sensors

MDPI

Review

A Survey of Authentication in Internet of Things-Enabled Healthcare Systems

Mudassar Ali Khan [1], Ikram Ud Din [1,*], Tha'er Majali [2] and Byung-Seo Kim [3,*]

[1] Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan
[2] Department of Management Information Systems, Applied Science Private University, Shafa Badran, Amman 11937, Jordan
[3] Department of Software and Communications Engineering, Hongik University, Sejong 30016, Republic of Korea
* Correspondence: ikramuddin205@yahoo.com (I.U.D.); jsnbs@hongik.ac.kr (B.-S.K.)

Abstract: The Internet of medical things (IoMT) provides an ecosystem in which to connect humans, devices, sensors, and systems and improve healthcare services through modern technologies. The IoMT has been around for quite some time, and many architectures/systems have been proposed to exploit its true potential. Healthcare through the Internet of things (IoT) is envisioned to be efficient, accessible, and secure in all possible ways. Even though the personalized health service through IoT is not limited to time or location, many associated challenges have emerged at an exponential pace. With the rapid shift toward IoT-enabled healthcare systems, there is an extensive need to examine possible threats and propose countermeasures. Authentication is one of the key processes in a system's security, where an individual, device, or another system is validated for its identity. This survey explores authentication techniques proposed for IoT-enabled healthcare systems. The exploration of the literature is categorized with respect to the technology deployment region, as in cloud, fog, and edge. A taxonomy of attacks, comprehensive analysis, and comparison of existing authentication techniques opens up possible future directions and paves the road ahead.

Keywords: authentication; healthcare; Internet of things; IoMT; security; vulnerability

Citation: Khan, M.A.; Din, I.U.; Majali, T., Kim, B.-S. A Survey of Authentication in Internet of Things-Enabled Healthcare Systems. *Sensors* **2022**, *22*, 9089. https://doi.org/10.3390/s22239089

Academic Editor: Nikos Fotiou

Received: 6 October 2022
Accepted: 20 November 2022
Published: 23 November 2022

1. Introduction

The Internet of medical things (IoMT) allows a variety of medical equipment and applications to communicate over the Internet, which has redefined healthcare over the past few decades [1,2]. Throughout the medical sector, wearable Internet of things (IoT) technologies have unleashed the era of smart healthcare [3,4], enabling the constant monitoring of patients under safe living conditions and thereby strengthening the existing hospital facilities [5–7].

According to the World Health Organization (WHO), human life expectancy has improved, and most people are likely to live more than 60 years [8]. Older adults are more vulnerable to infectious illnesses, disorders, and hospitalization [9]. According to an estimation made in 2008, the elderly population across the globe was approximately 506 million, which will further be increasing to around 1.3 billion by the year 2040 [10]. Technologies based on wireless sensors provide facilitation to patients and elderly populations specifically—i.e., those who require constant monitoring [11]. The deployment of medical sensor networks in healthcare applications has drastically improved the healthcare sector in the 21st century [12–14]. Humans who serve as actors in healthcare infrastructures, such as patients, doctors, staff, etc., have been involved in such wireless networks directly in a limited manner to increase the portability of gadgets and achieve higher transfer rates, along with keeping communication and other beneficiaries secure [15]. Small medical sensors are kept in close proximity to the patient and rarely connected with the body [16,17]. Their service is to monitor changes in the physiological state of the patient

promptly. These sensors observe patient vitals and usually communicate them through a gateway to some distant remote site, for detection of possible change [18]. During this process, human intercession is decreased to a minimum level [19]. A specialist can utilize these readings to append an expert appraisal of the patient's well-being. The most common vital signs include heart rate, temperature, blood pressure, body movement, pulse-oximetry, etc. [20,21]. Such a critical observation and fine-grain attention to detail benefit patients while also making a thorough health history [22].

Although the Internet of things comes with many opportunities, there are many challenges [23–25]. Like many other IoT challenges, security has been given a fair amount of attention in the past [26]. This survey extensively elaborates on authentication approaches (both user and device authentication) being utilized and developed for the IoMT specifically.

The rest of the article is structured as follows. Section 2 will discuss the key concepts related to the Internet of things and state-of-the-art healthcare systems. The literature review, Section 3, discusses various approaches related to the authentication process being used at multiple levels, including modern networks such as cloud, fog, and edge. A detailed comparative analysis of existing methods, for cloud, fog, and edge, is explained in the form of tables. Key findings of this study, related to authentication in IoT-enabled health care systems are discussed in Section 4, which is followed up with the conclusion. The list of acronyms used in the paper is listed in Table 1.

Table 1. Acronyms and their respective full forms.

Acronym	Full Form
AES	Advanced Encryption Standard
CUA	Client-based User Authentication
CBAC	Contextual Based Access Control
CV	Credential Vault
DED	Data Encryption/Decryption
DoS	Denial of Service
DA	Device Authentication
DACP	Dynamic Access Control Policy
ECC	Elliptic Curve Cryptographic
EHR	Electronic Health Record
EMR	Electronic Medical Record
EMR	Electronic Medical Records
HE-RSA	Homomorphic Encryption- Rivest Shamir Adleman
IMDs	Implantable Medical Devices
IaaS	Infrastructure as a Service
IMEI	International Mobile Equipment Identity
IoMT	Internet of Medical Things
IoT	Internet of Things
IPFS	Interplanetary File Systems
JPBC	Java Pairing-Based Cryptography Library
LPU	Local Processing Unit
MSN	Medical Sensor Network
MDHA	Modified Diffie-Hellman Agent
MA-EBA	Multi-Authority Encryption-Based Attribute
PHI	Personal Health Information
PUFs	Physical Unclonable Functions
PaaS	Platform as a Service
QoE	Quality of Experience
RFID	Radio-Frequency Identification authentication
RBAC	Role-based Access Control
SEA	Secured and Efficient Authentication
SPoC	Single Point of Contact
SaaS	Software as a Service
SSDP	Simple Service Discovery Protocol
SEMTN	Stateless Multiparty Trust Negotiation
TC	Trust Circles
TN	Trust Negotiation

Table 1. *Cont.*

Acronym	Full Form
TPM	Trusted Platform Module
UA	User Authentication
VF	Virtual Federations
WBAN	Wireless Body Area Network
WMSN	Wireless Medical Sensor Network
WSN	Wireless Sensor Network
WHO	World Health Organization
ZKP	Zero-Knowledge-Proof

2. Fundamentals of Internet of Things-Enabled Healthcare Systems

To the disbelief of critics, the IoT had a revolutionary experience in the last decade [27], whereby many ventures have taken place to revitalize hardware and software standards to overcome associated challenges. With many big companies, including Amazon, Microsoft, Intel, Cisco, etc. [28–30], and the research community investing efforts and resources into the field, standards of collaborating systems are being created while reducing human interventions, yet achieving quality lifestyles [31].

2.1. Internet of Things

The IoT [32], being a network of things, comes with software standards and a variety of electronic sensing devices to collectively address many real-world issues [33]. The "things" in the phrase IoT can be as simple as small home appliances, like ovens or refrigerators, or may be something as complex as a heavy production plant deployed in an industry [34]. According to an estimate presented by Cisco [35], the number of devices connected to the IoT will reach up to 500 billion by 2030. As per a report by IDC USA [36], $1.3 trillion is expected to be globally spent on IoT with projected revenue of $594 billion in the year 2022. With such a promising future, IoT is expanding to conquer many sectors, including smart homes [37,38], smart cities [39–41], industries [42–44], agriculture [45–47], Healthcare [48,49], transportation [50–52], and various other sectors [53–58].

2.2. Internet of Things-Enabled Healthcare Systems

With the exploration of prospective ventures in IoT, its applications in healthcare have shown steady growth over the past several years [59]. The IoMT (also referred to as the medical Internet of things) has emerged, attracting many studies proposing architectures [60], utilizing sensory gadgets [61], securing framework, and management of the things over an IoT deployed in a medical infrastructure [2]. Even though the scope of IoMT cannot be limited, as mentioned in many articles, IoMT encompasses the following broad areas.

- Control over medication and equipment: Although not restricting the scope within a healthcare infrastructure, the IoT empowers the management and control over medication [62] and medical sensory equipment [63]. Continuous as well as real-time monitoring [64] and control of production units [65] can help such automated industries keep up with the challenges faced while meeting end users' expectations.
- Health data management: It is a fact that in healthcare environmental spaces, such as hospitals, record generation takes place continuously. Though digital systems that help control healthcare infrastructure have been used for a couple of decades, many advancements, including the IoT, can further benefit mankind tremendously [66]. In an IoT-enabled infrastructure, the following tasks are given importance: management of data of patients [67], emergency management [68,69], management of inventory [70–72], resource scheduling [73], error prevention [74,75], etc.
- Medical administration and telemedicine: Administration of medical practice and consultation specifically had been limited within hospitals ensuring the physical presence of patients. Covid-19 has made us learn many lessons, including preparedness and remote treatments. Fortunately, with IoT, remote consultation is efficient [76–78],

and sensory devices play an important role in the recognition of vitals and symptoms [79]. Over the last two years, many e-health systems have been launched to provide proper care to patients across the globe [80,81].

2.3. Security Risks and Attacks

Security and privacy concerns emerge with every new technological discovery [82]. The IoT brings a paradigm for the interaction of digital devices that have sensory and communicative strengths. Figure 1 provides layers-based taxonomy of possible security attacks in an IoT environment, adopted from [83–85].

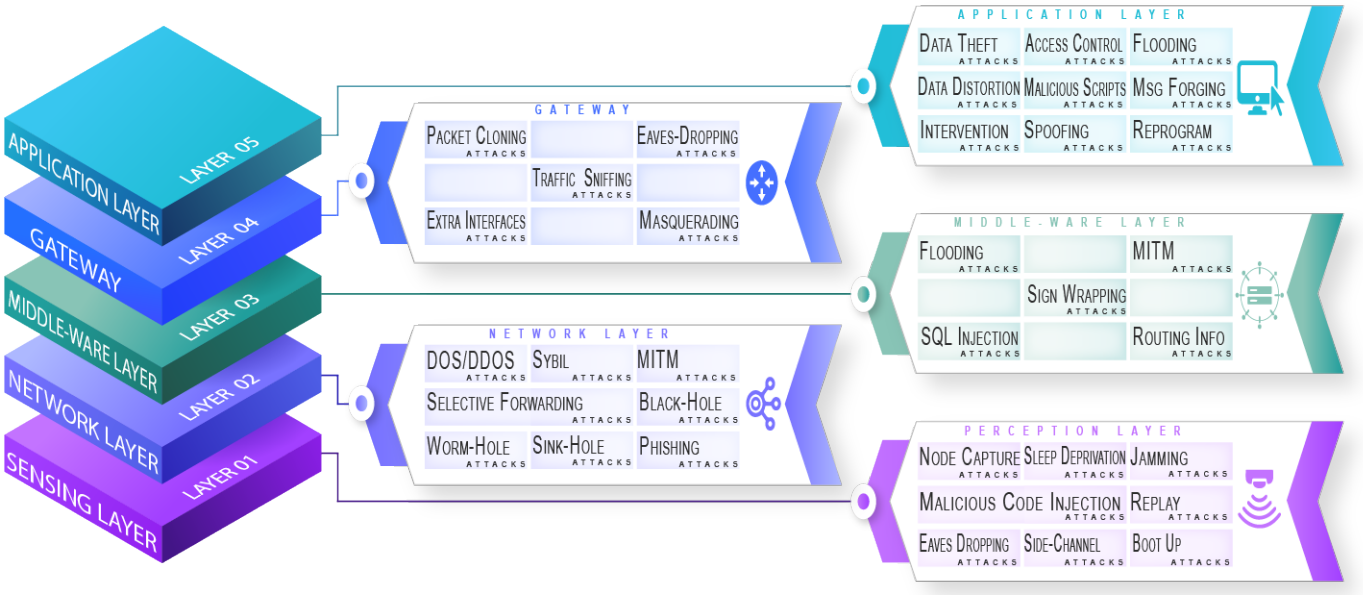

Figure 1. Taxonomy of attacks and threats attempted on IoT [83–85].

