of next-generation MFA, as well as the security requirements for these systems and their corresponding solutions [60]. On the other hand, Singla and Verma N (2023) presented a survey of research works published between 2010 and 2022, dealing with authentication techniques used in IoT systems. Their study provided a comprehensive description of three authentication techniques, namely knowledge-based authentication (based on information known by a legitimate-User), inherence-based authentication (based on integrated things to an individual), and possession-based authentication (based on something owned by the legitimate user). In addition, a review of the deployed performance metrics (such as accuracy, EER and FAR) is provided [176]. Similarly, Enrique et al. (2023) reviewed numerous papers dealing with different AI-based schemes that address security issues, withstand specific attacks and threats. They also described how AI techniques, including ML, DL, and reinforcement learning, can be employed to detect intrusion, malicious attacks, or other threats [5].

Khan et al. (2022) carried out extensive literature review on authentication process security. They analyzed the advantages of each type of authentication scheme, concluding it is challenging to design a suitable authentication framework with a complete package of security requirements to withstand hacking problems [177]. Some of these requirements include ward security, mutual authentication, privacy protection, integrity, key agreement, password change, scalability, confidentiality, and availability. On the other hand, Ghaffari et al. (2024) have comprehensively reviewed literature on IoT security based on DL and ML approaches, describing their advantages, and limitations. They identified vulnerabilities in IoT systems, such as eavesdropping, denial of service, unauthorized access to data and snooping threats. They emphasized the critical role of machine learning and deep learning techniques in mitigating these risks.

As explained in [178], ML techniques such as support vector machine (SVM), artificial neural network, and linear modeling are successful on small datasets while DL models have higher accuracies on large dataset. Dargaoui et al. (2024) have presented a comparative study of IoT security researches. They presented an analysis of latest authentication protocols developed in the period between 2018 and 2024. The aim of the authors was to summarize IoT security research, the most prominent vulnerabilities and attacks such as impersonation, reply, node capture, DoS, privileged insiders, and MITM. In addition, a review of appropriate security technologies such as BC, ML, physically unclonable function (PUF) and cryptography is provided. Moreover, the most commonly used formal security analysis tools are presented, such as ProVerif, Scyther, Random Oracle, and AVISPA [179]. Cobrado et al. (2024) have carried out a study that reviewed 24 published research works on the most common methods used for access control. These methods include identification, authentication, authorization, and accountability. The authors concluded that the most common mechanism is Attribute-Based Access Control (ABAC) [102].

Mohamed et al. (2024) conducted a literature review to study authentication protocols in an IoT environment. The authors discussed the applications and the appropriate type of authentication, as well as how to choose the key agreement and exchange mechanism. The cryptographic techniques used in this field,

and the methods of formal and informal threat analysis and countermeasures to these threats were also discussed. Furthermore, they mentioned using hybrid cryptography and authentication measures such as biometrics and multi-factor authentication to enhance security without compromising usability. However, the authors noted potential drawbacks such as data privacy concerns and new vulnerabilities [79].

Table 3 presents a comparison of the various authentication schemes for IoHT systems, as well as the probable solutions. On the other hand, Table 4 details the supported functionalities in some of the reviewed literature.

Table 3: A comparison of authentication schemes

Research & year	Methodology	Advantages	Attacks and limitations	Data set
[180] 2019	LACO authentication protocol	Works on resource-constrained devices such as sensors	DoS and insider attacks, higher communication cost	–
[168] 2019	Two-party authentication protocol, homomorphic encryption	Availability, authentication	Malicious attack, brute-force and dictionary attacks, data breaches, identity theft	–
[66] 2020	Ethereum blockchain	Confidentiality, and availability, data preservation, privacy, data security, integrity	Sybil attack, 51% attack, scalability challenges in blockchain-based data-sharing	DUO and ADA-M model
[16] 2021	Dynamic index-based Symmetric Searchable Encryption (DSSE) and Attribute-Based Encryption (ABE)	Real-time access, privacy and data security	Insider attack and time consuming	–
[170] 2021	BC, SVP	Security, efficiency, integrity	Network attacks, 51% attacks, scalability issues, false positives	–
[171] 2022	IPFS, private Ethereum BC	Security, efficiency, integrity, availabilty	DdoS, complexity, computational cost, less privacy and scalability	–
[12] 2022	IPFS, Ethereum BC	Security, scalability, and processing time	Network attacks, 51% attacks, reliability and validity	–
[98] 2022	Deep Learning-based Long Short-Term Memory classification algorithm	Continuous authentication detects insider threats	Insider attacks, privacy violation and resource consumption	–

(Continued)

Table 3 (continued)

Research & year	Methodology	Advantages	Attacks and limitations	Data set
[181] 2023	(SHA-1)	Mutual authentication, unlikability, key agreement, secrecy	MITM, DDOS, replay attack, impersonation attack and high communication cost	–
[174] 2023	Security Secret Key Provider (SSKP), SSK	Confidentiality, and availability, authentication, security, access control	Malicious insiders attack, long time for authentication	–
[62] 2023	EAP & Random numbers, Hash function, Encryption/Decryption	Authentication, availability	DoS, MITM attacks, time consumption with increasing number of users and key non-confidentiality	–
[169] 2023	Authentication and Key Agreement (AKA) Protocol	Mutual authentication; scalability, availability, Data security and integrity	MITM, higher computational and communication costs	–
[172] 2023	Ethereum BC	Privacy, security, and availability	MITM, 51% attack, not real implemented	Data must be requested
[173] 2023	BC, smart contract	Privacy, security, and security	MITM, DdoS attacks, integration with existing systems	Real-time Health data
[20] 2023	FDL + ABAC	Privacy, accuracy, and integrity	DDoS, physical attack, malicious attacks, latency	"https://toreopsahl.com/datasets/"
[11] 2024	ECC, SSS algorithm, and BC-based FC technologies	Decentralization of management and reduction of verification time	Botnet attack, Physical attack, spoofing, communication cost	–
[15] 2024	The graph theory, matrix (GTM) approach and AHP-TOPSIS	Privacy protection, integrity, key agreement, password change, scalability, confidentiality, and availability	Data manipulation attack, energy and time consumption, complexity of the algorithm, key size, and latency	Table 2 in the article

(Continued)

Table 3 (continued)

Research & year	Methodology	Advantages	Attacks and limitations	Data set
[131] 2024	Bloom Filter, Firebase Framework and BC Technology	Authentication, confidentiality, Availability, scalability and integrity	Physical attacks, Botnet attacks, complexity in Implementation	–

Table 4: Comparative of supported functionality, A1: Mutual authentication; A2: Session key agreement; A3: Key security; A4: Anonymity and confidentiality; A5: Formal verification; F1: DDoS; F2: MITM; F3: Eavesdropping; F4: Replay attack; F5: Spoofing; F6: Physical attack; F7: A Hijacking Attack; F8: Sybil attack; F9: Botnet attack; F10: 51% attack

