SN Computer Science (2022) 3: 382
https://doi.org/10.1007/s42979-022-01300-z

SURVEY ARTICLE

Authentication Schemes for Healthcare Applications Using Wireless Medical Sensor Networks: A Survey

Anwar Noureddine Bahache[1,2] · **Noureddine Chikouche**[3] · **Fares Mezrag**[3]

Received: 11 February 2022 / Accepted: 5 July 2022 / Published online: 18 July 2022

Abstract

Many applications are developed with the quick emergence of the Internet of things (IoT) and wireless sensor networks (WSNs) in the health sector. Healthcare applications that use wireless medical sensor networks (WMSNs) provide competent communication solutions for enhancing people life. WMSNs rely on highly sensitive and resource-constrained devices, so-called sensors, that sense patients' vital signs then send them through open channels via gateways to specialists. However, these transmitted data from WMSNs can be manipulated by adversaries without data security, resulting in crucial consequences. In light of this, efficient security solutions and authentication schemes are needed. Lately, researchers have focussed highly on authentication for WMSNs, and many schemes have been proposed to preserve privacy and security requirements. These schemes face a lot of security and performance issues due to the constrained devices used. This paper presents a new classification of authentication schemes in WMSNs based on its architecture; as far as we know, it is the first of its kind. It also provides a comprehensive study of the existing authentication schemes in terms of security and performance. The performance evaluation is based on experimental results. Moreover, it identifies some future research directions and recommendations for designing authentication schemes in WMSNs.

Keywords Authentication schemes · Healthcare applications · Resource constrained · Security · Wireless medical sensor networks

Introduction

Recently, with the Covid-19 appearance and the spread of this lethal epidemic worldwide, quarantine was a must for the infected people. With the infected people being quarantined, doctors had to watch their vital signs while minimising the amount of interaction with them to avoid getting infected. In this context, IoT-based healthcare applications played a critical role in remote patient monitoring and providing real-time access to health data. Based on these provided data, professionals can provide treatments or diagnose different diseases, where so many papers were proposed to diagnose this pandemic from such data [1–4]. In addition, these technical advances and services in e-health helped in increasing human life expectancy [5]. This led to an absolute need to develop sophisticated and well-designed electronic healthcare systems to provide a good life quality and longer lifespan and reduce the outlay cost needed to visit doctors. As it is known, tele-patient monitoring is one of the e-health applications that use wireless medical sensor networks (WMSNs).

In order to provide these high-quality healthcare applications, WMSN was introduced in 1996 by Zimmerman [6] a technology that helps in patient tele-monitoring and many other applications. This technology can capture vital health signs and transmit them to healthcare providers. They can use these health data in analysing or other actions by professionals. WMSNs can be seen as wearable or implantable devices connected to data sinks such

✉ Anwar Noureddine Bahache
anwarnoureddine.bahache@univ-msila.dz

Noureddine Chikouche
noureddine.chikouche@univ-msila.dz

Fares Mezrag
fares.mezrag@univ-msila.dz

[1] Department of Computer Science, University of M'sila, BP. 166 Ichebilia 28000 M'sila, Algeria

[2] Laboratoire d'Analyse des Signaux et Systèmes, Université Mohamed Boudiaf - M'Sila, M'sila, Algeria

[3] Laboratory of Informatics and its Applications of M'sila, University of M'sila, BP. 166 Ichebilia 28000 M'sila, Algeria

as personal assistants (PDAs)/smart devices that transfer the measured data to professionals via open channels for decision-making. These devices are widely used in healthcare applications which helps in achieving higher and better healthcare system values. In addition, this helps in improving citizen's life and increasing health indexes for countries. Health indexes for each country can be found detailed in [7].

The increased demand on WMSN for healthcare applications led to the development of a new international communication standard IEEE 802. 15.6 [8] which presented new lightweight communication protocols and lower power sensor devices to expand the applications of WMSN. Many healthcare systems are based on these devices and standards. Nevertheless, deploying these systems into the field is not possible without considering data security. Security failures in transferring patient lethal health data may lead to death sometimes. Hence, the collected and transferred data must be transmitted securely to authorised healthcare system providers and professionals. Further, the aforesaid devices, so-called sensors, are resource-constrained. Therefore, lightweight security mechanisms are inevitable to ensure that only legitimate authorities can access these vital data. In addition, protecting these data from being manipulated must be considered.

Among the used mechanisms to secure the WMSNs, we have authentication schemes, where they can ensure that only legitimate parties can access the transferred data and ensure that the data are legitimate and does not get modified by any adversary. Authentication schemes are considered as first-level mechanisms that ensure privacy and security requirements in WMSNs. The adoption of these schemes in WMSNs faces a lot of stability and performance issues due to the low capabilities of the used devices. The main reason for the aforementioned issues is the traditional cryptographic primitives usually used to secure authentication schemes such as RSA (Rivest–Shamir–Adleman) cryptosystem. These primitives put a lot of storage, calculation and energy exhaustion on the devices used in such networks. Lately, many techniques have been adopted to provide authentication schemes that are suitable and secure for WMSNs, for instance, using suitable cryptographic primitives. Among these primitives, we have: bitwise operators, one-way hash, symmetric encryption, elliptic curve cryptography (ECC), and pairing-based cryptography (PBC). In recent years, these primitives were widely adopted to secure the authentication in WMSNs.

In this paper, our contributions are summarised as follows:

- Providing a literature review of the existing surveys on authentication schemes for healthcare applications, we also include the comparison between them.
- Discussing different security requirements and possible attacks in authentication schemes in WMSNs. In addition, discussing the most used verification techniques that exists in the literature.
- Classifying studied authentication schemes based on healthcare system architecture on two main classes: user-based authentication schemes (UAS) and node-based authentication schemes (NAS), and as far as we know this is the first paper to classify authentication schemes based on these classes.
- Discussing and comparing surveyed schemes along with their strength and weaknesses in terms of security requirements, attacks, formal security verification techniques and performance costs.
- Evaluating the performance of studied schemes in terms: computational, storage, communication and energy costs. This evaluation is based on experimental results; we estimate the computational and energy costs of the studied schemes on an emulated WiSmote sensor platform.
- Providing directions of future research in the area of authentication schemes for WMSNs in order to design a secure and efficient authentication schemes.

The remainder of this survey paper is structured as follows: in the next section, we discuss the existing surveys on authentication schemes for healthcare applications. The third and fourth sections present WMSNs and the background on authentication schemes security, respectively. We present the research methodology in the fifth section. In the sixth section, the classification of authentication schemes in WMSNs and discussing them are provided in details. The security and performance evaluation is presented in the seventh section. Finally, in the eighth section, we discuss some directions of future research, and in the last section, we conclude our work.

Existing Surveys on Authentication Schemes for Healthcare Applications

Over the past decade, different studies and surveys have been conducted for healthcare applications. Several of them focussed on the security part and its application, giving a general overview of security essentials while highlighting the issues, requirements, and possible solutions, such as [9, 10]. In our study, we focussed only on surveys that included authentication schemes in WMSNs to be more specified. The different existing surveys that are related to authentications schemes in healthcare applications are listed in Table 1.

Aqeel-ur-Rehman et al. [11] conducted a critical review for some of the proposed authentication schemes for WBAN (Wireless Body Area Network) as per IEEE standard. From Table 1, we can notice that Aqeel-ur-Rehman et al. [11]

Table 1 Comparison of our survey with existing surveys

Survey paper	Year	SN	CL	SL	Security evaluation		Performance evaluation				O/F
					SF	FT	CC	SC	EC	CO	
Aqeel-ur-Rehman et al. [11]	2013	✓	*	✓	*	×	×	×	×	×	×
Masdari and Ahmadzadeh [12]	2016	✓	✓	✓	×	×	×	×	×	×	×
Wazid et al. [13]	2016	*	✓	✓	✓	×	✓	×	×	✓	✓
Aslam et al. [14]	2017	×	✓	✓	✓	×	✓	×	×	×	×
Joshi and Mohapatra [15]	2019	✓	*	*	×	×	×	×	×	×	*
Hussain et al. [16]	2019	✓	✓	✓	*	×	*	×	×	×	✓
Sowjanya and Dasgupta [17]	2020	✓	*	✓	✓	×	×	×	×	×	✓
Narwal and Mohapatra [18]	2020	*	✓	✓	✓	✓	×	×	×	×	✓
Our survey	-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

SAS: surveyed authentication schemes, SN: using sensor node in systm model of SAS, CL: classification, SL: surveying the literature of the SAS SF: security flaws in SAS, FT: formal security verification techniques CC: computational cost evaluation of SAS, SC: storage cost evaluation of SAS EC: energy cost evaluation of SAS, CO: communication overhead evaluation of SAS O/F: Open research issues/Future research directions ✓ indicates fully supported; × indicates not supported; * indicates partially supported

surveyed some of the literature authentication schemes by discussing partially some of the security flaws in each scheme. The authors highly focussed on IEEE standards used in studied schemes and ignored the security and performance issues. In the same paper, the classification approach was not clear and cannot be generalised for future works. This paper lacks a detailed security analysis and performance evaluation.

Masdari and Ahmadzadeh [12] analysed the existing authentication schemes in the WMSNs field. Moreover, they provided a classification based on the authentication technique applied in each with a detailed illustration. In addition, they highlighted the advantages and limitations of each discussed scheme with a comparison of their capabilities and features. For this paper's shortcoming, the authors did not give any security or performance analysis for the studied schemes.

Wazid et al. [13] discussed the security requirements, issues and threats that may face m-health systems. Moreover, they gave a taxonomy of the proposed security protocols in that period, demonstrating the strength and weaknesses in each with its computation and communication costs comparison. At the end of the paper, the authors presented challenges in security protocols for m-Health systems. However, the surveyed schemes did not fully address the sensor nodes (most focussed on telecare medicine). Even though the authors discussed security flaws, computational costs and communication costs, they did not discuss verification techniques, storage cost and energy cost, which are considered as main factors that impact the reliability of the schemes.

Aslam et al. [14] reviewed the authentication schemes that were proposed for telecare medicine and discussed the strengths and weaknesses of each based on the ensured security properties and computational cost. Moreover, they classified the schemes into three major categories based on the authentication factors. In the performance part, the authors adopted an approach based on the number of operations to decide whether the user/server efficiency is high, medium or low. Using this approach, the authors assumed that all operations have the same costs, which is not valid if we compare the performance of the studied schemes. In this survey, we notice that all the studied schemes did not include any sensor nodes in their system model (architecture). In addition, in the performance evaluation part, it is clear that the authors only compared the schemes based on the computational costs; such comparison is not enough to decide what schemes are more suitable and practical for this field.

In 2019, Joshi and Mohapatra [15] discussed various authentication schemes for WMSN/WBAN, pointing out the design issues in the protocols. They also listed the four types of authentication (crypto-based, biometric-based, channel-based and proximity-based) along with security requirements, and they concluded their work with future directions. Besides, this paper did not discuss any security or privacy issues or requirements. In addition, it lacks any performance evaluation.

In the same year, Hussain et al. [16] reviewed various authentication schemes with two types of classification. They also compared the different authentication schemes and highlighted their pros, cons, limitations, challenges, performance evaluation and robustness against different security attacks. However, the performance evaluation and security analysis conducted are partial. Concerning the security part, the authors only pointed out some of the found attacks. The performance part discussed only a part of the computational costs, and no storage/energy/communication costs were dealt with. Such a study is incomplete and does

not give detailed information on the short comes of surveyed authentication schemes.

Recently, Sowjanya and Dasgupta [17] presented their survey on symmetric and asymmetric key management protocols. They studied the relevant key management schemes (symmetric and asymmetric) in a period of six years. Then, they compared the schemes in terms of security features provided with a description of their pros and cons. However, this paper lacks an in-depth classification for authentication schemes. Even though the authors mentioned that the IoT devices used in WMSN are resource-constrained, they focussed only on the security analysis and ignored the performance issues. At the same time, Narwal and Mohapatra [18] presented a detailed survey on security and authentication in WMSN. An extensive review of security requirements, threats, attack techniques and possible solutions. Then they presented a classification of these security mechanisms focussing on the authentication approach, design, development and classification. Authentication scheme design steps are described in detail in this paper. In addition, adversary models and security protocols verifiers are presented with future open issues and future recommendations. However, they did not evaluate authentication schemes in terms of performance. However, this paper focussed on security analysis and classification and ignored the performance evaluation.

Based on the discussion above, we clearly notice that all the surveys lack a detailed security or performance evaluation for the studied schemes. These evaluations are considered critical factors in deciding what schemes are more suitable and practical for this field. Therefore, conducting a paper that gives detailed insight is needed. Unlike existing surveys, this survey presents a new classification of authentication schemes in WMSNs based on its architecture and evaluates different studied schemes in terms of security and performance. The performance evaluation is based on experimental results, we estimate the computational and energy costs of the studied schemes on an emulated WiSmote sensor platform, and we implement different cryptographic primitives using the RELIC Toolkit library. Moreover, we present several directions of future research depending on authentication schemes in WMSNs.

Wireless Medical Sensor Networks

Wireless sensor networks (WSNs) are known to be a group of connected sensors dedicated to sensing and monitoring [19, 20]. These sensors, which can be denoted as nodes, communicate and send the collected data through wireless links (gateways). The collected information will be forwarded to a central location (servers, databases, etc.) where it will be used. On the other hand, IoT can be seen as a group of connected machines, devices, and many other forms of physical, electronic equipment embedded with sensors dedicated to sensing and monitoring. These sensors enable the inter-connected devices to communicate and exchange data over the Internet or other communications networks. In IoT environment, embedded sensors send their data over the internet directly using IP protocols or indirectly via gateway or in other manners. Conversely, in a WSN, the sensors send the collected data to gateways that are responsible for routing this information to servers via the internet or other communication channels, and no direct communication shall exist.

As WMSN is a sub-net of WSN that used in e-health, they differ in terms of scale number where the WSN being larger includes hundreds of nodes, when WMSN has a small scale of about 20 nodes per body [21]. Moreover, WSN may communicate over kilometres, unlike WMSNs that are limited to metres. In addition, they are different in terms of energy usage/consumption (WSN: batteries, solar, wind power. WMSN: small batteries), calculation limitations (WSN has more calculation power), accuracy (WMSNs are more accurate than WSN), mobility (WMSN more mobile since it is implanted or body mounted. WSN can be static), node replacement and node size.

