*Journal on Internet of Things*
DOI:10.32604/jiot.2021.018088
***Article***

# Authentication in Wireless Body Area Network: Taxonomy and Open Challenges

**Abdullah M. Almuhaideb and Kawther S. Alqudaihi***

Department of Computer Science, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Dammam, 31441, Saudi Arabia

*Corresponding Author: Kawther S. Alqudaihi. Email: 2190500127@iau.edu.sa

Received: 01 August 2021; Accepted: 15 October 2021

**Abstract:** Wearable body area network (WBAN) aids the communication between the health providers and patients by supporting health monitoring services. It assists the users to maintain their health status records by collecting the body signals and transmitting them for further processing measurements. However, sensor data are publicly transferred through insecure network that facilitates the attacker malicious acts like performing masquerading attack, man in the middle, and snooping. Several authentication techniques were suggested to levitate the security of the communication channels to preserve the user data from exposure. Moreover, authentication schemes aid plenty of security issues related to user and data privacy, anonymity, repudiation, confidentiality, and integrity, but they lack performance efficiency. On the other hand, it is very hard to find the balance between security and efficiency in most of the authentication schemes, especially for the WBAN platform that consists of memory and processing constraint devices. Therefore, this paper surveys and discusses the latest authentication schemes types, techniques, and system features. Also, it highlights their strengths and weaknesses towards common knowingly attacks and provides a comparison between the popular scheme validation proofs and simulation tools. Thence, this paper draws a path for the new direction of the authentication technologies, the authentication schemes open issues, and the potential future evolution in this area.

**Keywords:** WBAN; protocol; authentication; key agreement; simulation; taxonomy

## 1 Introduction

Recently, Internet of Things (IoT) is a widely used concept that is defined by being a podium of linked devices that connect, distribute the data among them and occupies a very wide notion with an excessive amount of applications [1–4]. It converts devices into a shrewd object that interrelates with individuals and offers them the demanded service. Moreover, it ropes diverse tenacities such as cultivation, transaction, shrewd homes, and shrewd cities [5]. It serves many types of application and one of them is a wearable health monitoring system (WHMS) to monitor user health. It allows doctors and patients to profit from WHMS environment facilities at any time. Wearable body area network (WBAN) falls underneath the umbrella of the broader notion WHMS [6–8]. It aids the doctors in identifying many illnesses either by connecting it in the patients' body or outfits for diverse interpretations [9–13]. WBAN facilities allow nursing the aged and immobilize individuals alongside improving their existences and life quality [14]. Additionally, WBAN encompasses inexpensive and small memory radars with restricted administering potentials, which makes it susceptible to numerous attacks [15]. Consequently, variety of schemes were suggested to preserve a trade-off amid security and functionality for WBAN. Unauthorized access and alteration of physiological data can have life-threatening effects on patients and may result in inaccurate medication.

### *1.1 Related Work*

Different surveys were conducted to compare several authentication schemes that were proposed to show their weaknesses and strengths with their latest techniques. Abdullah Almuhaideb [16] explained ubiquitous mobile authentication schemes with a comparison between their approaches. Also, the survey exposed the security and system requirement to overcome the platform challenges. Meng et al. [17,18] discussed biometric authentication for user mobile and categorized it into physiological and behavioral. Also, they mentioned the various schemes, their attacks, and their used techniques alongside they listed the biometric system evaluation features such as acceptability, universality, performance, permanence, uniqueness, acceptability, and circumvention. Lastly, they showed that the biometric system still has open issues to be considered in designing authentication schemes like feature extraction and selection, algorithm optimization, shoulder surfing attack, usability issue, and security. Moreover, Masdari et al. [19] had discussed WBAN's latest schemes techniques and classified them into cryptography-based, biometric-based, and channel-based authentication. They measured the number of schemes that use anonymous authentication and showed that they are less than non-anonymous authentication. Also, they stated that the mutual authentication schemes are more than one-way authentication along with that message authentication code algorithm (MAC) is the most used algorithm in WBAN schemes. Besides, Kompara et al. [20] discussed the latest authentication schemes, their methods, weaknesses, key agreement, their security features, and efficiency. Moreover, Narwal et al. [21] mentioned WBAN schemes security features, attacks, threats and discussed the security standard to be implemented in WBAN for reliable communication which is IEEE 802.15.6. Nevertheless, according to [19] IEEE 802.15.6 has security issues, so allot of authentication schemes are enhanced to reduce energy consumption and levitate security by applying cryptography in them. Also, Dhanvijay et al. [22] explained WBAN network architectures, technologies, healthcare applications, performance metrics alongside suitable power for small sensors, open issues in WBAN such as scalability, security, algorithm optimization, quality of service (QoS), schemes implementation and development costs.