Functionality	[15]	[170]	[58]	[20]	[11]	[169]	[66]	[182]	[183]
A1	√	×	√	√	×	√	√	×	√
A2	√	√	√	√	√	√	×	√	√
A3	√	√	×	√	√	√	√	√	√
A4	√	√	√	×	×	√	√	√	√
A5	√	√	√	√	√	√	√	×	√
Disrupted attacks									
F1	√	√	×	×	√	√	√	√	√
F2	√	×	√	–	√	×	√	√	√
F3	√	×	×	–	√	√	√	–	×
F4	√	√	√	–	√	√	√	–	√
F5	√	√	×	–	×	√	√	–	×
F6	√	×	√	×	×	×	–	–	–
F7	×	×	√	–	√	√	–	–	√
F8	√	√	√	–	√	√	×	–	–
F9	×	×	×	–	×	√	×	–	–
F10	–	×	–	–	×	–	×	×	×
	√ supported			× not supported			– not considered		

7 Research Gaps

Based on the reviewed literature, it is clear that numerous research gaps exist in IoT-based healthcare security. Therefore, immediate countermeasures are needed to address these significant gaps in the field of authentication in health IoT systems. To attain this, the following interventions need to be put into place:

- *Encryption methods and algorithms*: the current key generation and distribution mechanisms have numerous weaknesses. Therefore, there is urgent need to explore techniques that can improve their design, construction and deployment.
- *Validated mathematical models of authentication*: the importance of these formal verification tools cannot be overstated. They are not only crucial, but also play a pivotal role in authentication mechanisms. Therefore, their validation and observation should be a top priority. The limitations in adopting biometric features negatively affect authentication accuracy. For example, fingerprints are frequently

utilized while other features such as facial, voice, and behavioral recognition are ignored or used in a small database.

- *BC and FC-based authentication*: there is need to address various potential gaps in BC and FC-based authentication for IoHTs. Such gaps include scalability, performance, integration with legacy systems and determining the consensus and governance mechanism. Bridging these gaps holds great promise and will lead to developing more robust and secure authentication solutions, giving us hope for a more secure future.

8 Recommendations and Future Concerns

The contributions of AI and DL in bolstering IoHT security cannot be overstated. These technologies have been shown to play a crucial role in addressing both well-known and emerging security threats. They have significantly enhanced threat detection ability in computer networks. There is therefore need to build and deploy applications that can operate in real time, train them to respond accurately and quickly to emergent security threats. This can be achieved by employing high-quality, high-performance IoT entities to reduce the duration of data collection and training time. In addition, low performance groups can be built to operate in parallel and managed by semi-central nodes to analyze their resulting data. This can greatly help in the reduction of processing delays. There is also need to develop DL mechanisms with low computational complexity. Mathematical optimization methods can also be deployed for best feature selections. In addition, the usage of technologies such as Apache Spark and Apache Flink can effectively reduce time complexity, enhancing real-time threat detection capabilities. These technologies can also improve the management of databases, collecting their data and analyzing them in real-time. This can help accelerate decision-making and preparing professional reports, especially when dealing with big data in modern healthcare applications. It is recommended that computational complexity be studied extensively in IoHT environment. In addition, fog and cloud computing need to be extensively adopted in the IoHT ecosystem since these platforms have huge servers for big data analytics, compared with resource-limited IoT devices.

Finally, it is recommended to study emerging security threats and keep pace with current updates in the structures of the internet of things, as well as distributed structure and frameworks of modern technologies. Such technologies that hold promise for IoHT include BC and FC, which greatly benefit from the inherent hybridization. As such, they are more efficient and secure approaches.

9 Conclusion

This study has provided a comprehensive discussion on the authentication of IoHT systems and the emergence of new technology in the healthcare sector. The intense focus was on access control and security aspects in IoHTs. We have thoroughly reviewed published articles in this domain for the last five years. The initial search yielded 974 articles, which were filtered by title and abstract, exclusion irrelevant and duplicate papers. This resulted in 186 articles IoHT-relevant to the core components of the IoHT system and the most utilized technologies in authentication and systematic reviews, and surveys. Such technologies include traditional biometrics as well as the most recent AI-based techniques. This paper has also discussed BC technology and other platforms such as fog and cloud computing highlighting their importance and efficiency in developing secure decentralized healthcare systems. The findings have indicated their promising characteristics for the future of IoHT security. This survey also addresses the security issues and challenges facing authentication and access control techniques in healthcare systems and identifies critical security requirements. Moreover, the paper provides a comprehensive overview of the current state of research in this field which leads to the identification of numerous challenges and future directions for further studies in this domain. Also, to build a robust IoHT system, a lightweight, multi-factor authentication scheme must be

employed using biometrics and AI enforcement tools for threat detection and prevention, ensuring a high level of security. Furthermore, integration with BC, FC and others improves system functionality to address the security issues and functionality.

Acknowledgement: We would like to thank the University of Basrah, the Jaramogi Oginga Odinga University of Science and Technology, and University of Debrecen for their role in providing the resources required to complete the research, as well as all the authors who participated in the article.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: Conceptualization, methodology, software, validation, formal analysis: Enas W. Abood, Ali A. Yassin and Zaid Ameen Abduljabbar; writing—original draft preparation, writing—review and editing: Enas W. Abood, Zaid Ameen Abduljabbar and Abdulla J. Y. Aldarwish; formal analysis, writing—review and editing: Vincent Omollo Nyangaresi, Iman Qays Abduljaleel, Abdulla J. Y. Aldarwish and Husam A. Neamah; supervision: Ali A. Yassin. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: No dataset is used in the paper.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Sodhro AH, Awad AI, van de Beek J, Nikolakopoulos G. Intelligent authentication of 5G healthcare devices: a survey. Internet Things. 2022;20(4):100610. doi:10.1016/j.iot.2022.100610.
2. Ansari RI, Chrysostomou C, Ali Hassan S, Guizani M, Mumtaz S, Rodriguez J, et al. 5G D2D networks: techniques, challenges, and future prospects. IEEE Syst J. 2018;12(4):3970–84. doi:10.1109/JSYST.2017.2773633.
3. Hussien ZA, Hai J, Abduljabbar ZA, Hussain MA, Yassin AA, Abbdal SH, et al. Secure and efficient e-health scheme based on the internet of things. In: 2016 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC); 2016 Aug 5–8; Hong Kong, China: IEEE. doi:10.1109/ICSPCC.2016.7753621.
4. Paul M, Maglaras L, Ferrag MA, Almomani I. Digitization of healthcare sector: a study on privacy and security concerns. ICT Express. 2023;9(4):571–88. doi:10.1016/j.icte.2023.02.007.
5. Castro OE, Deng X, Park JH. Comprehensive survey on AI-based technologies for enhancing IoT privacy and security: trends, challenges, and solutions. Hum Centric Comput Inf Sci. 2023;13(39):1–34.
6. Yaacoub JA, Noura M, Noura HN, Salman O, Yaacoub E, Couturier R, et al. Securing medical things systems: limitations, issues and recommendations. Future Gener Comput Syst. 2020;105(10):581–606. doi:10.1016/j.future.2019.12.028.
7. Minani JB, Sabir F, Moha N, Guéhéneuc YG. A systematic review of IoT systems testing: objectives, approaches, tools, and challenges. IEEE Trans Softw Eng. 2024;50(4):785–815. doi:10.1109/TSE.2024.3363611.
8. Dias JP, Ferreira HS, Sousa TB. Testing and deployment patterns for the internet-of-things. In: Proceedings of the 24th European Conference on Pattern Languages of Programs; 2019 Jul 3–7; Irsee, Germany. doi:10.1145/3361149.3361165.
9. Kamruzzaman MM, Yan B, Sarker MNI, Alruwaili O, Wu M, Alrashdi I. Blockchain and fog computing in IoT-driven healthcare services for smart cities. J Healthc Eng. 2022;2022(11):9957888–13. doi:10.1155/2022/9957888.
10. Huang J, Kong L, Chen G, Wu MY, Liu X, Zeng P. Towards secure industrial IoT: blockchain system with credit-based consensus mechanism. IEEE Trans Industr Inform. 2019;15(6):3680–9. doi:10.1109/TII.2019.2903342.
11. Alsaeed N, Nadeem F, Albalwy F. A scalable and lightweight group authentication framework for Internet of Medical Things using integrated blockchain and fog computing. Future Gener Comput Syst. 2024;151(2):162–81. doi:10.1016/j.future.2023.09.032.