3. Literature Review

Ensuring the security of all the stakeholders in an IoMT environment has been a challenge that has gotten a considerable amount of attention [86]. While performing the review of existing literature, an extensive search was carried out to find articles (both journal articles and conference proceedings) that propose authentication techniques in the context of the IoMT. While skimming such articles, it was observed that the literature could be categorized with respect to the deployment of authentication techniques, such as on the level of cloud, fog, or edge. Moreover, it was also observed that some techniques were generic for both user and device authentication whereas others were specific to each of them. While filtering based on the initial understanding of articles grasped from the title, abstract, and conclusion of the paper, only those techniques were kept that provided insight regarding the approach, testing, and analysis. The following subsections provide a brief description of the working and testing of all such approaches.

3.1. Cloud-Based Authentication Frameworks for Patient Monitoring

With the increased usage of the Internet and associated infrastructures, cloud computing offered its three specific models, i.e., SaaS, PasS, and IaaS [87]. Software as a service (SaaS) supplies customers with the infrastructure for running applications. The client accesses the software from other device applications, including a web browser. Platform as a service (PaaS) provides clients with a cloud storage infrastructure. Infrastructure as a service (IaaS) offers clients services, such as configuration processing, networks, servers, and other computing tools [87]. Table 2 briefly compares cloud-based authentication techniques.

Table 2. Cloud-based authentication techniques in IoT-enabled healthcare systems.

Study	Technique Used	Attacks Overcome	Main Contributions	Limitations
[87]	Asymmetric cryptography	Offline password guessing, replay, impersonation, man-in-the-middle and insider attacks	Cryptographic mechanisms, one-way hash function, symmetric encryption and the bit-wise exclusive-or operator are utilized to provide identity authentication and authorization through the cloud. The authors claim that authentication, integrity, privacy, and nonrepudiation issues are resolved.	At times of hurry, information that has been oversecured by encryption and digital signatures can become difficult to access. Moreover, if an adversary gets access to a patient's mobile or impersonates the IMEI on its cell phone, it can gain access and cause damage.
[88]	Client-based user authentication agent and modified Diffie–Hellman agent	Man-in-the-middle Brute Force Dimming	Scalable and efficient authentication technique is proposed. A cryptography agent is introduced to encrypt data before its storage	Use of multiple servers increase overall computational and communication cost. Data headers for transmission are not tagged and can cause additional overhead cost.
[89]	Multiauthority attribute-based encryption	Man-in-the-middle Eavesdropping DOS	Advance encryption standard is used to make the data secured. It is explored how a single point of contact can assist security e-health	Very limited analysis is performed and the approach may be prone to attacks like shoulder surfing attacks, impersonation attacks, etc.
[90]	ECC and hash function	Man-in-the-middle Impersonation Nonrepudiation Traceability Replay	HIPAA compliant framework 'SOTER' is proposed which is distributed personalized authentication based on MTN. Limitations of Identity Access Control Policies are attempted to be resolved primarily.	Limited Authorization model, having only a few stages. Formal or informal security evaluation lacks.
[91]	Multifactor mutual authentication	Reply attack, DOS, smart card loss attack, password guessing attack, etc.	An improved three-factor authentication approach is proposed specifically for the monitoring of patients remotely using WSNs. AVISPA Tool is utilized to perform formal security analysis	Communication cost is a bit high, but still, extensive evaluation has been performed.
[92]	Hash and XOR functions, lightweight key management	Malicious user attack, replay attack, password guessing attack, insider attack, hidden server attack, spoofing attack	A lightweight user authentication scheme is proposed to validate legitimate users using Hash and XOR functions while minimizing the number of cryptographic computations.	The scheme is lightweight due to the use of computationally constrained functions; however, it lacks security against some attacks such as shoulder surfing, eavesdropping, etc. An extensive security evaluation of various platforms is not provided.

As per [93] IBM and active health management, a subsidiary of Aetna (a leading American healthcare provider), based on cloud computing architecture, developed a "Collaborative Care Solution" in 2010. The solution aims to provide convenient access to a wide variety of information from various sources, such as electronic medical records (EMRs), claims, prescriptions, and laboratory data, for medical and healthcare professionals.

The authors in [87] proposed a cloud-based authentication and authorization scheme using cryptographic techniques as shown in Figure 2. This scheme mitigates medical resource misuse; a patient gets logged in to a public cloud through a mobile device using its credentials (username and password). However, the scheme is kept without a password and identity table being saved in a database. Hence, against attacks such as offline password guessing attacks, replay attacks, impersonation attacks, man-in-middle attacks, and insider attacks, the scheme provides a secure defense. In the proposed scheme, all patients and the hospital administrator are restricted from getting signed in with the public cloud. As a result, a personal attribute is utilized to generate a session key specifically for the user being logged in, such as a patient or hospital administrator. This session key is utilized by patients to get access to all the possible facilities being offered via the cloud. Usually, a patient has to be admitted and provide examinations to receive healthcare services. The healthcare staff then uploads the content with the patient's healthcare information while acquiring the patient's approval. Once such information is available on the cloud, any registered user can utilize it for any authorized task. During this process, the patient also permits the use of information through tokens. After successful authentication, a mobile application is used by the patient to generate its authorization token. The patient also has to authorize the hospital; later the authenticity of the patent is validated by the administrator. Once approved by the administrator, the tokens are sent to the public cloud. The next step is to check the token available in the public cloud. If the token is found to be correct, only then can the patient's treatment report can be accessed from the hospital, and the doctor can supply the patient with the relevant advice. It was reported that the communication cost of the proposed scheme is 7168 bits, whereas the current system requires 0.7168 ms for the data transfer of 10 Mbps bandwidth network infrastructure.

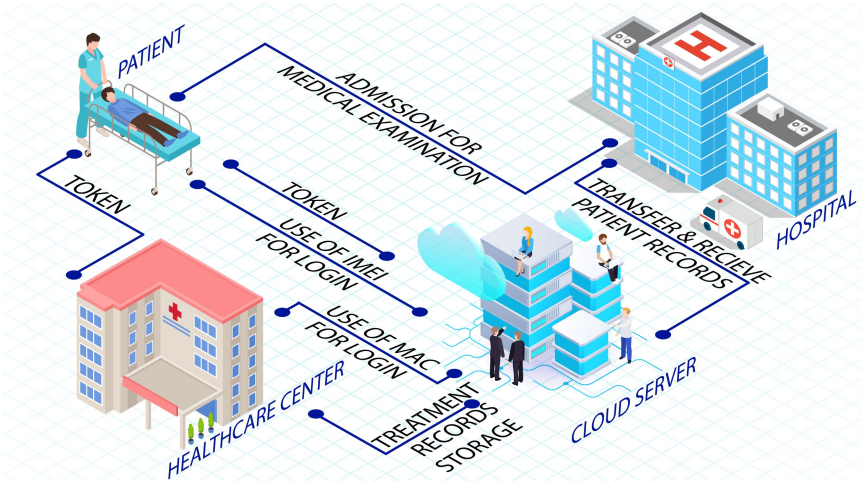

Figure 2. Healthcare authorization model based on cloud authentication [87].

In times of critical sensitivity and decision making, users face difficulty accessing authentic information that is kept encrypted and digitally signed, even after proving its authenticity. Moreover, if an adversary hijacks the IMEI of a patient's cell phone, it can clone to its own unsafe device and can get access to the network. Thus the scheme is vulnerable to known-key attacks and theft attacks. A user authentication scheme for cloud computing environments using different techniques (i.e., HE-RSA algorithm, AES-192 or AES-256 algorithm, and zero knowledge proof (ZKP) Diffie–Hellman) is proposed in [88]. In this framework, the authors have introduced many agents and a cloud-based SaaS program to

validate the authentication mechanism for unregistered devices. In their proposed model, the following entities were used:

3.1.1. Client-Based User Authentication Agent (CUA)

Traditionally, before getting access to a cloud server, a CUA refers to an application placed at the end of the user, or the user's Internet browser, which is used to validate the user's identity. In this sort of authentication process, the user's device gets registered to the website of such a service provider. An extension of the Internet browsers gets downloaded along with a unique encrypted code that provides access to the user. An alternative password would encrypt the unique code the user has selected by using the algorithm AES-192 or AES-256. Thus, to get access, the end user performs decryption of the code and setting up of the extension.

3.1.2. Modified Diffie–Hellman Agent (MDHA)

To improve the reliability rate of unregistered applications in user authentication, MDHA is implemented using zero knowledge proof (ZKP). In this technique, the users will be given temporary permission to access it from the unregistered device. After an extensive analysis of the framework, we have noticed that two separate servers for strong authentication and cryptography are used, which is a resource wastage framework. Therefore, from main servers, it can also be managed and might increase the overall cost and security like mitigating eavesdropping and DOS attacks. The complete scenario of [88] is shown in Figure 3.

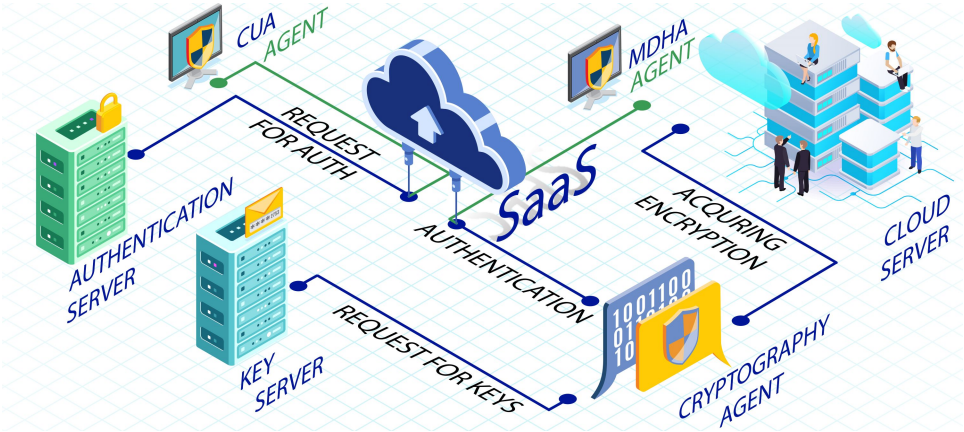

Figure 3. An architecture proposed in [88] for user authentication based on agents and SAAS model.

