Anonymous Authentication Protocols for IoT based-Healthcare Systems: A survey

Mahmoud Rajallah Asassfeh[1], Nadim Obeid[2] and Wesam Almobaideen[1,3]

[1]Department of Computer Science-King Abdullah II School for information technology, University of Jordan, Jordan.
[2]Department of Computer Information Systems, King Abdullah II School for Information Technology, University of Jordan, Jordan
[3]Rochester Institute of Technology Dubai, UAE.

***Abstract*:** Nowadays, with the increase in chronic diseases and the aging population in all countries, it has become a huge burden on hospitals to accommodate all patients and monitor them. Applying wireless sensors network for the IoT based medical systems enabled medical doctors and families to monitor patients' conditions all the time through the collected data from sensors connected to the patients. These sensitive data should be transmitted through secure channels to hospitals or medical centers. Many proposals in the literature have suggested solutions to IoT supported medical systems security issues. In this paper we present a review of the most relevant techniques that address the security in general and Anonymous Authentication particularly in the context of healthcare systems. Furthermore, we compare between these approaches in term of types of security attacks, security measures, the approaches that were used to solve some of the security issues, and the network technology used such as WSN and RFID. We found that every approach has some drawbacks regarding security attacks and security measures. Security attacks such as denial of service and modification attacks should be given more attention in future research. The same goes for security measures like non-traceability, and backward and forward secrecy. Moreover, 80%of authentication schemes use certificateless authentication. This type of authentication has low computation cost and saves energy which is convenient to the constrained devices. AVISPA and Ban logic are the most common tools used for validation in the surveyed approaches. A comparison between these techniques according to different features is illustrated which may help the researchers to easily identify the gaps in the surveyed approaches so as to propose solutions for these issues.

Keywords: Anonymous authentication; Certificateless authentication; Security attacks; Validation tool for authentication; IoT based healthcare.

1. Introduction

IoT will be the great revolution in technology since it offers many facilities to human being. It is expected that by 2025, devices or things which will be connected to the internet will exceed 75 billion, which include sensors, actuators, and mobile devices. IoT will have tremendous role in all domains because it creates an opportunity for promoting accuracy, efficiency in these domains [4].

In these days, besides food habit and life style, one of the most significant improvements in healthcare is the ability to monitor patients' conditions outside hospitals and medical centers by using sensors and devices connected to patient's body. Another major improvement is related to rural areas which usually suffer from a lack in medical expertise. However, by using IoT based healthcare systems, rural areas may get the proper benefit from medical experts by sending them all records and readings from the sensors to which they are connected, so that the medical experts can take the convenient measure to treat them according to their records. Moreover, IoT enabled healthcare systems shift from stationary to mobility in which elderly patients can be monitored while she/he is moving [11].

Security is one of the big challenges that face using IoT in healthcare systems because the transmitted data are sensitive and need to be transmitted through secure and authenticate transmission of data [64]. Only authenticated and permitted users can make use of the System to avoid security threats. Different authentication schemes have been proposed for wireless mobile communication and wireless sensor networks [3]. The significant requirements for a feasible authentication scheme development are: Lightweight algorithms and protocols for security, key management and distribution, mutual authentication, and using certificateless authentication that depends on cryptographic hash functions to reduce energy consumption and computation cost in order to be suitable to constrained devices [61].

The main contributions of this paper involve:

- Surveying some of the most prominent papers that tackled authentication for IoT focusing on the healthcare environment.
- Presenting a comparison in tabular form for the authentication protocol(s) used in term of security attack resistance, security measures and other authentication features.
- Summarizing the results of this survey by presenting the finding in terms of weaknesses and gaps that need to be tackled in future researches regarding authentication security attacks, measures and features.

The rest of this paper is organized as follows. In section 2 we present related work of surveys on authentication in IoT. In section 3 we present a survey of articles on Anonymous Authentication (AA) in healthcare systems. In section 4 we present some of prominent security attacks on authentication protocols. In section 5 we present the main security measures. In section 6 we present validation tools used and some authentication features like freshness identifier and authentication type. In section 7 we present performance evaluation of the reviewed articles. In section 8 we present network technology used and architecture components comparison. In section 9 we present conclusion and future research directions.

2. Related Work

There are many survey articles in the literature that deal with IoT, we reviewed it and compare between these surveys according to different factors such as Anonymity, scope of survey, architecture of components, mobility and year of publishing the survey.

El-hajj et al in [1] proposed the latest view of the IoT authentication field. The paper gives outlines of enormous

scope of authentication protocols presented in the literature, evaluates and compares the proposed authentication protocols, and shows their qualities and shortcomings. The objective of that paper is to set a basic initial step for researchers and developers working in this domain.

Sey in [2] presented a survey that focuses on authentication methods for IoT. The author mentioned that there are many authentication methods in IT industry, but they are not suitable for the IoT. She found that mutual authentication is necessary for IoT, and because IoT are constrained devices, she suggest that lightweight authentication protocol is a best choice to deal with low bandwidth in IoT. She concludes that by mixing various techniques of encryption and authentication, it is feasible to have a more lightweight and secure protocol.

Kavianpour et al in [3] have conducted a literature review of various authentication approaches to secure communication over IoT. The presented review was comprehensive and systematic that compares IoT specific authentication schemes found in the literature. The comparison has focus on IoT taxonomy, and open challenges that represent difficulties and opportunities that need additional efforts in order to be addressed.

Ferrag et al in [4] introduced a comprehensive survey of IoT specific authentication protocols. They select many authentication schemes and categorized them according to the application field; machine to machine, internet of vehicles, internet of energy, internet of sensors. They presented a comprehensive review of articles regarding IoT, review the threat models and their countermeasures and compare between them.

Das et al in [5] discussed basic security requirements that are essential to secure IoT environment. A threat model has been presented along with various attacks that can target IoT environment. They have introduced a classification of security protocols in the IoT context. Moreover, they have presented a detailed discussion of the functionality and features of contemporary security protocols proposed for IoT. Finally, challenges that are facing IoT security protocols development have been addressed

Silva et al., in [6], presented a review to identify primary studies that focus on the use of authentication, with its difficulties and opportunities. This systematic review has found various approaches to perform authentication in IoT environments and, among them, the utilization of ECC was presented in most of the articles aiming to guarantee security with low power consumption. This work also discussed the fundamental difficulties of applying authentication in an IoT environment. Low energy storage capacity of connected devices can be featured as one of the fundamental concerns.

Joshitta et al in [7] reviewed existing IoT authentication protocols, found in the literature, for securing transmission of information and presents analytical survey of the propose techniques. Furthermore, the authors lay out the challenges and difficulties of authentication in IoT that need further research, then the authors give a recommendation to make authentication mechanism stronger and well established.

A survey of IoT authentication protocols has been presented in [31]. The survey was conducted to help other researchers in digging into the details of such approaches by going through their taxonomy and comparison. The taxonomy takes into consideration various features of these authentication techniques; e.g. being centralized vs. distributed, hierarchical vs flat. A comparison between these techniques according to the used evaluation models and their security analysis is outlined.

Saadeh et al in [61] targeted object authentication over IoT by presenting a comprehensive survey of schemes that addressed this domain. The aim is to provide guidance for future researchers in how to grab the details of such authentication schemes especially in the context of IoT. The survey provides a taxonomy of authentication schemes based on the authentication method and the application domain. Moreover, it provides different comparisons between the studied schemes according to some criteria. Finally, the survey highlights the main issues and challenges in IoT object authentication and recommends some research directions for future researchers with regards to survey comparisons.

Table 1 compares between the above surveys. Several notes can be inferred from Table 1. The first note is that most of these surveys did not consider anonymity, the second note is that the scope of each survey is general not within a specific field, and the third note is that all the articles in the surveys support mobility.

Observation-0: no attempt has been made to present a survey on authentication for healthcare in IoT in general and on anonymous authentication in particular.

In this paper, we will fill the gap and introduce a survey on anonymous authentication for healthcare in the field of IoT.