12. Azbeg K, Ouchetto O, Jai Andaloussi S. BlockMedCare: a healthcare system based on IoT, Blockchain and IPFS for data management security. Egypt Inform J. 2022;23(2):329–43. doi:10.1016/j.eij.2022.02.004.
13. Enticott J, Johnson A, Teede H. Learning health systems using data to drive healthcare improvement and impact: a systematic review. BMC Health Serv Res. 2021;21(1):200. doi:10.1186/s12913-021-06215-8.
14. Dadkhah S, Neto ECP, Ferreira R, Molokwu RC, Sadeghi S, Ghorbani AA. CICIoMT2024: a benchmark dataset for multi-protocol security assessment in IoMT. Internet Things. 2024;28(5):101351. doi:10.1016/j.iot.2024.101351.
15. Khan HU, Ali Y. Modeling security evaluation framework for IoHT-driven systems using integrated decision-making methodology. Sci Rep. 2024;14(1):12233. doi:10.1038/s41598-024-62066-3.
16. de Oliveira MT, Dang HV, Reis LHA, Marquering HA, Olabarriaga SD. AC-AC: dynamic revocable access control for acute care teams to access medical records. Smart Health. 2021;20(4):100190. doi:10.1016/j.smhl.2021.100190.
17. Kumar R, Tripathi R. Towards design and implementation of security and privacy framework for internet of medical things (IoMT) by leveraging blockchain and IPFS technology. J Supercomput. 2021;77(8):7916–55. doi:10.1007/s11227-020-03570-x.
18. Moulahi W, Jdey I, Moulahi T, Alawida M, Alabdulatif A. A blockchain-based federated learning mechanism for privacy preservation of healthcare IoT data. Comput Biol Med. 2023;167(3):107630. doi:10.1016/j.compbiomed.2023.107630.
19. Hathaliya JJ, Tanwar S. An exhaustive survey on security and privacy issues in Healthcare 4.0. Comput Commun. 2020;153(6):311–35. doi:10.1016/j.comcom.2020.02.018.
20. Lin H, Kaur K, Wang X, Kaddoum G, Hu J, Hassan MM. Privacy-aware access control in IoT-enabled healthcare: a federated deep learning approach. IEEE Internet Things J. 2023;10(4):2893–902. doi:10.1109/JIOT.2021.3112686.
21. Gaur R, Prakash S, Kumar S, Abhishek K, Msahli M, Wahid A. A machine-learning-blockchain-based authentication using smart contracts for an IoHT system. Sensors. 2022;22(23):9074. doi:10.3390/s22239074.
22. Censys. [cited 2025 Jul 1]. Available from: https://censys.com/state-of-internet-of-healthcare-things/.
23. Kumar P, Javeed D, Kumar R, Islam AKMN. Blockchain and explainable AI for enhanced decision making in cyber threat detection. Softw Pract Exp. 2024;54(8):1337–60. doi:10.1002/spe.3319.
24. Al-Sulami ZA, Ali N, Ramli R, Lu S. Towards a comprehensive understanding of blockchain technology adoption in various industries in developing and emerging economies: a systematic review. Cogent Bus Manag. 2024;11(1):2294875. doi:10.1080/23311975.2023.2294875.
25. Rostad L, Edsberg O. A study of access control requirements for healthcare systems based on audit trails from access logs. In: 2006 22nd Annual Computer Security Applications Conference (ACSAC'06); 2006 Dec 11–15; Miami Beach, FL, USA. p. 175–86. doi:10.1109/ACSAC.2006.8.
26. Kanwal T, Anjum A, Malik SUR, Khan A, Khan MA. Privacy preservation of electronic health records with adversarial attacks identification in hybrid cloud. Comput Stand Interfaces. 2021;78(5):103522. doi:10.1016/j.csi.2021.103522.
27. Sengupta J, Ruj S, Das Bit S. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. J Netw Comput Appl. 2020;149(6):102481. doi:10.1016/j.jnca.2019.102481.
28. Villegas-Ch W, García-Ortiz J. Authentication, access, and monitoring system for critical areas with the use of artificial intelligence integrated into perimeter security in a data center. Front Big Data. 2023;6:1200390. doi:10.3389/fdata.2023.1200390.
29. Guo H, Li W, Nejad M, Shen CC. Access control for electronic health records with hybrid blockchain-edge architecture. arXiv:1906.01188. 2019.
30. Azbeg K, Ouchetto O, Andaloussi SJ, Fetjah L, Sekkaki A. Blockchain and IoT for security and privacy: a platform for diabetes self-management. In: 2018 4th International Conference on Cloud Computing Technologies and Applications (Cloudtech); 2018 Nov 26–28; Brussels, Belgium. doi:10.1109/CloudTech.2018.8713343.
31. Hamidi H. An approach to develop the smart health using internet of things and authentication based on biometric technology. Future Gener Comput Syst. 2019;91(3):434–49. doi:10.1016/j.future.2018.09.024.
32. Petru-Cristian N. A comprehensive analysis of high-impact cybersecurity incidents: case studies and implications [master's thesis]. Cluj-Napoca, Romania: Babes–Bolyai University; 2023.