The authors in [89] have proposed an enhanced security model with the functionality of authentication and authorization functionality while discovering the new multi-authority encryption-based attribute (MA-EBA) technique to protect healthcare against attacks by unauthorized users as illustrated in Figure 4. The method improves device scalability and allows the user to attain fine-grained access. In the proposed model, the user provides their identity, password, and personal biometric information in the first phase. The admission department generates a request for a service to obtain a request from the database and cloud servers. Upon request by the service administrator, the health requester (DAR) accesses the patient's stored personal health information. Only DAR can decode personal health information (PHI) after patient satisfaction and access policy definition. When seeking entry to PHI, the single point of contact (SPoC) tests whether the user has been granted access to fetch records from the database. Hence, access to the service becomes the key aspect; thus in a successful scenario, the administrator can access patients' information. Therefore, the information, PHI, is sent while utilizing the MA-EBA framework, which has been presented in Figure 3. However, if an adversary gets too close to the patient, it can acquire its login information and cause damage to the system. Therefore, the proposed scheme is vulnerable to hijacking attacks.

Figure 4. Privacy- and security-enhanced e-health framework [89] and SOTER: A trust discovery framework [94].

A framework is proposed in [94] for the authentication of healthcare devices using the Soter platform. This framework, also presented in Figure 4, has been reported to have many state-of-the-art features, including multiparty trust negotiation, to maintain trust amongst connected devices. Moreover, the scheme promotes the use of virtual federations (VFs), and trust circles (TCs) to attain a more robust experience having a customized and dynamic access control policy (DACP) intact. It also utilizes trust negotiation (TN), which is a very innovative approach to managing trust between two individuals having no information about each other.

The proposed framework notably simplifies the process of trust discovery. The transfer of credentials back and forth is decreased in the proposed scheme. This helps reduce communication costs while enhancing the privacy of stakeholders who are actors in the process of negotiations. In addition, it encouraged people to adapt their policies, which regulate the disclosure of their resources or credentials. The IoMT's credibility rating depends upon trust in the services it provides. The framework describes three trust levels in their research article, fully trusted, partially trusted, and nontrusted. The associated devices' authentication certificates are deposited in the credential vault (CV). The trust assessment module is carefully designed to keep track of trust and help share a stakeholder credential depending upon the trustworthiness of the one seeking it. It has been reported that if the degree of reliability is higher, very few requirements would be needed during the process. In the proposed model, a SEMTN trust communication technique is also introduced. It is a multiparty trust communication mechanism that enables the system to generate and manage trust between parties through the incremental implementation and dissemination of signed credentials. It also uses a negotiating approach to look for effective access control policy (ACP)-based negotiating. In the proposed architecture, the policy evaluation module decides which certificates are supposed to be sought by other peers within the IoMT system. Furthermore, it also determines which certificates can be sought from other peers and can be revealed by using the SEMTN technique.

An elliptic curve cryptographic-based framework for smart medical systems is proposed in [90]. The architecture works on wireless sensor network (WSN) technology, wherein the doctor provides a patient with online healthcare services via a cloud-oriented application program on a mobile device. It is reported that for such scenarios, security and privacy are the main issues for the users of cloud-based smart medical systems. Therefore, they designed an architecture to ensure security and privacy by using lightweight cryptographic key generation elliptic curve cryptographic for the proposed smart medical system. The four entities—patient, doctor, cloud server, and health care centre—are passed from their proposed scheme. These entities are processed in six phases: registration, smart medical system, uploading patient health records, treatment and checkup records, and a unique emergency phase, as shown in Figure 5.

In the proposed framework, the patient gets registered with the healthcare centre, which then controls the user's session key by using the cloud. The healthcare centre sends patients' medical records to the cloud. Moreover, even at the patient's request, data

gathered by the medical sensors is uploaded. The doctors access such records through their mobile devices and can provide expert opinions and advice remotely. Afterward, using the same method, patients can attain access to medical observations which a doctor and healthcare centre generate. When the patient has some emergency or issues with their pulse rate, respiratory system, heartbeat, etc., the intelligent body sensor informs the cloud. At the same time, the cloud reports onward to the healthcare centre. The said architecture is difficult to implement because the elliptic curve cryptographic (ECC) method consists of an arithmetic encryption function, digital signature function, and verification function. ECC software implementation needs moderate speed whereas hardware implementation consumes more energy, and scalar multiplication is time-consuming in ECC-based schemes. Zp (a group under multiplication modulo of prime number p), which comprises integers modulo having a large prime number p, is considered a challenge for ECC-based logarithms in finite fields. Similar to field sieve, this problem has some subexponential time solutions. It is known that, given sufficient processing strength, subexponential time solutions can be broken down by adversaries in a time of a few months. Thus, in this case, it cannot be considered practical. However, ECC has potentially fallen in the implementation footprint due to the smaller key length alone.

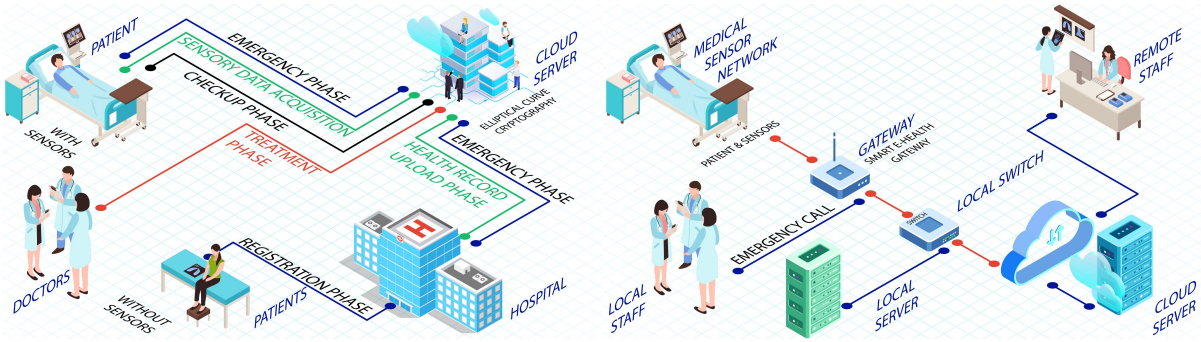

Figure 5. CSEF: Cloud-based secure and efficient framework [90] and An end-to-end security architecture for healthcare IoT [95].

When considering wireless sensor networks (WSNs), ref. [91] thoroughly examined three-factor authentication techniques, and based on the examined flaws of [96], an improved three-factor authentication approach was explicitly proposed for monitoring patients remotely by using WSNs. The revocation and re-registration phase was improved, which was confirmed by BAN logic in the form of a successful mutual authentication process. The AVISPA tool called "Automated Validation of Internet Security Protocols and Applications" was utilized to perform security analysis, where comparison was built with existing four other techniques including [96]. Security comparison was drawn, keeping 17 different security threats and the schemes were also compared for their respective computation and communication cost. It was reported for the proposed scheme that through simulation, resilience was observed for active and passive attacks. Whereas the informal security comparison assured that the mandatory security attributes were available in the proposed scheme that ensures efficient yet secured remote healthcare monitoring of a patient.

With the help of fuzzy logic, the authors of [97] have proposed an approach for the management of trust to authenticate devices and counter sybil attacks in IoMT, which leads to the generation of many fake nodes and imitating a real node to attain malicious objectives. By using fuzzy logic and associated filters, this novel technique calculates the trust score of nodes in an IoMT network based on submeasures like integrity, receptivity, and compatibility. By using simulations, a thorough comparison of energy, accuracy, packet delay ratio, trust computation, and quality of experience (QoE) is built with three other trust-management schemes, such as RobustTrust, SGSQoT, and GroupTrust. The evaluation results declare the proposed scheme significantly better than the rest; however, the authors

comment that the overhead cost of various aspects related to servers and the time taken for the delivery of packets can further be reduced to enhance the performance.

In [92], the authors have proposed a lightweight user authentication scheme. The proposed scheme helps monitor patients by using an insecure IoT-based framework. The scheme validates legitimate users to access patient data stored on a cloud server from a remote location. Hash and XOR functions have been utilized by the proposed scheme, which is then analyzed to be less costly with respect to computation complexity in comparison to five other schemes. The proposed scheme is implemented in different phases with assigned roles. First, the registrations center sets the parameters in offline mode, and then the medical professionals and patients get registered to the gateway node, respectively. Additionally, various entities involved, such as the gateway node, sensor node, and user, mutually authenticate each other. A random key for the session is generated after authentication is found to be successful in comparison to the saved information. Furthermore, authenticated users are also provided with the facility to change their passwords, hence replacing previously stored information.

Similar to [91], AVISPA is also used to validate the proposed scheme of [92] for robustness against possible threats and evaluate formal security standards. Comparing the proposed scheme's computational cost with existing schemes confirms the proposed technique's efficiency.

In [98], the authors propose a strategy addressing the privacy and security concerns of centralized medical record storage on the cloud-based system being generated by IoMT. It is reported that the proposed scheme is structured on blockchains and also on interplanetary file systems (IPFS) technology. The primary purpose here is to provide a distributed structure for the storage of records. It also ensures the authentication of different devices such as clinical gadgets. The use of these technologies helps in addressing security concerns associated with IoMT-enabled healthcare. Blockchain-based architecture assures that the system is decentralized and the patient and their medical devices are presented with a registration-based security model. A consortium blockchain is built and executed to ensure access control. However, a few issues have been recognized, namely that sustaining a distributed cluster by using IPFS and establishing a distributed cluster system, requires more processing time.

3.2. Fog-Based Authentication Frameworks for Patient Monitoring

Cisco Systems introduced the term fog computing in 2014. The term was coined because of its association with closeness to the earth. Similarly, a layer was created between edge and cloud, enabling software or services to be corrected and improvised [99].

Fog is a modern architecture, having a sense of processing, storage, and control that takes the resources closer to end users. The decentralization of resources at the edge of the network is done. Computation and control, both closer to the sensors, make the fog idea a more robust alternative to the cloud [100]. In addition, it encourages the versatility of users while keeping resources heterogeneous. It also acts as an interface, provides data analysis, and meets the requirement of low latency and hence has been utilized in distributed environments [101]. To meet the challenges of today's healthcare, fog computing is considered a critical competitive platform that assists the cloud in reducing delays, jitters and transmission costs and enhancing throughput [102]. A comparison of few Fog-based techniques are mentioned in Table 3.

The datagram transport layer security was worked on and enhanced by [95]. This security layer works between the two vital entities of fog-based architecture, i.e., gateway and end users. It was suggested that certificates were not required during the initiation of the session. The security was then analyzed of the proposed end-to-end security scheme by using the complete prototype healthcare method and keeping the hardware performance constant. The proposed architecture consisted of medical sensor network (MSN), Gateway, a powerful computer system, and a web interface (application program). However, each participant calculates their key each time, creating a privileged insider attack. Moreover,

identity information no longer forms the entire public key. The proposed secure and efficient authentication (SEA) architecture utilizes distributed gateways to safely and effectively perform the authentication and authorization processes on behalf of medical devices. The MSN captures biomedical and surrounding signals from the body/room to monitor and diagnose medical conditions in the proposed framework. The signals are then forwarded through wired or wireless communication protocols to the smart e-health gateway. With the help of communication protocols, the gateway works as a link between the MSN and the Internet. The backend infrastructure consists of a network switch, a cloud computing platform, and a central database (DB) for healthcare, which is shown in Figure 5.

