applied sciences

MDPI

Review

Authentication in the Internet of Medical Things: Taxonomy, Review, and Open Issues

Norah Alsaeed [1,2,*] and Farrukh Nadeem [1]

[1] Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia; fabdullatif@kau.edu.sa
[2] Department of Computer Science, The Applied College, King Khalid University, Abha 61421, Saudi Arabia
* Correspondence: nalsaeed@kku.edu.sa

Abstract: The Internet of Medical Things (IoMT) has revolutionized the world of healthcare by remotely connecting patients to healthcare providers through medical devices connected over the Internet. IoMT devices collect patients' medical data and share them with healthcare providers, who analyze it for early control of diseases. The security of patients' data is of prime importance in IoMT. Authentication of users and devices is the first layer of security in IoMT. However, because of diverse and resource-constrained devices, authentication in IoMT is a challenging task. Several authentication schemes for IoMT have been proposed in the literature. However, each of them has its own pros and cons. To identify, evaluate and summarize the current literature on authentication in IoMT, we conducted a systematic review of 118 articles published between 2016 and 2021. We also established a taxonomy of authentication schemes in IoMT from seven different perspectives. We observed that most of the authentication schemes use a distributed architecture and public key infrastructure. It was also observed that hybrid cryptography approaches have become popular to overcome the shortcomings of single cryptographic approaches. Authentication schemes in IoMT need to support end-to-end, cross-layer, and cross-domain authentication. Finally, we discuss some open issues and future directions.

Keywords: Internet of Medical Thing; security requirements; IoMT authentication scheme; IoMT authentication attacks

Citation: Alsaeed, N.; Nadeem, F. Authentication in the Internet of Medical Things: Taxonomy, Review, and Open Issues. *Appl. Sci.* **2022**, *12*, 7487. https://doi.org/10.3390/app12157487

Academic Editor: Pentti Nieminen

Received: 8 May 2022
Accepted: 30 June 2022
Published: 26 July 2022

1. Introduction

The current COVID-19 epidemic has again highlighted the importance of smart healthcare services that offer prevention, diagnosis, and treatment at a distance. Smart healthcare is not simply a technology improvement rather it provides multi-level and global changes in the healthcare arena. The smart healthcare is built around emerging technologies, such as cloud computing, Internet of Things (IoT), machine learning, and big data [1]. IoT has become an essential component to fulfill the connectivity requirements of the current smart healthcare systems. IoT, in the healthcare context, is called the Internet of Medical Things (IoMT). IoMT comprises medical devices connected to patients to sense their medical parameters and share that information with healthcare staff so that they may provide remote healthcare services. The IoMT security is an imperative need worthy of more research due to the need to safeguard the patient's sensitive information from exploitation [2]. To avoid such exploitation, and to ensure a high level of security, IoMT applications must maintain strict authentication schemes that prevent unauthorized access to patients' data, as well as the IoMT resources, and protect the entire system from various types of attacks [3,4]. Developing a strict authentication scheme within the IoMT context is challenging for three main reasons. First, IoMT devices are resource-constrained and cannot handle intensive computational and complex authentication procedures. Second, various IoMT products and vendors work through different platforms and protocols. Consequently, developing strict authentication requires deep knowledge of how different products, platforms, and

protocols collectively work. Third, highly distributed IoMT devices that share medical data through the Internet make IoMT systems intrinsically prone to security violations.

1.1. Motivation

IoMT is considered a major component of today's model for smart healthcare. On the other hand, IoMT systems are prone to many vulnerabilities because of the resource-constrained IoMT devices, their diversity, as well as a large number of IoMT users. Therefore, IoMT security becomes a significant and challenging task for IoMT systems. Data confidentiality and privacy, resources availability, and access control are critical security requirements. Authentication of IoMT devices and users is the first gate to access IoMT systems and plays a vital role in ensuring the security requirements directly or indirectly. That prompted the authors of this study to review IoMT authentication schemes to realize helpful insights from the IoMT authentication literature. Moreover, the study establishes an exhaustive taxonomy to provide researchers with a holistic view of IoMT authentication.

1.2. Contributions

The main contributions of this paper are as follows:

- This paper presents a systematic review of 118 recent articles related to authentication schemes in IoMT and published between 2016 and 2021.
- We establish a novel IoMT authentication taxonomy based on the most recent methods.
- Our study highlights major findings of the literature review analysis. The findings include significant insights about the implementation and evaluation of authentication schemes in the IoMT context.
- We conclude our study by discussing open issues and future research directions for significant improvements in IoMT authentication.

1.3. Scope

Some other researchers have reviewed authentication schemes in the IoT context. These studies have partially addressed some aspects of authentication in IoMT systems. Table 1 illustrates a brief comparison of these studies, published between 2016 and 2021. Trnka et al. [5] provided a systematic literature review of access control schemes, including authentication, authorization, and identity management in the IoT context. Another survey, developed by Albalawi et al. [6], introduced authentication classification to map their review of authentication schemes. They compared the reviewed schemes according to pre-specified criteria; the criteria are the degree of lightweight, multi-factor use, encryption use, and efficiency. Agrawal et al. [7] followed the same research method as Albalawi et al. [6] and depended on the existing classifications of IoT authentication to conduct their survey. Gamundani et al. [8] aimed to review authentication in IoT from the threats and attacks perspective. Their paper mainly targeted smart home applications and IoT-layered architecture as a base for mapping their review. However, the studies mentioned above did not present a taxonomy of authentication schemes in the IoT context. Moreover, they did not discuss the evaluation techniques and open issues regarding IoT authentication.

El-Hajj et al. [9] established a taxonomy of IoT authentication schemes. El-Hajj et al. [9] relied on their previous taxonomy to conduct a systematic literature review of techniques related to IoT authentication. Ferrag et al. [10] established a comprehensive review of attacks targeting IoT authentication. The paper classified IoT authentication protocols into Internet-of-Sensors, Internet-of-Energy, Internet-of-Vehicles, and Machine-to-Machine communication. They mapped the authentication attacks and schemes according to such a classification.

Kavianpour et al. [11] conducted an exhaustive systematic review of techniques for IoT authentication. The paper considered the review from multiple aspects, such as authentication phases, threats, evaluation of performance, and adopted technologies. Mamdouh et al. [1] discussed important issues, including security analysis techniques, evaluation platforms, and future directions related to IoMT authentication.

We considered the global aspects mentioned in Table 1. Our work establishes a taxonomy of authentication in the IoMT context. It then relies on the taxonomy developed to discuss the reviewed articles. Moreover, this work discusses authentication attacks, security analysis and evaluation techniques, open issues, and future directions related to IoMT authentication.

Table 1. Comparison of existing review papers.

Ref.	Year	Objective	IoMT Context	Taxonomy	Review	Open Issues	Attacks	Evaluation Techniques	Security Analysis Techniques
Saadeh et al. [12]	2016	A survey of authentication for IoT	×	×	✓	×	✓	✓	×
Thierre et al. [13]	2017	A review of authentication used in IoT	×	×	✓	✓	×	×	×
Ferrag et al. [10]	2017	A review of authentication protocols in IoT	×	✓	✓	✓	✓	✓	✓
Gamundani et al. [8]	2018	A review of attacks and threats of IoT authentication	×	×	✓	×	✓	×	×
El-Hajj et al. [9]	2018	Authentication taxonomy for IoT	×	✓	✓	×	×	×	×
Trnka et al. [5]	2018	A survey of IoT authentication, authorization	×	×	✓	×	×	×	×
Albalawi et al. [6]	2019	A survey of authentication for IoT	×	×	✓	×	✓	×	×
Kavianpour et al. [11]	2019	A systematic review of IoT authentication	×	×	✓	✓	✓	✓	×
El-Hajj et al. [14]	2019	IoT authentication taxonomy and survey	×	✓	✓	×	✓	×	×
Mehta et al. [15]	2020	A review and current issues in IoT authentication	×	×	✓	✓	✓	×	×
Agrawal et al. [7]	2020	A survey of authentication schemes in IoT	×	×	✓	×	×	×	×
Shu et al. [16]	2021	A review of ECC and authentication in IoT	×	×	✓	✓	×	×	×
Mamdouh et al. [1]	2021	A comprehensive survey of authentication mechanisms in IoMT	✓	×	✓	✓	✓	✓	✓
Current study	–	A taxonomy, review, and open issues of authentication in IoMT	✓	✓	✓	✓	✓	✓	✓

✓: indicates supported, × : indicates not supported.

1.4. Organization

The organization of the paper is the following. To set the stage, we briefly introduce smart healthcare, IoT in smart healthcare, and IoMT architecture and applications in Section 2. The security requirements for IoMT are presented in Section 2.4. Our overall research methodology including research questions is outlined in Section 3. Section 4 presents taxonomy of authentication schemes in IoMT. Section 5 discusses some findings of literature review analysis. Some open issues and future directions for IoMT authentication are presented in Section 6. Section 7 concludes the paper.

2. Background

Smart healthcare does not only adopt emerging technologies in the healthcare field, it includes global changes in the healthcare context. Today's healthcare focuses on patients instead of diseases, and personalized management instead of medical management [1]. It also aims at preventive care instead of disease care and meets personalized needs, thereby improving healthcare efficiency. This brief background starts with the smart healthcare concept. It then introduces the adoption of IoT in the role of supporting smart healthcare applications. Finally, it presents the IoMT system's context from architecture, applications, and devices perspectives.

2.1. Smart Healthcare

The evolution of technologies contributes to the high quality of services in the healthcare sector as patients receive faster and more personalized services [17]. Smart healthcare, or healthcare 4.0, is an intelligent healthcare asset that uses sensing devices to gather medical data, network devices to transmit data, and an advanced infrastructure to process, store, and display that data for enhancing healthcare services. In summary, smart healthcare involves the use of cutting-edge technologies to increase the effectiveness of medical assistance and, where possible, to decrease healthcare costs. Smart healthcare provides significant capabilities, such as continuous interaction between all the relevant parties in healthcare, helping the healthcare providers make knowledgeable decisions, and supporting the dynamic allocation of healthcare resources. In short, today's healthcare services need to be personalized and available anytime, anywhere, and for everyone. This goal is met through smart healthcare [1].

2.2. IoT in Smart Healthcare

In its basic form, IoT connects physical objects to the Internet to perform related activities remotely. This connection provided features such as context-awareness capabilities, autonomous data capture, and on-line communication facilities for a specific purpose. In particular, IoMT refers to smart medical devices connected via the Internet to a central entity, usually a cloud, to automatically gather, process, and share medical data for healthcare services [18].

Smart healthcare requires the IoT paradigm to provide solutions that can capture patients' health parameters, recognize symptoms, and thus recommend preventive actions. On the other hand, IoMT applications help the healthcare industry to design and develop new medical solutions based on big data analytics that use the data generated from IoMT devices, and to take other knowledge-based measures as needed. Patients, healthcare providers, such as doctors, nurses, pharmacists, physicians, and hospitals, as well as insurance companies, can benefit directly or indirectly from IoMT applications. IoMT applications are helpful for many healthcare areas, such as remote healthcare services, medical asset management, optimization of medical inventory, patient–doctor rapport, real-time medical data analytics, augmented surgeries, and treatment [4].

2.3. IoMT Context

This section presents the overall context of IoMT systems. It includes the IoMT system architecture and the way its layers are integrated to perform tasks remotely. Moreover, the IoMT context discusses some applications related to IoMT systems. At the end, it briefly classifies the IoMT devices and describes their functions.

2.3.1. IoMT Architecture

Figure 1 illustrates the IoMT layers. The IoMT architecture operates mainly through four layers [19], as described below.

- The data collection layer performs the data sensing and collecting activities. It acquires patients' medical parameters from sensors, actuators, edge servers, hand-held devices, and medical sensors via the data sensing acquisition protocols.

- The network layer transfers the collected medical data from the data collection layer through a wired or wireless network to deliver the data to the third layer (i.e., the data management layer). This layer connects all medical things in the network, and exchanges data.
- The data management layer uses the middle-ware applications and services needed by IoMT applications and users such that the interoperability between the heterogeneous entities being used is ensured in this layer. Other essential services, such as storing, processing, and interpreting the collected medical data, are provided in this layer.
- The application layer supports intelligent interaction between a user and the IoMT system. Here, the user can easily interconnect and manage medical things and display the medical data.

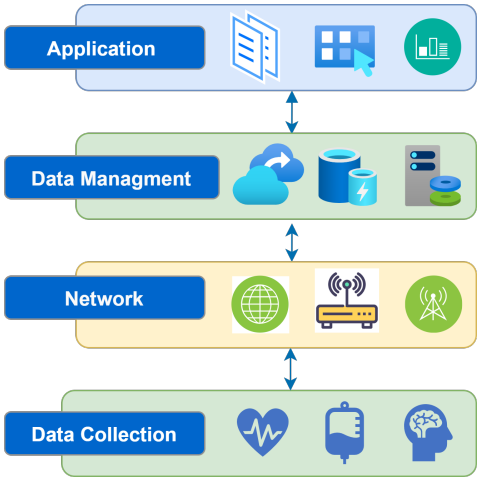

Figure 1. IoMT system architecture.