One of the many applications of WSN under IoT embedded environments is e-health. Different sensors are being implanted and used to monitor patients' biological signs and habits, making it easy to transfer this information to specialists for decision-making or even in sometimes automatically injecting medicines [22]. The collected and sensed information is being sent from the nodes to servers, specialists for diagnostic or database records through gateways. This technology in the health field gave the health specialists new opportunities in healthcare and patient monitoring.

Architecture of WMSNs

Depending on the approach and the application domain, different architectures of WMSNs under IoT environments can be seen in the literature. All the existing works in the literature share a basic three levels of architecture that exists in all. This basic architecture should exist in any WMSN-based e-health application under an IoT environment. Figure 1 shows the typical architecture of wireless medical sensor networks that rely on three different primary levels:

Level 1: It represents a special type of sensors so-called medical sensors. These nodes can measure, monitor and collect a specific biological sign continuously. Then these collected data are transferred to level 2 devices.

Level 2: Mainly can be seen as gateways (e.g. personal digital assistants, PDAs, computers, and smartphones) that represents the middle link between level 1 and level 3 devices, where they are responsible for transferring the

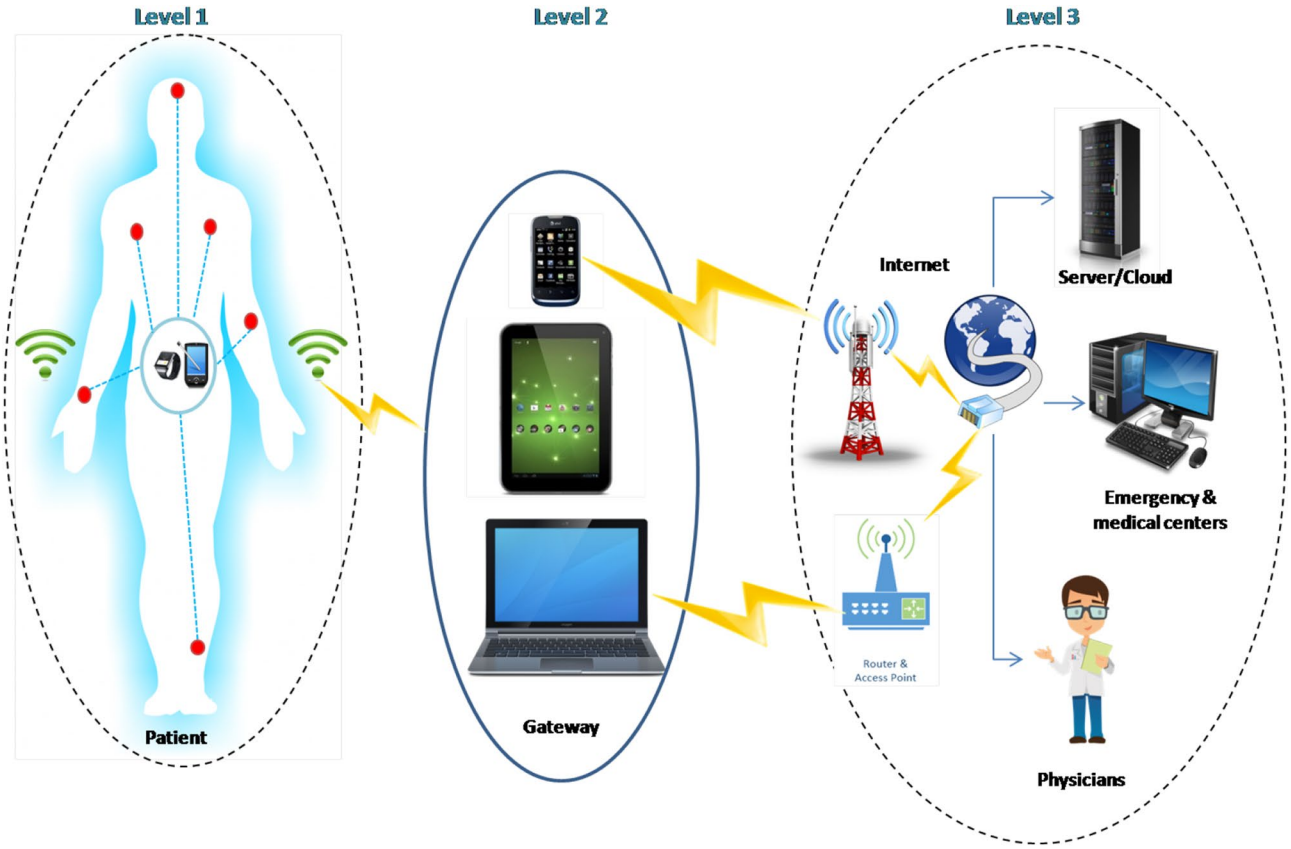

Fig. 1 Architecture of wireless medical sensor networks

collected data from nodes in level 1 to end level 3 users via open channels.

Level 3: The received data and information from level 2 devices are transferred to end-users via the internet at this level. These users differ depending on the design of WMSN where they can be: cloud, emergency physicians, professionals, service providers, data analysts, family members or even the patient himself.

Medical Sensors

Wireless medical sensors are a special kind of IoT sensors used to quantify physiologic metrics such as temperature, blood pressure, heart rate, electrocardiogram (ECG), and respiration. These sensors transmit the quantified biological information to a control device worn on the body or placed in an accessible location [23, 24]. Medical sensors can be divided into implant node, clothes attached, and body surface node(wearable). Each type can be seen and used differently [21, 25]. Mostly it can be seen as implanted or wearable devices. Due to it being related to the human body, it is used in medical and healthcare applications.

The medical IoT sensors have many types according to their functions, such as the electrocardiogram (ECG), electroencephalogram (EEG), blood pressure, and body temperature sensors. For example, the ECG sensor is used to monitor the heart rhythm and diagnose abnormal patterns. However, an EEG sensor is used to test and detect abnormalities in the brain's electrical activities. For more information about the types of medical sensors, we refer the reader to [26].

Medical sensors are constrained IoT devices that have many limitations. The primary limitations that should be taken into consideration are [27–29]:

Bandwidth: These constrained IoT devices typically have low data rates and mainly being used in simple applications to transfer small amounts of data. This bandwidth limitation limits the amount and speed of transmission. Therefore, it is not possible to implement complex protocols on them.

Memory capacity: The RAM capacity on these devices is minimal and variate from some to dozens of kilobytes. In addition, the storage capacity in such devices is minimal. The storage limitation requires only necessary data for implementing communication and security protocols to be stored.

Energy capacity: These devices are attached with power sources (batteries) that have limited energy and have to be recharged or replaced.

Computation capacity: This is an indicator of the amount of computing power a medical IoT sensor possesses. The computing power variate from low to medium and mostly low, therefore, adopting lightweight communication and security protocols to operate correctly.

Based on the limitations mentioned above, medical IoT sensors can be classified in terms of the capacities they hold. The Internet Engineering Task Force (IETF) has a classification for resource-constrained IoT devices (including medical sensors) [28]. Using this classification, we focus our efforts on medical sensors belonging to class 1 and class 2, given that they are the only ones that support the security functions and have enough power to run a protocol stack defined explicitly for medical sensors.

WMSNs for Healthcare Applications

Many e-health applications rely on WMSNs to achieve the needed efficiency and quality. Due to the significant capabilities that WMSN has, many new e-health applications in the areas of medicine, home healthcare, patient monitoring, and many more are being widely adopted [30–34].

In the following, we will list and describe a few of the most general healthcare applications nowadays:

- **Records**: It represents different types of health reports, and we can distinguish three forms of e-health record usage.
  - **Electronic Health Record (EHR)**: An e-version of patient's overall health reports that contains a clear description for the patient's health, which should be available securely to authorised users [31].
  - **Electronic Medical Record (EMR)**: An e-report that contains the entire history of a single patient from a specific clinic [32].
  - **Personal Health Record (PHR)**: A report where the patient keeps his health-related data in secret, private and a confidential spot [33].
- **Remote health monitoring**: Remote health monitoring is an automatic medical service for monitoring patients' vital signs through WMSNs. Different types of sensors can be placed on/in the patient's body to monitor his biosigns, such as heartbeats, blood pressure, and temperature. All the gathered and monitored data can be stored in a control unit or transferred remotely.
- **Assisted living**: The usage of WMSNs in health also offered a new type of healthcare where the patient can stay at home while wearing wearable medical sensors. These medical sensors continuously measure the physiological signs of the patients. It can store and transfer this data in a regular interval, or in another case; it can inject patients automatically with specific medicament (e.g. in the case of blood sugar sensors, it can inject insulin when needed). There is also the possibility of raising the alarm to the nearest health centre when needed.
- **Telecare medicine** Another field of e-health that uses WMSN is telecare medicine. In this type, healthcare services can be provided over a distance with the help of information and communication technologies (WMSNs) [30]. Using video and sensor technologies, the doctor can prescribe medicament to patients with the tele-sensed data from patients at a distance without body presence.

Background on Authentication Schemes Security

This section presents the essential security and privacy requirements that must be achieved and the possible attacks that must be resisted on authentication protocols in WMSNs for IoT environments. In addition, we present a brief description of the most used formal security techniques for authentication schemes.

Security and Privacy Requirements

Authentication in WMSN for the IoT environment demands strict security and privacy requirements to guarantee the scheme quality. Down below, we mention the significant security and privacy needs that must exist in any authentication protocol in WMSNs [14, 35, 36]:

Secrecy: It means that secrets like patient identity can only be read by the authorised parties.

Integrity: Refers to preventing and ensuring that an unauthorised party cannot alter the data.

Authentication: It ensures that our communicating entities are legitimate and authentic.

Perfect forward secrecy: It ensures that any exposure in secret long term keys (e.g. session keys) used in authentication does not compromise the secrecy of past session keys established before this exposure took place.

Session key establishment: A session key must be established between the sensor node/user and the server/user to ensure the ongoing communication's security.

Anonymity: It refers to the privacy and the protection of the user's real identity. The user's real identity must not be revealed by any means where it should be unidentifiable.

Untraceability: It guarantees that the adversary can not trace the communication back to the user (or sensor node) or any other participant in that session.

Attacks on Authentication Schemes in WMSN

There exists a variety of attacks on authentication protocols in WMSNs. The most known attacks that must be taken into consideration are described as follows [37–41]:

Man in the middle attack: The adversary alters the communication secretly and intercepts the communication messages between two parties or more(e. g. user, server and sensor node). Here the adversary can modify or impersonate one of the entities in addition to stealing authentication data. The adversary can start a communication with one of the parties and send or receive critical data.

Replay attack: The adversary uses the captured data (mostly authentication messages) after a successful eavesdrop on the communication channel and maliciously replay it to get access to the system or as a legitimate entity.

DoS attack: The adversary floods the network with many captured or fake messages targeting the server or sensor, preventing it from providing services compromising its availability. During this attack, the replayed messages tend to consume all the resources of the server or sensor (storage, computation power and energy), stopping it from processing any further requests.

Desynchronisation attack: It happens in schemes that rely on updating secret information (e.g. IDs and secret shared keys) in one of the authentication entities before concluding the scheme. Here, the adversary either blocks or modifies the updated data. Therefore, the scheme will not run successfully in the next session because one of the entities has a different value of secret information resulting in a successful desynchronisation attack.

Impersonation attack: The adversary intercepts the real identity of one of the legitimate communicating parties or more to get access. We can distinguish two different types of this attack, and in the context of IoT, we can define a third type: server impersonation, user impersonation and sensor impersonation.

Node capture attack: In this attack capturing a node gives the adversary the ability to get a clear look at the state of the authentication protocol. Capturing a node also gives the adversary a hold on the cryptographic keys and primitive used. Due to that, he can clone and redeploy malicious nodes in the network.

Password guessing attack: The attacker tends to guess the user's password; this can happen when the attacker intercepts an encrypted password then tries to match it with pre-guessed passwords. It can also happen just by trying to guess the password without any intercepted passwords. The attacker can pre-compute thousands of password dictionaries and try to match them to find the unencrypted form of the password or generate thousands of passwords per second and match them with the captured one. This attack can take place in two possible ways: online guessing attack and offline guessing attack.

Stolen mobile attack: The attacker tends to extract the secret information stored in the smart card/mobile device to access the system or duplicate the device.

Privileged insider attack: This attack can be perpetrated on the system server by a person with authorised system access. This person can steal, modify, or delete the user's information from the system server compromising his privacy and system integrity.

Stolen verifier attack: To reduce the risks, in most authentication schemes that rely on passwords, the authentication server stores user's password verifier table rather than the actual passwords. In this attack, the adversary steals this table and then can impersonate a user.

Analytical attacks: In this attack, the adversary uses the cryptanalysis of the intercepted messages to recover a cryptographic key.

Wormhole attack: This attack happens when an adversary captures the transferred messages in a specific location and tunnel it to another location to a second adversary who replays it in another location area.

Formal Security Analysis Techniques

Researchers use a variety of security verification techniques to validate and test the security of the authentication schemes. Any scheme that does not contain any formal verification is considered incomplete. Here, we present the most known and used security verification techniques.

AVISPA tool: It is widely used to validate the authentication protocols in different environments because of the modular and expressive formal language for specifying protocols and their security properties that it provides. In order to specify the protocol, AVISPA adopts a role-based language called HLPSL (High-Level Protocol Specification Language). Formal techniques are model-checking, attack searcher, SAT and tree automate. These techniques can also be seen as the four steps for validating a protocol in AVISPA [42].

BAN-Logic: Burrows–Abadi–Needham logic was first presented by Burrows et al. in [43] to examine, verify and prove the logical correctness of authentication schemes. It consists of a set of logical rules that are used to define and analyse information exchange protocols. For that, it follows three steps to verify the messages: origin verification, freshness verification and Trustworthiness. It is widely used to confirm the validity of authentication protocols.

Proverif: It is an automatic tool and symbolic protocol verifier. It is based on the formal model Dolev–Yao and the representation of protocols as Horn clauses. This tool provides the following features: it supports and handles a variety of cryptographic primitives, an unbound number of

protocol sessions and unbound message space. It can prove the following properties: authentication, secrecy and equivalence between processes. [44].