The fog-based access control model is proposed by [103], which protects the performance of cloud/fog-based IoMT. A fine-grained access management framework has been considered for the framework, which is shown in Figure 6. In this scheme, a cloud-based approach is applied by using an additional layer of fog servers. An access control environment is created by using this fog layer, which provides personalized access to the end user. Despite many similarities in storage and application between cloud and fog computing, fog computing differentiates from cloud computing in geographical distributions because it mixes centralized and distributed computing. The proposed approach's fundamental objective is to minimize the danger caused by using extra assortments by cloud-based applications. It establishes the grounds for essential issues in consent approval, which by default currently is configured by the operating system. For the most part, the standard contemporary settings are reported to be coarse-grained, and for most clients, it is difficult to change such settings. In the proposed framework, both permanent and temporary data are used to preserve privacy.

Access controller is the leading participant on the other peer called the fog server of the proposed scheme. The access controller subelements include register, repository metadata, and repository criterion. A register in access controller shall communicate with different applications. Repository metadata is responsible for compiling information, but it is not considered a shared space. The repository criterion is storing a specific privacy level setting. However, many attributes affect the execution time in such a scenario. If the number of attributes is increased, the performance of the model will degrade. The proposed scheme is also found vulnerable to several threats, such as impersonation and parallel session key attacks. It was also observed that the scheme lacks mutual authentication.

A proposal in [104] demonstrated that IoT architecture uses edge computing. This architecture uses extensive nodes for data transmission, which can disturb the application software models and create confusion. For this purpose, they prefer fog computing for healthcare industries to facilitate the application software models and enhance monitoring functionalities. They further stated that evolution is performed by utilizing smart devices by the patient by using a fog node for sharing sensitive personal information securely with physicians. The specified physician supervises their health situation and proposes preventive measures to the administrators in an emergency. The SparkIoT Platform prototype comprises three groups (i) wearable devices (which act on a personal level), (ii) a mobile application (this ensures access to a private edge cloud), and (iii) the Spark IoT platform core (the platform is deployed on the cloud). The first group consists of smart sensors attached to the patient. The patient's health data in encrypted form and alerts are stored in the storage of wearable devices. The mobile application is installed on the patient's cell phone and connected to the wearable devices to receive and store the alerts and traces. The mobile application manages wearable devices, patient body sensors, battery storage, alerts, and algorithm parameters. The third group Spark IoT platform core, provides secure user authentication, personal health assistance, access to the medical staff, and maintenance of patients' electronic health records (EHR). The proposed framework is insecure because all the data and alerts are stored on the mobile device; the attacker can steal it. Figure 6 shows the working of the proposed Spark IoT platform.

Table 3. Fog-based authentication techniques in IoT-enabled healthcare systems.

Study	Technique Used	Attacks Overcome	Main Contributions	Limitations
[95]	ECG-based cryptographic keys and certificate-based datagram transport layer security	Eavesdropping DoS Spoofing	The study explores an efficient end-to-end user authentication scheme assisted by DTLS certificate handshaking. It also stated to provide a session resumption feature with mobility as it builds smart gateways within the network.	Proper computational and communication analysis is performed, whereas formal or informal analysis of the scheme is missing.
[103]	Fog-based security and access-control determination algorithm	Spoofing Man-in-the-middle	This work proposes a fine-grained security, access control mechanism in specific. Reported suitable for various services like data storage, directories, and file management, while providing customized security features	Quantity of tasks is found out to be directly proportional to time complexity. Hence, in a scenario where tasks increase, time complexity will affect.
[104]	A core IoT platform, 'Spark'	Insider attack	Primarily a framework is proposed comprising of layers to increase the efficiency of data transfer and throughput while providing an additional layer of security and authentication.	Through network simulations transfer of health care data such as ECG is examined. No information regarding security or privacy preservation analysis is provided.
[105]	Dynamic framed slotted aloha and RFID	Tag-tracking attack, replay attack	An RFID batch authentication technique is presented to minimize tag costs and increase tag recognition efficiency. Furthermore, a linear homogeneous equation is utilized, and the scheme has a registration and authentication phase.	Tag anonymity and mutual authentication are provided yet lack formal evaluation of the security. Impersonation attack should have been dealt with.

Figure 6. An access control model for the IoMT proposed in [103] and framework of healthcare application [104].

It was observed that radio frequency identification authentication is utilized on many occasions for the IoMT to identify end nodes and users. In order to avoid tag collisions of RFIDs, a scheme is proposed by [105] using aloha. The scheme uses the dynamic framed slotted aloha, which is an anticollision protocol [106]. The three components of the proposed model include numerous batch tags, readers, and backend servers. Every product carried by the patient is attached with an RFID tag, and wireless channels are used to interact with them. An RFID batch authentication technique is presented to minimize tag costs and increase tag-recognition efficiency. Furthermore, a linear homogeneous equation is utilized in the RFID batch authentication system. The proposed scheme is a two-phase technique that includes the startup phase (registration) and authentication phase. To decrease the computational cost of batch authentication the properties of homogeneous linear equations are used. By sing Vivado, environment timing and behavioral simulation based on FPGA have been carried out in comparison to other super-lightweight authentication techniques. The proposed technique is found to be more secure and accurate, having less computational cost. However, comparisons on real-world scenarios in the field of medical health have not been made.

3.3. Edge-Based Authentication Frameworks for Patient Monitoring

With the takeover of technology in hospitals for medical applications, considerable efforts of the research and industrial community are being put into an edge-computing provision in health infrastructures. One of the critical challenges of IoMT systems focused on edge computing involves maintaining the power of medical equipment and raising the lifetime of the healthcare system [107]. Wireless body area networks are equipped with different sensory modules and gadgets. These sensory gadgets are placed around, in, or on the human body [108]. All such devices act as nodes and are usually linked through wireless communication technologies. WBANs may include wearable and implantable biosensors for remote observations, medical assistance, and other remote services [108]. Table 4 elaborates key features, attacks overcome and limitations of some of the recent work in Fog-based authentication.

As discussed in [109], high-speed ICT tools are usually installed for remote patient monitoring and supervision. It is noted that such an environment usually lacks security, which can lead to many issues for all the participants of such an environment. Therefore, they proposed a framework that resists all known threats inside the IoT. In the proposed architecture, as illustrated in Figure 7, first of all, data from the patients are verified by using device authentication (DA) and transferred after securing the channel (SC) and applying data encryption/decryption (DED). Access control models are applied at the gateway level, which includes contextual-based access control and role-based access control. DED and SC can also be used for additional security. Data is then transmitted to the hospital's electronic medical record (EMR), where user authentication (UA) is used with DED, SC, CBAC, and RBAC. After the authentication process, the services will be provided to a patient remotely. Their result shows that they have proposed a secure mechanism that ensures the participants' confidentiality, authorization, and privacy. With an in-depth study of the framework, it was observed that the proposed framework is not fast and secure. A GPU is required to enhance performance, while simple encryption/decryption cannot guarantee security. A random and robust key is necessary for the mutual transmission of data among all the participants.

Table 4. Edge-based authentication techniques in IoT-enabled healthcare systems.

Study	Technique Used	Attacks Overcome	Main Contributions	Limitations
[109]	Dynamic adaptability to changing in security needs through access control models	Device masquerade attack, spoofing, denial of service, Reflection attack, Eavesdropping	Service-oriented structure is proposed with the support to dynamic elements of security. These elements continuously change based on medical service providing remote points and are secured by assisted roles and situation-based access controls.	Preliminary comparison and security analysis is performed with no hint of evaluation details. Formal and informal security comparison needs to be performed.
[110]	Body sensor network-based architecture along with use of local processing unit (LPU)	Forgery attack, eavesdropping, False signal attack, Replay attack	Body sensor networks were used to propose an IoT-based healthcare system assisted by OCB to fulfill five security requirements, i.e., mutual authentication, enforcing anonymity of actors, secured localization, resistance to security attacks and data security.	Extensive computational analysis is performed compared to two BSN-based models; however, only security features are listed. The scheme may be prone to threats such as impersonation, lost key, and shoulder surfing attacks.
[111]	Legendre approximation of ECG and multilayer perception neural model	Eavesdropping, replay, and man-in-the-middle attacks	The method of Legendre polynomial extraction is used to propose an ECG authentication technique. Multi-layer perception neural network is also utilized for learning, identification, and authentication by using ECG signals.	The possible errors in the acquisition of ECG signals are not discussed. Security analysis, other than machine learning, should be performed.
[112]	Lightweight hash-chain-based and forward security enabled scheme for WBAN	impersonation attack, guessing attack, user/gateway forgery attack, insider attack, and DOS attack	A two-factor authentication scheme for both users and devices is proposed. ROR model is utilized for formal analysis, whereas, ProVerif is used with OPNET utilized for real-time simulation-based evaluation.	Even though a thorough analysis is performed, it seems like the cost of storage and communication is high for the proposed scheme.
[113]	Machine learning (SVM), pseudo-random binary sequence, trust management	Impersonation attack, denial of service attack, man-in-the-middle attack	Machine learning-enabled IoMT network to provide security, trust management and to achieve efficient authentication. Key agreements and trust values are based on securing the IoT healthcare system	There is no use of cryptographic functions; moreover, the formal and informal security analysis is needed.

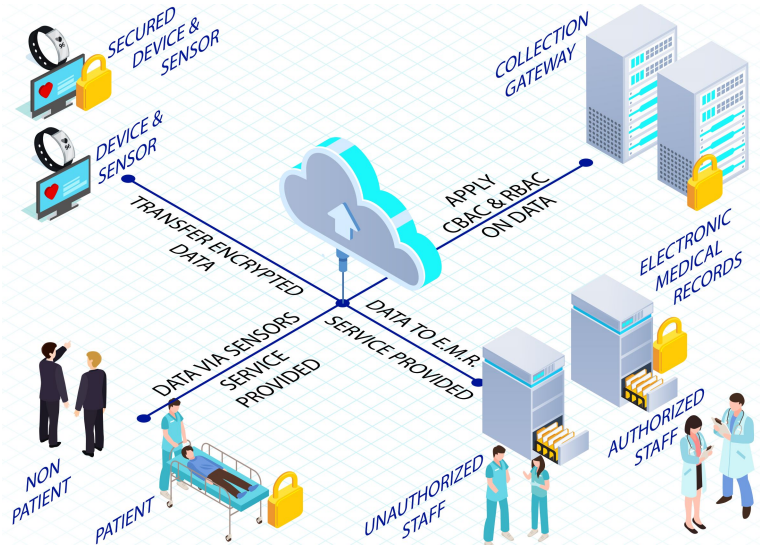

Figure 7. Service-oriented security framework in the IoT, proposed in [109].