33. Fang H, Qi A, Wang X. Fast authentication and progressive authorization in large-scale IoT: how to leverage AI for security enhancement. IEEE Netw. 2020;34(3):24–9. doi:10.1109/MNET.011.1900276.
34. Devi RM, Keerthika P, Suresh P, Sarangi PP, Sangeetha M, Sagana C, et al. Retina biometrics for personal authentication. In: Machine learning for biometrics. Amsterdam, The Netherlands: Elsevier; 2022. p. 87–104. doi:10.1016/b978-0-323-85209-8.00005-5.
35. Nakisa B, Ansarizadeh F, Oommen P, Kumar R. Using an extended technology acceptance model to investigate facial authentication. Telemat Inform Rep. 2023;12(5):100099. doi:10.1016/j.teler.2023.100099.
36. Nyangaresi VO, Al Sibahee MA, Abduljabbar ZA, Ma J, Khalefa MS. Biometric-based packet validation scheme for body area network smart healthcare devices. In: IEEE 21st Mediterranean Electrotechnical Conference (MELECON); 2022 Jun 14–16; Palermo, Italy. p. 726–31. doi:10.1109/MELECON53508.2022.9842900.
37. Mason J, Dave R, Chatterjee P, Graham-Allen I, Esterline A, Roy K. An investigation of biometric authentication in the healthcare environment. Array. 2020;8(2):100042. doi:10.1016/j.array.2020.100042.
38. Chenchev I, Aleksieva-Petrova A, Petrov M. Authentication mechanisms and classification: a literature survey. In: Intelligent computing. Cham, Germany: Springer International Publishing; 2021. p. 1051–70. doi:10.1007/978-3-030-80129-8_69.
39. Selvaraj S, Sundaravaradhan S. Challenges and opportunities in IoT healthcare systems: a systematic review. SN Appl Sci. 2019;2(1):139. doi:10.1007/s42452-019-1925-y.
40. Qiu X, Du Z, Sun X. Artificial intelligence-based security authentication: applications in wireless multimedia networks. IEEE Access. 2019;7:172004–11. doi:10.1109/access.2019.2956480.
41. Falco G, Viswanathan A, Caldera C, Shrobe H. A master attack methodology for an AI-based automated attack planner for smart cities. IEEE Access. 2018;6:48360–73. doi:10.1109/access.2018.2867556.
42. Galinkin E, Carter J, Mancoridis S. Evaluating attacker risk behavior in an internet of things ecosystem. In: Decision and game theory for security. Cham, Germany: Springer; 2021. p. 354–64. doi:10.1007/978-3-030-90370-1_19.
43. Shelke NA, Ahuja S, Banarjee A, Singh NP, Kasana SS, Kukreja S. AI-enabled IoT based multimodal authentication system for securing the hardware and software clients. In: 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON); 2022 May 26–27; Faridabad, India. p. 545–50. doi:10.1109/COM-IT-CON54601.2022.9850797.
44. Patel V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health Inform J. 2019;25(4):1398–411. doi:10.1177/1460458218769699.
45. Rahman MA, Hossain MS, Showail AJ, Alrajeh NA, Alhamid MF. A secure, private, and explainable IoHT framework to support sustainable health monitoring in a smart city. Sustain Cities Soc. 2021;72(3):103083. doi:10.1016/j.scs.2021.103083.
46. Merlec MM, Islam MM, Lee YK, In HP. A consortium blockchain-based secure and trusted electronic portfolio management scheme. Sensors. 2022;22(3):1271. doi:10.3390/s22031271.
47. Sadath L, Mehrotra D, Kumar A. Scalability performance analysis of blockchain using hierarchical model in healthcare. Blockchain Heal Today. 2024;7(1):7. doi:10.30953/bhty.v7.295.
48. Tuli S, Mahmud R, Tuli S, Buyya R. FogBus: a blockchain-based lightweight framework for edge and fog computing. J Syst Softw. 2019;154(5):22–36. doi:10.1016/j.jss.2019.04.050.
49. Gowda VD, Sharma A, Rao BK, Shankar R, Sarma P, Chaturvedi A, et al. Industrial quality healthcare services using Internet of things and fog computing approach. Meas Sens. 2022;24(5):100517. doi:10.1016/j.measen.2022.100517.
50. Meenu M, Kumar DD. Integration of blockchain with fog computing to improvise security & privacy issues. Int J Eng Technol Manag Sci. 2024;8(1):292–8. doi:10.46647/ijetms.2024.v08i01.038.
51. Hazra A, Rana P, Adhikari M, Amgoth T. Fog computing for next-generation internet of things: fundamental, state-of-the-art and research challenges. Comput Sci Rev. 2023;48(5):100549. doi:10.1016/j.cosrev.2023.100549.
52. Papaioannou M, Karageorgou M, Mantas G, Sucasas V, Essop I, Rodriguez J, et al. A survey on security threats and countermeasures in Internet of Medical Things (IoMT). Trans Emerg Telecommun Technol. 2022;33(6):e4049. doi:10.1002/ett.4049.

53. Wang X, Garg S, Lin H, Piran MJ, Hu J, Hossain MS. Enabling secure authentication in industrial IoT with transfer learning empowered blockchain. IEEE Trans Industr Inform. 2021;17(11):7725–33. doi:10.1109/TII.2021.3049405.
54. Washizaki H, Ogata S, Hazeyama A, Okubo T, Fernandez EB, Yoshioka N. Landscape of architecture and design patterns for IoT systems. IEEE Internet Things J. 2020;7(10):10091–101. doi:10.1109/jiot.2020.3003528.
55. Dattani N. A review paper on the internet of things (IoT) and its architecture; 2022. [cited 2025 Jul 1]. Available from: https://www.researchgate.net/publication/364126853.
56. Sikder AK, Petracca G, Aksu H, Jaeger T, Uluagac AS. A survey on sensor-based threats to internet-of-things (IoT) devices and applications. arXiv:1802.02041. 2018.
57. Mishra B, Kertesz A. The use of MQTT in M2M and IoT systems: a survey. IEEE Access. 2020;8:201071–86. doi:10.1109/access.2020.3035849.
58. Guo P, Liang W, Xu S. A privacy preserving four-factor authentication protocol for internet of medical things. Comput Secur. 2024;137(5):103632. doi:10.1016/j.cose.2023.103632.
59. Jawad M, Yassin AA, Ali Abed Al-Asadi H, Abduljabbar ZA, Omollo Nyangaresi V. IoHT system authentication through the blockchain technology: a review. In: 2024 10th International Conference on Control, Decision and Information Technologies (CoDIT); 2024 Jul 1–4; Vallette, Malta. p. 2253–8. doi:10.1109/CoDIT62066.2024.10708078.
60. Suleski T, Ahmed M, Yang W, Wang E. A review of multi-factor authentication in the internet of healthcare things. Digit Health. 2023;9:20552076231177144. doi:10.1177/20552076231177144.
61. Ouaddah A, Mousannif H, Abou Elkalam A, Ait Ouahman A. Access control in the internet of things: big challenges and new opportunities. Comput Netw. 2017;112(2):237–62. doi:10.1016/j.comnet.2016.11.007.
62. Yadav AK, Misra M, Pandey PK, Liyanage M. An EAP-based mutual authentication protocol for WLAN-connected IoT devices. IEEE Trans Ind Inform. 2022;19(2):1343–55. doi:10.1109/TII.2022.3194956.
63. Tuler De Oliveira M, Reis LHA, Verginadis Y, Mattos DMF, Olabarriaga SD. SmartAccess: attribute-based access control system for medical records based on smart contracts. IEEE Access. 2022;10:117836–54. doi:10.1109/access.2022.3217201.
64. Imdad M, Jacob DW, Mahdin H, Baharum Z, Shaharudin SM, Azmi MS. Internet of things: security requirements, attacks and counter measures. Indones J Electr Eng Comput Sci. 2020;18(3):1520. doi:10.11591/ijeecs.v18.i3.pp1520-1530.
65. Divya KS, Roopashree HR, Yogeesh AC. Non-repudiation-based network security system using multiparty computation. Int J Adv Comput Sci Appl. 2022;13(3):282–9. doi:10.14569/ijacsa.2022.0130335.
66. Jaiman V, Urovi V. A consent model for blockchain-based health data sharing platforms. IEEE Access. 2020;8:143734–45. doi:10.1109/access.2020.3014565.
67. Abduljabbar ZA, Nyangaresi VO, Jasim HM, Ma J, Hussain MA, Hussien ZA, et al. Elliptic curve cryptography-based scheme for secure signaling and data exchanges in precision agriculture. Sustainability. 2023;15(13):10264. doi:10.3390/su151310264.
68. Abduljabbar ZA, Omollo Nyangaresi V, Al Sibahee MA, Ghrabat MJJ, Ma J, Qays Abduljaleel I, et al. Session-dependent token-based payload enciphering scheme for integrity enhancements in wireless networks. J Sens Actuator Netw. 2022;11(3):55. doi:10.3390/jsan11030055.
69. Andrew J, Isravel DP, Sagayam KM, Bhushan B, Sei Y, Eunice J. Blockchain for healthcare systems: architecture, security challenges, trends and future directions. J Netw Comput Appl. 2023;215(21):103633. doi:10.1016/j.jnca.2023.103633.
70. Lei K, Du M, Huang J, Jin T. Groupchain: towards a scalable public blockchain in fog computing of IoT services computing. IEEE Trans Serv Comput. 2020;13(2):252–62. doi:10.1109/TSC.2019.2949801.
71. Nawir M, Amir A, Yaakob N, Lynn OB. Internet of things (IoT): taxonomy of security attacks. In: 2016 3rd International Conference on Electronic Design (ICED); 2016 Aug 11–12; Phuket, Thailand.
72. Nyangaresi VO, Jasim HM, Mutlaq KA, Abduljabbar ZA, Ma J, Abduljaleel IQ, et al. A symmetric key and elliptic curve cryptography-based protocol for message encryption in unmanned aerial vehicles. Electronics. 2023;12(17):3688. doi:10.3390/electronics12173688.