3. Survey on Anonymous Authentication (AA) in healthcare systems

Based on the observations mentioned in previous section in which we deduced that no attempt has been made to introduce a survey on authentication for healthcare in IoT in general and on anonymous authentication in particular. So in this section, we reviewed anonymous authentication in IoT based healthcare systems and discuss in depth the proposed articles that deal with anonymous authentication (AA) in IoT based medical system ,compare between them in tabular form to find the qualities and weakness of the reviewed articles, evaluate the performance of these articles in term of computation cost, we investigate some authentication features like authentication type, freshness identifier ,network technology used ,also we discuss the validation tools used to verify the reviewed authentication protocols. Before we continue with this survey there are some security attacks that appear in the reviewed articles that need to be clarified which are:

- Desynchronization attack. In which the intruder forces the RFID tag and the RFID reader to change their common values to different values. If the intruder succeeds, the tag will not be authenticated in future transactions. [58].
- Offline password guessing attack. In which it will pick the password hash offline and try to detect password in clear-text that give the hash value. This is done by using computer to calculate the hash function of the passwords and compare them quickly with selected password hash until a match is found.
- Sensor node capture attack. It is a critical attack through which an adversary can execute numerous operations on the network and can penetrate the entire network easily [59].

- Privileged insider attack. It is a malicious attack that done on a network or computer system by a person with authorized system access.
- Stolen-verifier attack. An intruder with a stolen verifier for a user's password can carry out this attack and impersonate that user. Obviously, if poor passwords are utilized, the stolen-verifier attack can be done using the dictionary attack [60].

The rest of the security attacks are illustrated in tabular form in section 4. The description of the reviewed articles is in the following paragraphs.

He et al in [8] presented anonymous authentication schemes for WBANs. Their detailed analysis of previous schemes shows that the presented protocol overcome the security drawbacks in previous articles and has similar computation cost at user side. An Anonymous Authentication (AA) scheme comprises of three algorithms Initialization, Registration and Authentication. They store data for confirmation purposes in network manager (NM) data base, which is located in a protected and secure place. The shortcoming of this scheme is that it is used for the third tier between WBAN user and the application provider and does not deem any authentication services in the second tier between access point (mobile phone) and body sensors [32].

Saxena et al in [9] presented authentication scheme for long term evolution (LTE) network, that enhance the security and efficiency of communication among various IoT devices as well as among the clients. Analysis showed that the scheme is efficient, secure and minimize bandwidth used through authentication. The shortcomings of this scheme are that the scalability is not considered [33] and there is a computation and storage overhead, moreover the bandwidth utilization still high [34].

Wu et al in [10] proposed lightweight and efficient authentication protocol for WMSNs, which fulfil the basic security needs and keeps the user away from tracking by attackers. The well-known tool Proverif is utilized to show that their scheme withstands the simulated attacks. Also, they demonstrate informal security on the scheme. The scheme in [10] has shortage in detection mechanism for unapproved login, and it can increase to unneeded communication and computational costs [35].

Joshitta et al in [11] presented a novel mechanism of authenticating for resource constrained medical devices. New algorithm for secure authentication and key agreement of the medical devices is also presented. Authentication utilizes electronic product code (EPC)of the medical devices and one-way hash function to secure the medical data. Although the scheme is effective in execution time and communication cost, the security vulnerabilities for this scheme is the utilization of the same session key between sessions, so if the key is disclosing all the information will be revealed [39].

Amin et al in [12] introduced an architecture for health-care system in WMSN and then develop protocol that preserve the anonymity and fulfil mutual authentication for mobile users. they utilized the AVISPA tool to validate the proposed protocol. The outcome obtained show that the presented authentication protocol withstands the well-known attacks. Besides that, the BAN logic model affirms mutual authentication feature of the proposed protocol. They perform a comparison between their protocol and the existent protocols, the comparative outcomes illustrate that the introduced protocol is effective and robust. The shortcomings of this scheme are showed by Ali et al. in [18] which are vulnerable to offline password guessing attack, known session key temporary information attack, and user impersonation attack.

Khemissa et al in [13] presented a novel lightweight authentication scheme convenient to the limited capabilities resources. This scheme permits both the remote client and sensor node to confirm each other in order to protect communication against intruders. In their scheme they use nonce, exclusive OR operations and keyed hash message. But The scheme did not withstand tracking, forward secrecy and man in the middle attack [11].

Arasteh et al in [14] analysed Amin et al [54] protocol and showed that this scheme is not protected against reply and DoS attacks. Moreover, inspired by this protocol, they introduced a robust scheme rely on the same assumptions. The result of analysis proved that their scheme outperforms Amin et al [54] scheme. However, Fan et al in [40] showed that the scheme presented in [14] cannot resist malicious attack because the intruder can be authenticated by the gateway user successfully.

Srinivas et al in [15] designed a symmetric key based authentication protocol for WMSN network. The proposed protocol uses operations with low cost computation to achieve lightweight feature. They use a formal security proof algorithm to prove the scheme's security against known attacks. Wu et al in [10] considered that the protocol in [15] had shortcomings such as off-line password guessing attacks, secret key disclosure and the scheme is not resilient to sensor node capture attack. [48].

Fan et al in [16] introduced lightweight RFID authentication protocol. The scheme guarantees security of the collected data through secure authentication. They claimed that the protocol can effectively prohibit the chance of medical sensitive data to be leaked easily. But Aghili et al in [21] confirm that the scheme is not protected against security attacks. They found and demonstrated that the protocol could not give all the basic security requirements, and it is vulnerable to secret key disclosure, reader impersonation, and tag tracking attacks. Moreover, they showed that the anonymity of the tag does not hold.

Das et al in [17] introduced lightweight authentication scheme which fit wearable device deployment. The scheme permits the user to authenticate wearable devices and the portable terminal mutually and establish session key between these devices. This scheme does not consider communication between the cloud server and mobile terminal as a lightweight feature [41].

Ali et al in [18] proposed three-factor based remote user authentication protocol for WMSNs networks. Which validated using Ban-logic and then simulated using (AVISPA) tool. The result of the analysis showed that the proposed scheme is robust against different kind of security attacks. But the schemes in [35] and [57] showed that this scheme is not secure as they mentioned and vulnerable to security attacks. The scheme did not withstand privileged insider attack, desynchronization attack, offline dictionary guessing attack, forward security attack and it has a flaw in the password change phase.

Li et al in [19] proposed the use of a biometric factor as a third authentication factor. The scheme is developed to overcome the shortcomings of He et al protocol [56]. Compared with other protocols, they claimed that the scheme

improves the security and maintain the computation efficiency. However, the scheme in [19] could not resist sensor node capture attack and privileged-insider attack as showed by Das et al in [36].

Challa et al in [20] presented authentication protocol based on three factors for healthcare system that use wireless sensor networks. The scheme supports scalability, it permits legal user to amend password and biometrics without referring the trusted authority, it also permits a revocation technique for misconduct nodes in the network. Moreover, the simulation through AVISPA tool proved that their scheme is protected against attacks. But the analysis of the scheme showed that the scheme could not resist forward security attack and has high computation cost, which does not fit realistic scenarios [35].

Aghili et al in [21] proposed novel secure lightweight RFID authentication protocol (SecLAP). Which enhance security and keeps privacy in medical IoT system. Their security analysis proves that the SecLAP scheme can resist desynchronization attack, replay attack, tag/reader impersonation attack, and tracking attack, and it guarantee forward and backward communication security. They used BAN-logic to validate the security features of SecLAP. Safkhani et al in [37] showed that the protocol has serious security flaws, by introducing traceability and passive secret disclosure attacks against this protocol.

Chen et al in [22] presented an authentication protocol for IoT, based on low-capability devices. Their scheme support numerous security features by which identities are encrypted, in addition to that it embraces elliptic curve (ECC) for key exchange protocol for the secrecy of the key. It also embraces a hash function which reduces computation and communication costs. Yang in [42] showed that this scheme cannot accomplish perfect forward secrecy (PFS) and explicit mutual authentication.