2.3.2. IoMT Applications

With rapid technological advancement, the various IoMT applications are exponentially increasing. Hundreds of applications are available for IoMT systems. These applications can be categorized as shown in Figure 2 [4]:

- Monitoring applications use pervasive computing to remotely monitor a patient's health for prevention purposes [20]. Examples of widespread applications under this category include monitoring oxygen levels, blood pressure, asthma, electrocardiogram (ECG), glucose, etc.
- Diagnostic applications mainly use the semantics explained in electronic healthcare records to diagnose diseases. The effectiveness of these applications is highly dependent upon the quality of data collected through the IoMT devices and the predefined observations in the electronic healthcare records.
- Therapeutic applications involve remote interventions, which lead to many challenges according to the level of intervention. Remote surgery is an example of such applications. Therapeutic IoMT applications are not currently popular because they need advanced technologies and experts from different fields to implement them.
- Rehabilitation applications are mainly used to identify the patients' problems and help them to regain the functions needed in everyday life. An example of rehabilitation applications is the stroke rehabilitation system.

2.3.3. IoMT Devices

D. Hemanth et al. [19] classified IoMT devices according to their position, such as in-community, in-hospital, in-clinic, in-home, and onbody devices. In this paper, IoMT devices are classified according to their distance from patients, as shown in Figure 3 [21–23]:

- Implantable devices are fitted inside patients' bodies, usually to help doctors in diagnostic and surgical tasks. Examples of these devices are a capsule containing a camera but which is small enough to be swallowed, and an embedded cardiac sensor.
- Wearable devices are developed by embedding different sensors in wearable accessories. Examples of these devices are necklaces, wristbands, shoes, and watches.
- Bearable devices are equipped with patients' computers for specific purposes. These commonly help people to obtain different services in everyday life. An air quality monitor is an example of a bearable device connected to an asthma patient's smartphone or tablet.
- Nearable devices are anchored on doors, tables, or even beds. The patients do not need to carry these devices. The interaction with these devices is natural, such as with door, motion, pressure, or temperature sensors. They are expected to alert patients, their relatives, or healthcare providers when abnormal signs are gathered. Such devices are aware of the patient's context to help them monitor their activities, such as their quality of sleep and number of bathroom visits.

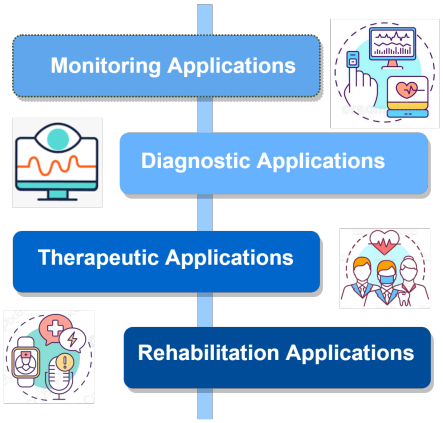

Figure 2. IoMT applications.

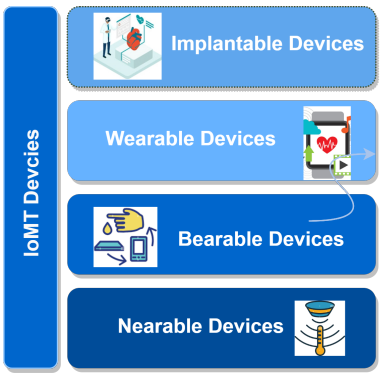

Figure 3. IoMT devices.

2.4. IoMT Security Requirements

The security requirements of the IoMT are divided into three levels: information security, function security, and access control, as illustrated in Figure 4. It is worth mentioning that the security requirements are interlinked and affected by each other [3]. The security requirements at these three levels are described as is detailed in the following section.

2.4.1. Information Level Security Requirements

Information level security requirements cover the security of data or information, either collected by IoMT devices or stored directly by healthcare providers. These data/information

include patients' monitoring, diagnoses, treatment, and medical history. Thus, keeping an acceptable level of privacy, integrity, and confidentiality standards is crucial.

- Confidentiality: ensures that only legitimate people can access the information. In other words, information has to be stored and represented so that unauthorized users cannot access it. Since the IoMT systems operate in a distributed and remote way, the need for ensuring data confidentiality is more critical.
- Integrity: ensures that the information is precise and consistent during collection, storage, and sharing. In IoMT applications, any possibility of sharing imprecise or corrupted information may lead to a patient's death.
- Privacy: it is a vital requirement in IoMT application, and it requires special attention. Private information is only accessed and used by legitimate users, and for the purpose for which it is collected. In IoMT systems, privacy standards should be maintained during all phases of information management.

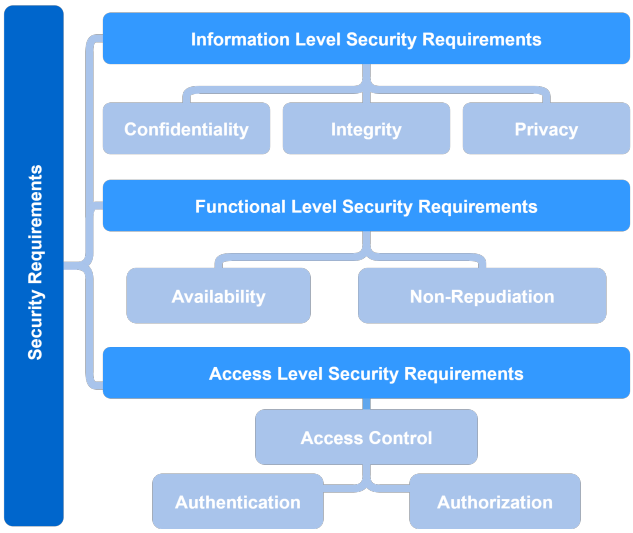

Figure 4. Levels of security requirements.

2.4.2. Functional Level Security Requirements

Functional security addresses the security of IoMT system's services and resources. It is divided into two aspects: availability and non-repudiation. Figure 4 shows the functional security requirements in IoMT.

- Availability ensures that a service is available to intended users anytime and anywhere. In IoMT systems, the availability requirement is extended to ensure the availability of IoMT entities themselves.
- Non-repudiation: it ensures the ability to determine how and by whom an event or a task occurred. In this way, an entity cannot deny the authenticity or refute its responsibility.

2.4.3. Access Level Security Requirements

The access level is related to the security requirements that control the access to IoMT systems. The access control mechanism plays an essential role in securing the overall system at this level. It is responsible for identifying entities in the system and determining their permissions to access its resources. Access control is working through two aspects: authentication and authorization.

- Authentication: it verifies the identity of an entity to permit its access to the IoMT system. Therefore, the authentication mechanism is the first gate for an entity to access and communicate with other entities.
- Authorization is responsible for determining the privileges for authenticated entities to access or use the system's services or resources.

3. Research Methodology

The major motivation behind our methodological choices is to find the answers to our research questions mentioned in Section 3.1. We believed that the methodology of systematic review is one of the most suitable choices to find answers to our research questions. In addition, we also planned to establish an exhaustive taxonomy of authentication schemes in IoMT, and the approach of systematic review also supports this purpose. Our study has a specific scope (authentication in IoMT) and constraints for selecting papers for review, the approach of systematic review is suitable to achieve these goals. This study followed the systematic review process. Accordingly, the study goes through the following process. The research methodology begins by generating the research questions. Next, we set the rules for selecting articles to include in our review, and then, we search for articles in credible digital databases. Next, we apply those research rules to the found articles and select only the relevant articles. Finally, we review the full text of the selected articles and establish the authentication taxonomy accordingly. The process of review is illustrated in Figure 5.

Figure 5. Research methodology.

3.1. Research Questions

This paper presents a literature review and a taxonomy of IoMT authentication, and the research questions are identified accordingly; Table 2 lists the questions.

Table 2. Research questions.

Q#	Research Questions
Q1	What are the levels of authentication in IoMT systems?
Q2	What are the architectures of authentication in IoMT systems?
Q3	What are the different types of credentials facilitated in IoMT authentication?
Q4	What are the authentication procedures in IoMT systems?
Q5	What are the authentication categories in IoMT systems?
Q6	What are the different schemes of authentication in IoMT?
Q7	What are the different attacks considered while proposing authentication schemes in IoMT systems?
Q8	What are the different techniques and tools for evaluating authentication schemes in IoMT systems?
Q9	What are the parameters used to evaluate the proposed authentication schemes in IoMT systems?

3.2. Rules of Selection

For achieving our research objectives, the following rules are specified for the review time frame, search string, and inclusion and exclusion criteria.

1. The research time frame for the selected articles is between 2015 to 2021. The time frame ensures a recent evolution of authentication in IoMT.
2. The search string is Authentication, IoMT, IoT-based healthcare , IoMT devices, Access control, Key agreement. Many articles were found using the specified search string, since the search string is not always present in the titles or abstracts, we searched the bodies of the digital sources to manually identify those articles.
3. Inclusion and exclusion criteria are presented in Table 3.

Table 3. Inclusion and exclusion criteria.

Criteria	Inclusion	Exclusion
Context	Articles consider IoT in the healthcare context.	Articles consider IoT in a different or general context.
Issue	Articles consider authentication as the main issue.	Articles consider other security requirements.
Purpose	Articles propose authentication schemes or improve previous ones.	Articles review authentication schemes or implement previous ones.

3.3. Article Search

The following digital sources were searched to search the related articles using the specified rules: Google Scholar, IGI, IEEE explore, Wiley, WoS, Springer, and Science Direct.

3.4. Article Selection

Figure 6 shows the selection phases and the number of input and output articles in each phase. The first phase scanned the titles of the articles according to the inclusion and exclusion rules. Then, in the second phase, we checked the articles' abstracts. In the last phase, we read the full text of the articles.

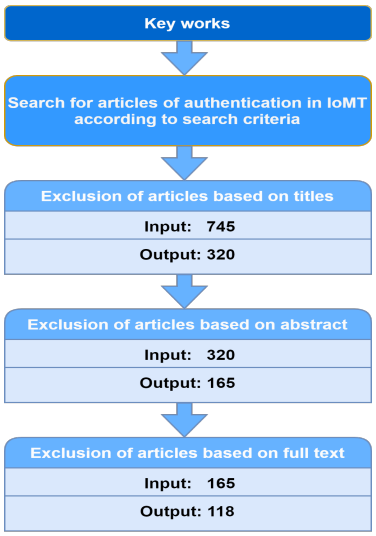

Figure 6. Article selection process.

3.5. Article Review

As shown in Figure 6, the review revealed 118 articles primarily related to authentication in IoMT. Those articles were thoroughly analyzed to discover the taxonomy perspectives.

3.6. Taxonomy

After reviewing the articles, we established a taxonomy of authentication in IoMT. The taxonomy is based on our deep analysis of the reviewed articles.

4. IoMT Authentication Taxonomy

IoMT authentication can be viewed from different perspectives. Figure 7 illustrates the IoMT authentication taxonomy's perspectives: authentication levels, architectures, credentials, procedures, categories, schemes, and preventing attacks. The perspectives are described in the following sections.

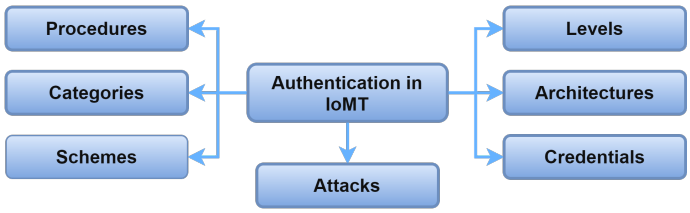

Figure 7. Taxonomy of authentication in IoMT.

4.1. Authentication Levels

Because IoMT systems are complex and distributed, it is challenging to propose generic authentication solutions for various IoMT systems nodes. Therefore, IoMT authentication is primarily considered at three levels: device-level, user-level, and network-level, as shown in Figure 8.

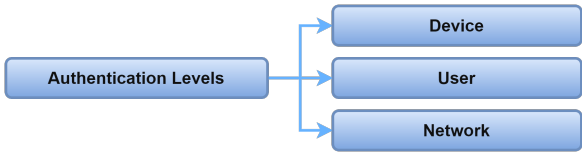

Figure 8. Authentication levels.

At the device level, authentication attempts to identify devices to the IoMT system [24–29]. Q. Wr et al. [30] developed an end-to-end protocol for authenticating resource-constrained IoMT devices. Using the Diffie–Hellman key establishment scheme, they offloaded the heavy security computation to the trusted neighboring nodes [30]. K. Park et al. [31] introduced a lightweight, provable, and secure scheme for IoT-healthcare systems. They developed a secure authentication protocol among sensor entities and servers using the non-verification table (NVT) technique.

Most of the reviewed papers considered user authentication in IoMT systems. The authentication at this level mainly attempts to identify and authenticate patients or healthcare providers at the application layer [32–35]. S. Aghili et al. [36] designed an energy-efficient scheme that supports key agreement, authentication, and access control mechanisms. It further preserves the doctors' and patients' privacy through the transfer of ownership. The transfer ownership technique prevents the old user from knowing the new user's identity. Y. Park [37] developed a selective-group technique for IoT authentication in the healthcare system. The group authentication scheme is based on a threshold mechanism to select users for authenticating them to IoMT.