73. Anajemba JH, Iwendi C, Razzak I, Ansere JA, Okpalaoguchi IM. A counter-eavesdropping technique for optimized privacy of wireless industrial IoT communications. IEEE Trans Ind Inform. 2022;18(9):6445–54. doi:10.1109/TII.2021.3140109.
74. Nosouhi MR, Sood K, Grobler M, Doss R. Towards spoofing resistant next generation IoT networks. IEEE Trans Inform Forensic Secur. 2022;17:1669–83. doi:10.1109/tifs.2022.3170276.
75. Mohammadnia H. IoT-NETZ: spoofing attack mitigation in IoT network [dissertation]. Stockholm, Sweden: KTH Royal Institute of Technology; 2019.
76. Manavi MT. Defense mechanisms against distributed denial of service attacks: a survey. Comput Electr Eng. 2018;72(2):26–38. doi:10.1016/j.compeleceng.2018.09.001.
77. Kumari P, Jain AK. A comprehensive study of DDoS attacks over IoT network and their countermeasures. Comput Secur. 2023;127(2):103096. doi:10.1016/j.cose.2023.103096.
78. Wang Y, Tan M. Defense against sybil attack in blockchain based on improved consensus algorithm. In: IEEE International Conference on Control, Electronics and Computer Technology (ICCECT); 2023 Apr 28–30; Jilin, China. p. 986–9. doi:10.1109/ICCECT57938.2023.10140278.
79. Hasan MK, Zhou W, Safie N, Ahmed FRA, Ghazal TM. A survey on key agreement and authentication protocol for internet of things application. IEEE Access. 2024;12(7):61642–66. doi:10.1109/access.2024.3393567.
80. Lin C, Wu G, Yu CW, Yao L. Maximizing destructiveness of node capture attack in wireless sensor networks. J Supercomput. 2015;71(8):3181–212. doi:10.1007/s11227-015-1435-7.
81. Bathla R, Ahlawat P. Matrix based optimal solution for node capture attack to enhance the attacking efficiency of attacker. Res Sq Forthcoming. 2023. doi:10.21203/rs.3.rs-1355213/v1.
82. Kaushik P, Majumdar R. Timing attack analysis on AES on modern processors. In: 2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO); 2017 Sep 20–22; Noida, India. p. 462–5. doi:10.1109/ICRITO.2017.8342471.
83. Lee K, Lee J, Yim K. Classification and analysis of malicious code detection techniques based on the APT attack. Appl Sci. 2023;13(5):2894. doi:10.3390/app13052894.
84. Zhang J, Guo R, Shi Y, Tang W. An anti-impersonation attack electronic health record sharing scheme based on proxy re-encryption and blockchain. Math Biosci Eng. 2024;21(6):6167–89. doi:10.3934/mbe.2024271.
85. Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, et al. Lightweight integrity preserving scheme for secure data exchange in cloud-based IoT systems. Appl Sci. 2023;13(2):691. doi:10.3390/app13020691.
86. Gupta R, Tanwar S, Tyagi S, Kumar N. Machine learning models for secure data analytics: a taxonomy and threat model. Comput Commun. 2020;153(5):406–40. doi:10.1016/j.comcom.2020.02.008.
87. Deb R, Roy S. A comprehensive survey of vulnerability and information security in SDN. Comput Netw. 2022;206(11):108802. doi:10.1016/j.comnet.2022.108802.
88. Hao Y. Research of the 51% attack based on blockchain. In: 2022 3rd International Conference on Computer Vision, Image and Deep Learning & International Conference on Computer Engineering and Applications (CVIDL & ICCEA); 2022 May 20–22; Changchun, China. p. 278–83. doi:10.1109/CVIDLICCEA56201.2022.9824528.
89. Abdullah S, Rothenberg S, Siegel E, Kim W. School of block-review of blockchain for the radiologists. Acad Radiol. 2020;27(1):47–57. doi:10.1016/j.acra.2019.06.025.
90. Aziz IT, Jin H, Abdulqadder IH, Hussien ZA, Abduljabbar ZA, Flaih FMF. A lightweight scheme to authenticate and secure the communication in smart grids. Appl Sci. 2018;8(9):1508. doi:10.3390/app8091508.
91. Wang Z, Zhao J, Sun P, Yang J, Wang R, Zhang X. A lightweight three-party mutual authentication protocol for internet of health things systems. J Healthc Eng. 2023;2023(1):1044282. doi:10.1155/2023/1044282.
92. Chen Y, Li M, Chen P, Xia S. Survey of cross-technology communication for IoT heterogeneous devices. IET Commun. 2019;13(12):1709–20. doi:10.1049/iet-com.2018.6069.
93. Shojaei P, Vlahu-Gjorgievska E, Chow YW. Security and privacy of technologies in health information systems: a systematic literature review. Computers. 2024;13(2):41. doi:10.3390/computers13020041.
94. Farooq U, Tariq N, Asim M, Baker T, Al-Shamma'a A. Machine learning and the internet of things security: solutions and open challenges. J Parallel Distrib Comput. 2022;162(1):89–104. doi:10.1016/j.jpdc.2022.01.015.