ROM model: Bellare and Rogaway first presented it in [45]. They mainly presented this new tool to give us the ability to give a rigorous "security proof" for cryptographic protocols [46]. It is a random chosen mathematical function (typically a hash function) that responds to every unique query with a random response chosen uniformly from its output domain.

ROR model: Real Or Random Model is a widely used technique to confirm the security of authentication schemes. ROR is considered a key exchange protocol for two entities authentication. In this technique, the pre-assumed adversary can test, execute and send queries as many times as he wants.

Scyther: It is a push-button tool used for verification, falsification and the analysis of security protocols. It has the possibility of unbounded verification of cryptographic protocols. It supports an unbounded number of sessions and can analyse multi-protocols. The security protocols are represented in SPDL language in scyther [47].

Methodology

This research paper analyses publications related to authentication schemes in healthcare applications using WMSN. In order to collect relevant data on the subject, many publishers of primary research literature were taken into consideration, such as IEEE, Elsevier, Springer and ACM. We adopted the following methodology for paper selection:

1. Searching the following electronic databases: Web of Science, Scopus, IEEE Xplore, ScienceDirect, Directory of Open Access Journals (DOAJ) and JSTOR using keywords that are relative to WMSN authentication.
2. Gathering papers from step 1.
3. Reducing number of papers by removing those that are not peer-reviewed journals.
4. Pruning the papers and keeping only those that dealt with the sensor as a main component.
5. Classifying papers into two types: user-based schemes and node-based schemes.

Using the mentioned search databases in English and an initial search for authentication in healthcare yielded more than 85,000 literature results. We pruned the initial dataset to include ("Wireless body area network" or "WBAN" or " wireless medical sensor network" or "WMSN") and ("authentication scheme" or "authentication protocol") and ("healthcare application" or "health" or "e-health"). This prune narrowed the dataset to more than 1,700 results. The same dataset was refined to include only research papers from or in 2016. This refinement left us with a much smaller dataset (1000 results). Again, we limited the search to include propositions or improvements of authentication schemes. Another refine to papers dataset to include only papers that dealt with the sensor nodes as a main component in the authentication process. However, we exclude the schemes that only focus on the user side without intervening the sensor node in the authentication scheme, such as [48–50]. As a result, the number of surveyed schemes is 36.

We mention that we chose those that focus on the sensor as one of the main components because the sensors are being widely considered and applied in different fields of IoT, healthcare systems in our case. Moreover, as we all know, the sensor nodes face issues with classical cryptographic algorithms in authentication due to their resource constraints and limited capabilities.

Classification of Authentication Schemes in WMSNs

Researchers adopted different classifications for authentication schemes in order to analyse their performance and be appropriately classified. In our classification, we focussed on authentication schemes in healthcare WMSNs. Figure 2 shows some of the possible classifications used to classify the authentication schemes in WMSNs. In Table 2, we classified the surveyed schemes based on three categories: authentication factors, cryptographic primitives and architecture-based, in other words, system component-based.

For more detailed classification to better understand the schemes, we have adopted a new classification so-called "system component based" or "architecture based" classification. Moreover, this classification is based on the involved communicating entities in WMSN that can be seen as user, nodes, server and gateways. The architecture classification that enables different medical scenarios (medical applications). The possible medical applications differ based on the communication between the entities. The main reason to adopt this classification is that we noticed that the literature contains different WMSN architectures that varieties depending on the possible medical scenarios that it will be applied on. In this classification, we can distinguish between user-based authentication schemes (UAS) and node-based authentication schemes (NAS). Different system architecture models (different entities) enable different applications. For example, telecare and living application need to communicate with the user (e.g. doctor) via WMSN. For these reasons, we use user-based schemes. Moreover, in the personal records application, the communication is focussed only between entities of WMSN (sensors and gateway); the node-based schemes are suitable for this scenario.

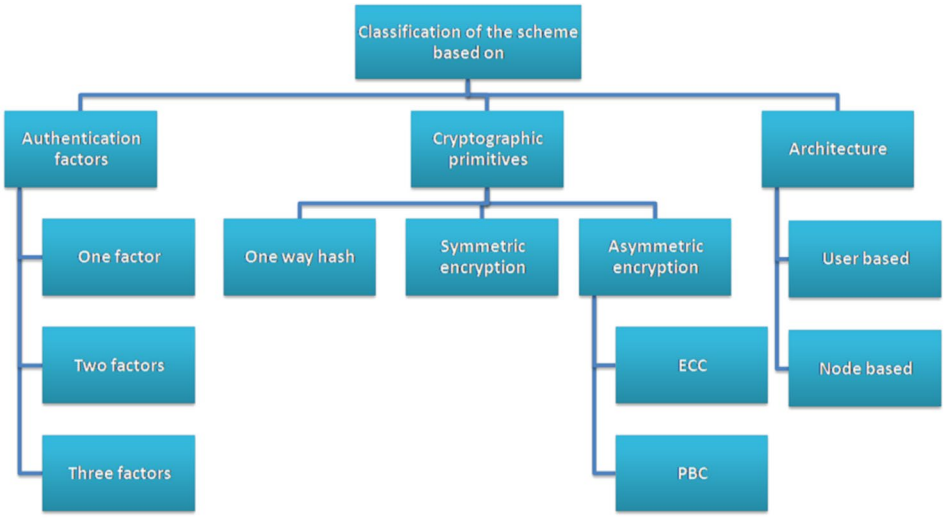

Fig. 2 Classification of authentication schemes in WMSNs

Table 2 Classification of the studied authentication schemes in WMSNs

Classification		Scheme
Authentication factor	Two factor	[51] [52] [53] [54] [55] [56] [57] [58] [59]
	Three factor	[60][61] [62][63] [64][65] [66] [67][68] [69][70] [71][72] [73][74] [75]
Cryptographic primitives	Hash function	[60] [61] [62][76] [63][51] [64][65] [52] [77][53] [78][54] [79][80] [81][82] [66] [55] [68] [83][69] [70][71] [56][57] [72][58] [73][84] [74][59][75] [85]
	Symmetric cryptography	[61][63] [65][53] [66] [56][58][75]
	Asymmetric cryptography	[62][64] [52][81] [55][68] [71][57] [73][74] [85]
Architecture	Node authentication schemes	[76] [77][78] [79][80] [81][82] [83][84][85]
	User authentication schemes	[60][61] [62][63] [51][64] [65][52] [53] [54][66] [55] [67][68] [69][70] [71][56] [57] [72] [58][73] [74][59][75]

We based our classification choice on the fact that a fair comparison between different schemes in terms of security and performance cannot be made unless we divide the schemes into UAS and NAS due to the following reasons: there are some specific attacks on the user side, an overhead comparison cannot be made since the user schemes have one more communication entity. Therefore, we cannot compare a scheme that has a user with another that does not have. Therefore, in order to give the performance evaluation more credibility, we adopted the Architecture-based classification. We will describe the two architectures with a presentation and a brief description of the related scheme in each class. Figure 3 shows different components of each architecture.

Bellow, we present different studied schemes according to their architecture classification. A Discussion on their strengths and limitations in terms of security and performance will be presented in Sect. 7.

User-Based Authentication Schemes (UAS)

In this class, we notice three main system components: user, gateway node and sensor node. The authentication process is mutual between every two entities in the scheme: user-gateway, gateway-sensor and user-sensor and vice versa. The user can use a smart card/mobile to authenticate in this class. He may also only use a password. In this class, the communication channels between two entities are open and insecure; therefore, they are vulnerable to several attacks. Many authors adopted the authentication factors in UAS as a means to increase the security of the authentication and make sure that the user is legitimate. Authentication factors variate depending on the usage and the authors; we may find one factor (1FA) password, two factors (2FA) password and smart card/mobile, or even three factors (3FA) which include all the stated factors plus biometrics. Mostly, in UAS, we can find two categories 2FA and 3FA, used to increase the

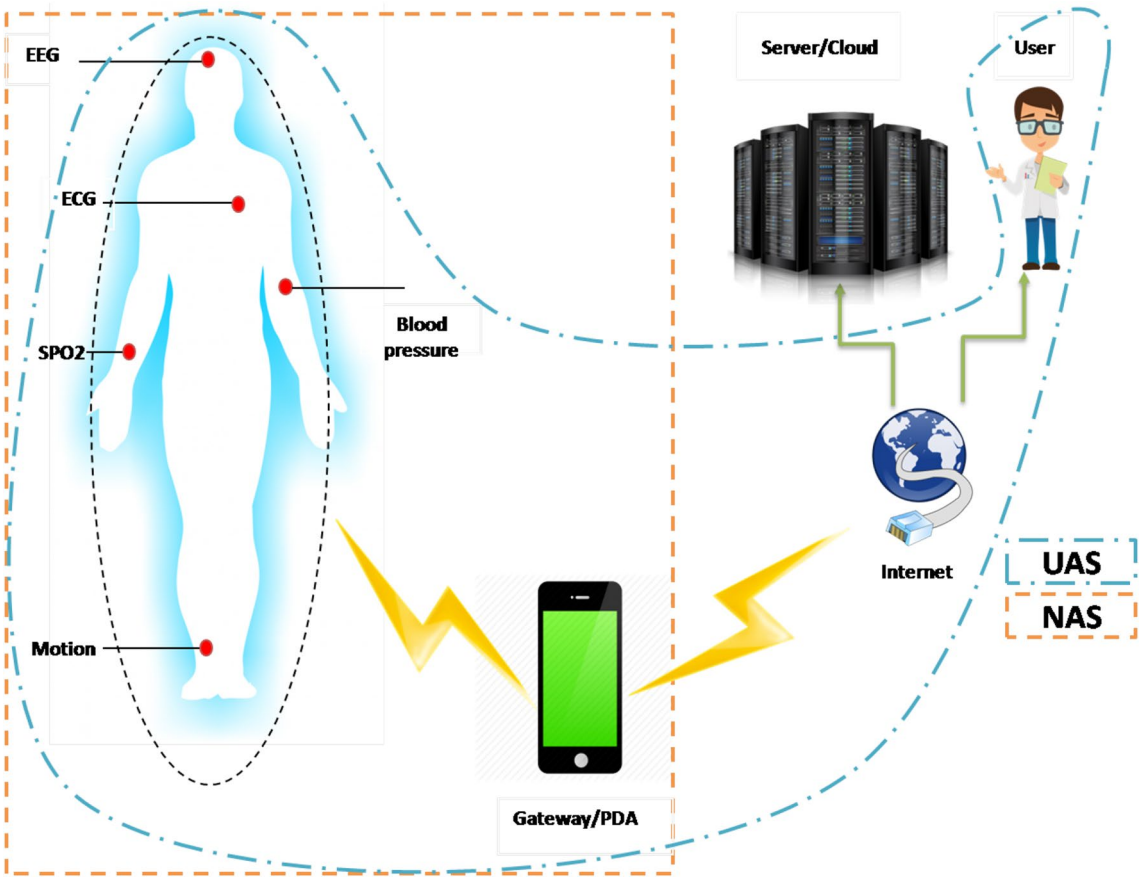

Fig. 3 NAS and UAS architectures

security level of the user's authentication. In order to ease the presentation of UAS that we surveyed, we decided to divide the schemes into two categories: UAS with (2FA) and UAS (3FA).

UAS with Two-Factor Authentication

He et al. [53] proposed a new scheme for WBAN. The authors took Kumar et al.'s scheme [86] as a reference and they proposed their new scheme to overcome the security flaws found in it. Later, Wu et al. [58] proposed a new anonymous mutual authentication protocol that mainly focussed on improving and filling the security flaws found in [53] such as impersonation attack, offline guessing and sensor node attack. Srinivas et al. [56] pointed out the security flaws in [58]. Then they proposed their new symmetric key-based authentication scheme.

Liu and Chung [55] proposed a user authentication scheme using bilinear pairing with a trusted authority. The scheme grants only legal, medical personnel access to patient information. In [51], Amin et al. designed a new authentication scheme for mobile users that focussed on anonymity and also presented their architecture for patient-monitoring healthcare systems in WMSN. The authors in [51] minimised the transmission distance and thus saved more power consumption that was going to be used in long-distance communication. Recently the authors of [54] analysed Amin et al.'s scheme [51] and showed its security drawbacks. Jiang et al. [54] presented a two-factor authentication protocol on quadratic residues with fuzzy verifiers as an improved version for the one proposed in [51].

Wazid et al. [57] derived by the security and privacy issues such as leakage of health data and malfunctioning of WBANs by unauthorised access proposed their new scheme. Ever et al. [52] aimed at improving existing authentication schemes by protecting healthcare infrastructures against potential, well-known attacks while minimising the overhead, so they presented an anonymous-based user authentication scheme.

Recently Masud et al. [59] proposed a new two authentication factor scheme for IoT healthcare applications. The main goal of the authors in this scheme was to preserve the anonymity of users. Table3 presents the main goals of each two-factor UAS scheme and the crypto-primitives that were used in its design.

Table 3 Summary of UAS with two-factor authentication

Scheme	Year	Method	Goal	Tools
He et al. [53]	2015	Symmetric encryption, Hash	Lightweight scheme Improving the flaws of [86]	BAN-Logic
Wu et al. [58]	2017	Symmetric Encryption, Hash	Improving the flaws of [53]	Proverif
Wazid et al. [57]	2017	ECC, Hash	Preventing leakage of health data Mutual secure authentication	AVISPA
Liu and Chung [55]	2017	Bilinear pairing+Hash	Establishing secure communication between a user and a sensor node	
Srinivas et al. [56]	2017	Symmetric Encryption, hash	Ensuring privacy Ensure secure and authorised communication Overcoming the flaws of [58]	AVISPA
Jiang et al. [54]	2017	Quadratic residues, Fuzzy verifiers, Hash	Endtoend mutual authentication - Overcoming the flaws of [51]	
Amin et al. [51]	2018	Hash	- Minimising the transmission distance - Saving more power consumption - Session key negotiation protocol	AVISPA, BAN-Logic
Masud et al. [59]	2021	Hash	- Preserving the anonymity of users - Permiting the registered and verified users to access the medical networks through secure sessions	AVISPA

UAS with Three-Factor Authentication

In 2016, Li et al. [66] presented their new authentication protocol for WMSNs. In their work, they discussed the flaws in He et al.'s work [53] and presented their new work to overcome the drawbacks in He et al.'s protocol. Later, Das et al. [65] presented their new scheme that was mainly derived by Li et al. [66] and He et al. [53] schemes and the flaws they found in both. The authors reviewed both protocols in [66] and [53] then showed that Li et al. [66] suffered from various attacks and design flaws, He al.'s scheme [53] suffered from the same attacks.