Li et al in [23] introduced an enhancement on Lui-Chung authentication scheme [55], the scheme is secure, and data is encrypted for IoT based healthcare system, in which user anonymity and resistance to password and replay attacks were introduced. Ku et al in [43] showed that this scheme is exposed to some attacks like sensed data forgery attack, stolen verifier attack and un-freshness of session key.

Wazid et al in [24] presented authentication scheme for medicine anti-counterfeiting system in the (IoT) context, which is utilized to check the genuineness of pharmaceutical items (dosage forms). The scheme utilized the near field communication (NFC) which fit mobility. They analyze the scheme using Real-Or-Random (ROR) model and AVISPA validation tool and proves that the protocol generates the session key (SK) securely. Moreover, the scheme is fortified against the reply and man in the middle attacks. They assess it using the broadly accepted NS-2 simulation. Deebak et al in [38] demonstrated that this scheme cannot be resilient to the potential attack such as message eavesdropping, denial of service and smart card forgery.

Gope et al in [25] presented firstly a focus on the security requirement in body sensor network (BSN) then secondly, they introduced a secure IoT-based medical care system utilizing (BSN). But this scheme does not consider access right verification and strong data encryption [44]. moreover, user anonymity is not offered and password guessing and man in the middle attack are not considered [48].

Shuai et al in [35] proposed secure and lightweight three-factor authentication scheme to monitor patient remotely using WMSNs. The proposed scheme embraces one-time hash chain mechanism to guarantee forward secrecy, and the pseudonym identity technique is used to provide user anonymity and withstand against desynchronization attack. The scheme is effective with reasonable computational and communication cost. The weaknesses of this scheme are offline dictionary guessing attack, privileged insider attack, and a flaw in the password change phase [57].

Soni et al in [52] introduced improved mechanism for building up a three-factor secure mutual authentication scheme to achieve successfully the security of the remote health-care system for patient monitoring. Further, the proper revocation and re-registration of users have been consolidated to support some additional securities in a case when a user loses his/her smartcard, or it is stolen. But Xu et al in [53] showed that the scheme has drawbacks such as sensor node capture attack and no forward secrecy.

In the following sections we will discuss deeply and in tabular form the reviewed papers starting with security attacks, security measures, other authentication features like authentication type, freshness identifier, also we illustrated the validation tool used, the performance evaluation of these articles and network technology used. Then we have observations and results of these reviewed papers.

4. Security Attacks

In the following subsections we discussed the attacks mentioned in the reviewed papers presented in section 3 we concentrate on five security attacks, which are mostly used to evaluate the reviewed schemes. These attacks are Impersonation attack, Replay attack, Man-in-the-middle attack, Modification attack, and Denial of service attack.

4.1 Impersonation attack

This attack happens when the intruder pretends to be a legal entity by replaying an original message intercepted from a previous successful communication. The intruders try to launch an impersonation attack by modifying the intercepted message parameters or replaying the intercepted messages [26]. From Table 2, papers [11-12], [16] and [22] did not consider impersonation attack, the rest of the papers consider it and present a solution for this attack which form 80% of the reviewed researches.

4.2 Replay attack

In replay attack, the intruder intercepts the message and retransmits it to the recipient entities to pretend that the message has been transmitted from real sender entity. i.e. the intruder would like to deceit the protocol entities by replaying previous used messages [26]. All the reviewed papers in Table 2 assure that they could resist the reply attack except [22], the rest of the researches consider it and present a solution for this attack which form 95% of the reviewed researches. Random numbers and timestamps are two of the mainly used mechanisms to resist replay attack.

4.3 Man-in-the-middle attack

This attack is the illegal intercept of communications of two parties with the intent to eavesdrop, change, delay, or discard the messages during communication. When a patient is in urgent need of medication, the intruder may prescribe worst kind of medication procedures which may lead to the loss of valuable life [26] and [65]. Resistance to man-in-the-middle

attack considered as one of the important security considerations to support authentication.
From Table 2 [8-12],[15],[17-18],[20],[22-25] and [52] research papers have taken care of the Man In The Middle attack which represent 70% of the reviewed researches.

4.4 Denial of service attack

In this attack the intruder tried to make the machine or resource unavailable. The intruder transmits unnecessary messages to the machine or resource to make the resource inaccessible to legal clients. Denial of service attack causes severe damage to the availability of resources. The server would be overburdened with too many fake requests to function it properly [26]. In Table 2 the papers [13-17], [19-20] and [52] overcome DoS attack which represent 40% of the reviewed researches.

4.5 Modification attack.

The intruder gains unauthorized access to health data and manipulate with it to create confusion and mislead innocent entities in the IoT health network. Table 2 illustrate that papers [8-10], [12-13], [23], [25] and [52] are immune from modification attack which represent 40% of the reviewed researches.
We observe that modification attack, denial of service attack, have the lowest percentage which mean that more attention should be paid to these attacks in future researches and studies.
Observation-1: None of the presented articles have discussed a solution or technique that is able to mitigate all the considered attacks.

Observation-2: Denial of service and Modification attacks are the least attacks to satisfied or considered by the presented articles.

5. Security Features

In this section we concentrate on some of the security measures that play significant role in preserving the privacy and security of the IoT devices such as mutual authentication, anonymity, non-traceability, session key agreement and forward and backward secrecy.

5.1 Mutual authentication

It means two-way authentication scheme which assure that only permitted client could access services. It is the basic prerequisites for IoT based medical systems to enhance secure communication. It improves the overall security of the system and eliminates spoofing and mimicking attacks [26]. All the reviewed papers in Table 3 have the mutual authentication except [11] and [22]. This represents 90% of the reviewed papers.

5.2 User anonymity

To protect the client's identity, a protocol has to provide user anonymity. This requirement guarantee that the intruder could never access the information of a legal party. The privacy of the client is kept secretive [65]. The user anonymity is significant requirement to be considered in preserving the security of the system [26]. From Table 3 we can notice that fifteen papers have considered anonymous authentication which represent 75% of the reviewed papers. The exceptions are [15], [16], [18-19] and [21] which did not provide anonymity.

5.3 Non-traceability

An authentication protocol should be able to support non-traceability; i.e. The adversary could not track the action of legal client. The location information of the patient is sent via communication channel. As this information is highly classified, this must be done in a secured way so that the intruder can never track the place of the patient [26]. From Table 3 we can notice that papers [8-10], [12], [14], [17], [19-20], [22], [35] and [52] support Non-traceability which represent 55% of the reviewed research papers.

5.4 Session key establishment

The session key agreement is a main property for entity authentication and secure communication. A session key shared between two communicating nodes is needed to ensure integrity of data and confidentiality. Therefore, an authentication protocol should provide the session key establishment [26]. All the reviewed papers in Table 3 have considered session key establishment except [12], this represent 95% of the reviewed papers.

5.5 Forward and backward secrecy.

In a crucial time of the live of healthcare applications, new medical sensors replaced the old ones when they go wrong, so it is important to take into account forward and backward secrecy. In forward secrecy, a medical sensor should not read messages sent after it leave the network, but in backward secrecy a sensor added to the network should not read any messages sent before joining the network [27]. From Table 3 papers [8-9], [11-12], [16], [21], [23] and [35] have been found to provide forward and backward secrecy which represent 40% of the reviewed research papers.
From previous analysis, papers have considered the above-mentioned security measures as follows: Mutual authentication 90%, Anonymity 75%, non-tractability 55%, session key agreement 95%, forward and backward secrecy 40%. We note that non-tractability and forward and backward secrecy have the lowest percentage. These features require more attention in future researches and studies regarding security requirements.
Observation-3: Most of the proposed articles did not discuss a solution or technique that is able to support all the considered security features which are mutual authentication, anonymity, non-tractability, forward and backward secrecy and session key agreement.
Observation-4: Non-tractability and forward and backward secrecy are the least features to be considered by the proposed articles.