95. Ghimire B, Rawat DB. Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for Internet of things. IEEE Internet Things J. 2022;9(11):8229–49. doi:10.1109/JIOT.2022.3150363.
96. de Oliveira MT, Verginadis Y, Reis LHA, Psarra E, Patiniotakis I, Olabarriaga SD. AC-ABAC: attribute-based access control for electronic medical records during acute care. Expert Syst Appl. 2023;213(4):119271. doi:10.1016/j.eswa.2022.119271.
97. Shen N, Bernier T, Sequeira L, Strauss J, Silver MP, Carter-Langford A, et al. Understanding the patient privacy perspective on health information exchange: a systematic review. Int J Med Inform. 2019;125(4):1–12. doi:10.1016/j.ijmedinf.2019.01.014.
98. Sahu AK, Sharma S, Raja R. Deep learning-based continuous authentication for an IoT-enabled healthcare service. Comput Electr Eng. 2022;99(3):107817. doi:10.1016/j.compeleceng.2022.107817.
99. Amiri-Zarandi M, Dara RA, Fraser E. A survey of machine learning-based solutions to protect privacy in the internet of things. Comput Secur. 2020;96(8):101921. doi:10.1016/j.cose.2020.101921.
100. Mamdouh M, Awad AI, Khalaf AAM, Hamed HFA. Authentication and identity management of IoHT devices: achievements, challenges, and future directions. Comput Secur. 2021;111(4):102491. doi:10.1016/j.cose.2021.102491.
101. Shafay M, Ahmad RW, Salah K, Yaqoob I, Jayaraman R, Omar M. Blockchain for deep learning: review and open challenges. Cluster Comput. 2023;26(1):197–221. doi:10.1007/s10586-022-03582-7.
102. Cobrado UN, Sharief S, Regahal NG, Zepka E, Mamauag M, Velasco LC. Access control solutions in electronic health record systems: a systematic review. Inform Med Unlocked. 2024;49(6):101552. doi:10.1016/j.imu.2024.101552.
103. Meng Y, Huang Z, Shen G, Ke C. SDN-based security enforcement framework for data sharing systems of smart healthcare. IEEE Trans Netw Serv Manag. 2020;17(1):308–18. doi:10.1109/TNSM.2019.2941214.
104. Al-Naji FH, Zagrouba R. A survey on continuous authentication methods in internet of things environment. Comput Commun. 2020;163(3):109–33. doi:10.1016/j.comcom.2020.09.006.
105. Lo NW, Wu CY, Chuang YH. An authentication and authorization mechanism for long-term electronic health records management. Procedia Comput Sci. 2017;111:145–53. doi:10.1016/j.procs.2017.06.021.
106. Mohamad Jawad HH, Bin Hassan Z, Zaidan BB, Mohammed Jawad FH, Mohamed Jawad DH, Alredany WHD. A systematic literature review of enabling IoT in healthcare: motivations, challenges, and recommendations. Electronics. 2022;11(19):3223. doi:10.3390/electronics11193223.
107. Son S, Lee J, Kim M, Yu S, Das AK, Park Y. Design of secure authentication protocol for cloud-assisted telecare medical information system using blockchain. IEEE Access. 2020;8:192177–91. doi:10.1109/access.2020.3032680.
108. Ussatova O, Makilenov S, Mukaddas A, Amanzholova S, Begimbayeva Y, Ussatov N. Enhancing healthcare data security: a two-step authentication scheme with cloud technology and blockchain. East Eur J Enterp Technol. 2023;6:6–16. doi:10.15587/1729-4061.2023.289325.
109. Saini A, Zhu Q, Singh N, Xiang Y, Gao L, Zhang Y. A smart-contract-based access control framework for cloud smart healthcare system. IEEE Int Things J. 2020;8(7):5914–25. doi:10.1109/JIOT.2020.3032997.
110. Ahmed NA, Ammar M, Hefny HA. Proposed authentication protocol for IoT using blockchain and fog nodes. Int J Adv Comput Sci Appl. 2020;11(4):710–6. doi:10.14569/ijacsa.2020.0110491.
111. Hankerson D, Menezes A. Elliptic curve discrete logarithm problem. In: Encyclopedia of cryptography and security. Boston, MA, USA: Springer; 2011. p. 397–400. doi:10.1007/978-1-4419-5906-5_246.
112. Jawad M, Yassin AA, AL-Asadi HA, Abduljabbar ZA, Nyangaresi VO. Towards building multi-factor authentication scheme for users in the healthcare sector based on blockchain technology. In: Cybernetics and control theory in systems. Berlin/Heidelberg, Germany: Springer; 2024.
113. Martino R, Cilardo A. Designing a SHA-256 processor for blockchain-based IoT applications. Int Things. 2020;11(3):100254. doi:10.1016/j.iot.2020.100254.
114. Lakshmi VS, Deepthi S, Deepthi PP. Collusion resistant secret sharing scheme for secure data storage and processing over cloud. J Inf Secur Appl. 2021;60(9):102869. doi:10.1016/j.jisa.2021.102869.
115. FIPS197. Advanced Encryption Standard (AES). Gaithersburg, MD, USA: Federal Information Processing Standards Publication; 2001. doi:10.6028/NIST.FIPS.197-upd1.