Challa et al. [64] proposed an ECC-based three-factor user authentication scheme for a healthcare system using WSN. The authors proposed a provably secure three-factor authentication and key agreement protocol to counter the security limitations found in Liu-Chung's scheme [55].

Soni et al. [71] presented a new scheme for WMSNs. Soni et al. [71] pointed out that Challa et al.'s [64] protocol is flawed with session key disclosure attack and forgery attack and introduced an improved protocol. Ali et al. [62] reviewed the schemes in [55, 64] and showed that they have severe flaws and fail to fulfil all the security requirements. Based on these flaws, the authors presented an improved three-factor(smartcard, biometric, password) authentication scheme for WMSNs to overcome the pitfalls in Liu-Chung and Challa et al.'s schemes, also mitigating the weaknesses found in both papers using hash and ECC.

In 2018 Wazid et al. [72] proposed a new user authentication that uses the could in the authentication process. They mainly focussed on presenting a scheme that allows mutual authentication between a user and personal server connected to WBAN via the healthcare server situated at the cloud. Ali et al. [61] proposed their new enhanced three-factor authentication scheme for WMSNs. In, this work the authors reviewed Amin et al.'s scheme [51] and pointed out the flaws that they found in it. Based on the flaws found, they designed their new scheme to overcome the flaws found. To secure the communication process and the authentication, they used one-way hash and symmetric encryption.

Mao et al. [68] proposed a trusted authority assisted authentication WMSN. This new protocol was an improved protocol for Wazid et al.'s scheme [57] and aimed to overcome the flaws found in Wazid et al.'s scheme [57].

Lately, in 2018, Sharma et al. [69] presented a remote patient monitoring authentication scheme-based on-body sensors for cloud-IoT-based healthcare services. Alzahrani et al. [63] reviewed the scheme of Sharma et al. [69] and pointed out the flaws they found in it, then they presented their new improved remote patient-monitoring authentication protocol for cloud-IoT. Derived by the lack of a secure enough scheme for patient health monitoring and a cloud-based environment for patient health monitoring.

Recently Liu et al. [67] proposed a robust authentication scheme with a dynamic password for WMSNs. The authors adopted a custom password computation algorithm to make each login round's password confidential and dynamic and resist the personal information disclosure attack. Such new addition made it the first authentication scheme that adopts a computable dynamic password for WMSNs. Aghili et al. [60] reviewed the ZZTL scheme [87] and pointed out its flaws. Derived by these flaws, and the need for a secure and energy-efficient protocol that not only provides secure authentication but also satisfies access control and preserves the privacy of doctors and patients with ownership transfer possibility, the authors proposed their new lightweight scheme.

Shuai et al. [70] proposed their new authentication scheme for remote patient monitoring using WMSNs. The authors pointed out that most of the previous proposed lightweight schemes lacked forward secrecy and suffered from the desynchronisation attack. Therefore, they presented their new authentication scheme for remote patient monitoring using WMSNs. In 2020, Xu et al. [73] reviewed and pointed out the flaws found in Soni et al.'s scheme [71], then they presented their improved authentication scheme for WMSNs using Rabin cryptosystem and chaotic maps, in which they established a secure session key at a minimum cost. The security of their scheme is based on the hardness of large number prime factorisation and Chebyshev chaotic Diffie-Hellman problem.

Khalid et al. [74] proposed a new multi-server authentication scheme for WMSN. This scheme is suitable for cloud IoT-based healthcare applications. Derived by the lack of papers that dealt with multi-server environments, the authors presented their new scheme that can be applied on such environments. Lately, Shadi Nashwan [75] proposed an end-to-end scheme with enhanced security for healthcare IoT systems. This scheme supports a flexible and robust authentication process. Moreover, the authors assumed that it ensures simultaneous anonymity of the patient and physician's simultaneous anonymity and perfect forward secrecy services. To ensure the mentioned requirements, the authors adopted an approach based on symmetric encryption and one-way hash.

Table 4 presents the main goals of each tree-factor UAS scheme and the crypto-primitives that were used in its design.

Node-Based Authentication Schemes (NAS)

In this class, the user is not one of the main participants. Therefore, the components treated in this authentication are gateway nodes and sensor nodes. Mutual authentication is done between either gateway and gateway, gateway and sensor, sensor and gateway or sensor and sensor depending on how many hops the architecture has. The communication between these participants is also considered insecure and vulnerable to several attacks. There may exist different types of sensor nodes and gateways in this type and. Sensors can also authenticate with each other. For example, an authentication between controller sensor nodes (super-nodes which is a special kind of WMSNs that communicate with different types of WMSN implants/wearables and collect or receive data from it in order to send it to the servers via gateways) and sensor nodes is needed (the implantable or wearable WMSN devices). In the following, there is a description of the surveyed schemes for this class.

In 2016, Ibrahim et al. [78] proposed their new two-tier WBAN authentication scheme. This scheme is the first literature that focuses on two-tire WBAN and does not include user authentication. Li et al. [82] proposed an authentication and key agreement scheme that is lightweight enough and suitable for WBAN sensor nodes. This scheme also considers node anonymity; in addition, it is suitable for two-hop centralised WBAN architecture. Later, Koya and Deepthi [80], Gupta et al. [77], and Kompara et al. [79] found that this scheme was vulnerable to several attacks. Koya and Deepthi [80] proposed a new scheme based on improving Li et al.'s scheme [82]. The authors reviewed Li et al.'s scheme, highlighted the security flaws found and proposed a new scheme based on physiological signals to resolve the flaws. However, using physiological signals requires all sensor nodes to measure the same physiological signal and implies extra computational costs in collecting and transforming data, resulting in more power consumption.

Gupta et al. [77] presented a new scheme to fulfil all the security and privacy requirements in WMSN-based healthcare systems. In addition, the authors reviewed Li et al.'s scheme [82] and pointed out the flaws they found in it. In Kompara et al. [79] the authors focussed on proposing a new authentication scheme that provides anonymity and untraceability of the sensor nodes in addition to confidentiality and mutual authentication of the communicating parties. They reviewed Li et al.'s scheme [82] and pointed out the flaws they found in it. However, later Rehman et al. [83] found it to be vulnerable. Rehman et al. [83] reviewed Kompara et al. [79]'s scheme and showed the security flaws that they found. Based on this, the authors proposed an authentication scheme that shows efficiency to protect against various known cyber-attacks, especially the base station compromise attack and sensor node impersonation attack. However, Rehman et al. [88] pointed it to be vulnerable.

Lately, Rehman et al. [88] proposed a new authentication scheme that represents an extension for their previous work [83]. The authors based their approach on combining physiological signs and lightweight cryptographic primitives (hash and XOR), resulting in a hybrid scheme. The extracted features from biological signs generate a bio key that enhances the authentication process, resilience against key escrow, anonymous unlinkable sessions.

Xu et al. [84] proposed their new lightweight authentication scheme. The main focus of this scheme was to save the resources in WMSNs. In this work, the authors discussed that most of the previous works in lightweight schemes depend on asymmetric encryption that is resource consuming and also these works suffer from various security vulnerabilities, especially the lack of forward secrecy. Empowered by the mentioned problems, Xu et al. [84] proposed their new scheme based on a two-hop centralised architecture. Kumar and Chand [81] due to the nature of WMSN being IoT constrained devices, they adopted the cloud environment to facilitate the storage and computation. Moreover, due to

Table 4 Summary of UAS with three-factor authentication

Scheme	Year	Method	Goals	Tools
Li et al. [66]	2016	Symmetric Encryption, Hash, Bio Hash	Overcoming the flaws in [53] A new wrong password detection mechanism	AVISPA, BAN-Logic
Das et al. [65]	2017	Symmetric Encryption, Hash, Bio Hash	Overcoming the flaws in [53, 66] Enhancing the security of [66]	AVISPA, BAN-Logic
Ever et al. [52]	2018	ECC, Symmetric Encryption, Hash	Protecting healthcare infrastructures Minimising overheads	AVISPA, ROM
Challa et al. [64]	2018	ECC, Hash, Bio Hash	- Overcoming the flaws found in [55] - Adopting a low bio-hash function - Providing a lightweight three-factor authentication	AVISPA, BAN-Logic, ROR
Wazid et al. [72]	2018	Hash, Bio Hash	- Using the could in the authentication - Reducing the overheads by adopting cloud - Providing essential management process for secret keys establishment	ROR
Mao et al. [68]	2018	ECC, Hash, Fuzzy verifier	- Overcoming the flaws found in [57] - Introducing the fuzzy verifier to prevent offline guessing attacks - Secure local login - Secure biometric template	ROM, ROR
Ali et al. [61]	2018	Symmetric encryption, Hash	- Overcoming the flaws found in [51]	AVISPA, BAN-Logic
Liu et al. [67]	2019	Hash, fuzzy extractor	- Providing a lightweight scheme - Dynamicity and randomness-based approaches - Dynamic secure passwords - Continuously updated pseudo identities	AVISPA, BAN-Logic
Sharma et al. [69]	2019	Hash	- Providing a lightweight scheme - Adopting mobiles in the authentication process	AVISPA
Soni et al. [71]	2019	ECC, Hash	- Overcoming the flaws found in [64] - New secure mechanism for developing a three-factor authentication - Providing support for revocation and re-registration of users	AVISPA, BAN-Logic
Aghili et al. [60]	2019	Hash	- Overcoming the flaws found in [87] - Providing access control liability for users - Considering ownership transfer possibility	Proverif
Shuai et al. [70]	2019	Hash	- Providing protection against forward secrecy and desynchronisation - Providing a low cost scheme - Pseudo-identities to achieve anonymity	BAN-Logic
Xu et al. [73]	2020	Chebyshev, Hash	- Securing the session establishment using Rabin cryptosystem and chaotic maps - Overcoming the flaws found in [71] - Reducing the costs in [71]	BAN-Logic, ROM
Alzahrani et al. [63]	2020	Symmetric Encryption, Hash, Bio Hash	- Overcoming the flaws found in [69] - Adopting a cloud-based environment	BAN-Logic, ROM, Proverif
Ali et al. [62]	2020	ECC, Hash	- Overcoming the found flaws in [55, 64] - Providing a suitable lightweight scheme for WMSNs	AVISPA, BAN-Logic
Khalid et al. [74]	2021	ECC, Hash	- Adopting cloud environment - Providing a scheme that supports multi-server environments - Protection against the well-known attacks	BAN-Logic
Shadi Nashwan [75]	2021	Symmetric Encryption, Hash	- Providing simultaneous anonymity - Providing perfect forward secrecy services	BAN-Logic

the open security challenges of the cloud and wireless communication, they proposed their new identity-based anonymous authentication and key agreement protocol for WMSN in the cloud-assisted environment so-called (IBAAKA). Almuhaideb and Alqudaihi [76] proposed a new authentication scheme for WBANs. The lack of nodes anonymity, key management, and size in the recently proposed schemes guided this work. To achieve that, they proposed a new

Table 5 Summary of the studied NAS

Scheme	Year	Method	Goals	Tools
Ibrahim et al. [78]	2016	Hash	- Two-tier WMSN authentication - Providing a lightweight scheme	BAN-Logic
Li et al. [82]	2017	Hash	- Providing a lightweight scheme - Preserving node anonymity	AVISPA, BAN-Logic
Koya & Deepthi [80]	2018	Hash	- Overcoming the flaws found in [82] - Using physiological signals to provide extra security features	AVISPA, BAN-Logic
Xu et al. [84]	2019	Hash	- Saving the resources in WMSN - Two-hop centralised architecture - Providing a lightweight scheme	Proverif
Kompara et al. [79]	2019	Hash	- Overcoming the flaws found in [82] - Providing nodes anonymity and untraceability - Providing a lows cost scheme	AVISPA, BAN-Logic, Scyther
Gupta et al. [77]	2020	Hash	- Overcoming the flaws found in [82] - Providing a lightweight scheme	AVISPA, BAN-Logic, ROR
Kumar and Chand [81]	2020	ECC	- Adopting the cloud environment to facilitate the storage and computation	ROM
Rehman et al. [83]	2020	Hash	- Overcoming the flaws in [79] - Protecting against base station compromise attack and sensor node impersonation attack - Providing a low cost scheme	AVISPA, BAN-Logic
Almuhaideb & Alqudaihi [76]	2020	Hash	- Providing nodes anonymity - Key management, and size	BAN-Logic
Wan et al. [85]	2021	ECC, Hash	- Continuous authentication scheme - Protecting against impersonation and sensor node capture attacks - Using physiological signals that are hard to imitate	BAN-Logic
Rehman et al. [88]	2021	Hash	- Improving the previous work [83] - Combining physiological signs and lightweight cryptographic primitives for extra protection	AVISPA, BAN-Logic

scheme that consists of two protocols, one for authentication and the other for re-authentication. They also adopted high randomness of the security parameters approach to provide higher protection as a trade-off between security and efficiency. Recently, Wan et al. [85] proposed a continuous authentication scheme based on physiological signals. The authors based their scheme on two main entities, sensor node and personal server, defined as PDA. The authors used different approaches in this scheme to overcome the impersonation and sensor node capture attacks. First, they used physiological signals to ensure it is impossible to impersonate any of the entities. Moreover, They used a continuous authentication process that happens periodically after several sessions to ensure that all the sensors were legitimate and did not fall for node capture attacks.

Table5 presents the main goals of each two-factor scheme and the crypto-primitives that were used in its design.

Evaluation and Analysis

This section discusses different security requirements and attacks on the surveyed schemes and different formal security techniques used. In addition, we evaluate the performance of the studied schemes.

Security Evaluation

Table 6 shows different attacks and requirements failures that were found and pointed out in the surveyed schemes. The different attacks presented here are found by other authors who proposed improvements or new schemes (see the column Ref.). We should point out that the blank cell in column ref indicates that no work has presented flaws in that scheme. We can see that not a single scheme succeeded in ensuring or proving all security and privacy requirements. In the following, we discuss the observed results, their reasons and important recommendations.