A study in [110] focused on the significant issue of security in the healthcare system and proposed a secure architecture by using the lightweight anonymous authentication protocol, namely BSN-Care. BSN architecture consists of wearable and implantable sensors. The physiological parameters of the patients are collected and transmitted to a local processing unit (LPU) such as PDA or smartphone. A central server termed the BSN-Care server controls the data flow between the nodes and LPU. Databases store medical records received from LPU, which are then analyzed for possible abnormalities. The degree of irregularities would determine if the family members and doctors are to be contacted or not. In case of extreme abnormalities, services of any emergency units in the close vicinity of the patient will be acquired. Such actions will be reflected in the action table through boolean variables as family response (FR), physician response (PR), and emergency response (ER). There are two phases within the authentication protocol. In the first of registration, the central BSN-Care server issues IDs to all the LPUs connected through a secured means. During the authentication phase, the LPU and BSN-Care servers mutually authenticate each other. Data transmission takes place after this phase. It was observed that if an adversary somehow gets access to an already authenticated LPU, it can quickly figure out the identity, masquerading and impersonating the whole system. The working of the proposed architecture is graphically represented in Figure 8.

Figure 8. BSN-Care: IoT-based healthcare system using body sensor network as discussed in [110].

Therefore, the scheme fails to provide secure services. Similarly, while looking into the first message transmission, it is noted that the message is sent publicly over the network

channel, in which an imposter can very easily attempt a replay attack. Also, the attacker can discover the identity. It can easily identify users' personal sensitive information, like location and the session start time. Thus, it can easily trace a legitimate user by launching a traceability attack over it.

Another study in [111] suggested a novel electrocardiogram authentication scheme using Legendre approximation integrated with the IoMT-enabled multi-layer security approach as shown in Figure 9. To provide network, data, and application-level security, they utilized wireless implantable medical devices (IMDs). In this scheme, all the QRS coefficients of legal doctors are stored inside the IMD of the patient to give authorization. Different doctors are given different privileges and permissions. Based on user IDs, complex and adaptive access control can be implemented in IMDs. An ECG machine is used as biometrical signal input in the application layer. Unique identities were assigned to patients to utilize the ECG signals. At the network layer, coefficients and unique identities become passed via a direct sequence spread spectrum method of encryption that guarantees the coefficients of authorized people. MLP classifier model works on the data link layer where the ECG signal is evaluated on a temporal basis. Another purpose of the MLP classifier is to protect the accuracy and completeness of the information.

However, no one accepts it as a standardization model, as it cannot adopt any changes in the biometric phase of a collection of samples. It also influences the environmental and mental conditions of a patient.

A study conducted in [114] introduces a computer authentication protocol used to authenticate network devices. The authentication process is performed without data being stored in memory. In the PMsec method, as shown in Figure 9, each device would incorporate a PUF module. All the sensors and devices in the IoMT get their unique identities from this module. The protocol's initialization happens any time a new device establishes a link with the network. The server utilizes the PUF module to enroll different keys throughout the process. A REQUEST input R1 is transferred to the said module. Consequently, a RESPONSE is given to the PUF module at the end devices for R2 response. The second response (R2) is again sent to the said module. Furthermore, a third response (R3) is generated where the hash of the same is also calculated as X = h (R3). The hash X and CHALLENGE input C1 are contained in the database. The device inputs a challenge message toward the node, which produces a hash value called X/. Hash values X/ are matched with the already stored value X for authentication of the device. However, device information is not stored explicitly in the cloud log, which provides an extra layer of security to the system.

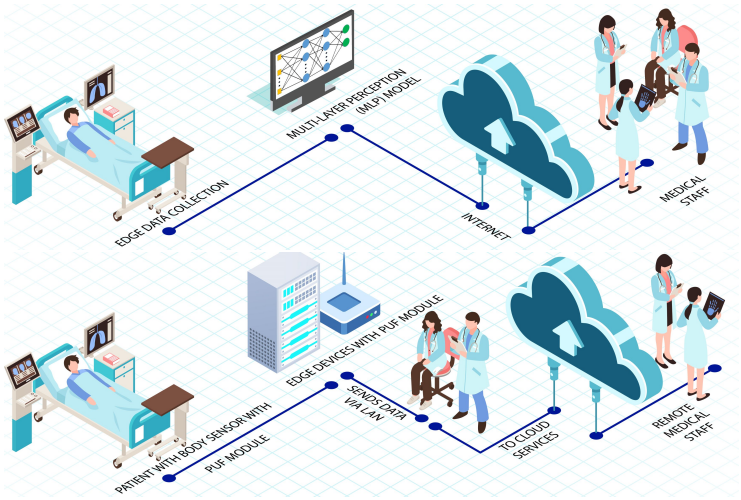

Figure 9. Framework of multilayer security scheme for implantable medical devices [111] and PUF-based energy-efficient authentication IoMT [114].

In [112], keeping the context of IoT-enabled healthcare systems, the authors have presented a lightweight authentication technique for WBAN, which is based upon two factors. The proposed scheme authenticates users and devices available over an IoT. The authors utilized ProVerif and OPNET tools to simulate and analyze the proposed scheme. Results have shown that key compromise impersonation attack and known session-specific temporary information attack have been countered while providing forward secrecy. Moreover, the real-or-random model, also called ROR model, is used to perform a formal analysis of the security of the proposed scheme.

A device authentication technique is proposed in [113] by using the SVM classifier model while keeping [115] as their base model. The sensors and gateway communications in an IoMT architecture are secured by machine learning in trust management strategies and authentication techniques. The tests show that the proposed schemes work well with various IoT-based medical frameworks with a lower computing cost than the physical unclonable functions (PUF) protocol. The proposed approach is found to be secure, efficient, and resource friendly.

To ensure the privacy of credentials in a scenario in which the session secrets get revealed to an attacker, a device authentication scheme for WBAN's is proposed in [116]. While avoiding the management of public keys in a large number, the CK-adversary model is utilized to provide strong security of credentials. By using Java pairing-based cryptography library (JPBC), the session keys are evaluated for communication, computational, and storage costs. The proposed scheme is efficient and more secure, suitable for telehealth applications.

In [117], the authors have proposed an authentication scheme claimed to be lightweight, namely slight. The technique is used for smart healthcare services to address security challenges while providing a lightweight architecture. This architecture is built to enable end users to receive medical advice from experts. Keeping three main entities, i.e., doctor, medical server, and sensor or patient, the system includes four phases: registration, authentication, transfer of rights, and update of password phase. Security analysis concerning resilience against security threats of the proposed scheme is performed and formally analyzed by using the Scyther tool.

If an adversary knows the IDs or secret keys, it still cannot retrieve the session key, and thus the proposed techniques are found to be suitable for forward secrecy. During the authentication process in slight, timestamps are embedded with messages to calculate their freshness. Moreover, a technique involving the use of random numbers is utilized to counter the denial of service attack and bound any adversary from sending repetitive messages. It is reported in [117] that the time complexity of slight is 0.0076 ms, which is very low. It has been analyzed that the communication overhead is also quite acceptable compared to similar frameworks. These two aspects make the proposed model suitable for any IoT-based solution with limited computational power at various sensors and devices.

3.4. Comparison with Other Surveys

Over a few years, many thorough surveys have been conducted in the broad area of IoMT while keeping various categorization strategies in discussing the existing literature. Table 5 provides a brief description of the taxonomies adopted by the surveys conducted for IoT-enabled Healthcare systems. Moreover, other security analysis details are also listed in the referred table.

Table 5. Overview of existing surveys of security in IoT-enabled healthcare systems.

Study	Title	Year	Description	Publisher
[26]	A Review of Security and Privacy in Internet of Medical Things (IoMT)	2019	Classification of Security aspects and protection mechanisms, (Device, Connectivity & Cloud Security), Categorization of Privacy aspects and protection mechanisms, (Private Data, Protection Mechanism, Identification & Anonymity, Data Destruction)	IEEE
[49]	Towards Secure and Intelligent Internet of Health Things: A Survey of Enabling Technologies and Applications	2022	Requirements, Security Challenges, Attacks in IoT based Healthcare Systems, Enabling Technologies for Secured IoHT (Convergence of Blockchain, Machine Learning and IoT), Future Paths and limitations of Existing Solutions	MDPI
[118]	A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions	2022	Classification of IoT Security parameters and objectives, Categorization of Authentication Scheme in IoTs (WSN based, IIOT based, IoMT based, VANET based, RFID based),Future directions	Elsevier
[119]	Security and privacy for the IoMT-enabled healthcare systems: A Survey	2019	Systems, networks, and design challenges for IOMT, security and privacy requirements, existing security schemes, discussion and future directions	IEEE
[120]	A systematic review of IoT in healthcare: Applications, techniques, and trends	2021	A systematic review leading into Comprehensive taxonomy for IoT-based healthcare systems (Sensors, Resource, Communication, Application & Security), Comparison of Analysis techniques and research objectives, Open Issues and Future directions	Elsevier
[121]	IoT Security in Healthcare using AI - A Survey	2021	Security for IoT and its types (Physical and Information), Classification of Security in IoT-Healthcare (IoT Security in Healthcare, AI Security in Healthcare, IoT Security in Healthcare using AI)	IEEE
[122]	Review of security challenges in healthcare internet of things	2021	Discussion about Security Issues in IoMT, Identification of Primary security risks, Risk Analysis and Impact Detection of Primary Security Threats	Springer
[123]	Secure Remote User Authentication Scheme on Health Care, IoT and Cloud Applications	2021	Systematic Review resulting into categorization of Remote User Authentication, Tele-medicine Application, IoT Applications, Cloud and multi-server Applications, Possible Security Requirements and Attacks	Acta Polytechnica Hungarica
[124]	A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT)	2022	Architecture of IoMT Edge Network and its Security Objectives (Data Confidentiality, User Integrity, Non-repudiation, Authentication, Authorization, Availability), Categorization of Threats and Attacks, Countermeasures for all such security risks	Wiley
[125]	Systematic Review of Authentication and Authorization Advancement for IoT	2022	Taxonomy of Authentication and Authorization Techniques for Iot (Years-based, Goals-based, Automation-based), Dominant Topologies, Communication types and Perspectives in Authorization and Authentication, Applicability of identified solutions	MDPI

4. Key Findings

The current state of the world, especially after encountering a deadly virus, i.e., covid, implores us to bring coherence in our efforts to provide better health services specifically while using state-of-the-art modern practices. While exploring authentication practices in the Internet of things enabled healthcare systems during our survey, we witnessed a sufficient amount of effort being delivered into the field. However, this section will attempt to raise questions and highlight pitfalls that may be addressed to pave the way forward in providing quality health services through modern communication technologies.

4.1. Lessons Learned

With the review of existing literature, we can summarize the lessons learned as follows.

Resource constrained strategies: It is known that the IoMT comes with a constrained environment with only limited storage, communication and processing power. More efforts are to be made to shift toward lightweight strategies that will assist not only in the field of healthcare but also in other IoT-based application areas.