Table 3. Security Measures Comparison

Paper	M1	M2	M3	M4	M5
He et al [8]	✓	✓	✓	✓	✓
Saxena et al [9]	✓	✓	✓	✓	✓
Wu et al [10]	✓	✓	✓	✓	__
Joshitta et al [11]	__	✓	__	✓	✓
Amin et al [12]	✓	✓	✓	__	✓
Khemissa et al [13]	✓	✓	__	✓	__
Arasteh et al [14]	✓	✓	✓	✓	__
Srinivas et al [15]	✓	✓	__	✓	__
Fan et al [16]	✓	__	__	✓	✓
Das et al [17]	✓	✓	✓	✓	__
Ali et al [18]	✓	__	__	✓	__
Li et al [19]	✓	__	✓	✓	__
Challa et al [20]	✓	✓	✓	✓	__
Aghili et al [21]	✓	__	__	✓	✓
Chen et al [22]	__	✓	✓	✓	__
Li et al [23]	✓	✓	__	✓	✓
Wazid et al [24]	✓	✓	__	✓	__
Gope et al [25]	✓	__	__	✓	__
Shuai et al [35]	✓	✓	✓	✓	✓
Soni et al [52]	✓	✓	✓	✓	__

M1: Mutual authentication**, M2:** Anonymity**, M3**: Non traceability**, M4**: Session key agreement**, M5**: forward and backward secrecy

6. Classification According to Some Authentication Features and Validation Tools.

In this section we discuss some features that used in authentication protocol to find out to what extent it convenient to the constrained IoT devices such as freshness identifier and authentication type. Also, we illustrate the validation tools used to verify the reviewed schemes and we mention the simulation and implementation used in some of these articles.

6.1 Freshness Identifier

It consists of two types:

6.1.1 Timestamps

The sender of the message adds the current time to the message when it is sent. This is checked by the recipient when the message is received by comparing with the local time. If the received time stamp is within an acceptable window of the current time, then the message is regarded as fresh. The difficulty of using timestamps is that synchronized time clocks are required and must be maintained securely. Gong [46] pointed out that if a principal's clock is advanced beyond the time in the rest of the system, a vulnerability can exist even after the clock has been corrected. This is because an adversary could have captured, and suppressed, a message that will become fresh in the future. Gong calls this a suppress relay attack [47]. From Table 4 papers [8-9], [15], [17-20], [22-24], [35] and [52] used timestamps as freshness identifier which form 60% of the reviewed papers.

6.1.2 Nonce (random challenges).

The recipient A of the message generates a nonce (number used only once) NA, and passes it to the sender of the message B. The nonce NA is then returned with the message after processing with some cryptographic function (f). A check the nonce on receipt and deduces that the message is fresh because the message cannot have been formed before the nonce was generated. A disadvantage of using a challenge is that it requires an interactive protocol which may increase the number of message exchanges. Attention must also be paid to the quality of random numbers produced, since if the nonce to be used is predictable a valid reply can be obtained in advance and later replayed [47]. From Table 4 papers [10-14], [16], [21] and [25] used Nonce as freshness identifier which form 40% of the reviewed papers.

6.2 Authentication Type.

New researches on authentication protocols in the IoT environment consist of two types which are authentication with certification and certificateless authentication. In this section, we shortly introduce these two classes:

6.2.1 Authentication with certification.

Each object has its own certificate, so the authentication is achieved based on this digital certificate [62]. However, in this type of authentication the consumption of energy is high because of using asymmetric encryption like RSA and PKI certificate exchange, which is considered as its main shortcoming. For that, RSA is replaced by Elliptic Curve Cryptography ECC. In fact, it can achieve less consumption of energy using smaller key size that achieve the same level of security. Many researchers presented an authentication schemes for WSNs using ECC based implicit certificate in distributed IoT applications, in order to minimise the computation, and save energy of the authentication process [63]. It offers more saving energy and low computation cost [13]. From Table 4 papers [8], [20], [22] and [23] have used authentication with certificates which form 20% of the reviewed papers.

6.2.2 Certificateless authentication.

In this type, certification is not required in authentication schemes. Instead of that they used hash function, exclusive or operation (Xor), and symmetric encryption. This type of authentication save energy and efficient regarding performance [13]. From Table 4 papers [9-19], [21], [24-25], [35] and [52] used certificateless authentication which form 80% of the reviewed papers.

6.3 validation tools.

Validation tools used for authentication protocols varies based on features they can support. Following are examples of verification tools which are used to validate authentication protocols:

6.3.1 Proverif.

This is one of the validation tools used to test the security features found in authentication schemes. Generally, it is utilized by specialists to assess security reachability, demonstrating session key secrecy [3]. From Table 4, only two papers [10] and [22] have validated the proposed authentication protocols using Proverif. This forms 10% of the reviewed researches.

6.3.2 Burrows-Abadi-Needham (BAN) Logic.

It is used to help in validation of authentication schemes which consist of set of rules to be utilized to analyse data

exchange protocols. And help users to make sure that the exchange data is trustworthy and secure [3] and [51]. From Table 4 we can notice that papers [12], [16], [18], [20], [21], [35] and [52] validated their authentication protocols using BAN logic which form 35% of the reviewed papers.

6.3.3 Real-or-Random (ROR Model).

ROR model is utilized to validate the security of key ROR model is utilized to validate the security of key exchange protocols 3]. From Table 4 papers [15], [17], [20], [23] and [24] have validated their propose key exchanged protocols using (ROR Model) which form 25% of the reviewed researches.

6.3.4 Automated Validation of Internet Security Protocols and Applications (AVISPA).

A simulation tool that approves resistance of an authentication protocol against replay and man-in-the-middle attacks [99]. It analyses large-scale of authentication protocol by using (HLPSL) language to code the protocols [3]. From Table 4 papers [12], [15], [17-18], [20], [22], [24] and [52] validated their authentication protocols using (AVISPA) which form 40 % of the reviewed researches [3].

6.4 Implementation And Simulation

From Table 4 we can notice that some papers implemented the protocol using FPGA [16] and [21] and C++ [22] and others simulated the protocols using NS3[10] and NS2 [17] and [24].

Observation-5: 80% of authentication schemes use certificateless authentication, a type of authentication that has low computation cost and saves energy to support constrained devices.
Observation-6: Regarding the validation tools, most of the schemes have used AVISPA and Ban-logic tools.
Observation-7: Most of the schemes use timestamps as freshness identifier which form about 60% of the reviewed papers. The remaining papers used nonce.
Observation-8: 30% of the schemes have been implemented using FPGA and C++ or simulated using NS2 and NS3.
Observation-9: Most of the schemes are developed to support mobile patients, in the sense that they give the patients the flexibility to move and practice their daily life interest.

7. Performance Evaluation

This section compares the computational efficiency of reviewed protocols. Firstly, because the registration phase is used once and the password exchange phase is not used frequently, the cost of these phases will be excluded. Moreover, the bit XOR operation need very low computation so it will be excluded. Secondly, the focus will be on the login phase and authentication phase of the evaluated protocols, and for simplicity of analysis, we select four computation notation Th, T_{ED}, T_{FE}, and T_{ECM} which illustrated in Table 5 according to the experiment's outcome in [49] and [50].
Table 6 shows the result of computation cost of the reviewed schemes in healthcare. The computation costs are calculated in user side (Ui), Gateway server side (GW) and sensor side (Si). From Table 6 we notice that the schemes which use hash functions are more efficient than those using asymmetric encryption.
Papers [10], [12-15], [17-18], [24-25] and [35] have the low computation cost and high energy saving. They use cryptographic operations such as exclusive-or operation (XOR), or hash functions. These schemes also are certificateless authentication. The rest of the papers [11], [19-20], [22-23] and [52] have higher computation cost which use asymmetric encryption.
Observation-10: The performance of schemes that use hash function and symmetric encryption is higher than schemes that use asymmetric encryption.