- We can see that several studied schemes fail to preserve the anonymity and compromise the integrity of the process, for example, [59, 69, 79, 80]. Such a failure can be fixed by: (1) never passing the IDs in plain-text over an insecure communication channel, (2) using the collision-resistant property of the one-way hash function to pass the IDs when necessary as in [70], and (3) using pseudo-random IDs for the authentication process.
- A replay attack is also observed to be spread in the studied scheme, for instance; [65, 79]. One of the many countermeasures for this attack is using random numbers and time stamps.

Table 6 Different security requirements and attacks in the surveyed schemes

Scheme	Class	FA	FT	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	Ref.
Ibrahim et al. [78]	NAS		1	Y	Y	Y	–	Y	N	Y	N	Y	–	–	–	N	[80]
Li et al. [82]	NAS		2	N	Y	N	–	N	Y	N	N	N	N	–	Y	Y	[77] [76]
Koya & Deepthi [80]	NAS		2	N	N	N	–	Y	Y	N	Y	N	N	–	–	Y	[79] [84]
Xu et al. [84]	NAS		1	N	–	N	–	N	Y	N	N	N	N	–	–	N	[89] [76]
Kompara et al. [79]	NAS		3	N	Y	N	–	Y	–	Y	N	N	–	–	–	–	[77] [83]
Gupta et al. [77]	NAS		3	Y	Y	Y	–	Y	–	Y	Y	Y	N	–	Y	–	[76]
Kumar and Chand [81]	NAS		1	Y	N	N	–	N	–	–	Y	–	–	–	–	Y	[90]
Rehman et al. [83]	NAS		2	Y	Y	Y	–	Y	N	Y	Y	–	–	–	–	–	[88]
Almuhaideb & Alqudaihi [76]	NAS		1	Y	Y	–	–	–	–	Y	Y	–	Y	–	–	–	
Wan et al. [85]	NAS		1	Y	Y	–	–	Y	–	Y	Y	Y	–	–	–	–	
Rehman et al. [88]	NAS		2	Y	Y	Y	–	Y	Y	Y	Y	–	–	–	–	–	
He et al. [53]	UAS	2	1	Y	–	–	–	N	–	–	N	N	N	Y	Y	Y	[66] [58]
Li et al. [66]	UAS	3	2	N	–	–	N	N	–	Y	N	N	Y	Y	N	Y	[65]
Wu et al. [58]	UAS	2	1	Y	–	–	N	N	Y	–	N	Y	N	N	Y	–	[56]
Wazid et al. [57]	UAS	2	1	Y	Y	Y	Y	N	–	Y	N	Y	N	Y	Y	Y	[68]
Das et al. [65]	UAS	3	2	Y	N	–	N	N	N	N	N	–	N	Y	Y	Y	[91]
Liu and Chung [55]	UAS	2		N	–	–	–	N	–	Y	N	–	N	N	N	Y	[64]
Srinivas et al. [56]	UAS	2	1	Y	N	–	Y	N	–	Y	Y	N	Y	Y	Y	N	[52]
Jiang et al. [54]	UAS	2		Y	Y	Y	N	Y	Y	Y	Y	–	–	Y	N	–	[92]
Ever et al. [52]	UAS	2	2	Y	Y	–	–	Y	–	Y	Y	Y	Y	Y	Y	Y	
Amin et al. [51]	UAS	2	2	N	Y	Y	N	Y	N	Y	Y	–	Y	N	N	N	[93] [54]
Challa et al. [64]	UAS	3	3	N	N	–	Y	N	–	Y	Y	N	N	Y	Y	–	[71] [62]
Wazid et al. [72]	UAS	3	1	Y	–	Y	Y	Y	–	Y	Y	–	Y	–	Y	–	
Mao et al. [68]	UAS	3	2	Y	Y	Y	Y	Y	–	Y	–	N	Y	Y	N	Y	[67]
Ali et al. [61]	UAS	3	2	Y	N	Y	–	–	N	Y	Y	Y	N	Y	N	–	[94]
Liu et al. [67]	UAS	3	2	Y	–	Y	–	–	–	Y	Y	Y	Y	Y	Y	–	
Sharma et al. [69]	UAS	3	1	N	Y	Y	Y	N	–	Y	N	–	N	N	Y	Y	[63]
Soni et al. [71]	UAS	3	2	Y	N	Y	Y	Y	–	Y	Y	N	Y	Y	Y	–	[73]
Aghili et al. [60]	UAS	3	1	Y	N	Y	Y	–	N	Y	N	–	Y	Y	Y	–	[95]
Shuai et al. [70]	UAS	3	1	Y	Y	–	–	–	Y	Y	Y	–	N	Y	N	Y	[94]
Xu et al. [73]	UAS	3	2	Y	Y	–	–	Y	Y	Y	–	Y	Y	–	Y	–	
Alzahrani et al. [63]	UAS	3	3	Y	Y	Y	–	Y	–	Y	Y	–	Y	Y	Y	Y	
Ali et al. [62]	UAS	3	2	Y	–	–	Y	Y	–	Y	Y	–	Y	Y	Y	–	
Masud et al. [59]	UAS	2	1	N	Y	Y	Y	Y	N	Y	N	–	N	–	N	-	[96]
Khalid et al. [74]	UAS	3	1	Y	Y	–	–	Y	–	Y	Y	–	Y	Y	Y	Y	
Shadi Nashwan [75]	UAS	3	1	Y	Y	Y	–	Y	Y	Y	Y	–	Y	Y	–	Y	

FA: Authentication factors, 2/3 FT: Number of security verification techniques used A1: Achieve anonymity of communication parties, A2: Achieve perfect forward secrecy, A3: Achieve untraceability, A4: Resist DoS attack A5: Resist MITM attack, A6: Resist desynchronisation attack, A7: Resist replay attack, A8: Resist impersonation attack A9: Sensor node capture A10: Resist guessing attacks, A11: Resist smart card/ mobile stolen A12: Resist insider attack, A13: Resist stolen verifier attack

– Many of the surveyed schemes suffer from impersonation attacks where the adversary can impersonate one or more communication parties (node, user, gateway). Some of the reasons that may lead to this attack are:
  – Stealing secret user information and node's identity. The identity of the communicating parties must be anonymous to avoid such conflicts.
  – Replay attack where the adversary replays the communication between communicating parties without getting detected, misleadingly assuming that communicating parties communicate directly.

To counter such an attack, there exist many countermeasures such as:

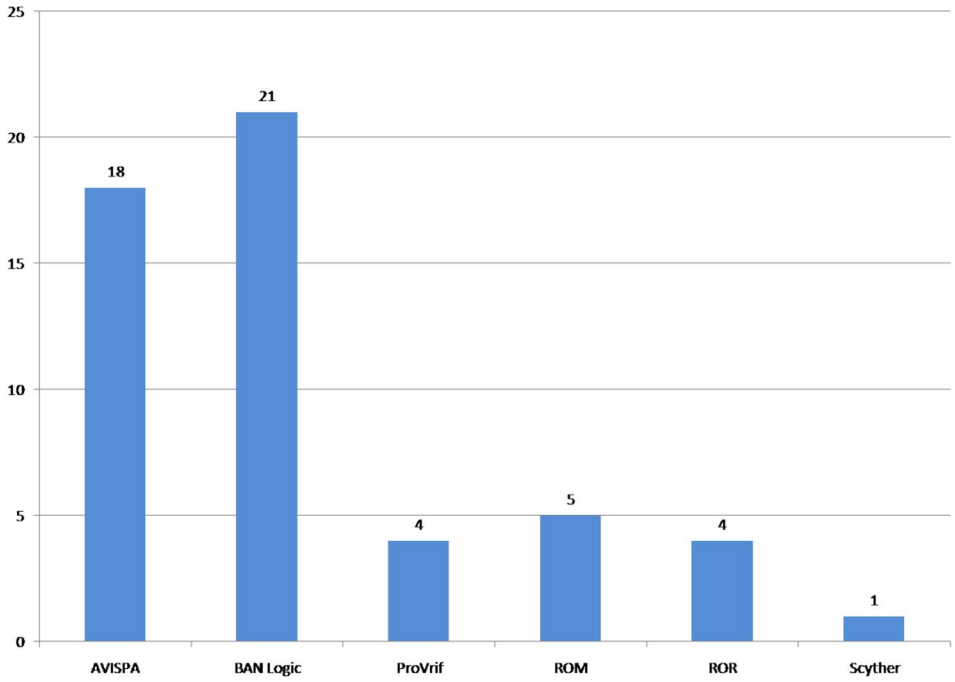

Fig. 4 Security verification techniques used in the studied schemes

  - The continued use of an access control list (ACL), focussing on using MAC addresses.
  - Generating bio-keys to overcome shortcomings of IoT sensor node impersonation attack [83, 85, 88].
  - Using combinations of password, smart card and biometrics as authentication factors, like in [63, 64].
  - Adopting the techniques mentioned above to protect against replay attack and preserve anonymity.

- Some schemes do not resist node capture attacks, such as [65, 80]. This flaw is due to the cryptographic keys getting compromised and exposed by adversaries. Therefore, keys used for securing communication in WMSNs should be periodically updated. Capturing a node may lead to cloning it. Therefore, an approach to detect cloned nodes must be adopted. A mechanism to detect compromised keys also need to be adopted. In addition, the legitimate nodes that used compromised keys must be updated with new keys.
- In addition, we can see that a guessing attack often appears in the table, especially on the node side, where an adversary can lunch a guessing attack on the nodes to recover the critical data it holds and to protect against such attack.

After reviewing the security flaws found in the literature surveyed schemes, we can summarise that insider, password guessing, replay, impersonation, node capture and smart card loss attack are the most common attacks/risks on the authentication schemes. Most of the mentioned attacks cannot be formally verified.

About the verification techniques, Table 6 (column of FT) and Fig. 4 present statistics of security verification techniques used in the studied schemes. We can see that most of the surveyed schemes 97% used one or more of the verification techniques to enhance their scheme. In addition, more than 50% used two or more verification techniques to support their assumptions.

The main remark concerning the verification techniques is that attacks exist in schemes despite being proved using verification techniques and tools by authors. For instance, [64] used three verification techniques (AVISPA, Ban-Logic and ROR), yet it failed in fulfilling the requirements and security features. We can summarise the main reasons why these verification techniques and tools do not detect some attacks:

- These tools do not use recent efficient techniques, such as machine learning and deep learning. These techniques prove their performance in some recent works, such as [97, 98].
- They do not prove different security requirements. For example, the Proverify tool can prove secrecy, integrity, and authentication requirements but cannot prove other ones, such as privacy and untraceability.
- They do not detect all possible attacks. For example, the AVISPA and Scyther tools can detect man in the middle attacks and replay attacks but cannot detect desynchronisation attacks.
- They do not support all cryptographic algebraic primitives in the specification of schemes. For example, different existing specification languages do not support scalar

Table 7 Theoretical performance evaluation of the studied schemes

Scheme	Class	Computational cost	Communication cost	Storage cost
Ibrahim et al. [78]	NAS	$6T_H$	14 L	2 L+L_{ID}
Li et al. [82]	NAS	$4T_H$	2 L_{ID}+16 L+2 L_{TS}	L_{ID}+2 L
Koya & Deepthi [80]	NAS	$3T_H$	21 L+3 L_{TS}	L_{ID}+2 L
Xu et al. [84]	NAS	$6T_H$	2 L_{ID}+14 L+4 L_{TS}	L_{ID}+3 L
Kompara et al. [79]	NAS	$4T_H$	14 L+2 L_{TS}	2 L+L_{ID}
Rehman et al. [83]	NAS	$4T_H$	6 L+1 L_{TS}	3 L+L_{ID}
Gupta et al. [77]	NAS	$8T_H$	20 L+5 L_{TS}	L_{ID}+4 L
Kumar et al. [81]	NAS	$5T_H$+$3T_{ECM}$	2 L_{ECC}+2 L+L_{TS}	LID+2 L_{ECC}
Almuhaideb & Alqudaihi [76]	NAS	$3T_H$	10 L+4 L_{TS}+ 2_{ID}	3 L_{ID}+2 L+L_{SES}
Wan et al. [85]	NAS	$15T_H$+$3T_{ECM}$	3 L_{ECC}+4 L+2 L_{TS}	3 L+L_{ECC}
Rehman et al. [88]	NAS	$2T_H$	6 L+1 L_{TS}	3 L+L_{ID}
He et al. [53]	UAS	T_H+2 T_S	10 L_{ID}+9 L+5 L_{TS}	L_{ID}+L
Li et al. [66]	UAS	$6T_H$+2 T_S	10 L_{ID}+10 L+7 L_{TS}	L_{ID}+L
Wu et al. [58]	UAS	$2T_S$+4 T_H	7 L_{ID}+16 L	L_{ID}+L
Das et al. [65]	UAS	$7T_H$+2 T_S	11 L_{ID}+12 L+6 L_{TS}	L_{ID}+L
Srinivas et al. [56]	UAS	$5T_H$+2 TS	9 L_{ID}+18 L+3 L_{TS}	L_{ID}+2 L
Jiang et al. [54]	UAS	$7T_H$	L_{ID}+10 L+2 L_{TS}	L_{ID}+2 L
Wazid et al. [57]	UAS	$6T_H$+$4T_{ECM}$+$1T_{ECA}$	2 L_{ECC}+3 L+3 L_{TS}	3 L+L_{ECC}
Liu et Chung [55]	UAS	$3T_H$+$1T_{pair}$	2 L_{ECC}+4 L+ 3 L_{ID}+3 L_{TS}	2 L_{ECC}+L
Amin et al. [51]	UAS	7 T_H	2 L_{ID}+12 L	L_{ID}+2 L
Wazid et al. [72]	UAS	$15T_H$	10 L+3 L_{TS}	3 L+L_{ECC}
Mao et al. [68]	UAS	$6T_H$+$2T_{ECM}$	3 L_{ECC}+8 L+3 L_{TS}	L_{ID}+L+2 L_{ECC}
Challa et al. [64]	UAS	$8T_H$	L_{ECC}+6 L+4 L_{TS}	L_{ID}+L
Ever et al. [52]	UAS	$2T_H$+$2T_S$	7 L_{ID}+8 L	L_{ID}+L
Ali et al. [61]	UAS	$8T_H$+T_S	14 L+6 L_{ID}+3 L_{TS}	2 L+L_{ID}
Soni et al. [71]	UAS	$7T_H$	9 L+2 L_{ECC}+6 L_{TS}	L_{ID}+2 L
Liu et al. [67]	UAS	$7T_H$	13 L+4 L_{TS}	L_{ID}+2 L
Sharma et al. [69]	UAS	$14T_H$	L_{ID}+16 L+6 L_{TS}	L_{ID}+2 L
Shuai et al. [70]	UAS	$8T_H$	11 L+L_{TS}	2 L+L_{ID}
Aghili et al. [60]	UAS	$5T_H$	12 L+4 L_{TS}	L_{ID}+L
Xu et al. [73]	UAS	$5T_H$+$2T_{cheb}$	9 L+2 L_{TS}	L_{ID}+L
Alzahrani et al. [63]	UAS	$13T_H$+T_S	L_{ID}+16 L+6 L_{TS}	2 L+L_{ID}
Ali et al. [62]	UAS	$5T_H$+T_{pair}+T_{ECM}	4 L_{ECC}+2 L_{ID}+9 L+L_{TS}	L_{ID}+2 L_{ECC}
Masud et al. [59]	UAS	$2T_H$	16 L	3 L+L_{ID}
Khalid et al. [74]	UAS	$4T_H$+$2T_{ECM}$	16 L+4 L_{ECC}	2 L+ L_{ECC}
Shadi Nashwan [75]	UAS	$6T_H$	4 L_{ID} + 17 L	2 L+L_{ID}

multiplication in ECC. The existing languages specify it as a one-way function, but these languages or models do not support other proprieties of scalar multiplication.