Dataset generation: A considerable amount of effort needs to be focused on creating usable datasets for precise approximation during simulations. It was observed that actual datasets were either unavailable or not made public. Given the sensitivity of the healthcare domain, almost every simulation needs to be tested on real datasets and testbeds.

Standardization: Redundancy was found in the creation of frameworks being proposed by various researchers. A more coherent and standardized approach may be adopted, which will save potential and direct them toward efficiency.

Evaluation: Evaluation of security models was noticed to be not uniform in many of the proposed schemes. The use of formal and informal security analysis practices with the help of simulation-based tools needs to be practiced.

Toward usable security: The aspect of providing usability with security or privacy was found to be very rare. More efforts must be made to bring in user-friendly technologies such as augmented reality, virtual reality, etc., for a better user experience. Steps may be directed to keep humans in the loop while providing security.

4.2. The Road Ahead

With a detailed discussion of different existing authentication techniques in the IoMT, we conclude this article with open issues in the respective field. Though the survey is structured with respect to levels of the network including cloud-, fog-, and edge-based authentication, however, keeping in view the limitations of the various approaches, a summarized set of prospect open issues are mentioned below.

- Use of cryptographic keys is found to be abundant in security architectures; still, very little work is performed in creating, managing, and moving such keys in resource constraint environments. Moreover, trusted platform module (TPM) or similar hardware-based solutions may be utilized on various levels of IoT to provide secure utilization of keys.
- In the context of the IoT in general, usability and interfacing of its various layers is compelled to be kept very limited. Usable privacy and security with the help of modern UI/UX standards can help make many efficient solutions. It has also been observed that the end user has been neglected during the creation of specialized solutions, creating a gap in usability and utility in security standards.
- End-to-end authentication of users has yet to be explored, keeping IoT infrastructures and limited resource availability in context. Moreover, the perspective of provision of security standards, authentication in specific, has been limited to a certain number of security threats, and many other attacks may also be given importance, such as cloning attacks, node compromise issues, desynchronization attacks, and masquerading problems, etc.

- Authentication techniques may also be revised to provide better security and privacy to different types of end users of the IoT. It has been observed that the process of revamping of security standards, specifically authentication techniques, improves the security of the platform, which is not compromised easily, and the end user stays interested in keeping itself secure and updated. Keeping in view the limitations and strengths of different types of specialized IoTs, end-to-end user authentication may also be improved.

5. Conclusions

The IoT has earned its due attention over time. The last few years emphasized the need for technology in almost every sector of life. The IoT has many prospects in applied areas, but healthcare has been one of the most explored fields. This study orbits around authentication techniques being designed for the IoMT. Furthermore, the authentication schemes designed on different levels of the network, such as cloud, fog, and edge, have been analyzed for their contribution and limitations. Similarly, the role of authentication in an IoMT-based environment is studied. The study's essential findings implore the research community's attention to focus on providing quality healthcare services through modern technologies.

Author Contributions: Conceptualization, M.A.K. and I.U.D.; methodology, M.A.A.; software, M.A.K.; validation, I.U.D., T.M. and B.-S.K.; formal analysis, M.A.K.; investigation, I.U.D.; resources, B.-S.K.; data curation, I.U.D. and T.M.; writing—original draft preparation, M.A.K.; writing—review and editing, I.U.D. and B.-S.K.; visualization, T.M.; supervision, I.U.D.; project administration, B.-S.K.; funding acquisition, B.-S.K. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Research Foundation (NRF), Republic of Korea, under the project BK21 FOUR (F21YY8102068).

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Roy, M.; Chowdhury, C.; Aslam, N. Designing transmission strategies for enhancing communications in medical IoT using Markov decision process. *Sensors* **2018**, *18*, 4450. [CrossRef]
2. Vishnu, S.; Ramson, S.J.; Jegan, R. Internet of medical things (IoMT)-An overview. In Proceedings of the 2020 5th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, 5–6 March 2020; pp. 101–104.
3. Qureshi, F.; Krishnan, S. Wearable hardware design for the internet of medical things (IoMT). *Sensors* **2018**, *18*, 3812. [CrossRef]
4. AlShorman, O.; AlShorman, B.; Alkhassaweneh, M.; Alkahtani, F. A review of internet of medical things (IoMT)-based remote health monitoring through wearable sensors: A case study for diabetic patients. *Indones. J. Electr. Eng. Comput. Sci.* **2020**, *20*, 414–422. [CrossRef]
5. Kelly, J.T.; Campbell, K.L.; Gong, E.; Scuffham, P. The Internet of Things: Impact and implications for health care delivery. *J. Med. Internet Res.* **2020**, *22*, e20135. [CrossRef]
6. Rayan, R.A.; Tsagkaris, C.; Papazoglou, A.S.; Moysidis, D.V. The Internet of Medical Things for Monitoring Health. In *Internet of Things*; CRC Press: Boca Raton, FL, USA, 2022; pp. 213–228.
7. Arora, S. IoMT (Internet of Medical Things): Reducing cost while improving patient care. *IEEE Pulse* **2020**, *11*, 24–27. [CrossRef]
8. Ahmadi, H.; Arji, G.; Shahmoradi, L.; Safdari, R.; Nishi, M.; Alizadeh, M. The application of Internet of things in healthcare: A systematic literature review and classification. *Univers. Access Inf. Soc.* **2019**, *18*, 837–869. [CrossRef]
9. Tun, S.Y.Y.; Madanian, S.; Mirza, F. Internet of things (IoT) applications for elderly care: A reflective review. *Aging Clin. Exp. Res.* **2021**, *33*, 855–867. [CrossRef]
10. Kinsella, K.; He, W. *An Aging World: 2008, International Population Reports*; U.S. Department of Health and Human Services & U.S. Department of Commerce: Washington, DC, USA, 2009.
11. Hasan, K.; Biswas, K.; Ahmed, K.; Nafi, N.S.; Islam, M.S. A comprehensive review of wireless body area network. *J. Netw. Comput. Appl.* **2019**, *143*, 178–198. [CrossRef]
12. Ali, S.; Singh, R.P.; Javaid, M.; Haleem, A.; Pasricha, H.; Suman, R.; Karloopia, J. A review of the role of smart wireless medical sensor network in COVID-19. *J. Ind. Integr. Manag.* **2020**, *5*, 413–425. [CrossRef]

13. Khan, R.A.; Pathan, A.S.K. The state-of-the-art wireless body area sensor networks: A survey. *Int. J. Distrib. Sens. Netw.* **2018**, *14*. [CrossRef]
14. Kris, D.; Nakas, C.; Vomvas, D.; Koulouras, G. Applications of wireless sensor networks: An up-to-date survey. *Appl. Syst. Innov.* **2020**, *3*, 14.
15. Sinha, A.; Singh, S. Detailed Analysis of Medical IoT Using Wireless Body Sensor Network and Application of IoT in Healthcare. In *Human Communication Technology: Internet of Robotic Things and Ubiquitous Computing*; Wiley: New York, NY, USA, 2021; pp. 401–434.
16. Ray, P.P.; Dash, D.; Kumar, N. Sensors for internet of medical things: State-of-the-art, security and privacy issues, challenges and future directions. *Comput. Commun.* **2020**, *160*, 111–131. [CrossRef]
17. Karthick, R.; Ramkumar, R.; Akram, M.; Kumar, M.V. Overcome the challenges in bio-medical instruments using IOT—A review. *Mater. Today Proc.* **2021**, *45*, 1614–1619. [CrossRef]
18. Al-Turjman, F.; Nawaz, M.H.; Ulusar, U.D. Intelligence in the Internet of Medical Things era: A systematic review of current and future trends. *Comput. Commun.* **2020**, *150*, 644–660. [CrossRef]
19. Paul, A.; Jeyaraj, R. Internet of Things: A primer. *Hum. Behav. Emerg. Technol.* **2019**, *1*, 37–47. [CrossRef]
20. Alizadeh, M.; Shaker, G.; De Almeida, J.C.M.; Morita, P.P.; Safavi-Naeini, S. Remote monitoring of human vital signs using mm-wave FMCW radar. *IEEE Access* **2019**, *7*, 54958–54968. [CrossRef]
21. Kebe, M.; Gadhafi, R.; Mohammad, B.; Sanduleanu, M.; Saleh, H.; Al-Qutayri, M. Human vital signs detection methods and potential using radars: A review. *Sensors* **2020**, *20*, 1454. [CrossRef]
22. Kumar, P.; Lee, H.J. Security issues in healthcare applications using wireless medical sensor networks: A survey. *Sensors* **2012**, *12*, 55–91. [CrossRef]
23. Grammatikis, P.I.R.; Sarigiannidis, P.G.; Moscholios, I.D. Securing the Internet of Things: Challenges, threats and solutions. *Internet Things* **2019**, *5*, 41–70. [CrossRef]
24. Nižetić, S.; Šolić, P.; González-de, D.L.D.I.; Patrono, L. Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *J. Clean. Prod.* **2020**, *274*, 122877. [CrossRef]
25. Manogaran, G.; Chilamkurti, N.; Hsu, C.H. Emerging trends, issues, and challenges in Internet of Medical Things and wireless networks. *Pers. Ubiquitous Comput.* **2018**, *22*, 879–882. [CrossRef]
26. Hatzivasilis, G.; Soultatos, O.; Ioannidis, S.; Verikoukis, C.; Demetriou, G.; Tsatsoulis, C. Review of security and privacy for the Internet of Medical Things (IoMT). In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini, Greece, 29–31 May 2019; pp. 457–464.
27. Da Xu, L.; He, W.; Li, S. Internet of things in industries: A survey. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2233–2243.
28. Pierleoni, P.; Concetti, R.; Belli, A.; Palma, L. Amazon, Google and Microsoft solutions for IoT: Architectures and a performance comparison. *IEEE Access* **2019**, *8*, 5455–5470. [CrossRef]
29. Ucuz, D. Comparison of the IoT platform vendors, microsoft Azure, Amazon web services, and Google cloud, from users' perspectives. In Proceedings of the 2020 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Lebanon, 1–2 June 2020; pp. 1–4.
30. Bakhshi, Z.; Balador, A.; Mustafa, J. Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models. In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Barcelona, Spain, 15–18 April 2018; pp. 173–178.
31. Dohr, A.; Modre-Opsrian, R.; Drobics, M.; Hayn, D.; Schreier, G. The internet of things for ambient assisted living. In Proceedings of the 2010 Seventh International Conference on Information Technology: New Generations, Las Vegas, NV, USA, 12–14 April 2010; pp. 804–809.
32. Ashton, K. That 'internet of things' thing. *RFID J.* **2009**, *22*, 97–114.
33. Kumar, S.; Tiwari, P.; Zymbler, M. Internet of Things is a revolutionary approach for future technology enhancement: A review. *J. Big Data* **2019**, *6*, 111. [CrossRef]
34. Srinivasan, C.R.; Rajesh, B.; Saikalyan, P.; Premsagar, K.; Yadav, E.S. A review on the different types of Internet of Things (IoT). *J. Adv. Res. Dyn. Control Syst.* **2019**, *11*, 154–158.
35. Cisco Systems Inc. Internet of Things at a Glance. Available online: https://emarsonindia.com/wp-content/uploads/2020/02/Internet-of-Things.pdf (accessed on 22 November 2022).
36. IDC Corporate USA, Worldwide Internet of Things Spending Guide. Available online: https://www.idc.com/getdoc.jsp?containerId=IDC_P29475 (accessed on 22 November 2022).
37. Stojkoska, B.L.R.; Trivodaliev, K.V. A review of Internet of Things for smart home: Challenges and solutions. *J. Clean. Prod.* **2017**, *140*, 1454–1464. [CrossRef]
38. Ghayvat, H.; Liu, J.; Babu, A.; Alahi, E.E.; Gui, X.; Mukhopadhyay, S.C. Internet of Things for smart homes and buildings: Opportunities and Challenges. *J. Telecommun. Digit. Econ.* **2015**, *3*, 33–47. [CrossRef]
39. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of things for smart cities. *IEEE Internet Things J.* **2014**, *1*, 22–32. [CrossRef]
40. Alavi, A.H.; Jiao, P.; Buttlar, W.G.; Lajnef, N. Internet of Things-enabled smart cities: State-of-the-art and future trends. *Measurement* **2018**, *129*, 589–606. [CrossRef]