At the network level, the communicating entities must register and authenticate users or devices to secure the overall IoMT network [38–41]. In [42], M. Fotouhi et al. considered both the user and sensor registration in the system while developing their authentication scheme. Moreover, R. Kumar and R. Tripathi [43] proposed a smart contract using blockchain. They adopted an interplanetary file system (IPFS) within the cluster which implements the smart contracts at the beginning of authenticating patients and the IoMT devices.

4.2. Authentication Architectures

Authentication in IoMT systems depends on either a centralized or decentralized architecture. Centralized authentication requires a centralized server to identify and authenticate the system entities. In contrast, the distributed architecture depends on multiple distributed nodes to accomplish the authentication process. Both the centralized and distributed architecture can be a flat or multi-level architecture. The flat architecture means the nodes are authenticated by authentication servers with the same roles. In a multi-level architecture, the authentication process is performed by authentication servers with different roles, according to their level of communication. That implies that the server at the lower level is used for authenticating nodes at the lower level. Figure 9 shows the authentication architectures for IoMT systems.

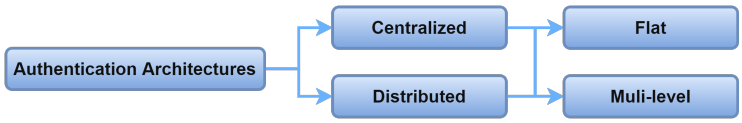

Figure 9. Authentication architectures.

Many researchers proposed robust, centralized authentication schemes by authentication servers in cloud-based IoMT systems [25,44–46]. They adopted a flat, centralized architecture where all nodes are authenticated through cloud-based authentication servers. Undoubtedly, the centralized server may have a high latency, which is unacceptable for time-sensitive IoMT systems [47,48]. Therefore, the flat, centralized architecture is not applicable for very large IoMT systems. In some studies [49–52], the authentication process is delegated to a smart gateway, near the IoMT devices, to identify and authenticate them.

Similarly, K. Renuka et al. [53] and P. Soni et al. [54] adopted the fog computing concept to establish a fog node responsible for authenticating IoMT devices. Moosavi et al. [55] proposed a user authentication method by decentralized gateways to release the medical devices from authentication activities. A large number of studies [49–55] are based on a multi-level centralized authentication architecture.

Multiple nodes are responsible for authenticating other nodes in the distributed authentication architecture. The concept of a distributed authentication architecture mainly depends on the blockchain technology [40,56–58]. M. Tahir et al. [57] presented a novel architecture for authentication in a blockchain-based IoMT system using a probability technique. N. Garg et al. [59] developed an authentication framework for IoMT environment using blockchain technology. It is called blockchain-based authenticated-key management (BAKMP). The framework ensures secure key-agreement for cloud servers, personal servers, and IoMT devices. M. Tahir et al. [57] and N. Garg et al. [59] used the flat distributed architecture because they adopted one blockchain platform for all of the IoMT nodes. In comparison, D. C. Nguyen et al. [58] proposed an authentication scheme called BEdgeHealth, which relies on a multi-level blockchain architecture. A local blockchain is deployed for authenticating the IoMT under the same cluster, and a global blockchain is deployed for authenticating the IoMT at different clusters.

4.3. Authentication Credentials

The authentication process asks for unique credentials from the entities to allow them to access the IoMT systems. This process can be performed through a third, trusted, party or directly between the communicating entities. Whatever the credentials used, it is necessary to consider their uniqueness, universality, and storability [60]. The credentials required for authentication are classified into four categories [61]. These types are depicted in Figure 10.

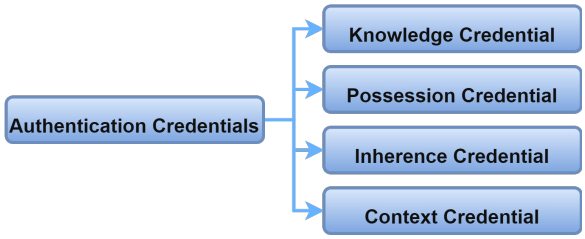

Figure 10. Authentication credentials.

Knowledge credentials refer to the information known by the entity, such as passwords, identification numbers, or user names. This type of credential is straightforward and does not need a technique for extracting its value. This authentication scheme facilitates cryptography, steganography, or shadow to hide such credentials [42,62–67]. F. Wu et al. [68] facilitated a dynamic pseudo-identity and a collision-resistant cryptographic function to hide users' identities. M. Hashim et al. [65] used three steganography-based random iterations to anonymize the patient's identity and authenticate him.

Possession credentials refer to the information possessed by the entity, such as a smart card or passport for user authentication, and radio waves for device authentication. The researchers in [25,44–46] used Radio-Frequency Identification (RFID) technology as a possession credential to identify devices anonymously and perform the authentication process. Other device authentication schemes used Physically Unclonable Function (PUF) to identify IoMT devices [49,52]. Authentication schemes in studies [35,69–74] required smart cards as credentials to identify the IoMT systems users. The possessed credential method requires a way to input its value and use it as an identifier [75].

Inherence credentials refer to something inherited by the entity, such as face/voice recognition, fingerprints, or all kinds of biometrics for user authentication. Currently, user authentication in the IoMT system primarily depends on the user's biometric informa-

tion [76–81]. A fuzzy extractor is adopted in studies [70,76] to provide unique and storable credentials through biometric authentication.

Context credential refers to something in the entity's context that can be used for authentication, such as location, time, or IP address. This kind of credential is the least adopted due to its low level of security, especially for healthcare applications. A good instance of context credential is the device's location, which can authenticate the related devices uniquely. A. Patwary et al. [82] developed a location-enabled authentication protocol utilizing fog computing and blockchain technology. Their scheme identifies a fog entity through its location and further connects a group of IoMT devices by a specific fog entity. That allows the IoMT system to authenticate fog entities and their related IoMT devices.

4.4. Authentication Procedures

The authentication in IoMT systems can be classified based on the direction of authenticating entities. The authentication procedure in the IoMT system can be one-way, two-way, and three-way [7]. Figure 11 shows the authentication procedure in the IoMT system.

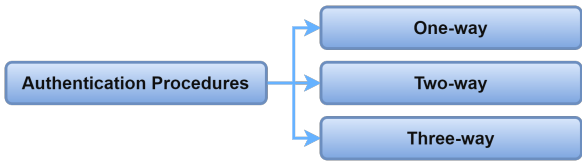

Figure 11. Authentication procedures.

Only one of the communicating entities is authenticated in a one-way authentication procedure. In other words, only one entity is identified to the other entity [83–85]. S. Aghili et al. [36] improved an authentication scheme where doctors authenticate themselves through the IoMT server to access patients' data. In studies [33,76,77], the researchers are concerned about the authentication of patients to the IoMT system through their biometric data.

Two-way authentication refers to the need for authenticating both entities to establish a communication channel [66,70,73,86–89]. The communicating entities are identified to each other to accomplish the authentication process. This authentication procedure is also known as mutual authentication. R. Hajian et al. [90] designed a two-way authentication protocol for communicating between devices and users where the change of biometrics and password is allowed without the involvement of a third party. P. Kumar et al. [91] developed a mutual authentication between a user and smart gateway within the Constrained application protocol (CoAP).

Both entities are authenticated using a third trusted entity in the three-way authentication procedure. The third entity can be centralized to establish authenticity of the system's various entities. These are called authentication servers [21,77,92–95]. The third entity also can be decentralized for authenticating a group of the system's entities [52,58,96].

4.5. Authentication Categories

The IoMT systems need a continuous feed of data from IoMT to look after the patient's situation. Accordingly, the IoMT systems need to authenticate those devices for a long period of time. IoMT authentication is classified into continuous and static from that perspective shown in Figure 12.

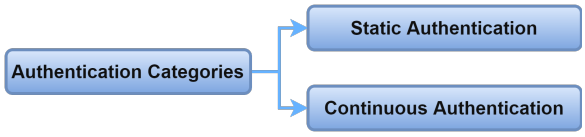

Figure 12. Authentication categories.

Static authentication is used to initiate a secure connection between entities. Once the authentication between entities is achieved, they can start communicating [97]. The entities stay authenticated as long as the connection exists, according to time passed, or according to other specified settings. Entities are authenticated once when the communication session starts. Therefore, this category is prone to many attacks which can capture active sessions such as hijacking attacks [4,98].

In contrast, continuous authentication is implemented repeatedly at every point in time. Even if an adversary impersonates the session, he needs to be authenticated continuously to the system. That guarantees better security for the IoMT system [99]. Continuous authentication cannot be substituted for static authentication; it is a complementary procedure [100,101]. A. Arfaoui et al. [24] considered context-aware authentication of IoMT devices. They proposed two schemes, one for normal situations and the other for emergent situations. The proposed schemes enhance the patient experience and avoid delays in emergent situations.

4.6. Authentication Schemes

Authentication in IoMT systems can depend on a basic, key-based, certificate-based, or cryptography-based scheme. Researchers have recently adopted hybrid schemes to improve system performance and security. Figure 13 shows a classification of authentication schemes.

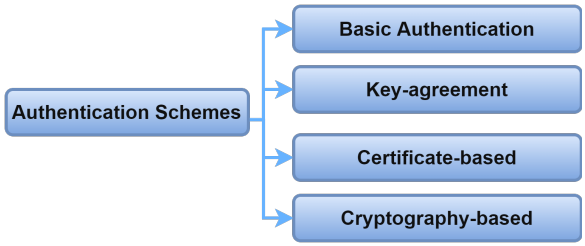

Figure 13. Authentication schemes.

4.6.1. Basic Authentication

In basic authentication, the credentials used to authenticate an entity are the factors used to identify that entity. The accuracy and efficiency of the authentication schemes will rely on how many factors are required to perform the authentication process. Figure 14 shows a classification of authentication schemes according to the number of factors involved in identifying entities for the IoMT systems. Usually, two factors are used for basic authentication; entities need to provide identification data and biometric information to access the IoMT system [50,72]. To enhance the security and make the problem of authentication harder for adversaries to compromise, many schemes depend on three factors by combining knowledge, inheritance, and possession credentials [53,54,88,102–104].

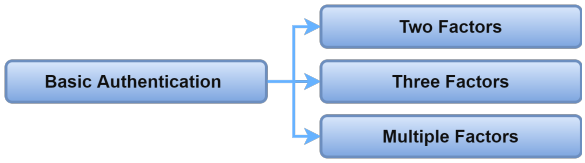

Figure 14. Basic Authentication.

Furthermore, P. Dhillon [78] used multiple factors such as smart card, user name, password, and biometric information for basic authentication. It is worth mentioning that some schemes facilitate a multi-mode of the same factor to identify an entity in IoMT systems. A multi-mode of the same factor means that the authentication factor may carry two values according to the predefined situation. In one study [24], the multi-mode factor is adopted to distinguish the emergency level of patients to enhance IoMT system response.

4.6.2. Authentication and Key Agreement

IoMT authentication can be achieved by creating a key shared between the communicating entities to ensure secure communication. Authentication protocols can adopt a simple key agreement where two entities negotiate upon a key to secure their communication [98,98,99]. G. Mwitende et al. [105] proposed a key agreement between two entities with a blind signing mechanism based on blockchain technology. On the other hand, authentication protocols can adopt a group key agreement [106,107]. Group-key agreement protocols require more than two entities to generate a group-key such that anyone of these entities can use it for communication [105]. Figure 15a shows the key agreement classification.

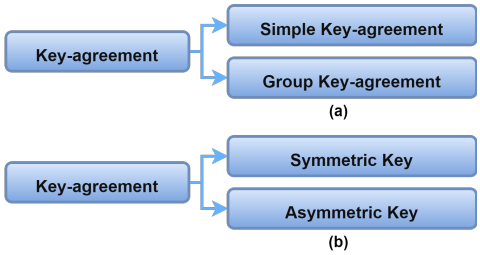

Figure 15. (**a**,**b**) Key agreement scheme.

Moreover, keys can be classified according to the type of shared key, either symmetric or asymmetric (see Figure 15b). In symmetric key-based authentication schemes, entities employ the same key for encrypting and decrypting data. C. Chunka et al. [108] developed a symmetric key agreement scheme where entities use the same key for encrypting their messages, which is more lightweight for the IoMT environment. J. Xu et al. [80] designed a streaming data authentication technique for the IoMT system using symmetric key agreement. In asymmetric key agreement, different keys are used for encrypting and decrypting authentication messages between entities. The researchers of [109,110] supported cross-domain authentication through asymmetric key a greement.