Performance Evaluation

This section presents the performance evaluation of studied schemes in terms of four metrics, including computational cost, communication cost, storage overhead, and energy consumption.

Table 7 represents a theoretical performance comparison of the studied schemes. We will use the data of this table to compute different costs.

Experimental Results

To implement symmetric and asymmetric cryptographic primitives, we used RELIC Toolkit [99]. It is considered a lightweight asymmetric cryptographic library. The experimental measurements are based on the WiSMote sensor platform. It is equipped with an MSP430F5437 micro-controller, 16 KB of static RAM, 256 KB of flash ROM and CC2520 transceiver [100, 101]. According to the classification of

Table 8 Performance of implementation of cryptographic primitives in sensor nodes

Operation	Notation	Computational time (Second)	Energy consumption (mJ)
Hash function (SHA-256)	T_H	0.013	0.086
Symmetric decryption (AES-256)	T_S	0.015	0.099
Scalar point multiplication (160 bits)	T_{ECM}	1.049	6.923
ECC Addition (160 bits)	T_{ECA}	0.007	0.046
Bilinear pairing operation	T_{pair}	8.142	53.74

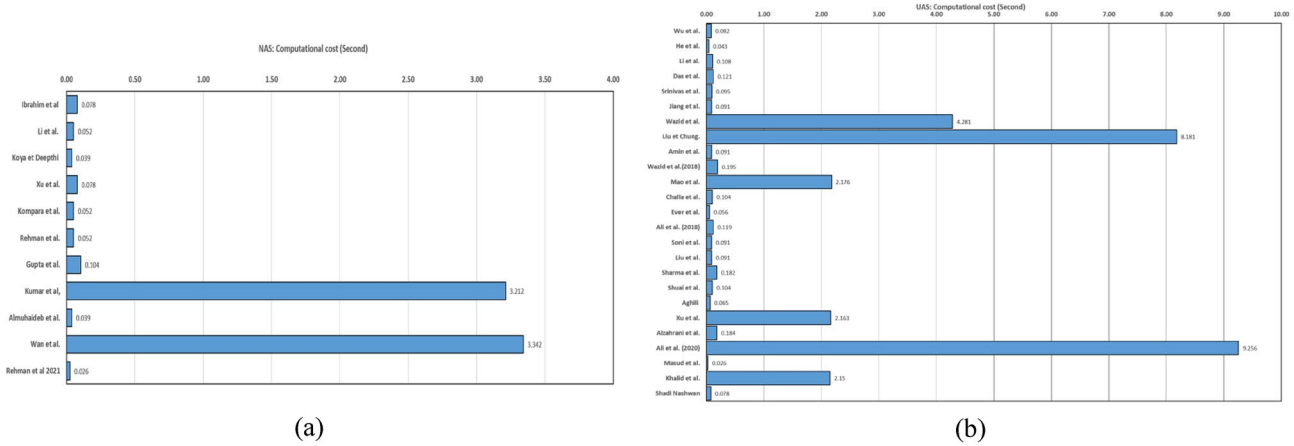

Fig. 5 Sensor node computational cost of the NAS and UAS

IETF, this sensor is approximately in Class 1 by memory size. The MSP430 family is an ultra-low-power micro-controller that is used in medical sensors [102, 103].

Table 8 shows the different cryptographic primitives used in the studied schemes, as well as their computational times and their energy consumption based on our implementation. In addition, lengths of different primitives and data are as follow:

- L_{ID}: Length of ID is 8 bytes.
- L: Length of the hash function, symmetric key, the modulus operation result and the nonce are 32 bytes.
- L_{ECC}: Length of ECC point is 40 bytes.
- L_{TS}: Length of timestamp is 4 bytes.
- L_{SES}: Length of session number is 4 bytes.

Above we presented the experimental results of the cryptographic primitives that were used on class 1 sensors. We should note that to evaluate a scheme experimentally researchers have agreed on the following these steps:

- Implementing the cryptographic primitives on real devices (Sensors, PCs, etc.)
- Calculating the costs (time, storage, energy consumption) of each implemented primitive.
- Then for each scheme cost on a specific device they multiply the number of each primitive used by its cost then summing up the different costs of each primitive to get the final result.

In the following we present an example of how the cost is calculated: For Kumar et al. [81] has a calculation time of: $5T_H+3T_{ECM}$. This means that the cost is the sum of $5T_H$ and $3T_{ECM}$ in another word; 5*0.013 s + 6*1.049 s. The final cost is: 3.212 s. These tools are applicable for all costs.

Here, we present different obtained calculated costs:

- **Computational cost**: Fig. 5a, b illustrates the computational cost (in second) of studied schemes on both NAS and UAS classes on the sensor side. At first glance, we can observe that Rehman et al.'s scheme [88] takes 0.026 s in NAS class, and Masud et al.'s scheme [59] takes 0.026 s in UAS class. These results are considered as the smaller computational cost compared to studied schemes where we observe that Wan et al. scheme [85] takes 3.342 s in NAS has a way higher computational time, and same for Ali et al. [62], and Liu et Chang [55]

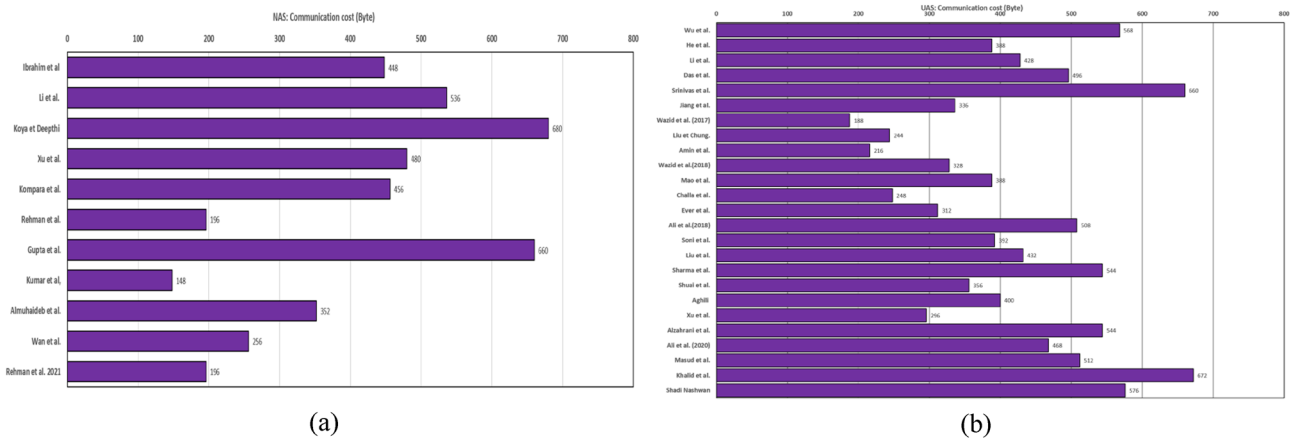

Fig. 6 Evaluation of communication cost in NAS and UAS

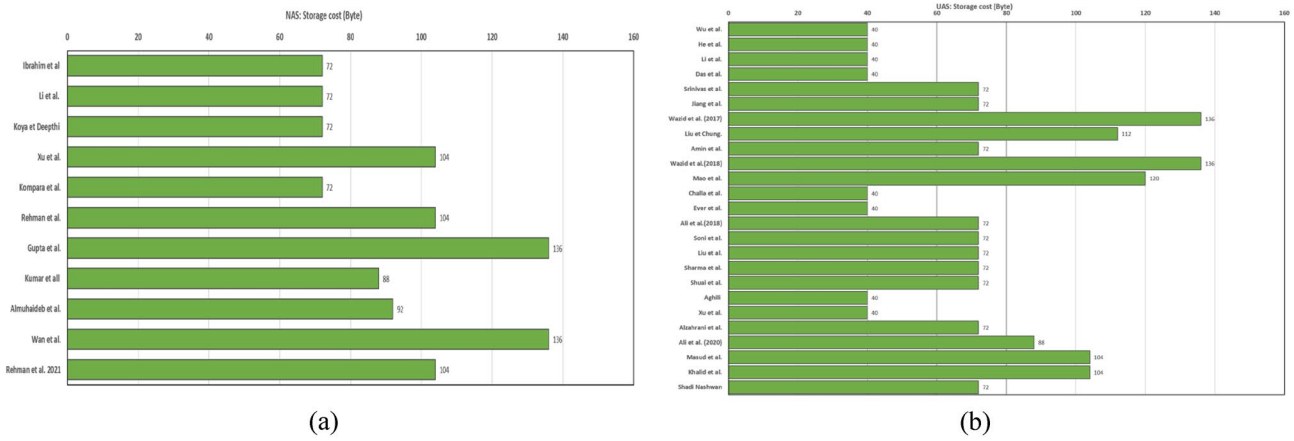

Fig. 7 Sensor node storage cost of the NAS and UAS

schemes in UAS class which take 9.256 s and 8.181 s respectively.

- **Communication cost**: Fig. 6a, b illustrates the communication cost of studied schemes on both NAS and UAS classes. From the comparison in Fig. 6a, we notice that Kumar and Chand scheme [81] offers better performance in terms of communication cost on NAS class. While in Fig. 6b which shows the communication cost in NAS we can clearly notice that Wazid et al.'s scheme [57] provides the lowest overhead and Khalid et al. [74] as the highest.
- **Storage cost**: Fig. 7a, b shows the memory space required from the sensor in the studied schemes in both UAS and NAS. From the comparison in Fig. 7a, it is clear that a few schemes share the same cost, such as [78–80, 82] with 72 Byte. On the other hand, we notice the same in UAS where the schemes of [52, 53, 58, 60, 64–66, 73] share the same cost of 40 Byte. These results are due to storing only the necessary information for authentication. Reducing the storage cost, especially on the sensor side, is demanded from all authors due to it being storage constrained device.
- **Energy consumption cost**: Fig. 8a, b shows the energy consumption in the sensor node in the studied schemes. To estimate the energy consumption during the computation process, we used the equation $W = V \times I \times t$, where W, V, I and t denote the consumption power in millijoules (mJ), the voltage in volts (V), the current draw in active mode in milliamps (mA) and the time in seconds (s), respectively [104]. According to the WiSMote platform, the current draw is 2.2 mA, and the supply voltage is 3V. From the comparison in Fig. 8a, we can observe that the energy consumption of Wan et al.'s [85] scheme is greater than other studied schemes, and Rehman et al. scheme [88] is the lowest (0,172mJ) in NAS class. In addition, the comparison between UAS-schemes in Fig. 8b, indicates that [55, 57, 62, 68, 73] require more

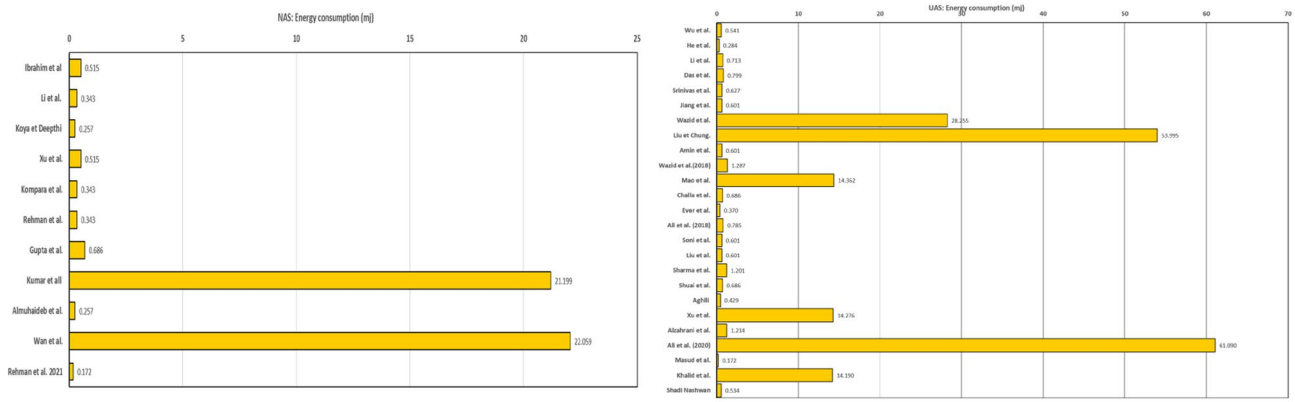

Fig. 8 Evaluation of energy consumption cost in UAS and NAS

energy consumption while Masud et al. scheme [59] requires less (0,172mJ).

Discussion

The observed results concerning computation, communication, storage and energy costs are related to various of reasons. In the following, we discuss the observed results, their reasons and important recommendations.