Table 5. Computation Notation Cost

Notations	Meaning	Experimental Results Time
T_h	The time cost of hash function operation.	0.00032 s
T_{ED}	The time cost of general symmetric encryption/decryption operation	0.0056s
T_{FE}	The time cost of Fuzzy extractor	0.0171s
T_{ECM}	The time cost of an elliptic curve points relative multiplication operation	0.0171s

Observation-11: Most of the schemes use low computation operation like hash function in the sensor node except schemes [22] and [11] which use asymmetric encryption.

8. Network Technology and Architecture Components Comparison.

In this section we illustrate the network technologies that used to transmit data between participants in the network. These networks vary between each other in distance covered and, in the component used. The authors in the reviewed articles propose authentication protocols for these networks to make sure that the transmitted data is secure against security attacks.

8.1 RFID

It uses electromagnetic fields to automatically identify and track tags connected to objects. A tag is composed of tiny transceiver. It communicates directly with RFID reader, the computation capabilities and memory storage of RFID tag is limited [28]. From Table 7 papers [16] and [21] are implemented on RFID network which represent 10% of the reviewed papers.

8.2 WBAN

It is special purpose medical sensors which consist of two types, wearable on the body or implantable under the skin. Wireless body area network (WBAN) can present two great advantages, the first one, supporting the mobility of the patient, the second one is that (WBAN) is location independent monitoring facility, which can search and find a suitable communication network to transmit data to remote data base server [28]. From Table 7 papers [8], [11] and [25] are implemented on WBAN network which represent 15% of the reviewed papers.

8.3 LTE

Long Term Evolution (LTE) is a modern and powerful high-speed broadband technology for wireless communication for mobile devices and data terminals. The standard is developed by the 3GPP (3rd Generation Partnership Project). Multi-band phones are able to use LTE because different LTE bands and frequencies used in different countries [29]. From

Table 7 paper [9] implemented using LTE network which represent 5% of the reviewed papers.

8.4 WSN

WSN is a collecting of number of sensors nodes for recording and monitoring the physical phenomena of the environment and sorting out the gathered data at central location. WSNs measure environmental phenomena like temperature, heat, pollution levels, humidity, wind, and so on [30]. From Table 7 papers [10], [12], [13-15], [18-20], [22-23], [25] and [52] are implemented using WSN network which represent 60% of the reviewed papers.

8.5 NFC (Near Field Communication)

NFC is a set of communication protocols used to communicate between two electronic devices over 4 cm distance or less. The first device is called the initiator which starts the communication, whereas the second device is called the target and responds to the initiator's requests. [45]. From table 7 paper [24] is implemented on NFC network which represent 5% of the reviewed papers.

8.6 Bluetooth

It is a wireless technology standard that used for transmitting data between stationary and mobile devices over short distances using UHF radio frequencies. From Table 7 paper [17] is implemented using Bluetooth which represent 5% of the reviewed papers.

Observation-12: Most of the schemes use WSN network technology which fits IoT devices capabilities.

9. Conclusion and Future Research Directions

Security is the most significant challenge in IoT infrastructure, that face IoT devices especially in critical applications like healthcare environments which exchange sensitive data that require protection against intruders. Since no attempt has been made to present a survey on authentication for healthcare in IoT in general and on anonymous authentication in particular. we reviewed in this paper the most prominent papers that addressed security challenges in general and anonymous authentication in healthcare environments in particular. These surveyed papers proposed approaches to tackle some security challenges in IoT taking into account the limitations of IoT devices with regard to computation, storage and speed. However, some of these approaches have many drawbacks like vulnerable to different kind of security attacks because the cryptography is weak and easy to break. Some other approaches did not have the capability to hide the identity of the user which is important in healthcare. Moreover, some of threating attacks like denial of service and modification attack need to be considered in future research and the same goes for security measures like non-traceability and Forward and backward secrecy. Moreover, 80% of authentication schemes use certificateless authentication which has low computation cost and saves energy which is convenient to the constrained devices. AVISPA and Ban logic are the most common tools used in validation in the reviewed papers. Most of the reviewed papers support mobility, this lead us to think about solution to hide the location of the mobile patient so as to achieve location privacy beside the authentication protocol. we propose recommendations to researchers as directions for future research. These recommendations are based on observations we deduced from analyzing tables in this survey.

- Recommendation-1: based on Observation-1 and Observation-2 we recommend the developing of a comprehensive technique that is able to mitigate Replay attack, Impersonation attack, Man-in-the-middle attack and with more attention to be paid to Modification attack and Denial of service attack.
- Recommendation-2: based on Observation-3 and Observation-4 we recommend the developing of a comprehensive technique that can support anonymity, session key agreement, mutual authentication with more focus on non-tractability, forward and backward secrecy.
- Recommendation-3: based on Observation-5 and Observation-10 certificateless authentication which depends on hash function and symmetric encryption should be adopted in IoT devices because it saves energy and has low cost of computation.
- Recommendation-4: based on Observation-6 the mostly recommended two validation tools to be used to validate authentication protocols are AVISPA and BAN logic tools. Each one of these tools can validate a protocol against different kinds of attacks. For example, AVISPA tool have been mostly used to validate the authentication protocol against replay attack, and man in the middle attack., while BAN logic tool has been mostly used to determine whether exchanged information is trustworthy and secured against eavesdropping. So, we recommend using both tools to validate authentication protocols.
- Recommendation-5: based on Observation-7 although most of the reviewed techniques use timestamp as freshness identifier, we recommend using nonce because timestamp technique requires time clocks synchronization to be maintained securely, which is beyond the capabilities of the IoT constrained devices.
- Recommendation-6: based on Observation-8 an authentication protocol should be implemented using efficient programming languages like C++ or hardware description language like Verilog HDL on FPGA or simulated using NS2, NS3 or similar simulation packages to make sure that the scheme is applicable.
- Recommendation-7: based on Observation-9 because of the mobility of the user(patient) more effort should be done to the location privacy of the patient who send his location periodically to medical center, we recommend developing a technique to hide the location of the patient while in moving by using spatial cloaking.
- Recommendation-8: based on Observation-11 we should focus on the sensor node or IoT device and make sure that computation is as minimum as possible at IoT devices side.
- Recommendation-9: based on Observation-12 WSN is the recommended network to be used to connect sensors or IoT devices.
- Recommendation-10: there is a necessity to develop lightweight authentication protocols that are efficient by using low computation operations especially in the IoT devices, beside that it should be robust against security attacks. These requirements are satisfied by using hash function and symmetric encryption or efficient asymmetric encryption like ECC encryption algorithm which has less computation requirement and more security strength than other public key cryptosystems.

This protocol should be enhanced by location privacy for mobile users.