4.6.3. Certificate-Based Authentication

The authentication schema in IoMT can depend on using a certificate to identify legitimate entities. Accordingly, authentication schemes may require a hard certificate, soft certificate, implicit certificate, or no certificate for identifying entities, see Figure 16. Most of the authentication literature in the IoMT environment suggests a hard certificate to accomplish the authentication process. A smart card is a hard certificate used to authenticate users in the IoMT system [73,92]. Similarly, an RFID chip is used to authenticate IoMT devices uniquely by providing it as a device identifier [25,44–46]. A hard certificate also requires to be validated and signed by a reliable party. The second type of certificate is a soft certificate, or a digital certificate that refers to a token that requires to be validated by a reliable party [111,112]. The reliable party is called a certificate authority (CA) or a delegated entity.

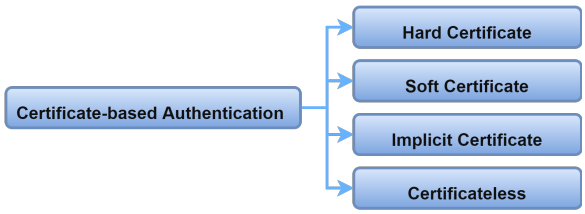

Figure 16. Certificate-based authentication.

Implicit certificate-based authentication schemes are more lightweight than soft and hard certificates. The advantages of implicit certificates over explicit certificates (i.e., soft

and hard certificates) include fast processing, small size, and no need for verification from a trusted party [113]. The Digital Signature Algorithm (DSA), and the Elliptic Curve Digital Signature Algorithm (ECDSA) operate as examples of the implicit certificate [32,43,91]. Elliptic Curve Qu–Vanstone (ECQV) is also an implicit certificate that offers faster processing and less certificate storage for generating certificates. S. Moosavi et al. [55] adopted a suitable IP security solution for IoMT since it relies on a certificate-enabled DTLS scheme. J. Alzubi [56] designed an authentication technique to identify IoMT devices to users through the blockchain-based Lamport–Merkle scheme for generating and verifying the implicit certificate.

For enhancing lightweight authentication in the IoMT environment, there is a recent focus on adopting certificateless schemes. The researchers in [114] proposed a lightweight certificateless authentication method that depends on an aggregated-signature and pairing-free scheme in the IoMT system. They exploited an aggregation mechanism that does not use pairings, thus reducing the communication and computation transmission overhead. G. Mwitende et al. [115] developed a certificateless-based authenticated key agreement (CALKA). CALKA releases the IoMT system from the burden of certificate storage and management.

4.6.4. Cryptography-Based Authentication

Currently, cryptography is an essential part of authentication, and various cryptography techniques offer a good opportunity to empower IoMT security. Figure 17 illustrates different cryptographic-based authentication schemes. Cryptographic-based authentication commonly uses a hash function, which is efficient for resource-constrained IoMT devices [116]. H. Khemissa et al. [28] adopted a keyed-hash authentication message code (HMAC) calculated by an iterative hash function such as SHA-1 or MD5.

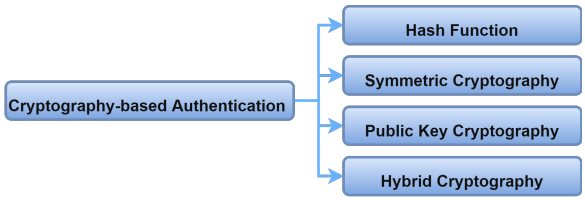

Figure 17. Cryptography-based authentication.

In the IoMT environment, many researchers adopted symmetric cryptography, such as Data Encryption Standard (DES) and advanced encryption standard (AES) [106,117]. T. Le and C. Hsu [106] proposed authentication in IoMT based on AES and a bio-hash function to improve the cryptographic scheme. In [118], K. Quist-Aphetsi et al. improved real-time access to IoMT devices through a Diffie–Hellman shared key DES for credential encrypting. G. Srivastava et al. [119] used another symmetric technique, called Addition/Rotation XOR (ARX), to support lightweight cryptography for IoMT devices.

Asymmetric cryptography, also known as the public-key technique, recently gained attention. Rivest–Shamir–Adleman (RSA) is a public-key cryptography that adopts two types of keys: one is called a public-key, and the other used as a signature is called a private-key [120]. The investigation clarifies that RSA has a higher level of security than the AES and DES techniques [29]. However, Elliptic Curve Cryptography (ECC) offers similar level of security as RSA and less storage requirement [2,6]. Therefore, most of reviewed authentication schemes adopted ECC, which supports small keys and certificates [22,34,48,99–104,114]. In the same direction, S. Moosavi et al. [55] used an elliptic curve Diffie–Hellman (ECDHE) scheme for generating keys, as well as ECDSA for authenticating entities.

Recently, it has become popular to combine multiple techniques for cryptography to increase the security level. This is referred to as hybrid cryptography. That combination of more than one technique overcomes the shortcomings of depending on one technique. B.

Fadi et al. [77], V. Gaikwad et al. [121], and B. Deebak et al. [122] adopted a hybrid authentication method through Chaotic-Map. Furthermore, R. Mahendran, P. Velusamy [76] and T. Lu et al. [87] accomplished authentication through fuzzy extractor and hash functions.

4.7. Authentication Attacks

The main purpose of adopting authentication schemes in IoMT is to ensure that only authorized users and devices are enabled to use system resources and services. Therefore, it is necessary to test the authentication schemes against attacks that succeed in getting unauthorized access to IoMT systems. Figure 18 shows the widespread attacks used in IoMT authentication. Those attacks are shown as being prevented in different ways in the literature, according to the proposed authentication scheme.

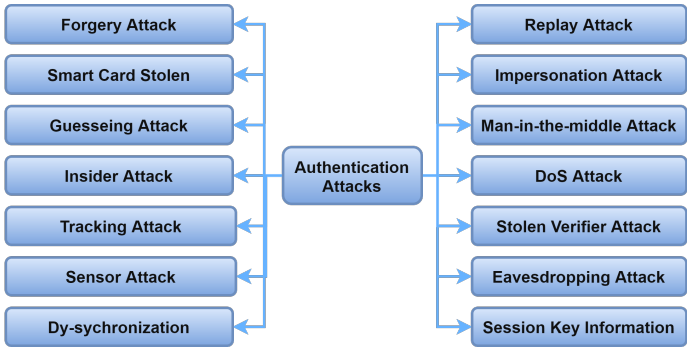

Figure 18. Authentication attacks.

M. Fotouhi et al. [42] combined long and short term parameters to securely create and share a key of the communication session.

That combination avoids compromising the session key information. R. Hajian et al. [90] developed an authentication scheme that resists guessing and privileged insider attacks. To pass the authentication process successfully, the adversary must guess three double-hashed values. Therefore, guessing an attack is impossible. Furthermore, to avoid privileged insider attacks, the network entities cannot access the security parameters and make even slight changes due to the time stamp technique. F. Wu et al. [68] utilized a dynamic pseudo-identity for authenticating entities to each other. The technique prevents forging messages between entities and improves security for tracking and sensor capture attacks.

DoS is common within IoT environments due to the use of resource-constrained sensors. The method proposed by V. Sureshkumar et al. [69] proves its resistance to Denial of Service attack (DoS). The scheme is based on request–response communication and timestamp techniques; the user needs to obtain a time-stamped confirmation from the sensor to be connected. That means that the DoS attack is not simply accomplished. The scheme of P. Bhuarya et al. [123] provides anonymous authentication of entities based on the Elliptic Curve Computational Diffie–Hellman schema (ECCDHP). That implies that impersonating entities is not possible, and impersonation attacks can be identified easily. Furthermore, using random session numbers and timestamps ensures synchronized communication and avoids de-synchronization attacks. R. Kumar and R. Tripathi [43] designed and improved a scheme that leverages a transaction-based blockchain. The verified transactions are stamped by time and identifier; therefore, replay attempts are unlikely to succeed.

A. Das's scheme [88] provides tolerance against the man-in-middle (MIM) Attack. The scheme uses a temporal credential so that the adversary cannot exploit the communication even if he knows other private credentials for both communicating entities. Moreover, the proposed scheme does not rely on credentials provided during the authentication process to derive the verifier. The scheme has been successfully tested against verifier stolen attacks. In the same direction, M. Tahir et al. [57] developed a blockchain-enabled technique for IoMT authentication using cryptographic random values to avoid MIMA

and eavesdropping attacks. For eavesdropping attack, the adversary attempts to build a weak connection between entities. A. Das et al.'s scheme [71] is based on smart card authentication. Although using a smart card is vulnerable to theft, the proposed scheme also requires the users' biometric information to verify their authentication.

5. Review Findings

This section presents some findings of the literature review analysis based on the taxonomy perspectives. Figure 19 reveals the articles distribution based on scientific sources. The pie chart emphasizes that most of the reviewed articles published in Springer link with 35%, followed by IEEE with 31% of articles. Nineteen percent of the articles were published in Science Direct, and about 14% were published in different scientific databases.

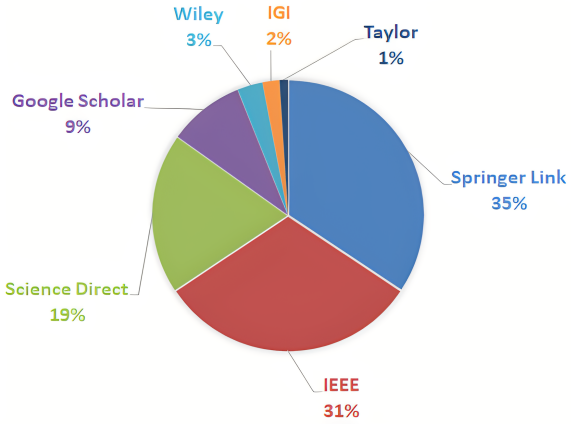

Figure 19. Article distribution based on scientific sources.

As illustrated in Figure 20, there is a focus on user-level authentication. That focus implies that the essential role of the authentication scheme is to secure the end-user applications since such applications are the first gateway to access IoMT systems. Beginning in 2016, the research efforts started focusing on the network level, and these have gradually increased. The researchers realized the need for authenticating all of the communicating entities on the network, whatever their computation and storage capacities. The device-level authentication is of concern in 20% of the reviewed articles. The device authentication is strongly related to resource-constrained IoMT devices. Consequently, the development of device authentication methods requires particular considerations.

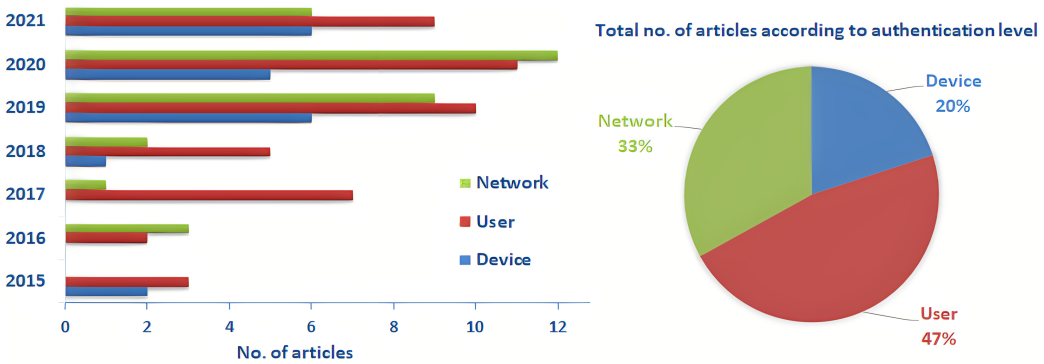

Figure 20. Article distribution based on the authentication level.

The article distribution showed that a centralized authentication architecture is mostly adopted for authentication schemes. That can be explained by the nature of the healthcare field, where patient privacy is highly prioritized. Privacy is fully achieved by keeping the information at centralized entities. The centralized architecture ensures that the patient credentials are kept under the control of a centralized authority responsible for the patient's

privacy. Moreover, the centralized architecture ensures high governing of healthcare standards.However, the distributed authentication architecture has become more common in the last three years, see Figure 21.That refers to the maturity of distributed security solutions such as blockchain and edge computing. Blockchain technology offers high anonymity, transparency, and privacy, encouraging researchers to adopt this distributed architecture. The patient's privacy is highly supported through an anonymous blockchain network. In 2021, the need to address scalability, coordination, and data management of the distributed architecture became the main issue of the reviewed articles.

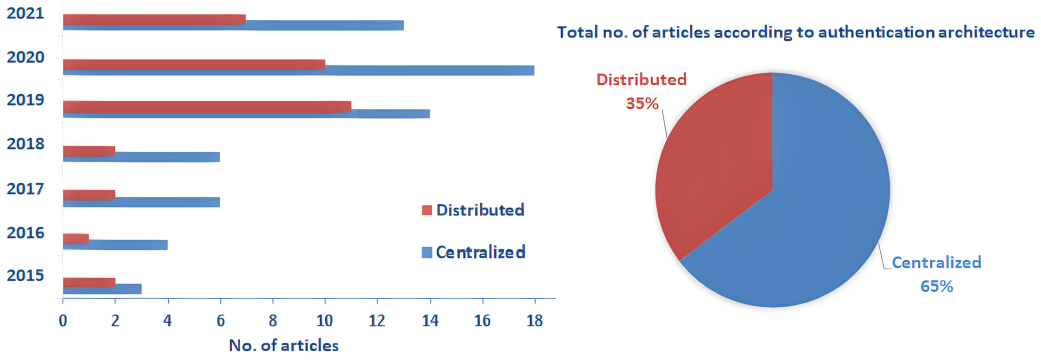

Figure 21. Article distribution based on authentication architecture.