- From Fig. 5, we can notice a variation in results. The main reason is due to the cryptographic primitives used in each scheme, we can notice that to achieve the low computational cost in Rehman et al. scheme [88] they used only hash and XOR operations, and the same goes for Masud's scheme [59]. Therefore, these schemes that put low exhaustion on IoT devices are highly recommended for class 1 devices.
- As a trade of security over performance Wan et al. [85], Kumar and Chand [81], Ali et al. [62], Liu and Chang [55] schemes used ECC/PBC to increase the security level, knowing that ECC and PBC are considered more resilient to attacks. Resulting in more exhaustion applied on medical IoT nodes.
- ECC can be applied in class 1 medical IoT sensors with a slight optimisation, but class 2 is more suitable as a recommendation. However, for BPC, the time required to compute a single bilinear pairing is seven times greater than one elliptic curve point multiplication. Thus, class 1 is not an option, and only class 2 medical IoT sensors can manage the high computations it requires.
- It is important to optimise the implementation of different operations of ECC, in particular the scalar multiplication. For this, Oudjida & Liacha [105] presented a new approach (Radix-2^w) to solve the problems of elliptic curve scalar multiplication. They showed that their new method is secure and more efficient than the old one.
- We exclude pairing-based schemes where they require a high execution time and consume more energy, for instance: Ali et al. [62] with is 9.256 s in medical IoT sensors. Because of this long time, it may endanger the patient's health.
- Hash and symmetric encryption are more suitable and recommended to be used on medical IoT sensors. However, they do not provide a solution for key exchange problems to create a session key.
- In terms of storage, all the schemes managed to keep it at its lowest. All the schemes are suitable for class 1 devices in terms of storage. We mention that the size of the disk in medical sensors of Class 1, is about 100 KB.
- The variation in communication overhead results in both categories is due to the different authentication techniques used: messages and information exchanged to confirm the communicating parties' identity. Therefore, we can conclude that the overhead depends on the author's approach, either low or high and what they consider as enough to secure the operation.
- The energy consumed during the computation process is estimated based on the computational time. Whenever the computational time is greater, the energy consumed is also greater. This energy consumption is also related to the crypto-primitives used.
- Increasing the security level using primitives considered more resilient to attacks (e.g. ECC, PBC) can put more energy exhaustion on the system.

Future Research Directions

This section identifies some directions of future research related to designing secure and efficient authentication schemes for healthcare applications.

Security and Privacy Analysis Techniques

When authors proposed a novel authentication scheme in recent years, they verified their security using one or more formal techniques. The majority of existing formal techniques can verify that the security protocol (e.g. authentication protocol) achieves a limited number of security requirements.

Using artificial intelligence techniques (e.g. machine learning and deep learning) is an important direction to develop a new tool to prove the security of applications and protocols. Here, we mention some recent works in this field, Montes et al. [98] improve the detection capabilities of the Web Application Firewall using machine learning and deep learning, respectively, used to detect and prevent attacks. In addition, Ma et al. [106] proposed a new machine learning-based scheme for the automatic security analysis of authentication and key agreement protocols.

Designing tools to automatically prove the privacy and security requirements of authentication schemes and detect possible attacks is a significant challenge in the security of authentication protocols in WMSN.

Blockchain-Based Authentication Schemes

Blockchain technology is considered a solution for providing trusted networks into the healthcare area due to the features of decentralised storage and achieving consensus. However, the interoperation between WMSNs and the blockchain's security specifications makes an open challenge of providing Blockchain-based authentication in WMSN because there is no trade-off between resource-constrained sensors in WMSN and the complex computations required in the blockchain. Moreover, blockchain systems are vulnerable to 51% attack. Once the probability of computing power reaches 51%, the node can cause security issues such as modifying transaction data, and double-spending attack [107].

Identity-Based Authentication Schemes

In literature, identity-based authentication schemes in WMSN are based on two main techniques, including bilinear pairings and elliptic curves. According to the IoT resource-constrained devices in healthcare applications, a bilinear pairing is considered an expensive primitive, as shown in Table 8, where the time required to compute a single bilinear pairing is seven times greater than one elliptic curve point multiplication. Therefore, pairing-based authentication schemes are quite computationally expensive and have a high impact on network lifetime, primarily if several pairings are used. The open research challenge in this area is how to minimise the pairing computation overhead to suit WMSN.

Post-quantum Cryptography

ECC is a more lightweight public-key cryptosystem than other cryptosystems (e.g. RSA cryptosystem) and suitable with limitation capabilities of sensor nodes. There exist a significant number of surveyed schemes that used ECC as a security mechanism, such as [68, 74, 85]. Unfortunately, it cannot resist quantum computing attacks. In 1994, P. W. Shor [108] proposed an algorithm to break cryptosystems based on discrete logarithms and prime factorisation problems with quantum computers. In recent years, several researchers and companies have been working to build quantum computers. On the other hand, there exist computational problems that resist the quantum attacks, such as quasi-cyclic syndrome decoding (QCSD) with parity problem, and ring learning with rounding (RLWR) problems. These problems can be adopted to construct secure post-quantum cryptography (PQC).

In 2017, the National Institute of Standards and Technology (NIST) had launched a standardisation process to select one or more post-quantum cryptography algorithms, and it began with 69 candidates of key-establishment mechanisms, public-key encryption and signatures algorithms. These algorithms are classified into four categories: code-based, lattice-based, hash-based, and isogeny-based cryptography. In order to select the standardised PQC algorithms, NIST identified three aspects of evaluation criteria: (1) algorithm and implementation characteristics, (2) cost and performance, and (3) security. NIST is currently in the third round of the NIST PQC standardisation process with 15 candidate algorithms, including seven finalist and eight alternate candidate algorithms. NIST expects to select a small number of candidates for standardisation by early 2022 [109].

Thus, designing and implementing authentication schemes in healthcare WMSN by adopting post-quantum cryptography is a fundamental challenge to ensure the security of healthcare systems.

Physiological Value-Based Schemes

Several dynamic biometrics such as blood glucose, body temperature, and cardiac signals were proposed to improve the authentication process under physiological value-based schemes. These physiological value-based schemes tend to synchronise all implanted and wearable nodes to measure

the same value simultaneously to use it in the authentication process. For instance, the cardiac inter-pulse interval(IPI) can be defined as the time interval between consecutive heartbeats. IPI is measured from different physiological signals related to the cardiac system, for example, blood pressure (BP) and electrocardiogram ECG.

Many works have adopted physiological signs, for instance, [110], where the authors used the randomness of the binary sequence generated from multi IPIs used to generate a unique random identifier. In addition, many other approaches that use physiological signals and their randomness in generating identifiers or session keys and even crypto-keys were adopted in the literature. These approaches share that they all synchronise the nodes to sense the same physio-sign in a time interval, which highly increases the computational and energy exhaustion. Even that these approaches proved their security and privacy effectiveness, they failed in reducing the computation and energy consumption on the node's side. They increased it, which was a trade of security over performance that would lead to complete resource exhaustion. Knowing that the recent schemes all tend to secure the authentication process while keeping the costs at their minimum, the physiological schemes fail to do that. Therefore, researchers are demanded to provide more physiological signal studies where they can be adopted in WMSN authentication while minimising all the costs and keeping the same level of security.

Machine Learning for Authentication

In the recent years, several studies are being carried out that involve the use of: blockchain, artificial intelligence, and cloud computing to secure IoT communication and secure medial data [111]. The use of machine learning techniques to help in the authentication process for IoT networks is being widely considered [112]. Machine learning in IoT authentication include three types of algorithms:

- Supervised Learning: use a structured data datasets to filter, detect spectrum and determine locations. However, these algorithms are still far from being efficient in IoT due to high amount of memory and processing power they require. They proved to be useful against intrusion and DDoS attacks.
- Unsupervised Learning: use unstructured datasets and inputs heuristically to learn patterns. They are used to identify irregularities, patterns and anomalies without previous knowledge. They are used to detect communication attacks such as Sybil attacks.
- Reinforcement Learning: used to find an optimal set of actions that maximise the reward in a given environment. They are simple to use, but they take a long time due to the slow convergence of the optimal state.

As a sum up, the Machine Learning (ML) or the Artificial Intelligence (IA) approaches give high competent solutions to protect against attacks in IoT authentication. However, these solution still put some high computations and memory usage on the IoT resource-constrained devices. Researchers are interested in making these approaches efficient in such resource-constrained environments.

Conclusion

In our paper, we surveyed various authentication schemes on WMSNs. We presented various attacks targeting WMSNs, and formal verification techniques used to verify the privacy and security requirements. We have classified these schemes into two categories based on the WMSN architecture. Table 2 provides the architecture classification. In addition, this survey discussed, compared, summarised and evaluated their security and performance based on experimental results. Security comparison in Table 6 and performance comparison in Table 7 are provided. Furthermore, this paper outlines applications, future research directions and recommendations for authentication schemes in WMSNs. All in all, our survey gives a wider view of WMSN technology, its applications, system architecture, and a closer look at it in terms of security and authentication.

As a further and upcoming study, we plan to design and implement a new authentication scheme for WMSNs in IoT environment. The new scheme will use lightweight cryptographic primitives, that are suitable with the resource-constrained medical sensors and resist different possible attacks.

Declarations

Conflict of Interest The authors declare that they have no conflict of interest.

References

1. Muhammad L, Algehyne EA, Usman SS, Ahmad A, Chakraborty C, Mohammed IA. Supervised machine learning models for prediction of covid-19 infection using epidemiology dataset. SN Comput Sci. 2021;2(1):1–13.
2. Bharati S, Podder P, Mondal M, Prasath V. Medical imaging with deep learning for covid-19 diagnosis: a comprehensive review. 2021. arXiv:2107.09602
3. Bharati S, Podder P, Mondal M, Prasath V. Co-resnet: Optimized resnet model for covid-19 diagnosis from X-ray images. Int J Hybrid Intell Syst (Preprint), pp. 1–15; 2021.
4. Meraihi Y, Gabis AB, Mirjalili S, Ramdane-Cherif A, Alsaadi FE. Machine learning-based research for covid-19 detection, diagnosis, and prediction: A survey. SN Comput Sci. 2022;3(4):1–35.

5. Bharati S, Podder P, Mondal M. Artificial neural network based breast cancer screening: a comprehensive review, 2020. arXiv preprint arXiv:2006.01767
6. Zimmerman TG. Personal area networks: near-field intrabody communication. IBM Syst J. 1996;35(3.4):609–17.
7. Numbeo: Healthcare index by country 2021 (2021). https://www.numbeo.com/health-care/rankings_by_country.jsp. Accessed January 2021
8. Nabila A, et al. A qos based comparative analysis of the ieee standards 802.15. 4 & 802.15. 6 in wban-based healthcare monitoring systems. In: 2019 International conference on wireless technologies, embedded and intelligent systems (WITS), 2019; pp. 1–5. IEEE.
9. Bharathi K.S, Venkateswari R. Security challenges and solutions for wireless body area networks. In: Computing, Communication and Signal Processing, 2019; pp. 275–283. Springer, New York.
10. Chenthara S, Ahmed K, Wang H, Whittaker F. Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE Access. 2019;7:74361–82.
11. Aqeel-ur Rehman IUK, Khan AY. A review on authentication schemes for wireless body area networks. In: 3rd International Conference on Computer & Emerging Technologies, 2013. Pakistan.
12. Masdari M, Ahmadzadeh S. Comprehensive analysis of the authentication methods in wireless body area networks. Secur Commun Netw. 2016;9(17):4777–803.
13. Wazid M, Zeadally S, Das AK, Odelu V. Analysis of security protocols for mobile healthcare. J Med Syst. 2016;40(11):1–10.
14. Aslam MU, Derhab A, Saleem K, Abbas H, Orgun M, Iqbal W, Aslam B. A survey of authentication schemes in telecare medicine information systems. J Med Syst. 2017;41(1):1–26.
15. Joshi A, Mohapatra AK. Authentication protocols for wireless body area network with key management approach. J Discr Math Sci Cryptogr. 2019;22(2):219–40.
16. Hussain M, Mehmood A, Khan S, Khan MA, Iqbal Z. Authentication techniques and methodologies used in wireless body area networks. J Syst Architect. 2019;101: 101655.
17. Sowjanya K, Dasgupta M. Survey of symmetric and asymmetric key management schemes in the context of iot based healthcare system. In: 2020 First International Conference on Power, Control and Computing Technologies (ICPC2T), 2020;pp. 283–288. IEEE.
18. Narwal B, Mohapatra AK. A survey on security and authentication in wireless body area networks. J Syst Architect. 2020; 101883.
19. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks. IEEE Commun Magn. 2002;40(8):102–14.
20. Buratti C, Conti A, Dardari D, Verdone R. An overview on wireless sensor networks technology and evolution. Sensors. 2009;9(9):6869–96.
21. Ragesh G, Baskaran K. An overview of applications, standards and challenges in futuristic wireless body area networks. Int J Comput Sci Issue (IJCSI). 2012;9(1):180.
22. Bharati S, Podder P, Mondal M, Paul P.K. Applications and challenges of cloud integrated iomt. In: Cognitive Internet of Medical Things for Smart Healthcare, 2021; 67–85. Springer.
23. Topol EJ, Steinhubl SR, Torkamani A. Digital medical tools and sensors. JAMA. 2015;313(4):353–4.
24. Elayan H, Shubair R.M, Kiourti A. Wireless sensors for medical applications: Current status and future challenges. In: 2017 11th European Conference on Antennas and Propagation (EUCAP), pp. 2478–2482. IEEE (2017)
25. Bouazizi A, Zaibi G, Samet M, Kachouri A. Wireless body area network for e-health applications: overview. In: 2017 International Conference on Smart, Monitored and Controlled Cities (SM2C), 2017; pp. 64–68. IEEE.
26. Karthick G, Pankajavalli P. A review on human healthcare internet of things: a technical perspective. SN Comput Sci. 2020;1(4):1–19.
27. Bello O, Zeadally S, Badra M. Network layer inter-operation of device-to-device communication technologies in internet of things (iot). Ad Hoc Netw. 2017;57:52–62.
28. Bormann C, Ersue M, Keranen A. Terminology for constrained-node networks. Internet Engineering Task Force (IETF): Fremont, CA, USA;2014; pp. 2070–1721.
29. Piccolo F.L, Battaglino D, Bracciale L, Bragagnini A, Turolla M.S, Melazzi N.B. On the ip support in ieee 802.15. 4 lr-wpans: self-configuring solutions for real application scenarios. In: 2010 the 9th IFIP Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), 2010;pp. 1–10. IEEE.
30. Arefin MT, Ali MH, Haque AF. Wireless body area network: an overview and various applications. J Comput Commun. 2017;5(7):53–64.
31. Car J, Black A, Anandan C, Cresswell K, Pagliari C, McKinstry B, Procter R, Majeed A, Sheikh A. The impact of ehealth on the quality and safety of healthcare. A Systemic Overview & Synthesis of the Literature Report for the NHS Connecting for Health Evaluation Programme. 2008.
32. Hillestad R, Bigelow J, Bower A, Girosi F, Meili R, Scoville R, Taylor R. Can electronic medical record systems transform health care? potential health benefits, savings, and costs. Health Aff. 2005;24(5):1103–17.
33. Laxman K, Krishnan SB, Dhillon JS. Barriers to adoption of consumer health informatics applications for health self management. Health Sci J. 2015;9(5):1.
34. Zhang X, Yu P, Yan J. Patients' adoption of the e-appointment scheduling service: A case study in primary healthcare. In: HIC, 2014;pp. 176–181.
35. Adrian D, Bhargavan K, Durumeric Z, Gaudry P, Green M, Halderman J.A, Heninger N, Springall D, Thomé E, Valenta L, et al. Imperfect forward secrecy: How diffie-hellman fails in practice. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015;pp. 5–17.
36. Zhu J, Ma J. A new authentication scheme with anonymity for wireless environments. IEEE Trans Consum Electron. 2004;50(1):231–5.
37. Bilal M, Kang SG. An authentication protocol for future sensor networks. Sensors. 2017;17(5):979.
38. Nandy T, Idris MYIB, Noor RM, Kiah MLM, Lun LS, Juma'at NBA, Ahmedy I, Ghani NA, Bhattacharyya S. Review on security of internet of things authentication mechanism. IEEE Access. 2019;7:151054–89.
39. Schuba C.L, Krsul I.V, Kuhn M.G, Spafford E.H, Sundaram A, Zamboni D. Analysis of a denial of service attack on tcp. In: Proceedings of 1997 IEEE Symposium on Security and Privacy (Cat. No. 97CB36097), 1997;pp. 208–223. IEEE.
40. Bilal M, Kang SG. A secure key agreement protocol for dynamic group. Clust Comput. 2017;20(3):2779–92.
41. Gope P, Lee J, Quek TQ. Resilience of dos attacks in designing anonymous user authentication protocol for wireless sensor networks. IEEE Sens J. 2016;17(2):498–503.
42. Armando A, Basin D, Boichut Y, Chevalier Y, Compagna L, Cuéllar J, Drielsma P.H, Héam P.C, Kouchnarenko O, Mantovani J, et al. The avispa tool for the automated validation of internet security protocols and applications. In: International conference on computer aided verification, 2005;pp. 281–285. Springer.
43. Burrows M, Abadi M, Needham R.M. A logic of authentication. Proc R Soc Lond A Math Phys Sci. 1989;426(1871), 233–271.
44. Blanchet B. Modeling and verifying security protocols with the applied pi calculus and proverif. Found Trends Privacy Secur. 2016;1(1–2):1–135.