116. Nyangaresi VO, Abduljabbar ZA, Ma J, Al Sibahee MA. Verifiable security and privacy provisioning protocol for high reliability in smart healthcare communication environment. In: 2022 4th Global Power, Energy and Communication Conference (GPECOM); 2022 Jun 14–17; Nevsehir, Turkey. p. 569–74. doi:10.1109/GPECOM55404.2022.9815685.
117. Fu X, Ding Y, Li H, Ning J, Wu T, Li F. A survey of lattice based expressive attribute based encryption. Comput Sci Rev. 2022;43(5):100438. doi:10.1016/j.cosrev.2021.100438.
118. Jones RW. HarmonicCrypt: a waveform-based encryption paradigm. OSF Preprints Forthcoming. 2025. doi:10.31219/osf.io/ngrx9_v1.
119. Shuriya B, Kumar SV, Bagyalakshmi K. Noise-resilient homomorphic encryption: a framework for secure data processing in health care domain. arXiv:2412.11474. 2024.
120. Alwahedi F, Aldhaheri A, Ferrag MA, Battah A, Tihanyi N. Machine learning techniques for IoT security: current research and future vision with generative AI and large language models. Int Things Cyber-Phys Syst. 2024;4(4):167–85. doi:10.1016/j.iotcps.2023.12.003.
121. Corthis PB, Ramesh GP, García-Torres M, Ruíz R. Effective identification and authentication of healthcare IoT using fog computing with hybrid cryptographic algorithm. Symmetry. 2024;16(6):726. doi:10.3390/sym16060726.
122. Xiao L, Wan X, Lu X, Zhang Y, Wu D. IoT security techniques based on machine learning: how do IoT devices use AI to enhance security? IEEE Signal Process Mag. 2018;35(5):41–9. doi:10.1109/MSP.2018.2825478.
123. Jahangir H, Lakshminarayana S, Maple C, Epiphaniou G. A deep-learning-based solution for securing the power grid against load altering threats by IoT-enabled devices. IEEE Internet Things J. 2023;10(12):10687–97. doi:10.1109/JIOT.2023.3240289.
124. Dahou A, Al-qaness MAA, Abd Elaziz M, Helmi A. Human activity recognition in IoHT applications using arithmetic optimization algorithm and deep learning. Measurement. 2022;199(41):111445. doi:10.1016/j.measurement.2022.111445.
125. Umran SM, Lu S, Ameen Abduljabbar Z, Tang X. A blockchain-based architecture for securing industrial IoTs data in electric smart grid. Comput Mater Contin. 2023;74(3):5389–416. doi:10.32604/cmc.2023.034331.
126. De Novi G, Sofia N, Vasiliu-Feltes I, Zang CY, Ricotta F. Blockchain technology predictions 2024: transformations in healthcare, patient identity, and public health. Blockchain Healthc Today. 2023;6(2):6. doi:10.30953/bhty.v6.287.
127. Sonkamble RG, Phansalkar SP, Potdar VM, Bongale AM. Survey of interoperability in electronic health records management and proposed blockchain based framework: MyBlockEHR. IEEE Access. 2021;9:158367–401. doi:10.1109/access.2021.3129284.
128. Alkhdour TA, Almaiah MA, Ali AI, Al-Ali RO, Tin TT, Aldahyani TH. Improving secure routing in IoMT: enhanced blockchain cybersecurity scheme using hyperledger fabric. J Theor Appl Inf Technol. 2024;102(14):5663–89.
129. Ali Siyal A, Junejo AZ, Zawish M, Ahmed K, Khalil A, Soursou G. Applications of blockchain technology in medicine and healthcare: challenges and future perspectives. Cryptography. 2019;3(1):3. doi:10.3390/cryptography3010003.
130. Almaiah MA, Hajjej F, Ali A, Pasha MF, Almomani O. A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS. Sensors. 2022;22(4):1448. doi:10.3390/s22041448.
131. Al-ali M, A.Yassin A, Ali Abed AL-Asadi H. Adoption of bloom filter and firebase framework to enhance authentication time for healthcare systems based on blockchain technology. J Basrah Res. 2024;50(1):16. doi:10.56714/bjrs.50.1.23.
132. Barj S, Youjil A. Blockchain and cryptocurrency security from a new layered perspective and a novel MITRE ATT&CK-based approach for understanding cyberattacks and mitigating their impacts. Int J Eng Trends Technol. 2024;72(4):1–14. doi:10.14445/22315381/ijett-v72i4p101.
133. Paul P, Aithal PS, Saavedra R, Ghosh S. Blockchain technology and its types—a short review. Int J Appl Sci Eng. 2021;9(2):189–200. doi:10.30954/2322-0465.2.2021.7.
134. Islam MS, Rahman MA, Bin Ameedeen MA, Ajra H, Ismail ZB, Zain JM. Blockchain-enabled cybersecurity provision for scalable heterogeneous network: a comprehensive survey. Comput Model Eng Sci. 2024;138(1):43–123. doi:10.32604/cmes.2023.028687.

135. Baniata H, Kertesz A. Partial pre-image attack on proof-of-work based blockchains. Blockchain Res Appl. 2024;5(3):100194. doi:10.1016/j.bcra.2024.100194.
136. Verma S, Yadav D, Chandra G. Introduction of formal methods in blockchain consensus mechanism and its associated protocols. IEEE Access. 2022;10(37):66611–24. doi:10.1109/access.2022.3184799.
137. Alzaidi ZS, Yassin AA, Abduljabbar ZA, Omollo Nyangaresi V. Development anonymous authentication maria et al.'s scheme of VANETs using blockchain and fog computing with QR code technique. In: 2024 10th International Conference on Control, Decision and Information Technologies (CoDIT); 2024 Jul 1–4; Vallette, Malta. p. 2247–52. doi:10.1109/CoDIT62066.2024.10708495.
138. Quy VK, Hau NV, Anh DV, Ngoc LA. Smart healthcare IoT applications based on fog computing: architecture, applications and challenges. Complex Intell Systems. 2022;8(5):3805–15. doi:10.1007/s40747-021-00582-9.
139. Abouaomar A, Cherkaoui S, Kobbane A, Dambri OA. A resources representation for resource allocation in fog computing networks. In: 2019 IEEE Global Communications Conference (GLOBECOM); 2019 Dec 9–13; Waikoloa, HI, USA. doi:10.1109/globecom38437.2019.9014146.
140. Mahmud R, Kotagiri R, Buyya R. Fog computing: a taxonomy, survey and future directions. In: Internet of everything: algorithms, methodologies, technologies and perspectives. Singapore: Springer; 2017. p. 103–30. doi:10.1007/978-981-10-5861-5_5.
141. Ghani N, Abu Bakar Sajak A, Qureshi R, Azril Zuhairi MF, Ahmad Baidowi ZMP. A review of fog computing concept, architecture, application, parameters and challenges. Int J Inform Vis. 2024;8(2):564. doi:10.62527/joiv.8.2.2187.
142. Habibi P, Farhoudi M, Kazemian S, Khorsandi S, Leon-Garcia A. Fog computing: a comprehensive architectural survey. IEEE Access. 2020;8:69105–33. doi:10.1109/access.2020.2983253.
143. Alzoubi YI, Gill A, Mishra A. A systematic review of the purposes of Blockchain and fog computing integration: classification and open issues. J Cloud Comput. 2022;11(1):80. doi:10.1186/s13677-022-00353-y.
144. Shiriaev E, Ermakova T, Bezuglova E, Lapina MA, Babenko M. Reliablity and security for fog computing systems. Information. 2024;15(6):317. doi:10.3390/info15060317.
145. Fan S, Song L, Sang C. Research on privacy protection in IoT system based on blockchain. In: Smart blockchain. Berlin/Heidelberg, Germany: Springer; 2019. p. 1–10. doi:10.1007/978-3-030-34083-4_1.
146. Batchu S, Patel K, Henry OS, Mohamed A, Agarwal AA, Hundal H, et al. Using ethereum smart contracts to store and share COVID-19 patient data. Cureus. 2022;14(1):e21378. doi:10.7759/cureus.21378.
147. Kushwaha SS, Joshi S, Singh D, Kaur M, Lee HN. Systematic review of security vulnerabilities in ethereum blockchain smart contract. IEEE Access. 2022;10(6):6605–21. doi:10.1109/access.2021.3140091.
148. Ethereum.org. [cited 2025 Jul 1]. Available from: https://ethereum.org/en/.
149. Ullah I, Havinga PJM. Governance of a blockchain-enabled IoT ecosystem: a variable geometry approach. Sensors. 2023;23(22):9031. doi:10.3390/s23229031.
150. Vujičić D, Jagodić D, Ranđić S. Blockchain technology, Bitcoin, and ethereum: a brief overview. In: 17th International Symposium Infoteh-JAHORINA (INFOTEH); 2018 Mar 21–23; East Sarajevo, Bosnia and Herzegovina. doi:10.1109/INFOTEH.2018.8345547.
151. REMIX_Solidity compiler. [cited 2025 Jul 1]. Available from: https://remix-ide.readthedocs.io/en/latest/compile.html.
152. Chopra UK, Rathore AK, Pandey R. Rendering blockchain immutability in chatserver: a node.js approach. In: Decision analytics applications in industry. Singapore: Springer; 2020. p. 147–55. doi:10.1007/978-981-15-3643-4_10.
153. Run JavaScript Everywhere. [cited 2025 Jul 1]. Available from: https://nodejs.org/en.
154. Duldulao DB, Cabagnot RJL. Getting started with the node package manager. In: Practical enterprise react. Berkeley, CA, USA: Apress; 2021. p. 11–9. doi:10.1007/978-1-4842-6975-6_2.
155. Blockchain-council page. [cited 2025 Jul 1]. Available from: https://www.blockchain-council.org/.
156. Mathur G. GANACHE: a robust framework for efficient and secure storage of data on private ethereum blockchains. Res Sq Forthcoming. 2023;82(5):395. doi:10.21203/rs.3.rs-3495549/v1.