References

[1] M. El-hajj, A. Fadlallah, M. Chamoun and A. Serhrouchni , "A survey of internet of things (IoT) Authentication schemes," Sensors, vol. 19, no. 5, p. 1141, 2019.
[2] D. Sey, "A survey on authentication methods for the Internet of Things," PeerJ Preprints, vol. 6, 2018.
[3] S. Kavianpour, B. Shanmugam, S. Azam , M. Zamani, G. Narayana Samy and F. De Boer, "A Systematic Literature Review of Authentication in Internet of Things for Heterogeneous Devices," Journal of Computer Networks and Communications, 2019.
[4] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang and L. Shu, "Authentication Protocols for Internet of Things: A Comprehensive Survey," Security and Communication Networks, 2017.
[5] A. K. Das, S. Zeadally and D. He, "Taxonomy and analysis of security protocols for Internet of Things," Future Generation Computer Systems, vol. 89 , pp. 110-125, 2018.
[6] E. D. O. e Silva, W. T. S. de Lima, F. S. Ferraz, and F. I. do ascimento Ribeiro, " Authentication and the Internet of Things: A Survey Based on a Systematic Mapping," ICSEA, vol. 4, no. 6, 2017.
[7] S. M. Joshitta, and L. Arockiam, "Authentication in IoT Environment: A Survey," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 6, 2016.
[8] D. He, S. Zeadally, N. Kumar and J. H. Lee, "Anonymous authentication for wireless body area networks with provable security," IEEE Systems Journal, vol.11, no. 4 , pp. 2590-2601, 2017.
[9] N. Saxena, S. Grijalva and N. S. Chaudhari, "Authentication protocol for an IoT-enabled LTE network," ACM Transactions on Internet Technology (TOIT), vol. 16, no. 4, pp. 1-20, 2016.
[10] F. Wu, X. Li, A. K. Sangaiah, L. Xu, S. Kumari, L. Wu and J. Shen, "A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks," Future Generation Computer Systems, vol. 82, pp. 727-737, 2018.
[11] R. S. M. Joshitta and L. Arockiam, "Device authentication mechanism for IoT enabled healthcare system," In 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), pp. 1-6, 2017.
[12] R Amin, S. H. Islam, G. P. Biswas, M. K. Khan and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," Future Generation Computer Systems, vol. 80, pp. 483-495, 2018.
[13] H. Khemissa and D. Tandjaoui, "A novel lightweight authentication scheme for heterogeneous wireless sensor networks in the context of internet of things," In Wireless Telecommunications Symposium (WTS), pp. 1-6, 2016.
[14] S. Arasteh, S. F. Aghili and H. Mala, "A new lightweight authentication and key agreement protocol for Internet of Things," In 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC), pp. 52-59, 2016.
[15] J. Srinivas, D. Mishra and S. Mukhopadhyay, "A mutual authentication framework for wireless medical sensor networks," Journal of medical systems, vol. 41, no. 5, pp. 80-99, 2017.
[16] K. Fan, W. Jiang, H. Li and Y. Yang, "Lightweight RFID Protocol for Medical Privacy Protection in IoT," IEEE Transactions on Industrial Informatics, vol. 14, no.4, pp. 1656-1665, 2018.
[17] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K. K. R. Choo and Y. Park, "Design of secure and lightweight authentication protocol for wearable devices environment," IEEE journal of biomedical and health informatics, vol. 22, no 4, pp. 1310-1322, 2017.
[18] R. Ali, A. K. Pal, S. Kumari, A. K. Sangaiah, X. Li and F. Wu, "An enhanced three factor based authentication protocol using wireless medical sensor networks for healthcare monitoring," Journal of Ambient Intelligence and Humanized Computing, pp. 1-22, 2018.
[19] X. Li, J. Niu, S. Kumari, J. Liao, W. Liang and M. K. Khan, "A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity," Security and Communication Networks, vol. 9, no. 15, pp. 2643-2655, 2016.
[20] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan and A. V. Vasilakos, "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," Computers & Electrical Engineering, vol. 69, pp. 534-554, 2018.
[21] S. F Aghili, H. Mala, P. Kaliyar and M. Conti, "SecLAP: Secure and lightweight RFID authentication protocol for Medical IoT," Future Generation Computer Systems, vol. 101, pp. 621-634, 2019.
[22] Y. Chen, J. F. Martínez, P. Castillejo and L. López, "A Privacy Protection User Authentication and Key Agreement Scheme Tailored for the Internet of Things Environment: PriAuth," Wireless Communications and Mobile Computing, 2017.
[23] C. T Li, T. Y. Wu, C. L. Chen, C. C. Lee and C. M. Chen, "An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system," Sensors, vol. 17, no.7, p. 1482, 2017.
[24] M. Wazid, A. K. Das, M. K. Khan, A. A. D. Al-Ghaiheb, N. Kumar and A. V. Vasilakos, "Secure authentication scheme for medicine anti-counterfeiting system in IoT environment," IEEE Internet of Things Journal, vol. 4, no. 5, pp.1634-1646, 2017.
[25] P. Gope and T. Hwang, "BSN-Care: A secure IoT-based modern healthcare system using body sensor network," IEEE Sensors Journal, vol 16, no. 5, pp. 1368-1376, 2016.
[26] P. Jeyadurga, S. E. Juliet, I. J. Selwyn, P. Sivanisha, "Security in Smart Healthcare System: A Comprehensive Survey," International Journals of Advanced Research in Computer Science and Software Engineering, vol. 7, no. 10, pp. 39-48, 2017.
[27] P. Kumar and H. J. Lee, " Security issues in healthcare applications using wireless medical sensor networks: A survey," Sensors, vol. 12, no. 1, pp. 55-91, 2012.
[28] D. He and S. Zeadally, "An analysis of rfid authentication schemes for internet of things in healthcare environment using elliptic curve cryptography," IEEE internet of things journal, vol. 2, no. 1, pp. 72-83, 2015.
[29] (2020, September 3). LTE (telecommunication) [online]. Available: https://en.wikipedia.org/wiki/LTE_(telecommunication)
[30] (2020, September 25). Wireless sensor network [online]. Available: https://en.wikipedia.org/wiki/Wireless_sensor_network
[31] M. Saadeh, A. Sleit, M. Qatawneh and W. Almobaideen, "Authentication techniques for the internet of things: A survey," In 2016 cybersecurity and cyberforensics conference (CCC), pp. 28-34, 2016.
[32] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta and K. K. R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," Computer Networks, vol. 129, pp. 429-443, 2017.
[33] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving

schemes," Journal of Network and Computer Applications, vol. 101, pp. 55-82, 2018.
[34] V. Sharma, I. You, K. Andersson, F. Palmieri and M. H. Rehmani, "Security, Privacy and Trust for Smart Mobile-Internet of Things (M-IoT): A Survey," IEEE Access, vol. 8, pp. 167123-167163, 2019.
[35] M. Shuai, , B. Liu, N. Yu and L. Xiong, "Lightweight and Secure Three-Factor Authentication Scheme for Remote Patient Monitoring Using On-Body Wireless Networks," Security and Communication Networks, 2019.
[36] A. K. Das, A. K. Sutrala, V. Odelu and A. Goswami, "A secure smartcard-based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks," Wireless Personal Communications, vol. 94, no 3, pp. 1899-1933, 2017.
[37] M. Safkhani, Y. Bendavid, S. Rostampour and N. Bagheri, "On designing lightweight rfid security protocols for medical IoT," IACR Cryptology ePrint Archive, p. 851, 2019.
[38] B. D. Deebak, F. Al-Turjman, M. Aloqaily and O. Alfandi, "An Authentic-Based Privacy Preservation Protocol for Smart e-Healthcare Systems in IoT," IEEE Access, vol. 7, pp. 135632-135649, 2019.
[39] E. Lara, L. Aguilar, M. A. Sanchez and J. A. García, "Lightweight Authentication Protocol for M2M Communications of Resource-Constrained Devices in Industrial Internet of Things," Sensors, vol. 20, no. 2, p. 501, 2020.
[40] X. Fan and B. Niu, "Security of a new lightweight authentication and key agreement protocol for internet of things," In 2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN), pp. 107-111, 2017.
[41] A. Gupta, M. Tripathi, T. J. Shaikh and A. Sharma, "A lightweight anonymous user authentication and key establishment scheme for wearable devices," Computer Networks, vol. 149, pp. 29-42, 2019.
[42] Z. Yang, J. He, Y. Tian and J. Zhou, "Faster Authenticated Key Agreement with Perfect Forward Secrecy for Industrial Internet-of-Things," IEEE Transactions on Industrial Informatics, 2019.
[43] D. Ku and H. Kim, "Enhanced User Authentication with Privacy for IoT-Based Medical Care System," International Journal of Computer Theory and Engineering, vol. 10, no. 4, pp. 125-129, 2018.
[44] R. Chaudhary, A. Jindal, G. S. Aujla, N. Kumar, A. K. Das and N. Saxena, "Lscsh: Lattice-based secure cryptosystem for smart healthcare in smart cities environment," IEEE Communications Magazine, vol. 56, no. 4, pp. 24-32, 2018.
[45] A. Rahul, G. Krishnan, U. H. Krishnan and S. Rao, "Near Field Communication (NFC) Technology: A Survey," International Journal on Cybernetics & Informatics (IJCI), vol. 4, no. 2, pp. 133-144, 2015.
[46] L. Gong, "A security risk of depending on synchronized clocks," ACM SIGOPS Operating Systems Review, vol. 26, no. 1, pp. 49-53, 1992
[47] C. Boyd, A. Mathuria and D. Stebila, "Protocols for authentication and key establishment," Heidelberg: Springer, vol. 1, 2003.
[48] Y. K. Ever," Secure-anonymous user Authentication scheme for e-healthcare application using wireless medical sensor networks," IEEE systems journal, vol. 13, no. 1, pp. 456-467, 2018.
[49] C. C. Lee, C. T. Chen, P. H. Wu and T. Y. Chen, "Three-factor control protocol based on elliptic curve cryptosystem for universal serial bus mass storage devices," IET Computers & Digital Techniques, vol. 7, no. 1, pp. 48-55, 2013
[50] D. He, N. Kumar, J. H. Lee and R. S. Sherratt, "Enhanced three-factor security protocol for consumer USB mass storage devices," IEEE Transactions on Consumer Electronics, vol. 60, no. 1, pp. 30-37, 2014.
[51] M. Saadeh, A. Sleit, K. E. Sabri and W. Almobaideen, "Hierarchical architecture and protocol for mobile object authentication in the context of IoT smart cities," Journal of Network and Computer Applications, vol. 121, pp. 1-19, 2018.
[52] P. Soni, A. K. Pal and S. H. Islam, "An improved three-factor authentication scheme for patient monitoring using WSN in remote health-care system," Computer methods and programs in biomedicine, vol. 182, p. 105054, 2019.
[53] G. Xu, F. Wang, M Zhang and J. Peng, "Efficient and Provably Secure Anonymous User Authentication Scheme for Patient Monitoring Using Wireless Medical Sensor Networks," IEEE Access, vol. 8, pp. 47282-47294, 2020.
[54] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, L. Leng and N. Kumar, "Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks," Computer Networks, vol. 101, pp. 42-62, 2016.
[55] C. H. Liu and Y. F. Chung, "Secure user authentication scheme for wireless healthcare sensor networks," Computers & Electrical Engineering, vol. 59, pp. 250-261, 2017.
[56] D. He, N. Kumar, J. Chen, C. C. Lee, N. Chilamkurti and S. S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks," Multimedia Systems, vol. 21, no. 1, pp. 49-60, 2015.
[57] J. Mo, Z. Hu and Y. Lin, "Cryptanalysis and Security Improvement of Two Authentication Schemes for Healthcare Systems Using Wireless Medical Sensor Networks," Security and Communication Networks, 2020.
[58] M. Deng and W. Zhu, "Desynchronization attacks on RFID security protocols," TELKOMNIKA Indonesian Journal of Electrical Engineering, vol. 11, no. 2, pp. 681-688, 2013.
[59] M. V. Bharathi, R. C. Tanguturi, C. Jayakumar and K. Selvamani, "Node capture attack in Wireless Sensor Network: A survey," In 2012 IEEE International Conference on Computational Intelligence and Computing Research, pp. 1-3, 2012.
[60] C. M. Chen and W. C. Ku, "Stolen-verifier attack on two new strong-password authentication protocols," IEICE Transactions on communications, vol. 85, no. 11, pp. 2519-2521, 2020.
[61] M. Saadeh, A. Sleit, K. E. Sabri and W. Almobaideen, "Object Authentication in the Context of the Internet of Things: A Survey," Journal of Cyber Security and Mobility, Vol. 9, no. 3, pp. 385–448, 2020.
[62] W. Almobaideen and M. Saadeh, "Lightweight Authentication for Mobile Users in the Context of Fog Computing," International Journal of Advanced Computational Engineering and Networking, vol. 6, no. 12, pp. 2321-2063, 2018.
[63] M. Saadeh, A. Sleit, K. E. Sabri, W. Almobaideen "Lightweight Identity Based Signature for Mobile Object Authentication in the Internet of Things," Journal of Theoretical & Applied Information Technology, vol. 96, no. 3, pp.788-798, 2018.
[64] M. R Asassfeh, M. Qatawneh, and F. M AL-Azzeh, "Performance evaluation of blowfish algorithm on supercomputer iman1," International Journal of Computer Networks & Communications (IJCNC), vol. 10 no. 2 , 2018.
[65] U. Verma, and D. Bhardwaj, "Design of Lightweight Authentication Protocol for Fog enabled Internet of Things-A Centralized Authentication Framework," International Journal of Communication Networks and Information Security, vol. 12 no. 2, pp. 162-167,2020.

Table 1. Comparison between surveys deal with authentication in IoT

Author	Anonymity	Scope of survey	Architecture Components	Stationary/mobile	Year
El-hajj et al [1]	Not mentioned	Authentication protocols for IoT	1. Machine-to-Machine (M2M) 2. Human-to-Machine (H2M)	Mobile	2019
Sey [2]	Anonymous	Authentication approaches for IoT.	1.Authentication Cloud Sever. 2.Home IoT Server (HIoTS). 3.Sensor nodes (SNs).	Mobile and stationary	2018
Kavianpour et al. [3]	Not mentioned	Various authentication mechanisms in the context of Heterogeneous Devices IoT have been investigated in a comprehensive and systematic way.	1. IoT-cloud architecture 2. Scheme depends on physical unclonable functions (PUFs).	Mobile and stationary	2019
Ferrag et al [4]	Anonymous	Comprehensive review of authentication approaches for the IoT.	1. M2M communication 2. Internet of vehicles (IOV) 3. Internet of Energy (IOE) 4. Internet of sensor (IOS)	Mobile and stationary	2016
Das et al [5]	Not mentioned	Present a taxonomy of security protocols for the IoT.	1. IoT devices 2. Gateway node 3. Users	Mobile and stationary	2018
e Silva et al [6]	Not mentioned	Systematic Mapping and Highlighting of the security issues and the main approaches used in authentication solutions for IoT.	1.RFID Tag, Tag Reader, Server. 2.Sensor node, Gateway, Server.	Mobile and stationary	2017
Joshitta et al [7]	Not mentioned	Analytical survey of existing IoT authentication protocols.	1. IoT devices. 2. Gateway node. 3.Cloud server.	Mobile and stationary	2016
Saadeh et al [31]	Not mentioned	Authentication Techniques for IoT.	1. Centralized. 2. Distributed. 3. Hierarchical. 4.Flat.	Mobile and stationary	2017
Saadeh et al [61]	Not mentioned	Object Authentication in IoT.	1. Centralized 2. Hierarchical 3. Decentralized flat	Mobile and stationary	2020

TABLE 2. Resistance to Threat Attack comparison

Paper	Impersonation attack	Replay attack	Modification attack	Man in the middle Attack,	Denial of Service
He et al [8]	✓	✓	✓	✓	-
Saxena et al [9]	✓	✓	✓	✓	-
Wu et al [10]	✓	✓	✓	✓	-
Joshitta et al [11]	-	✓	-	✓	-
Amin et al [12]	-	✓	✓	✓	-
Khemissa et al [13]	✓	✓	✓	-	✓
Arasteh et al [14]	✓	✓	-	-	✓
Srinivas et al [15]	✓	✓	-	-	✓
Fan et al [16]	-	✓	-	-	✓
Das et al [17]	✓	✓	-	✓	✓
Ali et al [18]	✓	✓	-	✓	-

Li et al [19]	✓	✓	-	-	✓
Challa et al [20]	✓	✓	-	✓	✓
Aghili et al [21]	✓	✓	-	-	-
Chen et al [22]	-	-	-	✓	-
Li et al [23]	✓	✓	✓	✓	-
Wazid et al [24]	✓	✓	-	✓	-
Gope et al [25]	✓	✓	✓	✓	-
Shuai et al [35]	✓	✓	-	-	-
Soni et al [52]	✓	✓	✓	✓	✓

TABLE 4. Classification according to some Authentication Features and validation tools