The frequency distribution of reviewed articles confirms that the symmetric key approach was not commonly used for authentication in the IoMT context. That referred to the low-security level of using symmetric keys within highly distributed systems. In contrast, the asymmetric key approach was mainly used for IoMT authentication systems. Asymmetric key-based authentication schemes offer high security since the communicating entities do not need to share the same keys to authenticate each other. From 2019 on, almost all articles suggested the asymmetric key approach for securing their authentication schemes as shown in Figure 22.

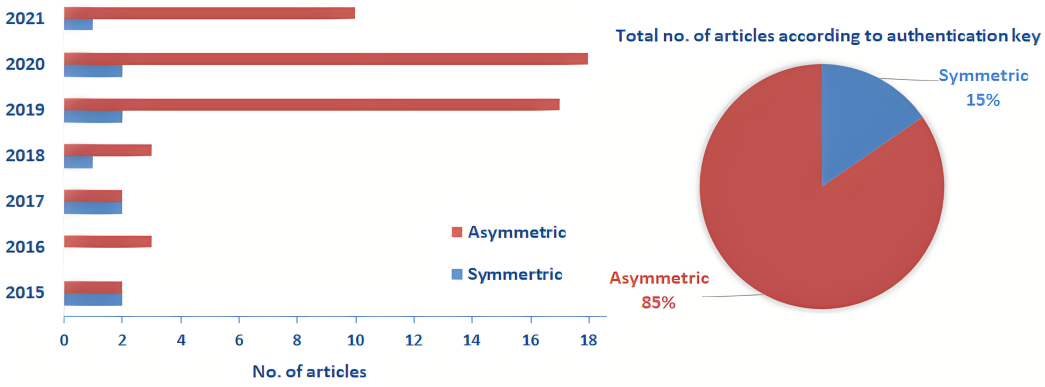

Figure 22. Article distribution based on authentication key.

The analysis of articles reveals that about 40% of them adopted the public-key cryptography approach, as shown in Figure 23. That implies that public-key cryptography provides good security and robust authentication in a distributed IoMT environment. In addition, hash cryptography is primarily integrated with the public key approach for the authentication schemes. About one-third of the articles discussed using hash cryptography to secure the sharing of authentication credentials. The hybrid cryptography approach became popular in articles published from 2019 to 2021. The hybrid approach integrates more than one cryptography approach, which increases the robustness of the authentication schemes. However, the adoption of the hybrid approach is not straightforward in the IoMT context, because it requires a high computation and storage capacity.

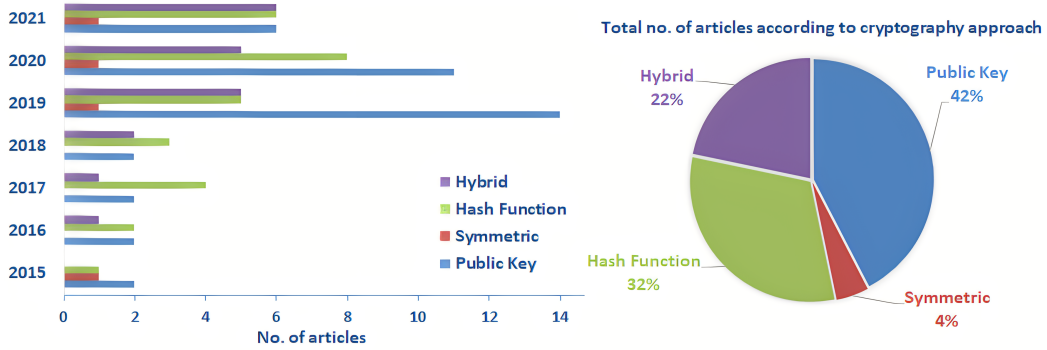

Figure 23. Article distribution based on cryptography approach.

There are many ways to evaluate the proposed authentication schemes for performance parameters. Many researchers implemented different schemes through programming and prototyping [28,112]. Moreover, the research experiments can be conducted using performance testing of the amount of memory required, the number of steps for authentication, and the amount of CPU time required. By reviewing the literature, the evaluation process is mainly based on scheme simulation. The popular simulation tools are shown in Figure 24.

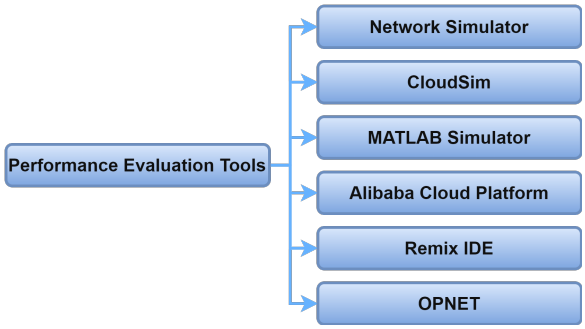

Figure 24. Performance evaluation tools for authentication schemes.

One of the popular tools for evaluating authentication schemes in IoMT environments is called Network Simulator (NS). It is useful for education and research since it is based on discrete-event simulation [24,31,46,68,75,81,95,124,125]. J. Alzubi [56], B. Deepshikha, and S. Chauhan [83] took advantage of the CloudSim tool to evaluate their proposed authentication schemes. CloudSim is a modeling and simulation framework used to test cloud infrastructure and services that are not only used for education and research. MATLAB Simulator is a model-based tool where a researcher needs to design a mathematical model for the proposed authentication scheme [76,85,126]. It is a powerful tool since it generates codes automatically, depending on the predefined model. X. Jia et al. [96] used the Elastic Compute Service (ECS) host offered by the Alibaba Cloud platform. The Alibaba platform helped them to simulate their proposed cloud server and fog nodes authentication method in an IoMT system. B. Egala et al. [43] used Remix IDE as a powerful tool to simulate their smart contracts through the Solidity programming language. M. Fotouhi et al. [42] demonstrated the performance of their proposed authentication scheme through the OPNET simulator network tool.

Using one simulation tool rather than the other is related to the researcher's preferences and background experience with a particular tool. Therefore, the distribution frequency of articles shows the spread of usage percentages among different tools. However, the network simulator records the highest percentage with 16%. Figure 25 shows the article distribution based on the use of evaluation tools.

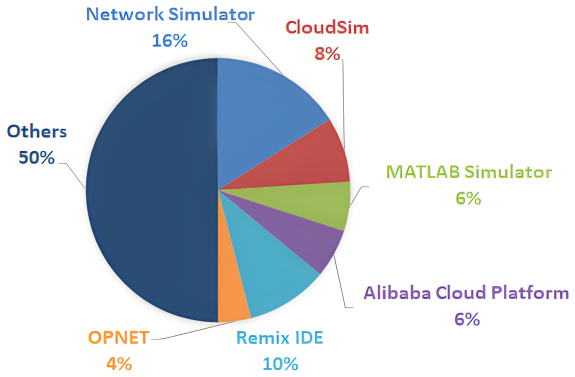

Figure 25. Article distribution based on evaluation tools usage.

The evaluation of authentication schemes for IoMT is conducted primarily for three performance parameters: computation, communication, and storage overhead. The evaluation of computation overhead relies on the extent to which authentication schemes are lightweight in terms of time as related to any resource-constrained IoMT environment. Therefore, less time is required to achieve the authentication process, which implies less cost and a more lightweight authentication scheme. To enhance the authentication scheme for communication overhead, the data pass among entities must be as least as possible. The storage overhead refers to the memory needed to accomplish the authentication process. Storage overhead is a vital parameter to evaluate authentication schemes because of the limited storage capacity of the IoMT devices. Table 4 briefly compares computation, communication, and storage overhead among the recently proposed IoMT authentication schemes. The values of Table 4 indicate the evaluation results on the terminal side.

Table 4. Comparison among recent authentication schemes according to their performance parameters.

Ref.	Year	Scheme	Computation	Communication	Storage
Z. Mahmood et al. [95]	2017	ECC	0.0087 ms	480 bits	480 bits
X. Li et al. [121]	2018	ECC	0.00602 ms	480 bits	1456 bits
R. Ali and A Pal [77]	2018	Hash function	1.0610 s	1504 bits	3008 bits
K. Sowjanya et al. [127]	2019	ECC	92.035 ms	3456 bits	1408 bits
Z. Xu [66]	2019	Hash function	0.0624 ms	3904 bits	1280 bits
X. Yang et al. [113]	2019	ECDH	3.17 ms	1280 bits	1472 bits
T. Wu et al. [96]	2021	Hash function	196.02 ms	7744 bits	640 bits
K. Sowjanya et al. [128]	2021	ECC	6.6968 ms	4640 bits	1568 bits
T. Le et al. [106]	2021	AES, Biohash	0.00744 ms	1280 bits	1824 bits
J. Li et al. [92]	2021	Hash function	5.312 ms	98 bytes	289 bytes
T. Liu et al. [87]	2021	Hash function, fuzzy extractor	0.6663 ms	1280 bits	640 bits
S. Nashwan [129]	2021	Hash function	0.51712 s	13984 bits	256 bits

Many techniques and tools are available for validating the security properties of authentication schemes. The Automated Validation of Security Applications and Protocols tool (AVISPA) is widely employed for such a purpose. It is based on an expressive formal language, and many back-ends, to automatically analyze application and protocol security properties [31]. Scyther is another verification tool for testing the sensitivity of Internet protocols to security properties. It is designed as a framework to model adversaries for analyzing a protocol's security [130]. It simulates a basic Dolev–Yao threat model, and also more powerful adversary models [24]. Another verification tool is a protocol verifier called ProVerif. It offers cryptanalysis primitives such as public-key, symmetric, hash functions, Diffie–Hellman signatures, and key agreements [131]. Cryptanalysis primitives are designed as equations or rules [132]. The Random Oracle Model (ROM) provides rigid security proofing for cryptographic-based schemes [133]. Random Oracle is employed to simulate the hash function and present all possible hash results. All entities, either legitimate or not, have to query the Random Oracle for the hash value. Burrows–Abadi–Needham (BAN) logic is a collection of rules to evaluate protocols against predefined security theories. BAN logic explicitly allows its users to decide if the information shared

is trusted and secure [134]. BAN logic begins with the presumption that data transfers on media are vulnerable to public monitoring. Figure 26 illustrates the usage distribution of security validation tools. Commonly, researchers use more than one tool or technique to prove an authentication scheme's security. Therefore, the numbers in Figure 26 are overlapped. Using BAN logic for analysis of authentication schemes increased due to its reliable security proofing. Scyther and AVISPA tools are commonly used beside BAN logic, because they offer powerful predefined threat models and ease of user interfaces. Table 5 shows an overall comparison among authentication schemes according to the taxonomy.

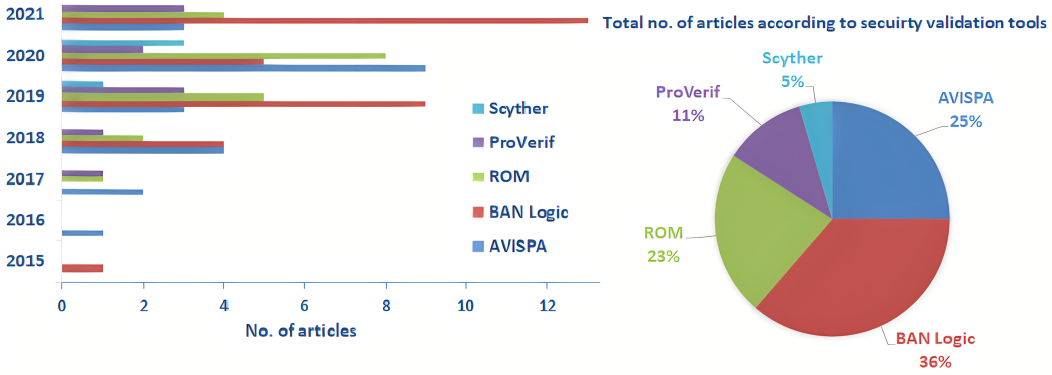

Figure 26. Article distribution based on security validation tools usage.

Table 5. Comparison of authentication schemes based on the taxonomy.