41. Lai, K.L.; Chen, J.I.Z.; Zong, J.I. Development of smart cities with fog computing and internet of things. *J. Ubiquitous Comput. Commun. Technol. (UCCT)* **2021**, *3*, 52–60.
42. Malik, P.K.; Sharma, R.; Singh, R.; Gehlot, A.; Satapathy, S.C.; Alnumay, W.S.; Pelusi, D.; Ghosh, U.; Nayak, J. Industrial Internet of Things and its applications in industry 4.0: State of the art. *Comput. Commun.* **2021**, *166*, 125–139. [CrossRef]
43. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial internet of things: Challenges, opportunities, and directions. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4724–4734. [CrossRef]
44. Khan, W.Z.; Rehman, M.H.; Zangoti, H.M.; Afzal, M.K.; Armi, N.; Salah, K. Industrial internet of things: Recent advances, enabling technologies and open challenges. *Comput. Electr. Eng.* **2020**, *81*, 106522. [CrossRef]
45. Kim, W.S.; Lee, W.S.; Kim, Y.J. A review of the applications of the internet of things (IoT) for agricultural automation. *J. Biosyst. Eng.* **2020**, *45*, 385–400. [CrossRef]
46. Salam, A. Internet of things in agricultural innovation and security. In *Internet of Things for Sustainable Community Development*; Springer: Cham, Switerland, 2020; pp. 71–112.
47. Ojha, T.; Misra, S.; Raghuwanshi, N.S. Internet of things for agricultural applications: The state of the art. *IEEE Internet Things J.* **2021**, *8*, 10973–10997. [CrossRef]
48. Bai, B.; Nazir, S.; Bai, Y.; Anees, A. Security and provenance for Internet of Health Things: A systematic literature review. *J. Software Evol. Process.* **2021**, *33*, e2335. [CrossRef]
49. Zaman, U.; Mehmood, F.; Iqbal, N.; Kim, J.; Ibrahim, M. Towards Secure and Intelligent Internet of Health Things: A Survey of Enabling Technologies and Applications. *Electronics* **2022**, *11*, 1893. [CrossRef]
50. Fantin Irudaya Raj, E.; Appadurai, M. Internet of Things-Based Smart Transportation System for Smart Cities. In *Intelligent Systems for Social Good*; Springer: Singapore, 2022; pp. 39–50.
51. Sharma, A.; Battula, R.B. The Internet of Things Solutions for Transportation. In *AI and IoT for Sustainable Development in Emerging Countries*; Springer: Cham, Switerland, 2022; pp. 291–324.
52. Jan B.; Farman, H.; Khan, M.; Talha, M.; Din, I.U. Designing a smart transportation system: An internet of things and big data approach. *IEEE Wirel. Commun.* **2019**, *26*, 73–79. [CrossRef]
53. Manavalan, E.; Jayakrishna, K. A review of Internet of Things (IoT) embedded sustainable supply chain for industry 4.0 requirements. *Comput. Ind. Eng.* **2019**, *127*, 925–953. [CrossRef]
54. Ghasempour, A. Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges. *Inventions* **2019**, *4*, 22. [CrossRef]
55. Caro, F.; Sadr, R. The Internet of Things (IoT) in retail: Bridging supply and demand. *Bus. Horizons* **2019**, *62*, 47–54. [CrossRef]
56. Priyan, M.K.; Devi, G.U. A survey on internet of vehicles: Applications, technologies, challenges and opportunities. *Int. J. Adv. Intell. Paradig.* **2019**, *12*, 98–119. [CrossRef]
57. Gbadamosi, A.Q.; Oyedele, L.; Mahamadu, A.M.; Kusimo, H.; Olawale, O. The role of internet of things in delivering smart construction. In Proceedings of the CIB World Building Congress 2019, Hong Kong, China, 17–21 June 2019.
58. Car, T.; Stifanich, L.P.; Šimunić, M. Internet of things (iot) in tourism and hospitality: Opportunities and challenges. *Tour. South East Eur.* **2019**, *5*, 163–175.
59. Karako, K.; Song, P.; Chen, Y.; Tang, W. Increasing demand for point-of-care testing and the potential to incorporate the Internet of medical things in an integrated health management system. *BioScience Trends* **2022**, *16*, 4–6. [CrossRef]
60. Naresh, V.S.; Pericherla, S.S.; Murty, P.S.R.; Sivaranjani, R. Internet of Things in Healthcare: Architecture, Applications, Challenges, and Solutions. *Comput. Syst. Sci. Eng.* **2020**, *35*, 411–421. [CrossRef]
61. Morgan, V.; Birtus, M.; Zauskova, A. Medical internet of Things-based Healthcare Systems, wearable biometric sensors, and personalized clinical care in remotely monitoring and caring for confirmed or suspected COVID-19 patients. *Am. J. Med Res.* **2021**, *8*, 81–90.
62. Reddy, M.A.; Pradhan, B.K.; Qureshi, D.; Pal, S.K.; Pal, K. Internet-of-things-enabled dual-channel iontophoretic drug delivery system for elderly patient medication management. *J. Med. Devices* **2020**, *14*, 011104. [CrossRef]
63. Latif, G.; Shankar, A.; Alghazo, J.M.; Kalyanasundaram, V.; Boopathi, C.S.; Arfan Jaffar, M. I-CARES: Advancing health diagnosis and medication through IoT. *Wirel. Netw.* **2020**, *26*, 2375–2389. [CrossRef]
64. Kang, M.; Park, E.; Cho, B.H.; Lee, K.S. Recent patient health monitoring platforms incorporating internet of things-enabled smart devices. *Int. Neurourol. J.* **2018**, *22* (Suppl. 2), S76. [CrossRef]
65. Ashima, R.; Haleem, A.; Bahl, S.; Javaid, M.; Mahla, S.K.; Singh, S. Automation and manufacturing of smart materials in Additive Manufacturing technologies using Internet of Things towards the adoption of Industry 4.0. *Mater. Today Proc.* **2021**, *45*, 5081–5088. [CrossRef]
66. Ismail, L.; Materwala, H.; Karduck, A.P.; Adem, A. Requirements of health data management systems for biomedical care and research: Scoping review. *J. Med. Internet Res.* **2020**, *22*, e17508. [CrossRef] [PubMed]
67. Setiawan, R.; Budiman, F.; Basori, W.I. Stress diagnostic system and digital medical record based on Internet of Things. In Proceedings of the 2019 International Seminar on Intelligent Technology and Its Applications (ISITIA), Surabaya, Indonesia, 28–29 August 2019; pp. 348–353.
68. Feng, Y.; Pan, Z. Optimization of remote public medical emergency management system with low delay based on internet of things. *J. Healthc. Eng.* **2021**, *2021*, 5570500. [CrossRef] [PubMed]