45. Bellare M, Rogaway,P. Random oracles are practical: A paradigm for designing efficient protocols. In: Proceedings of the 1st ACM Conference on Computer and Communications Security, pp. 62–73 (1993)
46. Koblitz N, Menezes AJ. The random oracle model: a twenty-year retrospective. Des Codes Crypt. 2015;77(2):587–610.
47. Cremers C.J. The scyther tool: Verification, falsification, and analysis of security protocols. In: International conference on computer aided verification, pp. 414–418. Springer (2008)
48. Kumar P, Chouhan L. A privacy and session key based authentication scheme for medical iot networks. Comput Commun. 2021;166:154–64.
49. Alzubi JA. Blockchain-based lamport merkle digital signature: Authentication tool in iot healthcare. Comput Commun. 2021;170:200–8.
50. Juyal S, Sharma S, Shukla A.S. Security and privacy issues in unified iot-based skin monitoring system. Materials Today: Proceedings (2021)
51. Amin R, Islam SH, Biswas G, Khan MK, Kumar N. A robust and anonymous patient monitoring system using wireless medical sensor networks. Fut Gen Comput Syst. 2018;80:483–95.
52. Ever YK. Secure-anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks. IEEE Syst J. 2018;13(1):456–67.
53. He D, Kumar N, Chen J, Lee CC, Chilamkurti N, Yeo SS. Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. Multimed Syst. 2015;21(1):49–60.
54. Jiang Q, Ma J, Yang C, Ma X, Shen J, Chaudhry SA. Efficient end-to-end authentication protocol for wearable health monitoring systems. Comput Electr Eng. 2017;63:182–95.
55. Liu CH, Chung YF. Secure user authentication scheme for wireless healthcare sensor networks. Comput Electr Eng. 2017;59:250–61.
56. Srinivas J, Mishra D, Mukhopadhyay S. A mutual authentication framework for wireless medical sensor networks. J Med Syst. 2017;41(5):80.
57. Wazid M, Das AK, Kumar N, Conti M, Vasilakos AV. A novel authentication and key agreement scheme for implantable medical devices deployment. IEEE J Biomed Health Inform. 2017;22(4):1299–309.
58. Wu F, Xu L, Kumari S, Li X. An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks. Multimed Syst. 2017;2(23):195–205.
59. Masud M, Gaba G.S, Choudhary K, Hossain MS, Alhamid M.F, Muhammad G. Lightweight and anonymity-preserving user authentication scheme for iot-based healthcare. IEEE Internet Things J. 2021.
60. Aghili SF, Mala H, Shojafar M, Peris-Lopez P. Laco: lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in iot. Fut Gen Comput Syst. 2019;96:410–24.
61. 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. Journal of Ambient Intelligence and Humanized Computing pp. 1–22 (2018)
62. Ali Z, Ghani A, Khan I, Chaudhry SA, Islam SH, Giri D. A robust authentication and access control protocol for securing wireless healthcare sensor networks. J Inf Secur Appl. 2020;52:102502.
63. Alzahrani B.A, Irshad A, Alsubhi K, Albeshri A. A secure and efficient remote patient-monitoring authentication protocol for cloud-iot. In J Commun Syst. 2020;p. e4423.
64. Challa S, Das AK, Odelu V, Kumar N, Kumari S, Khan MK, Vasilakos AV. An efficient ecc-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks. Comput Electr Eng. 2018;69:534–54.
65. Das AK, Sutrala AK, Odelu V, Goswami A. A secure smart-card-based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks. Wireless Pers Commun. 2017;94(3):1899–933.
66. Li X, Niu J, Kumari S, Liao J, Liang W, Khan MK. A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity. Secur Commun Netw. 2016;9(15):2643–55.
67. Liu X, Zhang R, Zhao M. A robust authentication scheme with dynamic password for wireless body area networks. Comput Netw. 2019;161:220–34.
68. Mao D, Zhang L, Li X, Mu D. Trusted authority assisted three-factor authentication and key agreement protocol for the implantable medical system. Wirel Commun Mob Comput. 2018.
69. Sharma G, Kalra S. A lightweight user authentication scheme for cloud-iot based healthcare services. Iran J Sci Technol Trans Electr Eng. 2019;43(1):619–36.
70. 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.
71. Soni P, Pal AK, Islam SH. An improved three-factor authentication scheme for patient monitoring using wsn in remote healthcare system. Comput Methods Programs Biomed. 2019;182:105054.
72. Wazid M, Das AK, Vasilakos AV. Authenticated key management protocol for cloud-assisted body area sensor networks. J Netw Comput Appl. 2018;123:112–26.
73. 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;8:47282–94.
74. Khalid H, Hashim SJ, Syed Ahmad SM, Hashim F, Chaudhary MA. Cross-sn: A lightweight authentication scheme for a multi-server platform using iot-based wireless medical sensor network. Electronics. 2021;10(7):790.
75. Nashwan S. An end-to-end authentication scheme for healthcare iot systems using wmsn. CMC. 2021;68(1):607–42.
76. Almuhaideb AM, Alqudaihi KS. A lightweight and secure anonymity preserving protocol for wban. IEEE Access. 2020;8:178183–94.
77. Gupta A, Tripathi M, Sharma A. A provably secure and efficient anonymous mutual authentication and key agreement protocol for wearable devices in wban. Computer Communications;2020.
78. Ibrahim MH, Kumari S, Das AK, Wazid M, Odelu V. Secure anonymous mutual authentication for star two-tier wireless body area networks. Comput Methods Programs Biomed. 2016;135:37–50.
79. Kompara M, Islam SH, Hölbl M. A robust and efficient mutual authentication and key agreement scheme with untraceability for wbans. Comput Netw. 2019;148:196–213.
80. Koya AM, Deepthi P. Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network. Comput Netw. 2018;140:138–51.
81. Kumar M, Chand S. A lightweight cloud-assisted identity-based anonymous authentication and key agreement protocol for secure wireless body area network. IEEE Systems Journal (2020)
82. Li X, Ibrahim MH, Kumari S, Sangaiah AK, Gupta V, Choo KKR. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. Comput Netw. 2017;129:429–43.

83. Rehman ZU, Altaf S, Iqbal S. An efficient lightweight key agreement and authentication scheme for wban. IEEE Access. 2020;8:175385–97.
84. 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;7:53922–31.
85. Wan T, Wang L, Liao W, Yue S. A lightweight continuous authentication scheme for medical wireless body area networks. Peer-to-Peer Networking and Applications pp. 1–15 (2021)
86. Kumar P, Lee SG, Lee HJ. E-sap: efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. Sensors. 2012;12(2):1625–47.
87. Zhang L, Zhang Y, Tang S, Luo H. Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement. IEEE Trans Industr Electron. 2017;65(3):2795–805.
88. ur Rehman Z, Altaf S, Ahmed S, Huda S, Al-Shayea A.M, Iqbal S. An efficient, hybrid authentication using ecg and lightweight cryptographic scheme for wban. IEEE Access (2021)
89. 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)
90. Rakeei MA, Moazami F. Cryptanalysis of an anonymous authentication and key agreement protocol for secure wireless body area network. IACR Cryptol ePrint Arch. 2020;2020:1465.
91. Singh D, Kumar B, Singh S, Chand S. Evaluating authentication schemes for real-time data in wireless sensor network. Wireless Pers Commun. 2020;114(1):629–55.
92. Mo J, Shen W, Pan W. An improved anonymous authentication protocol for wearable health monitoring systems. Wireless Communications and Mobile Computing **2020** (2020)
93. Mridha M, Al Imran M, Wadud M, Hussen A, Abdul Hamid M. An improved user anonymous secure authentication protocol for healthcare system using wireless medical sensor network. Int J Comput Digit Syst. 2020;10:2–12.
94. Mo J, Hu Z, Lin Y. Cryptanalysis and security improvement of two authentication schemes for healthcare systems using wireless medical sensor networks. Secur Commun Netw. 2020.
95. Wang F, Xu G, Xu G. A provably secure anonymous biometrics-based authentication scheme for wireless sensor networks using chaotic map. IEEE Access. 2019;7:101596–608.
96. Kwon D, Park Y, Park Y. Provably secure three-factor-based mutual authentication scheme with puf for wireless medical sensor networks. Sensors. 2021;21(18):6039.
97. Betarte G, Pardo Á, Martínez R. Web application attacks detection using machine learning techniques. In: 2018 17th ieee International Conference on Machine Learning and Applications (icmla), pp. 1065–1072. IEEE 2018.
98. Montes N, Betarte G, Pardo Á, Martínez R. Web application attacks detection using deep learning. In: 25th Iberoamerican Congress on Pattern Recognition. Porto, Portugal. 2021.
99. Aranha DF, Gouvêa CP. RELIC is an Efficient LIbrary for Cryptography. 2020. https://github.com/relic-toolkit/relic
100. Texas Instruments: Data sheet of MSP430F5437) (2009). http://www.ti.com/product/MSP430F5437. Accessed March 2020
101. Texas Instruments: CC2520 2.4 Ghz IEEE 802.15.4 / ZigBee RF Transceiver Datasheet, 2007. http://www.ti.com/product/CC2520. Accessed March 2020
102. Texas Instruments: Medical-Products (2021). https://www.ti.com/applications/industrial/medical/products.html. Accessed October 2021
103. Song A, Si G, Gu Q. Study on remote medical monitoring system based on msp430 and cc2530. In: 2016 Chinese Control and Decision Conference (CCDC), pp. 2415–2418 (2016)
104. Shim KA. S2DRP: Secure implementations of distributed reprogramming protocol for wireless sensor networks. Ad Hoc Netw. 2014;19:1–8.
105. Oudjida AK, Liacha A. Radix-2 w arithmetic for scalar multiplication in elliptic curve cryptography. IEEE Trans Circuits Syst I Regul Pap. 2021;68(5):1979–89.
106. Ma Z, Liu Y, Wang Z, Ge H, Zhao M. A machine learning-based scheme for the security analysis of authentication and key agreement protocols. Neural Comput Appl. 2020;32(22):16819–31.
107. Li X, Jiang P, Chen T, Luo X, Wen Q. A survey on the security of blockchain systems. Futur Gener Comput Syst. 2020;107:841–53.
108. Shor P. Polynomial-time algorithm for prime factorization and discrete logarithms on a quantum computer. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, vol. 124, 1994.
109. Alagic G, Alperin-Sheriff J, Apon D, Cooper D, Dang Q, Kelsey J, Liu YK, Miller C, Moody D, Peralta R, et al. Status report on the second round of the nist post-quantum cryptography standardization process. NIST: US Department of Commerce; 2020.
110. Bao SD, Poon CC, Zhang YT, Shen LF. Using the timing information of heartbeats as an entity identifier to secure body sensor network. IEEE Trans Inf Technol Biomed. 2008;12(6):772–9.
111. Zhang G, Zhang X, Bilal M, Dou W, Xu X, Rodrigues J.J. Identifying fraud in medical insurance based on blockchain and deep learning. Future Generation Computer Systems, 2022, pp. 140–154.
112. Istiaque Ahmed K, Tahir M, Hadi Habaebi M, Lun Lau S, Ahad A. Machine learning for authentication and authorization in iot: taxonomy, challenges and future research direction. Sensors. 2021;21(15):5122.