Ref.	Source	Year	Purpose	Level	Procedure	Performance Evaluation	Evaluation Parameters	Cryptography Approach	Key-Based	Security Validation
[46]	Springer link	2016	RFID-based authentication for healthcare in mobile vehicular applications	Network	Two-way	NS-2 simulator	Computation overhead, complexity, and service delivery.	ECC	Asymmetric	Informal
[68]	Science Direct	2017	A lightweight, and robust two-factor authentication for personalized healthcare systems in wireless-sensor networks	Network	Two-way	NS-3	Delivery ratio, throughput, delay, communication cost, practicality	Dynamic Pseudo-identity	Symmetric	Informal, Proverif tool
[95]	Google scholar	2017	Authentication framework for pervasive healthcare services	User	Three-way	NS-2 simulator	Communication computation, storage overhead	ECC	Asymmetric	Informal
[121]	Springer link	2018	Efficient, anonymous, and secure authentication in mobile three-tier healthcare with wearable medical devices	Network	Three-way	SPAN animator software	Communication computation, storage overhead	ECC	Asymmetric	Informal, BAN logic, AVISPA
[93]	Springer link	2019	Authenticated key agreement for healthcare systems in fog-based IoT network	Network	Three-way	Alibaba Cloud platform	Computation and communication costs	Bilinear pairings	Asymmetric	Informal and formal proof
[69]	Science Direct	2019	Robust and secure authentication protocol with the implementation of Field-Programmable Gate Array in healthcare applications	Network	Two-way	Altera Quartus II simulation	Computation and communication overhead	ECC	Asymmetric	Informal. BAN logic
[24]	Science Direct	2019	Anonymous and context-aware authentication protocol for IoT-healthcare systems	Device	One-way	NS2 2.35 simulator	Computation and communication overhead, energy consumption	Unlikable shadow-IDs	Symmetric	Informal, BAN logic, ROR, Scyther tool
[75]	IEEE	2019	Authentic-enabled privacy scheme for smart-healthcare applications using IoT	User	Two-way	NS-3 simulator	end-to-end delay, throughput rate, routing, and delivery ratio overhead	ECC	Asymmetric	Informal, ROM, BAN logic
[42]	Science Direct	2020	Two-factor authentication for healthcare services in wireless medical-sensor networks	Network	Two-way	OPNET	Computation and communication overhead	Hash function	N/A	ROR, Proverif

Table 5. *Cont.*

Ref.	Source	Year	Purpose	Level	Procedure	Performance Evaluation	Evaluation Parameters	Cryptography Approach	Key-Based	Security Validation
[124]	Springer link	2020	Chaotic-map authentication scheme with preservation of privacy for IoMT	Network	Three-way	NS-3 simulator	Transmission delay, throughput, computation cost, and time	Chaotic-map	Asymmetric	ROM, informal
[81]	Science Direct	2020	Session key-based and privacy authentication for IoMT-based networks	Network	Three-way	NS-3 simulator	Throughput, delay	Hash function	N/A	Informal, AVISPA, BAN logic
[41]	Google scholar	2020	Improved authentication for IoT-enabled smart-healthcare applications	Network	Three-way	Netbeans IDE 6.8	Communication and computation costs	ECC	Asymmetric	Informal, AVISPA tool
[31]	IEEE	2020	Secure, lightweight, and provably authentic-based key agreement without the need for a table of verification for IoMT	User, Device	Three-way	NS-2 simulator	Communication and computation overhead	Hash function	N/A	AVISPA, BAN logic, ROR
[112]	IEEE	2020	Blockchain-enabled model for sustainable and trust IoT-healthcare IoT application	Device	Two-way	Prototype using ripple chain	Scalability, authentication, availability, interoperability, confidentiality, integrity, privacy	ECC	Asymmetric	N/A
[126]	IEEE	2020	Effective blockchain-enabled access control for privacy assurance in IoMT	Device	Two-way	Remix IDE	Communication and computation, overhead	ECC	Asymmetric	Scyther tool
[43]	Springer link	2021	Design of blockchain-enabled security framework for IoMT with interplanetary file-system	Network	Two-way	node.js, solidity and remix IDE	Computation time and cost	ECDSA	Asymmetric	Informal
[73]	IEEE	2021	Two-way authentication for IoMT in cloud-based healthcare	Network	Two-way	FPGA and Moteiv TMote Sky-Mote	Communication and computation overheads	Hash function	N/A	Informal, BAN logic

6. Open Issues and Future Directions

IoMT systems are subject to many vulnerabilities because of their reliance on the distributed resource-constrained devices that cannot handle heavy security solutions. Moreover, IoMT devices are accessible online, which can be easily breached. Therefore, the need for considering those challenges in a robust and lightweight authentication scheme is persistent. Although the researchers may prove their secure and lightweight authentication schemes within the IoMT environment, there remain open issues. This section highlights some of them as follows:

- Cross-domain authentication: It implies that the authentication scheme can authenticate entities from their trusted domain. Cross-domain authentication has become an urgent need since integrating multiple healthcare applications has become popular.
- Cross-layer authentication: The concept of cross-layer authentication must be supported for improving the security of the authentication process within IoMT networks. Cross-layer authentication ensures that all entities involved in communication at different layers are authenticated to each other. This issue requires a comprehensive authentication scheme to support layered IoMT architecture.
- Scalability: Since IoMT is the building block of today's smart healthcare applications, it has become massive and highly distributed. Authentication solutions need to cope with such improvements by supporting the scalable schemes. A scalable scheme refers to adding IoMT entities as required without sacrificing the system's performance. Many researchers attempted to handle scalability issues through a decentralized authentication scheme. However, those schemes require high governance and privacy standards, especially for healthcare applications.
- Adjustability: It is the ability of an authentication scheme to be adjusted in response to changes in the IoMT network. It is a challenging task for a static authentication scheme. Therefore, a continuously developing authentication scheme will gain more research attention in the next few years. Furthermore, context-aware authentication schemes need a research focus to improve the response to the changing performance of IoMT networks.
- Anonymity: This issue relates to the cryptographic-based scheme where entities are authenticated anonymously. This scenario implies full-anonymity where it is easy for an exploited entity to access the system's resources without discovering its identification. For the majority of IoMT use cases, partial anonymity supported by some authentication schemes is adequate for keeping privacy acceptable.
- The number of exchanged messages: The authentication scheme performance is affected by the number of messages required to achieve the authentication task. Consequently, it is necessary to reduce the number of exchanged messages to support real-time authentication for entities within time-sensitive healthcare applications such as remote monitoring healthcare services. This issue seems easy to accomplish, but the trade-off here is to reduce the number of messages and keep a high level of security.
- Re-authentication: It is more efficient to authenticate IoMT entities only once to reduce communication overhead. However, this can affect the security level of the overall system. Many research efforts intended to balance the communication overhead and the re-authentication need by delegating the re-authentication process to the edge entities instead of relying on a centralized authentication server.
- User-friendly authentication: This issue is subject to quality assurance in smart healthcare applications where their stakeholders are not interested in the latest technological techniques for security. The authentication scheme for such an application requires considering a straightforward process, and keeping the same level of security for the IoMT systems.

7. Conclusions

Highly heterogeneous IoMT devices create voluminous data that must be accessible to only authorized users. The connecting of millions of IoMT devices rapidly expands the

possible vulnerabilities. Building robust, lightweight authentication is not straightforward in a large-scale, diverse and resource-constrained IoMT context. Many researchers intended to develop authentication schemes that are potentially different from one another and adapted to various IoMT applications. This paper conducted a systematic review of authentication schemes in IoMT. About 118 articles were analyzed to establish an exhaustive authentication taxonomy. The authentication schemes were reviewed from seven perspectives: authentication levels, architectures, credentials, procedures, categories, schemes, and preventing attacks. Review findings showed that the authentication schemes proposed in the literature mainly depended on the distributed architecture and public key infrastructure. In addition, the adoption of hybrid cryptography approaches has also become popular to overcome the shortcomings of a single cryptographic approach. In conclusion, authentication schemes need to go beyond identifying IoMT entities to the system. Authentication schemes need to support scalability, end-to-end, cross-layer, and cross-domain IoMT authentication.

Author Contributions: Conceptualization, N.A.; preparation, N.A.; writing original draft, N.A.; editing, F.N.; review, F.N.; supervision, F.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Institutional Fund Projects under grant number D-128-611-1443.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This research work was funded by Institutional Fund Projects under grant no. (D-128-611-1443). Therefore, the authors gratefully acknowledge technical and financial support from Ministry of Education and Deanship of Scientific Research (DSR), King Abdulaziz University (KAU), Jeddah, Saudi Arabia.

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

References

1. Mamdouh, M.; Awad, A.I.; Khalaf, A.A.; Hamed, H.F. Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions. *Comput. Secur.* **2021**, *111*, 102491. [CrossRef]
2. Alsubaei, F.; Abuhussein, A.; Shandilya, V.; Shiva, S. IoMT-SAF: Internet of Medical Things Security Assessment Framework. *Internet Things* **2019**, *8*, 100123. [CrossRef]
3. 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 Island, Greece, 29–31 May 2019; pp. 457–464. [CrossRef]
4. Liyanage, M.; Braeken A.; Kumar, P.; Ylianttila, M. *IoT Security: Advances in Authentication*; John Wiley and Sons: Hoboken, NJ, USA, 2020.
5. Trnka, M.; Cerny, T.; Stickney, N. Survey of Authentication and Authorization for the Internet of Things. *Secur. Commun. Netw.* **2018**, *2018*, 4351603. [CrossRef]
6. Albalawi, A.; Almrshed, A.; Badhib, A.; Alshehri, S. A Survey on Authentication Techniques for the Internet of Things. In Proceedings of the 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 3–4 April 2019; pp. 1–5. [CrossRef]
7. Science, C. A Survey on the Authentication Techniques in Internet of Things. In Proceedings of the 2020 IEEE International Students' Conference on Electrical,Electronics and Computer Science (SCEECS), Bhopal, India, 22–23 February 2020.
8. Gamundani, A.M.; Phillips, A.; Muyingi, H.N. An Overview of Potential Authentication Threats and Attacks on Internet of Things(IoT): A Focus on Smart Home Applications. In Proceedings of the IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 50–57.
9. El-Hajj, M.; Chamoun, M.; Fadlallah, A.; Serhrouchni, A. Taxonomy of authentication techniques in Internet of Things (IoT). In Proceedings of the IEEE 15th Student Conference on Research and Development (SCOReD) Wilayah Persekutuan Putrajaya, Malaysia, 13–14 December 2017; pp. 67–71. [CrossRef]
10. Ferrag, M.A.; Maglaras, L.A.; Janicke, H.; Jiang, J.; Shu, L. Authentication Protocols for Internet of Things: A Comprehensive Survey. *Secur. Commun. Netw.* **2017**, *2017*, 6562953. [CrossRef]