Paper	**Freshness identifier**	**Authentication type**	**Validation type**	**Mobile/ Stationary**	**Simulation\ Implementation**
He et al [8]	Time stamp	Authentication with certificate	Formal mathematical proof(validation)	Mobile	—
Saxena et al [9]	Time stamp	Certificateless authentication	Security analysis in terms of goals and proprieties	Mobile + Stationary	—
Wu et al [10]	Random nonce	Certificateless authentication	Proverif tool	Mobile	NS-3
Joshitta et al [11]	Random nonce	Certificateless authentication	Formal security analysis	Mobile	—
Amin et al [12]	Random nonce	Certificateless authentication	AVISPA tool +Ban logic	Mobile	—
Khemissa et al [13]	Random nonce	Certificateless authentication	Informal security analysis	Stationary	—
Arasteh et al [14]	Random nonce	Certificateless authentication	Informal security analysis	Stationary	—
Srinivas et al [15]	Time stamp	Certificateless authentication	Real Or Random (ROR) model + AVISPA tool + informal security analysis	Mobile + Stationary	—
Fan et al [16]	Random nonce	Certificateless authentication	Ban logic	Mobile + Stationary	FPGA
Das et al [17]	Time stamp	Certificateless authentication	Real-Or-Random (ROR) model+ AVISPA tool	Mobil	NS2
Ali et al [18]	Time stamp	Certificateless authentication	Ban logic + AVISPA tool	Mobile	—
Li et al [19]	Time stamp	Certificateless authentication	Informal security analysis	Mobile + Stationary	—
Challa et al [20]	Time stamp	Authentication with certificate	Real Or Random model (ROR)+Ban logic+ AVISPA tool	Mobile	—
Aghili et al [21]	Random nonce	Certificateless authentication	Ban logic+ informal security analysis	Mobile + Stationary	FPGA
Chen et al [22]	Time stamp	Authentication with certificate	Proverif +AVISPA tool	Mobile + Stationary	Visual studio C++

Li et al [23]	Time stamp	Authentication with implicit certificate	Real Or Random (ROR) model	Mobile	—
Wazid et al [24]	Time stamp	Certificateless authentication	Real Or Random (ROR) model +AVISPA tool	Mobile	NS2
Gope et al [25]	Random nonce	Certificateless Authentication	Informal security analysis	Mobile	—
Shuai et al [35]	Time stamp	Certificateless Authentication	Ban logic	Mobile	—
Soni et al [52]	Time stamp	Authentication with implicit certificate	Ban logic + AVISPA tool	Mobile + Stationary	—

TABLE 6. Computation cost of the schemes

Paper reference	Ui	GW/Server	Si	Total Cost
Wu et al [10]	$11T_h$	$17\ T_h$	$6\ T_h$	$34\ T_h \approx 0.0109$ s
Joshitta et al [11]	T_{ECM}	$3\ T_h + 2T_{ECM}$	T_{ECM}	$3T_h+4\ T_{ECM} \approx 0.0694$ s
Amin et al [12]	$12\ T_h$	$18\ T_h$	$6\ T_h$	$36\ T_h \approx 0.0115$ s
Khemissa et al [13]	$4T_h + T_{ED}$	$2T_h$	$2T_h + T_{ED}$	$8T_h + 2T_{ED} \approx 0.0138$ s
Arasteh et al [14]	$5T_h$	8Th	$5T_h$	$18Th \approx 0.00576$ s
Srinivas et al [15]	$8T_h + 2T_{ED}$	$4Th + T_{ED}$	$4T_h + 2T_{ED}$	$16T_h + 5\ T_{ED} \approx 0.0331$ s
Das et al [17]	$10T_h + T_{FE}$	---	$7T_h$	$17T_h + T_{FE} \approx 0.0225$ s
Ali et al [18]	$11T_h + 2T_{ED}$	$`16T_{h+}3T_{ED}$	$6T_h + T_{ED}$	$33T_h + 6T_{ED} \approx 0.0442$ s
Li et al [19]	$5T_h + T_{FE} + 2T_{ED}$	$6T_h + 6T_{ED}$	$5T_h + 2T_{ED}$	$16T_h + T_{FE} + 10T_{ED} \approx 0.0782$ s
Challa et al [20]	$10\ T_h + T_{FE} + 2T_{ECD}$	$4T_h + T_{ECM}$	$5T_h$	$19T_h + T_{FE} + 3T_{ECM} \approx 0.0745$ s
Chen et al [22]	$5\ T_h + 2T_{ECM}$	$8T_h$	$4T_h + 2T_{ECM}$	$17T_h + 4T_{ECM} \approx 0.0738$ s
Li et al [23]	$8\ T_h + 2T_{ECM}$	$4T_h + T_{ECM}$	$4T_h$	$16\ T_h + 3T_{ECM} \approx 0.0564$ s
Wazid et al [24]	$6\ T_h$	$7T_h + 2T_{ED}$	---	$7Th + 2T_{ED} \approx 0.0134$ s
Gope et al [25]	$7\ T_h + 2\ T_{ED}$	$7\ T_h + T_{ED}$	T_{ED}	$14\ Th + 4\ T_{ED} \approx 0.0269$ s
Shuai et al [35]	$11T_h + T_{FE}$	$12T_h$	$7T_h$	$30Th + T_{FE} \approx 0.0267$ s
Soni et al [52]	$13T_h + 3T_{ECM} + T_{FE}$	$12T_h + 3T_{ECM}$	$6T_h$	$31T_h + 6\ T_{ECM} + T_{FE} \approx 0.1296$ s

Table 7. Network technology and architecture components comparison

paper	Type of network	Architecture components	Field of application	Year
He et al [8]	WBAN	It consists of: network manager, application provider, WBAN client	Healthcare	2017
Saxena et al [9]	LTA	It used the LTE network which consists of user entity (UE), mobility management entity (MME), home subscriber server (HSS)	IoT environment	2016
Wu et al [10]	WMSN	It used (WMSN) which consists of Users like doctors, Gateway node, and patient with sensors.	Healthcare	2017
Joshitta et al [11]	WBAN	It composes of: medical devices, patient, authentication server	Healthcare	2017
Amin et al [12]	WMSN	It used (WMSN) which consists of patient with monitoring sensors, Gateway node.	Healthcare	2016
Khemissa et al [13]	WSN	It used (WSN) which composes of: sensor node, gate way node and the remote user.	IoT environment	2016
Arasteh et al [14]	WSN	It composes of: sensor node, gate way node, user with smartcard.	IoT environment	2016
Srinivas et al [15]	WMSN	It used (WMSN) which composes of users like doctors and nurses, Gateway node, tiny sensors connected to patient.	Healthcare	2017
Fan et al [16]	RFID	It used RFID which composes of RFID tag, tag reader, server.	Healthcare	2018
Das et al [17]	Bluetooth	It composes of: Wearable devices (WD) and Mobile Terminal (MT) and Cloud Server (CS).	Healthcare	2017
Ali et al [18]	WMSN	It used (WMSN) which consists of users like doctors, Gateway node, and patient with sensors.	Healthcare	2018
Li et al [19]	WMSN	It used (WMSN) which consists of users like doctors, Gateway node, and patient with sensors.	Healthcare	2015
Challa et al [20]	WMSN	It used (WMSN) which consists of users like doctors, Gateway node (Trusted authority TA), and patient with sensors.	Healthcare	2017
Aghili et al [21]	RFID	It used (RFID) which consists of RFID tag, RFID Reader, and database server.	Healthcare	2019
Chen et al [22]	WSN	It consists of: user, gate way, sensors.	Healthcare	2017
Li et al[23]	WSN	The scheme composes of: user like doctors, Trusted Authority (TA), patient with sensors.	Healthcare	2017
Wazid et al [24]	NFC	It used NFC which consists of NFC tag (mobile device MU), Authentication server.	Healthcare	2017
Gope et al [25]	BSN	The scheme composes of: wearable sensors, local processing unit (LPU) which act as a router, central server called (BSN)-care server	Healthcare	2016
Shuai et al [35]	WMSN	The scheme composes of sensor node, user, and gateway node	Healthcare	2019
Soni et al [52]	WMSN	The scheme composed of : user like doctors, Trusted Authority (TA), patient with sensors.	Healthcare	2019