157. Cheval V, Cortier V, Turuani M. A little more conversation, a little less action, a lot more satisfaction: global states in ProVerif. In: 2018 IEEE 31st Computer Security Foundations Symposium (CSF); 2018 Jul 9–12; Oxford, UK. p. 344–58. doi:10.1109/CSF.2018.00032.
158. Cong LW, He Z. Blockchain disruption and smart contracts. Rev Financ Stud. 2019;32(5):1754–97. doi:10.1093/rfs/hhz007.
159. Edris EKK, Aiash M, Loo J. Formal verification of authentication and service authorization protocols in 5G-enabled device-to-device communications using ProVerif. Electronics. 2021;10(13):1608. doi:10.3390/electronics10131608.
160. Al Fikri M, Ramli K, Sudiana D. Formal verification of the authentication and voice communication protocol security on device X using scyther tool. IOP Conf Ser Mater Sci Eng. 2021;1077(1):012057. doi:10.1088/1757-899x/1077/1/012057.
161. Viganò L. Automated security protocol analysis with the AVISPA tool. Electron Notes Theor Comput Sci. 2006;155(1):61–86. doi:10.1016/j.entcs.2005.11.052.
162. Liu B, Yang B, Su X. An improved two-way security authentication protocol for RFID system. Information. 2018;9(4):86. doi:10.3390/info9040086.
163. Becerra J, Iovino V, Ostrev D, Škrobot M. On the relation between SIM and IND-RoR security models for PAKEs with forward secrecy. In: E-business and telecommunications. Berlin/Heidelberg, Germany: Springer; 2019. p. 173–98. doi:10.1007/978-3-030-11039-0_9.
164. Barman S, Shum HPH, Chattopadhyay S, Samanta D. A secure authentication protocol for multi-server-based E-healthcare using a fuzzy commitment scheme. IEEE Access. 2019;7:12557–74. doi:10.1109/access.2019.2893185.
165. Millen JK, Clark SC, Freedman SB. The interrogator: protocol secuity analysis. IEEE Trans Softw Eng. 1987;SE-13(2):274–88. doi:10.1109/TSE.1987.233151.
166. Hassan A, Minilla J. Automated verification tools for cryptographic protocols. In: 2021 International Conference on Promising Electronic Technologies (ICPET); 2021 Nov 17–18; Palestine: Deir Al-Balah.
167. Escobar S, Meadows C, Meseguer J. A rewriting-based inference system for the NRL protocol analyzer: grammar generation. In: Proceedings of the 2005 ACM Workshop on Formal Methods in Security Engineering; 2005 Nov 11; Fairfax, VA, USA. doi:10.1145/1103576.1103578.
168. Feng Q, He D, Wang H, Zhou L, Choo KR. Lightweight collaborative authentication with key protection for smart electronic health record system. IEEE Sens J. 2020;20(4):2181–96. doi:10.1109/JSEN.2019.2949717.
169. Wu TY, Wang L, Chen CM. Enhancing the security: a lightweight authentication and key agreement protocol for smart medical services in the IoHT. Mathematics. 2023;11(17):3701. doi:10.3390/math11173701.
170. Ray PP, Kumar N, Dash D. BLWN: blockchain-based lightweight simplified payment verification in IoT-assisted e-healthcare. IEEE Syst J. 2021;15(1):134–45. doi:10.1109/JSYST.2020.2968614.
171. Alnuaimi A, Alshehhi A, Salah K, Jayaraman R, Omar IA, Battah A. Blockchain-based processing of health insurance claims for prescription drugs. IEEE Access. 2022;10:118093–107. doi:10.1109/access.2022.3219837.
172. Elvas LB, Serrão C, Ferreira JC. Sharing health information using a blockchain. Healthcare. 2023;11(2):170. doi:10.3390/healthcare11020170.
173. Agha D. Securing electronic health records using blockchain. VFAST Trans Softw Eng. 2023;11(4):57–66. doi:10.21015/vtse.v11i4.1656.
174. Qadir GA, Hussan BK. An authentication and access control model for healthcare based cloud services. J Eng. 2023;29(3):15–26. doi:10.31026/j.eng.2023.03.02.
175. Abbasi IA, Jan SU, Alqahtani AS, Khan AS, Algarni F. A lightweight and robust authentication scheme for the healthcare system using public cloud server. PLoS One. 2024;19(1):e0294429. doi:10.1371/journal.pone.0294429.
176. Velásquez I, Caro A, Rodríguez A. Authentication schemes and methods: a systematic literature review. Inf Softw Technol. 2018;94:30–7. doi:10.1016/j.infsof.2017.09.012.
177. Khan MA, Din IU, Majali T, Kim BS. A survey of authentication in internet of things-enabled healthcare systems. Sensors. 2022;22(23):9089. doi:10.3390/s22239089.
178. Shankar K, Perumal E, Gupta D. IoHT-based improved grey optimization with support vector machine for gastrointestinal hemorrhage detection and diagnosis model. In: Artificial intelligence for the internet of health things. Boca Raton, FL, USA: CRC Press; 2021. p. 45–58.

179. Albalawi A, Almrshed A, Badhib A, Alshehri S. A survey on authentication techniques for the Internet of things. In: 2019 International Conference on Computer and Information Sciences (ICCIS); 2019 Apr 3–4; Sakaka, Saudi Arabia. doi:10.1109/iccisci.2019.8716401.
180. Aghili SF, Mala H, Shojafar M, Peris-Lopez P. LACO: lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT. Future Gener Comput Syst. 2019;96(1):410–24. doi:10.1016/j.future.2019.02.020.
181. Jan SU, Ghani A, Alzahrani A, Saqlain SM, Yahya K, Sajjad H. Bandwidth and power efficient lightweight authentication scheme for healthcare system. J King Saud Univ Comput Inf Sci. 2023;35(7):101601. doi:10.1016/j.jksuci.2023.101601.
182. Sun S, Du R, Chen S, Li W. Blockchain-based IoT access control system: towards security, lightweight, and cross-domain. IEEE Access. 2021;9:36868–78. doi:10.1109/access.2021.3059863.
183. Patel C, Bashir AK, Ali AlZubi A, Jhaveri R. EBAKE-SE: a novel ECC-based authenticated key exchange between industrial IoT devices using secure element. Digit Commun Netw. 2023;9(2):358–66. doi:10.1016/j.dcan.2022.11.001.