11. Kavianpour, S.; Shanmugam, B.; Azam, S.; Zamani, M.; Narayana, Samy, G.; De Boer, F. A systematic literature review of authentication in Internet of Things for heterogeneous devices. *J. Comput. Netw. Commun.* **2019**, *2019* 5747136. [CrossRef]
12. Saadeh, M.; Sleit, A.; Qatawneh, M.; Almobaideen, W. August. Authentication techniques for the internet of things: A survey. In Proceedings of the Cybersecurity and Cyberforensics Conference (CCC), Amman, Jordan, 2–4 August 2016. [CrossRef]
13. Thierre, W.; De Lima, S.; Ferraz, F.S. Authentication and the Internet of Things. In Proceedings of the The Twelfth International Conference on Software Engineering Advances (ICSEA), Athens, Greece, 8–12 October 2017; pp. 34–40.
14. El-Hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A Survey of Internet of Things (IoT) Authentication Schemes. *Sensors* **2019**, *19*, 1141. [CrossRef] [PubMed]
15. Mehta, M.; Patel, K. A review for IOT authentication–current research trends and open challenges. *Mater. Today Proc.* 2020, *in press*.
16. Shu, N.; Phwhu, V.; Ri, D. A Review on Authentication Protocol and ECC in IOT. In Proceedings of the 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 4–5 March 2021.
17. Sundaravadivel, P.; Kougianos, E.; Mohanty, S.P.; Ganapathiraju, M.K. Everything You Wanted to Know about Smart Health Care: Evaluating the Different Technologies and Components of the Internet of Things for Better Health. *IEEE Consum. Electron. Mag.* **2017**, *7*, 18–28. [CrossRef]
18. Koutras, D.; Stergiopoulos, G.; Dasaklis, T.; Kotzanikolaou, P.; Glynos, D.; Douligeris, C. Security in IoMT Communications: A Survey. *Sensors* **2020**, *20*, 4828. [CrossRef]
19. Hemanth, J.A.D.J.; George, A. *Internet of Medical Things: Remote Healthcare Systems and Applications*; Springer: Berlin/Heidelberg, Germany, 2021.
20. Alsaeed, N.I.; Aldahwan, N.S. Ubiquitous Health Care Monitoring Services (UHCMS): Review of Opportunities and Challenges. *Int. J. Comput. Appl.* **2020**, *975*, 8887. [CrossRef]
21. Kumar, T.; Braeken, A.; Jurcut, A.D.; Liyanage, M.; Ylianttila, M. AGE: Authentication in gadget-free healthcare environments. *Inf. Technol. Manag.* **2019**, *21*, 95–114. [CrossRef]
22. Pradhan, B.; Bhattacharyya, S.; Pal, K. IoT-Based Applications in Healthcare Devices. *J. Health Eng.* **2021**, *2021*, 6632599. [CrossRef] [PubMed]
23. Alsubaei, F.; Abuhussein, A.; Shiva, S. Security and privacy in the internet of medical things: taxonomy and risk assessment. In Proceedings of the 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), Singapore, 9 October 2017; pp. 112–120.
24. Arfaoui, A.; Kribeche, A.; Senouci, S.-M. Context-aware anonymous authentication protocols in the internet of things dedicated to e-health applications. *Comput. Netw.* **2019**, *159*, 23–36. [CrossRef]
25. Aghili, S.F.; Mala, H.; Kaliyar, P.; Conti, M. SecLAP: Secure and lightweight RFID authentication protocol for Medical IoT. *Futur. Gener. Comput. Syst.* **2019**, *101*, 621–634. [CrossRef]
26. Chatterjee, U.; Sadhukhan, D.; Ray, S. *An Improved Authentication and Key Agreement Protocol for Smart Healthcare System in the Context of Internet of Things Using Elliptic Curve Cryptography*; Springer: Singapore, 2020. [CrossRef]
27. Alzahrani, B.A.; Irshad, A.; Albeshri, A.; Alsubhi, K. A Provably Secure and Lightweight Patient-Healthcare Authentication Protocol in Wireless Body Area Networks. *Wirel. Pers. Commun.* **2020**, *117*, 47–69. [CrossRef]
28. Khemissa, H.; Tandjaoui, D. A Lightweight Authentication Scheme for E-Health Applications in the Context of Internet of Things. In Proceedings of the 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, UK, 9–11 September 2015; pp. 90–95.
29. Palve, A.; Patel, H. Towards securing real time data in IoMT environment. In Proceedings of the 2018 8th International Conference on Communication Systems and Network technologies (CSNT), Bhopal, India, 24–26 November 2018; pp. 113–119.
30. Iqbal, M.A.; Bayoumi, M. Secure End-to-End key establishment protocol for resource-constrained healthcare sensors in the context of IoT. In Proceedings of the 2016 International Conference on High Performance Computing & Simulation (HPCS), Innsbruck, Austria, 18–22 July 2016; pp. 523–530.
31. Park, K.; Noh, S.; Lee, H.; Das, A.K.; Kim, M.; Park, Y.; Wazid, M. LAKS-NVT: Provably Secure and Lightweight Authentication and Key Agreement Scheme Without Verification Table in Medical Internet of Things. *IEEE Access* **2020**, *8*, 119387–119404. [CrossRef]
32. Xu, G.; Wang, F.; Zhang, M.; Peng, J. Efficient and Provably Secure Anonymous User Authentication Scheme for Patient Monitoring Using Wireless Medical Sensor Networks. *IEEE Access* **2020**, *8*, 47282–47294. [CrossRef]
33. Zhang, Y.; Gravina, R.; Lu, H.; Villari, M.; Fortino, G. PEA: Parallel electrocardiogram-based authentication for smart healthcare systems. *J. Netw. Comput. Appl.* **2018**, *117*, 10–16. [CrossRef]
34. Minahil; Ayub, M.F.; Mahmood, K.; Kumari, S.; Sangaiah, A.K. Lightweight authentication protocol for e-health clouds in IoT-based applications through 5G technology. *Digit. Commun. Netw.* **2020**, *7*, 235–244. [CrossRef]
35. Srinivas, J.; Mishra, D.; Mukhopadhyay, S. A Mutual Authentication Framework for Wireless Medical Sensor Networks. *J. Med. Syst.* **2017**, *41*, 80. [CrossRef]
36. Aghili, S.F.; Mala, H.; Shojafar, M.; Peris-Lopez, P. LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT. *Future Gener. Comput. Syst.* **2019**, *96*, 410–424. [CrossRef]
37. Park, Y.; Park, Y. A Selective Group Authentication Scheme for IoT-Based Medical Information System. *J. Med. Syst.* **2017**, *41*, 48 . [CrossRef] [PubMed]

38. Sahoo, S.S.; Mohanty, S.; Majhi, B. A secure three factor based authentication scheme for health care systems using IoT enabled devices. *J. Ambient Intell. Humaniz. Comput.* **2020**, *12*, 1419–1434. [CrossRef]
39. Khalid, H.; Hashim, S.; Ahmad, S.S.; Hashim, F.; Chaudhary, M. Cross-SN: A Lightweight Authentication Scheme for a Multi-Server Platform Using IoT-Based Wireless Medical Sensor Network. *Electronics* **2021**, *10*, 790. [CrossRef]
40. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. *Sensors* **2019**, *19*, 326. [CrossRef] [PubMed]
41. Chaudhary, R.R.K.; Singh, A.; Chatterjee, K. An Enhanced Authentication Scheme for Internet of Things Based E-Healthcare System. *J. Comput. Theor. Nanosci.* **2020**, *17*, 246–253. [CrossRef]
42. Fotouhi, M.; Bayat, M.; Das, A.K.; Far, H.A.N.; Pournaghi, S.M.; Doostari, M.A. A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. *Comput. Netw.* **2020**, *177*, 107333. [CrossRef]
43. 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]
44. Kang, J.; Fan, K.; Zhang, K.; Cheng, X.; Li, H.; Yang, Y. An ultra light weight and secure RFID batch authentication scheme for IoMT. *Comput. Commun.* **2020**, *167*, 48–54. [CrossRef]
45. He, D.; Zeadally, S. An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography. *IEEE Internet Things J.* **2014**, *2*, 72–83. [CrossRef]
46. Kumar, N.; Kaur, K.; Misra, S.C.; Iqbal, R. An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud. *Peer-to-Peer Netw. Appl.* **2015**, *9*, 824–840. [CrossRef]
47. Satamraju, K.P. Proof of Concept of Scalable Integration of Internet of Things and Blockchain in Healthcare. *Sensors* **2020**, *20*, 1389. [CrossRef] [PubMed]
48. 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]
49. Yanambaka, V.P.; Mohanty, S.P.; Kougianos, E.D. Puthal, PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things. *IEEE Trans. Consum. Electron.* **2019**, *65*, 388–397. [CrossRef]
50. Li, X.; Niu, J.; Karuppiah, M.; Kumari, S.; Wu, F. Secure and Efficient Two-Factor User Authentication Scheme with User Anonymity for Network Based E-Health Care Applications. *J. Med. Syst.* **2016**, *40*, 1–12. [CrossRef] [PubMed]
51. Srinivas, J.; Das, A.K.; Kumar, N.; Rodrigues, J.J. Cloud centric authentication for wearable healthcare monitoring system. *IEEE Trans. Dependable Secur. Comput.* **2018**, *17*, 942–956. [CrossRef]
52. Lee, T.F.; Chen, W.Y. Lightweight fog computing-based authentication protocols using physically unclonable functions for internet of medical things . *J. Inf. Secur. Appl.* **2021**, *59*, 102817. [CrossRef]
53. Renuka, K.; Kumari, S.; Li, X. Design of a Secure Three-Factor Authentication Scheme for Smart Healthcare. *J. Med. Syst.* **2019**, *43*, 133. [CrossRef]
54. 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]
55. Moosavi, S.R.; Gia, T.N.; Rahmani, A.-M.; Nigussie, E.; Virtanen, S.; Isoaho, J.; Tenhunen, H. SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways. *Procedia Comput. Sci.* **2015**, *52*, 452–459. [CrossRef]
56. Alzubi, J.A. Blockchain-based Lamport Merkle digital signature: Authentication tool in IoT healthcare. *Comput. Commun.* **2021**, *170*, 200–208. [CrossRef]
57. Tahir, M.; Sardaraz, M.; Muhammad, S.; Khan, M.S. A Lightweight Authentication and Authorization Framework for Blockchain-Enabled IoT Network in Health-Informatics. *Sustainability* **2020**, *12*, 6960. [CrossRef]
58. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. BEdgeHealth: A Decentralized Architecture for Edge-Based IoMT Networks Using Blockchain. *IEEE Internet Things J.* **2021**, *8*, 11743–11757. [CrossRef]
59. Garg, N.; Wazid, M.; Das, A.K.; Singh, D.P.; Rodrigues, J.J.P.C.; Park, Y. BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment. *IEEE Access* **2020**, *8*, 95956–95977. [CrossRef]
60. Dasgupta, D.; Roy, A.; Nag, A. *Advances in User Authentication*; Springer: Berlin/Heidelberg, Germany, 2017.
61. Ducray, B. *Authentication by Gesture Recognition: A Dynamic Biometric Application Submitted by Royal Holloway*; University of London: London, UK, 2017.
62. Binu, S.; Misbahuddin, M.; Paulose, J. A Signature-Based Mutual Authentication Protocol for Remote Health Monitoring. *SN Comput. Sci.* **2019**, *1*, 8. [CrossRef]
63. Mohit, P.; Amin, R.; Karati, A.; Biswas, G.P.; Khan, M.K. A standard mutual authentication protocol for cloud computing based health care system. *J. Med. Syst.* **2017**, *41*, 1–13. [CrossRef]
64. Alzahrani, B.A.; Irshad, A. A secure and efficient TMIS-based authentication scheme improved against Zhang et al.'s scheme. *Arab. J. Sci. Eng.* **2018**, *43*, 8239–8253. [CrossRef]
65. Hashim, M.M.; Rhaif, S.H.; Abdulrazzaq, A.A.; Ali, A.H.; Taha, M.S. Based on IoT Healthcare Application for Medical Data Authentication: Towards A New Secure Framework Using Steganography. *IOP Conf. Ser. Mater. Sci. Eng.* **2020**, *881*, 012120. [CrossRef]
66. Xu, Z.; Xu, C.; Liang, W.; Xu, J.; Chen, H. A Lightweight Mutual Authentication and Key Agreement Scheme for Medical Internet of Things. *IEEE Access* **2019**, *7*, 53922–53931. [CrossRef]