69. Rathore, M.M.; Ahmad, A.; Paul, A. The Internet of Things based medical emergency management using Hadoop ecosystem. In Proceedings of the 2015 IEEE SENSORS, Busan, Republic of Korea, 1–4 November 2015; pp. 1–4.
70. Yerpude, S.; Singhal, T.K. Smart warehouse with internet of things supported inventory management system. *Int. J. Pure Appl. Math.* **2018**, *118*, 1–15.
71. Mathaba, S.; Adigun, M.; Oladosu, J.; Oki, O. On the use of the Internet of Things and Web 2.0 in inventory management. *J. Intell. Fuzzy Syst.* **2017**, *32*, 3091–3101. [CrossRef]
72. Velasco, J.; Alberto, L.; Ambatali, H.D.; Canilang, M.; Daria, V.; Liwanag, J.B.; Madrigal, G.A. Internet of things-based (IoT) inventory monitoring refrigerator using arduino sensor network. *arXiv* **2019**, arXiv:1911.11265.
73. Qiu, T.; Qiao, R.; Wu, D.O. EABS: An event-aware backpressure scheduling scheme for emergency Internet of Things. *IEEE Trans. Mob. Comput.* **2017**, *17*, 72–84. [CrossRef]
74. Yaacoub, J.P.A.; Noura, M.; Noura, H.N.; Salman, O.; Yaacoub, E.; Couturier, R.; Chehab, A. Securing internet of medical things systems: Limitations, issues and recommendations. *Future Gener. Comput. Syst.* **2020**, *105*, 581–606. [CrossRef]
75. Abbas, A.; Alroobaea, R.; Krichen, M.; Rubaiee, S.; Vimal, S.; Almansour, F.M. Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. *Pers. Ubiquitous Comput.* **2021**, 1–14. [CrossRef]
76. Marwah, K.; Hajati, F. A Survey on Internet of Things in Telehealth. In Proceedings of the Conference on Complex, Intelligent, and Software Intensive Systems, Asan, Republic of Korea, 1–3 July 2021; Springer: Cham, Switerland, 2021; pp. 235–248.
77. Mendes, D.; Jorge, D.; Pires, G.; Panda, R.; António, R.; Dias, P.; Oliveira, L. VITASENIOR-MT: A distributed and scalable cloud-based telehealth solution. In Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019; pp. 767–772.
78. Emokpae, L.E.; Emokpae, R.N.; Lalouani, W.; Younis, M. Smart multimodal telehealth-IoT system for COVID-19 patients. *IEEE Pervasive Comput.* **2021**, *20*, 73–80. [CrossRef]
79. Albahri, A.S.; Alwan, J.K.; Taha, Z.K.; Ismail, S.F.; Hamid, R.A.; Zaidan, A.A.; Albahri, O.S.; Zaidan, B.B.; Alamoodi, A.H.; Alsalem, M.A. IoT-based telemedicine for disease prevention and health promotion: State-of-the-Art. *J. Netw. Comput. Appl.* **2021**, *173*, 102873. [CrossRef]
80. Bayo-Monton, J.L.; Martinez-Millana, A.; Han, W.; Fernandez-Llatas, C.; Sun, Y.; Traver, V. Wearable sensors integrated with Internet of Things for advancing eHealth care. *Sensors* **2018**, *18*, 1851. [CrossRef] [PubMed]
81. Amira, A.; Agoulmine, N.; Bensaali, F.; Bermak, A.; Dimitrakopoulos, G. Empowering eHealth with smart internet of things (IoT) medical devices. *J. Sens. Actuator Netw.* **2019**, *8*, 33. [CrossRef]
82. Chanal, P.M.; Kakkasageri, M.S. Security and privacy in IOT: A survey. *Wirel. Pers. Commun.* **2020**, *115*, 1667–1693. [CrossRef]
83. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access* **2019**, *7*, 82721–82743. [CrossRef]
84. Khanam, S.; Ahmedy, I.B.; Idris, M.Y.I.; Jaward, M.H.; Sabri, A.Q.B.M. A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things. *IEEE Access* **2020**, *8*, 219709–219743. [CrossRef]
85. Abosata, N.; Al-Rubaye, S.; Inalhan, G.; Emmanouilidis, C. Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. *Sensors* **2021**, *21*, 3654. [CrossRef]
86. Ghubaish, A.; Salman, T.; Zolanvari, M.; Unal, D.; Al-Ali, A.; Jain, R. Recent advances in the internet-of-medical-things (IoMT) systems security. *IEEE Internet Things J.* **2020**, *8*, 8707–8718. [CrossRef]
87. Chen, C.L.; Yang, T.T.; Leu, F.Y.; Huang, Y.L. Designing a healthcare authorization model based on cloud authentication. *Intell. Autom. Soft Comput.* **2014**, *20*, 65–379. [CrossRef]
88. Moghaddam, F.F.; Moghaddam, S.G.; Rouzbeh, S.; Araghi, S.K.; Alibeigi, N.M.; Varnosfaderani, S.D. A scalable and efficient user authentication scheme for cloud computing environments. In Proceedings of the 2014 IEEE Region 10 Symposium, Kuala Lumpur, Malaysia, 14–16 April 2014; pp. 508–513.
89. Shrestha, N.M.; Alsadoon, A.; Prasad, P.W.; Hourany, L.; Elchouemi, A. Enhanced e-health framework for security and privacy in healthcare system. In Proceedings of the 2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC), Beirut, Lebanon, 21–23 April 2016; pp. 75–79.
90. Kumari, A.; Kumar, V.; Abbasi, M.Y.; Kumari, S.; Chaudhary, P.; Chen, C.M. CSEF: Cloud-Based Secure and Efficient Framework for Smart Medical System Using ECC. *IEEE Access* **2020**, *8*, 107838–107852. [CrossRef]
91. Soni, P.; Pal, A.K.; Islam, S.H. An Improved Three-Factor Authentication Scheme for Patient Monitoring using WSN in Remote Health-care System. *Comput. Methods Programs Biomed.* **2019**, *182*, 105054. [CrossRef] [PubMed]
92. Sharma, G.; Kalra, S. A Lightweight User Authentication Scheme for Cloud-IoT Based Healthcare Services. *Iran J. Sci. Technol. Trans. Electr. Eng.* **2019**, *43*, 619–636. [CrossRef]
93. Sultan, N. Making use of cloud computing for healthcare provision: Opportunities and challenges. *Int. J. Inf. Manag.* **2014**, *34*, 177–184. [CrossRef]
94. Allouzi, M.A.; Khan, J.I. Soter: Trust Discovery Framework for Internet of Medical Things (IoMT). In Proceedings of the 2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Washington, DC, USA, 10–12 June 2019; pp. 1–9.
95. Moosavi, S.R.; Nigussie, E.; Levorato, M.; Virtanen, S.; Isoaho, J. Performance analysis of end-to-end security schemes in healthcare IoT. *Procedia Comput. Sci.* **2018**, *130*, 432–439. [CrossRef]

96. Challa, S.; Das, A.K.; Odelu, V.; Kumar, N.; Kumari, S.; Khan, M.K.; Vasilakos, A.V. An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks. *Comput. Electr. Eng.* **2017**, *69*, 534–554. [CrossRef]
97. Almogren, A.; Mohiuddin, I.; Din, I.U.; Almajed, H.; Guizani, N. FTM-IoMT: Fuzzy-based Trust Management for Preventing Sybil Attacks in Internet of Medical Things. *IEEE Internet Things J.* **2020**, *8*, 4485–4497. [CrossRef]
98. 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*, 7916–7955. [CrossRef]
99. Klonoff, D.C. Fog computing and edge computing architectures for processing data from diabetes devices connected to the medical Internet of things. *J. Diabetes Sci. Technol.* **2017**, *11*, 647–652. [CrossRef]
100. Borthakur, D.; Dubey, H.; Constant, N.; Mahler, L.; Mankodiya, K. Smart fog: Fog computing framework for unsupervised clustering analytics in wearable Internet of things. In Proceedings of the 2017 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Montreal, QC, Canada, 14–16 November 2017; pp. 472–476.
101. Dastjerdi, A.V.; Buyya, R. Fog computing: Helping the Internet of Things realize its potential. *Computer* **2016**, *49*, 112–116. [CrossRef]
102. Engineer, M.; Tusha, R.; Shah, A.; Adhvaryu, K. Insight into the Importance of Fog Computing in Internet of Medical Things (IoMT). In Proceedings of the 2019 International Conference on Recent Advances in Energy-efficient Computing and Communication (ICRAECC), Nagercoil, India, 7–8 March 2019; pp. 1–7.
103. Wang, X.; Wang, L.; Li, Y.; Gai, K. Privacy-aware efficient fine-grained data access control in Internet of medical things based fog computing. *IEEE Access* **2018**, *6*, 47657–47665. [CrossRef]
104. Akrivopoulos, O.; Chatzigiannakis, I.; Tselios, C.; Antoniou, A. On the deployment of healthcare applications over fog computing infrastructure. In Proceedings of the 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), Turin, Italy, 4–8 July 2017; Volume 2, pp. 288–293.
105. Kang, J.; Fan, K.; Zhang, K.; Cheng, X.; Li, H.; Yang, Y. An ultra-lightweight and secure RFID batch authentication scheme for IoMT. *Comput. Commun.* **2021**, *167*, 48–54. [CrossRef]
106. Cha, J.R.; Kim, J.H. Dynamic framed slotted ALOHA algorithms using fast tag estimation method for RFID system. In Proceedings of the CCNC 2006, 2006 3rd IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, 8–10 January 2006; Volume 2, pp. 768–772.
107. Han, T.; Zhang, L.; Pirbhulal, S.; Wu, W.; de Albuquerque, V.H.C. A novel cluster head selection technique for edge-computing based IoMT systems. *Comput. Netw.* **2019**, *158*, 114–122. [CrossRef]
108. Saeed, M.E.S.; Liu, Q.Y.; Tian, G.; Gao, B.; Li, F. Remote authentication schemes for wireless body area networks based on the Internet of Things. *IEEE Internet Things J.* **2018**, *5*, 4926–4944. [CrossRef]
109. Lee, J.D.; Yoon, T.S.; Chung, S.H.; Cha, H.S. Service-oriented security framework for remote medical services in the Internet of Things environment. *Healthc. Inform. Res.* **2015**, *21*, 271–282. [CrossRef]
110. Gope, P.; Hwang, T. BSN-Care: A secure IoT-based modern healthcare system using body sensor network. *IEEE Sens. J.* **2015**, *16*, 1368–1376. [CrossRef]
111. Rathore, H.; Fu, C.; Mohamed, A.; Al-Ali, A.; Du, X.; Guizani, M.; Yu, Z. Multi-layer security scheme for implantable medical devices. *Neural Comput. Appl.* **2018**, *32*, 4347–4360. [CrossRef]
112. Fotouhi, M.; Bayat, M.; Das, A.K.; Far, H.A.; Pournaghi, S.M.; Doostari, M.A. A lightweight and secure two-factor authentication scheme for wireless body area networks in healthcare IoT. *Comput. Netw.* **2020**, *177*, 107333. j.comnet.2020.107333. [CrossRef]
113. Mawgoud, A.A.; Karadawy, A.I.; Tawfik, B.S. A Secure Authentication Technique in Internet of Medical Things through Machine Learning. *J. Contrib.* **2020**,
114. Yanambaka, V.; Mohanty, S.; Kougianos, E.; Puthal, D.; Rachakonda, L. PMsec: PUF-Based Energy-Efficient Authentication of Devices in the Internet of Medical Things (IoMT). In Proceedings of the 2019 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), Rourkela, India, 16–18 December 2019; pp. 320–321.
115. Yang, J.C.; Hao, P.A.N.G.; Zhang, X. Enhanced mutual authentication model of IoT. *J. China Univ. Posts Telecommun.* **2013**, *20*, 69–74. [CrossRef]
116. Odelu, V.; Saha, S.; Prasath, R.; Sadineni, L.; Conti, M.; Jo, M. Efficient Privacy-Preserving Device Authentication in WBANs for Industrial e-Health Applications. *Comput. Secur.* **2019**, *83*, 300–312. [CrossRef]
117. Amintoosi, H.; Nikooghadam, M.; Shojafar, M.; Kumari, S.; Alazab, M. Slight: A lightweight authentication scheme for smart healthcare services. *Comput. Electr. Eng.* **2022**, *99*, 107803. [CrossRef]
118. Kumar, A.; Saha, R.; Conti, M.; Kumar, G.; Buchanan, W.J.; Kim, T.H. A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions. *J. Netw. Comput. Appl.* **2022**, *204*, 103414. [CrossRef]
119. Sun, Y.; Lo, F.P.W.; Lo, B. Security and privacy for the Internet of medical things enabled healthcare systems: A survey. *IEEE Access* **2019**, *7*, 183339–183355. [CrossRef]
120. Kashani, M.H.; Madanipour, M.; Nikravan, M.; Asghari, P.; Mahdipour, E. A systematic review of IoT in healthcare: Applications, techniques, and trends. *J. Netw. Comput. Appl.* **2021**, *192*, 103164. [CrossRef]

121. Gopalan, S.S.; Raza, A.; Almobaideen, W. IoT security in healthcare using AI: A survey. In Proceedings of the 2020 International Conference on Communications, Signal Processing, and Their Applications (ICCSPA), Sharjah, United Arab Emirates, 16–18 March 2021; pp. 1–6.
122. Somasundaram, R.; Thirugnanam, M. Review of security challenges in healthcare internet of things. *Wirel. Netw.* **2021**, *27*, 5503–5509. [CrossRef]
123. Rajasekar, V.; Premalatha, J.; Sathya, K.; Saračević, M. Secure remote user authentication scheme on health care, IoT and cloud applications: A Multilayer Systematic Survey. *Acta Polytech. Hung.* **2021**, *18*, 87–106. [CrossRef]
124. Papaioannou, M.; Karageorgou, M.; Mantas, G.; Sucasas, V.; Essop, I.; Rodriguez, J.; Lymberopoulos, D. A survey on security threats and countermeasures in Internet of medical things (IoMT). *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4049. [CrossRef]
125. Trnka, M.; Abdelfattah, A.S.; Shrestha, A.; Coffey, M.; Cerny, T. Systematic Review of Authentication and Authorization Advancements for the Internet of Things. *Sensors* **2022**, *22*, 1361. [CrossRef]