67. Guo, J.; Lu, S.; Gu, C.; Chen, X.; Wei, F. December. Security analysis and design of authentication key agreement protocol in medical internet of things. In Proceedings of the International Conference on Networking and Network Applications (NaNA), Haikou, China, 10–13 December 2020; pp. 233–240.
68. Wu, F.; Li, X.; Sangaiah, A.K.; Xu, L.; Kumari, S.; Wu, L.; Shen, J. A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. *Futur. Gener. Comput. Syst.* **2018**, *82*, 727–737. [CrossRef]
69. Sureshkumar, V.; Aminb, R.; Vijaykumar, V.; Sekar, S.R. Robust secure communication protocol for smart healthcare system with FPGA implementation. *Futur. Gener. Comput. Syst.* **2019**, *100*, 938–951. [CrossRef]
70. Ravanbakhsh, N.; Nazari, M. An efficient improvement remote user mutual authentication and session key agreement scheme for E-health care systems. *Multimedia Tools Appl.* **2016**, *77*, 55–88. [CrossRef]
71. Das, A.K.; Sutrala, A.K.; Odelu, V.; Goswami, A. A Secure Smartcard-Based Anonymous User Authentication Scheme for Healthcare Applications Using Wireless Medical Sensor Networks. *Wirel. Pers. Commun.* **2016**, *94*, 1899–1933. [CrossRef]
72. Karthigaiveni, M.; Indrani, B. An efficient two-factor authentication scheme with key agreement for IoT based E-health care application using smart card. *J. Ambient Intell. Humaniz. Comput.* **2019**, 1–12. doi: 10.1007/s12652-019-01513-w. [CrossRef]
73. Deebak, B.D.; Al-Turjman, F. Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things. *IEEE J. Sel. Areas Commun.* **2020**, *39*, 346–360. [CrossRef]
74. Ever, Y.K. Secure-anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks. *IEEE Syst. J.* **2018**, *13*, 456–467. [CrossRef]
75. Deebak, B.D.; Al-Turjman, F.; Aloqaily, M.; Alfandi, O. An Authentic-Based Privacy Preservation Protocol for Smart e-Healthcare Systems in IoT. *IEEE Access* **2019**, *7*, 135632–135649. [CrossRef]
76. Mahendran, R.K.; Velusamy, P. A secure fuzzy extractor based biometric key authentication scheme for body sensor network in Internet of Medical Things. *Comput. Commun.* **2020**, *153*, 545–552. [CrossRef]
77. Deebak, B.D.; Al-Turjman, F. Secure-user sign-in authentication for IoT-based eHealth systems . *Complex Intell. Syst.* **2021**, 1–21. [CrossRef]
78. Dhillon, P.K.; Kalra, S. Multi-factor user authentication scheme for IoT-based healthcare services. *J. Reliab. Intell. Environ.* **2018**, *4*, 141–160. [CrossRef]
79. Ali, R.; Pal, A.K. Cryptanalysis and Biometric-Based Enhancement of a Remote User Authentication Scheme for E-Healthcare System. *Arab. J. Sci. Eng.* **2018**, *43*, 7837–7852. [CrossRef]
80. Xu, J.; Wei, L.; Wu, W.; Wang, A.; Zhang, Y.; Zhou, F. Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber–physical system. Futur. Gener. *Comput. Syst.* **2018**, *108*, 1287–1296. [CrossRef]
81. Kumar, P.; Chouhan, L. A privacy and session key based authentication scheme for medical IoT networks. *Comput. Commun.* **2021**, *166*, 154–164. [CrossRef]
82. Patwary, A.A.N.; Fu, A.; Battula, S.K.; Naha, R.K.; Garg, S.; Mahanti, A. FogAuthChain: A secure location-based authentication scheme in fog computing environments using Blockchain. *Comput. Commun.* **2020**, *162*, 212–224. [CrossRef]
83. Chauhan, S. Aadhaar-Based Authentication and Authorization Scheme for Remote Healthcare Monitoring. In *Innovations in Computational Intelligence and Computer Vision*; Springer: Singapore, 2021; pp. 311–318.
84. Almalki, F.A.; Soufiene, B.O. EPPDA: An efficient and privacy-preserving data aggregation scheme with authentication and authorization for IoT-based healthcare applications. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 5594159. [CrossRef]
85. Parah, S.A.; Kaw, J.A.; Bellavista, P.; Loan, N.A.; Bhat, G.M.; Muhammad, K.; de Albuquerque, V.H.C. Efficient Security and Authentication for Edge-Based Internet of Medical Things. *IEEE Internet Things J.* **2020**, *8*, 15652–15662. [CrossRef] [PubMed]
86. Adeli, M.; Bagheri, N.; Meimani, H.R. On the designing a secure biometric-based remote patient authentication scheme for mobile healthcare environments. *J. Ambient Intell. Humaniz. Comput.* **2020**, *12*, 3075–3089. [CrossRef]
87. Liu, T.; Liu, X.; Li, X.; Amin, R.; Liang, W.; Hsieh, M.-Y. RETRACTED ARTICLE: Cloud enabled robust authenticated key agreement scheme for telecare medical information system. *Connect. Sci.* **2021**, *33*, I–XX. [CrossRef]
88. Das, A.K. A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks. *Peer-to-Peer Netw. Appl.* **2014**, *9*, 223–244. [CrossRef]
89. Liu, C.-H.; Chung, Y.-F. Secure user authentication scheme for wireless healthcare sensor networks. *Comput. Electr. Eng.* **2017**, *59*, 250–261. [CrossRef]
90. Hajian, R.; ZakeriKia, S.; Erfani, S.H.; Mirabi, M. SHAPARAK: Scalable healthcare authentication protocol with attack-resilience and anonymous key-agreement. *Comput. Netw.* **2020**, *183*, 107567. [CrossRef]
91. Kumar, P.M.; Gandhi, U.D. Enhanced DTLS with CoAP-based authentication scheme for the internet of things in healthcare application. *J. Supercomput.* **2017**, *76*, 3963–3983. [CrossRef]
92. Li, J.; Su, Z.; Guo, D.; Choo, K.-K.R.; Ji, Y. PSL-MAAKA: Provably Secure and Lightweight Mutual Authentication and Key Agreement Protocol for Fully Public Channels in Internet of Medical Things. *IEEE Internet Things J.* **2021**, *8*, 13183–13195. [CrossRef]
93. Hou, J.-L.; Yeh, K.-H. Novel Authentication Schemes for IoT Based Healthcare Systems. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 183659. [CrossRef]
94. Li, C.-T.; Wu, T.-Y.; Chen, C.-L.; Lee, C.-C.; Chen, C.-M. An Efficient User Authentication and User Anonymity Scheme with Provably Security for IoT-Based Medical Care System. *Sensors* **2017**, *17*, 1482. [CrossRef] [PubMed]
95. Mahmood, Z.; Ning, H.; Ullah, A.; Yao, X. Secure Authentication and Prescription Safety Protocol for Telecare Health Services Using Ubiquitous IoT. *Appl. Sci.* **2017**, *7*, 1069. [CrossRef]

96. Jia, X.; He, D.; Kumar, N.; Choo, K.-K.R. Authenticated key agreement scheme for fog-driven IoT healthcare system . *Wirel. Netw.* **2018**, *25*, 4737–4750. [CrossRef]
97. Hamidi, H. An approach to develop the smart health using Internet of Things and authentication based on biometric technology. *Futur. Gener. Comput. Syst.* **2018**, *91*, 434–449. [CrossRef]
98. Al-Naji, F.H.; Zagrouba, R. CAB-IoT: Continuous authentication architecture based on Blockchain for internet of things. *J. King Saud Univ. -Comput. Inf. Sci.* **2020**, *34*, 2497–2514. [CrossRef]
99. Al-Naji, F.H.; Zagrouba, R. A survey on continuous authentication methods in Internet of Things environment. *Comput. Commun.* **2020**, *163*, 109–133. [CrossRef]
100. Mohsen, N.R.; Ying, B.; Nayak, A. Authentication protocol for real-time wearable medical sensor networks using biometrics and continuous monitoring. In Proceedings of the International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Atlanta, GA, USA, 14–17 July 2019; pp. 1199–1206.
101. Ashibani, Y.; Kauling, D.; Mahmoud, Q.H. Design and Implementation of a Contextual-Based Continuous Authentication Framework for Smart Homes. *Appl. Syst. Innov.* **2019**, *2*, 4. [CrossRef]
102. Shuai, M.; Liu, B.; Yu, N.; Xiong, L. Lightweight and Secure Three-Factor Authentication Scheme for Remote Patient Monitoring Using On-Body Wireless Networks. *Secur. Commun. Netw.* **2019**, *2019*, 8145087. [CrossRef]
103. Shuai, M.; Yu, N.; Wang, H.; Xiong, L.; Li, Y. A Lightweight Three-Factor Anonymous Authentication Scheme With Privacy Protection for Personalized Healthcare Applications. *J. Organ. End User Comput.* **2021**, *33*, 1–18. [CrossRef]
104. Ali, R.; Pal, A.K.; Kumari, S.; Sangaiah, A.K.; Li, X.; Wu, F. An enhanced three factor based authentication protocol using wireless medical sensor networks for healthcare monitoring. *J. Ambient Intell. Humaniz. Comput.* **2018**, 1–22. [CrossRef]
105. Chen, C.-M.; Deng, X.; Gan, W.; Chen, J.; Islam, S.K.H. A secure blockchain-based group key agreement protocol for IoT. *J. Supercomput.* **2021**, *77*, 9046–9068. [CrossRef]
106. Le, T.-V.; Hsu, C.-L. An Anonymous Key Distribution Scheme for Group Healthcare Services in 5G-Enabled Multi-Server Environments. *IEEE Access* **2021**, *9*, 53408–53422. [CrossRef]
107. Chen, M.; Lee, T.-F. Anonymous Group-Oriented Time-Bound Key Agreement for Internet of Medical Things in Telemonitoring Using Chaotic Maps. *IEEE Internet Things J.* **2021**, *8*, 13939–13949. [CrossRef]
108. Chunka, C.; Banerjee, S. An Efficient Mutual Authentication and Symmetric Key Agreement Scheme for Wireless Body Area Network. *Arab. J. Sci. Eng.* **2021**, *46*, 8457–8473. [CrossRef]
109. Zhang, L.; Wu, Q.; Qin, B.; Domingo-Ferrer, J. Provably secure one-round identity-based authenticated asymmetric group key agreement protocol. *Inf. Sci.* **2011**, *181*, 4318–4329. [CrossRef]
110. Chen, Q.; Wu, T.; Hu, C.; Chen, A.; Zheng, Q. An Identity-Based Cross-Domain Authenticated Asymmetric Group Key Agreement. *Information* **2021**, *12*, 112. [CrossRef]
111. Cheng, X.; Zhang, Z.; Chen, F.; Zhao, C.; Wang, T.; Sun, H.; Huang, C. Secure Identity Authentication of Community Medical Internet of Things. *IEEE Access* **2019**, *7*, 115966–115977. [CrossRef]
112. Abou-Nassar, E.M.; Iliyasu, A.M.; El-Kafrawy, P.M.; Song, O.Y.; Bashir, A.K.; Abd El-Latif, A.A. DITrust chain: Towards blockchain-based trust models for sustainable healthcare IoT systems. *IEEE Access* **2020**, *8*, 111223–111238. [CrossRef]
113. Yang, X.; Yi, X.; Nepal, S.; Khalil, I.; Huang, X.; Shen, J. Efficient and Anonymous Authentication for Healthcare Service with Cloud based WBANs. *IEEE Trans. Serv. Comput.* **2021**. [CrossRef]
114. Gayathri, N.B.; Thumbur, G.; Kumar, P.R.; Rahman, Z.U.; Reddy, P.V.; Lay-Ekuakille, A. Efficient and Secure Pairing-Free Certificateless Aggregate Signature Scheme for Healthcare Wireless Medical Sensor Networks. *IEEE Internet Things J.* **2019**, *6*, 9064–9075. [CrossRef]
115. Mwitende, G.; Ali, I.; Eltayieb, N.; Wang, B.; Li, F. Authenticated key agreement for blockchain-based WBAN. *Telecommun. Syst.* **2020**, *74*, 347–365. [CrossRef]
116. Nandy, T.; Bin Idris, M.Y.I.; Noor, R.M.; Kiah, M.L.M.; Lun, L.S.; Juma'At, N.B.A.; Ahmedy, I.; Ghani, N.A.; Bhattacharyya, S. Review on Security of Internet of Things Authentication Mechanism. *IEEE Access* **2019**, *7*, 151054–151089. [CrossRef]
117. Meneghello, F.; Calore, M.; Zucchetto, D.; Polese, M.; Zanella, A. IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. *IEEE Internet Things J.* **2019**, *6*, 8182–8201. [CrossRef]
118. Quist-Aphetsi, K.; Xenya, M.C. Securing medical IoT devices using Diffie-Hellman and DES cryptographic schemes. In Proceedings of the 2019 International Conference on Cyber Security and Internet of Things (ICSIoT), Accra, Ghana, 29–31 May 2019; pp. 105–108. [CrossRef]
119. Srivastava, G.; Crichigno, J.; Dhar, S. A light and secure healthcare blockchain for iot medical devices. In Proceedings of the 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada, 5–8 May 2019; pp. 1–5. [CrossRef]
120. Dharminder, D.; Mishra, D.; Li, X. Construction of RSA-Based Authentication Scheme in Authorized Access to Healthcare Services. *J. Med. Syst.* **2019**, *44*, 6. [CrossRef]
121. Gaikwad, V.P.; Tembhurne, J.V.; Meshram, C.; Lee, C.C. Provably secure lightweight client authentication scheme with anonymity for TMIS using chaotic hash function. *J. Supercomput.* **2021**, *77*, 8281–8304. [CrossRef]
122. Deebak, B.D.; Al-Turjman, F.; Nayyar, A. Chaotic-map based authenticated security framework with privacy preservation for remote point-of-care. *Multimed. Tools Appl.* **2021**, *80*, 17103–17128. [CrossRef]

123. Bhuarya, P.; Chandrakar, P.; Ali, R.; Sharaff, A. An enhanced authentication scheme for Internet of Things and cloud based on elliptic curve cryptography. *Int. J. Commun. Syst.* **2021**, *34*, e4834. [CrossRef]
124. Singh, D.; Kumar, B.; Singh, S.; Chand, S. A Secure IoT-Based Mutual Authentication for Healthcare Applications in Wireless Sensor Networks Using ECC. *Int. J. Health Inf. Syst. Inform.* **2021**, *16*, 21–48. [CrossRef]
125. Khan, M.A.; Quasim, M.T.; Alghamdi, N.S.; Khan, M.Y. A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data. *IEEE Access* **2020**, *8*, 52018–52027. [CrossRef]
126. Almulhim, M.; Islam, N.; Zaman, N. A lightweight and secure authentication scheme for IoT based e-health applications. *Int. J. Comput. Sci. Netw. Secur.* **2019**, *19*, 107–120.
127. Sowjanya, K.; Dasgupta, M.; Ray, S. An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems. *Int. J. Inf. Secur.* **2020**, *19*, 129–146. [CrossRef]
128. Sowjanya, K.; Dasgupta, M.; Ray, S. Elliptic curve cryptography based authentication scheme for Internet of medical things. *J. Inf. Secur. Appl.* **2021**, *58*, 102761. [CrossRef]
129. Nashwan, S. An End-to-End Authentication Scheme for Healthcare IoT Systems Using WMSN. *Comput. Mater. Contin.* **2021**, *68*, 607–642. [CrossRef]
130. Cremers, C.J.F. The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols. In *International Conference on Computer Aided Verification*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 414–418.
131. Blanchet, B. Automatic Verification of Security Protocols in the Symbolic Model: The Verifier Proverif. In *Foundations of Security Analysis and Design VII*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 54–87.
132. Jiang, Q.; Chen, Z.; Li, B.; Shen, J.; Yang, L.; Ma, J. Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems. *J. Ambient Intell. Humaniz. Comput.* **2018**, *9*, 1061–1073. [CrossRef]
133. Shang, T.; Liu, J. Security Analysis Based on Quantum Random Oracle Model. In *Secure Quantum Network Coding Theory*; Springer: Singapore, 2020; pp. 213–239. [CrossRef]
134. Burrows, M.; Abadi, M.; Needham, R.M. A logic of authentication. *Proc. R. Soc. Lond. A Math. Phys. Sci.* **1989**, *426*, 233–271.