Thus, Hussain et al. [14] had discussed WBAN well-known applications, characteristics of WBANs, list of security requirements, authentication types, well-known authentication protocols, classification of schemes based on their types, platforms such as mobile, cloud, blockchain, and artificial intelligence schemes, but it did not highlight the most used encryption algorithms and simulation tools. From the above, the related surveys did not cover the analysis of the cryptographic algorithm used in authentication for WBAN schemes regarding their preference, performance, the favored simulation tools and proofs. Therefore, we constructed a comparison of the most used encryption algorithm, simulation and proof tools along with the open issues. The below figure shows the related surveys to the field, refer to Fig. 1. In the Table 1, we presented the related surveys gaps and findings.

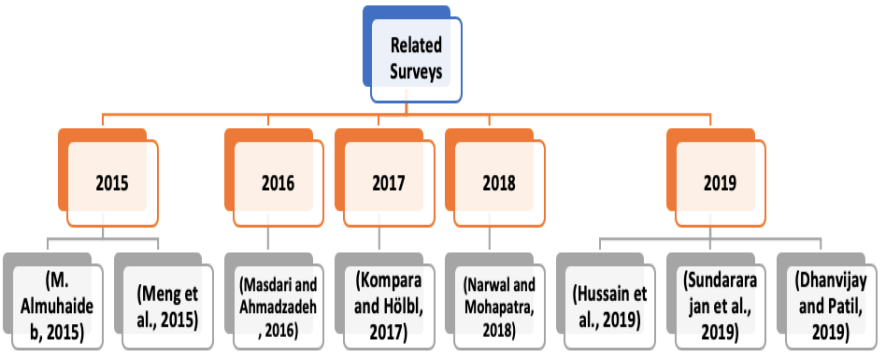


**Figure 1:** Classification of related surveys

**Table 1:** Related surveys gaps and findings

| Related surveys | Findings | Gaps |
|---|---|---|
| [14] | -WBAN applications<br>-Characteristics of WBANs<br>-Security requirements<br>-Authentication types, protocols, and schemes classification | -Statistics of encryption algorithms simulation tools<br>-Challenges, and opportunities |
| [16] | -Comparison of ubiquitous mobile authentication schemes approach<br>-Recommendations to deal with challenges in the field | -Statistics of encryption algorithms simulation tools |
| [17,18] | -Biometric authentication for user mobile<br>-Various schemes, their attacks, their used techniques, and evaluation features<br>-Open issues | -Statistics of encryption algorithms simulation tools |
| [19] | -WBAN's latest schemes, techniques and classifications<br>-A statistics for the most used type of scheme regarding anonymous authentication, mutual authentication, and one-way authentication | -Statistics of encryption algorithms simulation tools<br>-Challenges, and opportunities |
| [20] | -Authentication schemes, their methods, weaknesses, key agreement, their security features, and efficiency | -Statistics of encryption algorithms simulation tools<br>-Challenges, and opportunities |
| [21] | -WBAN schemes security features, attacks, and threats | -Statistics of encryption algorithms simulation tools<br>-Challenges, and opportunities |
| [22] | -WBAN network architectures, technologies, healthcare applications, and performance metrics<br>-Open issues in WBAN | -Statistics of encryption algorithms simulation tools |

### *1.2 Problem Statement*

From the previous discussion in Section 1.1, we identified our problem statement that shows the need for an intensely comprehensive comparison between authentication schemes along with developing the previous surveys through inclusive analysis, and evaluation to define the research gap and open issues. Scheming the WBAN authentication system bearing in mind scalability along with the balance between security and efficiency is a challenging task. Moreover, many authentications and key agreement structures can accomplish a certain level of security but degrade the system performance [1,23,24]. Otherwise, the latest schemes deliberated performance competence and efficiency to attain an elevated level of security [10,11,25]. Therefore, studying and analyzing the recent authentication schemes, their techniques, varieties, flaws, and strengths is essential to build a bridge for the attentive researchers in this area. Also, several survey papers had been conducted lately to clarify the practices of different authentication schemes and their feasibility [14,16,22]. All of the above had discussed authentication schemes alongside their techniques and analyzed the schemes based on their methods, types, and efficiency, but the field still needs more analysis regarding the formal proofs, security deficiencies and the latest approaches such as blockchain and artificial intelligence (AI).

### *1.3 Contribution*

Our review paper surveyed the WBAN authentication schemes in the period of (2016–2020), their methods, tools, and drawbacks, to offer great guidance for whom might be interested in this area. The contribution covers and analyzes authentication methods, system security features, possible attacks on the authentication schemes. Also, it compares statistically the most used authentication techniques and validation tools to highlight the latest practices with the reasons by describing each validation tool features. Lastly, we compared the surveyed schemes and we pointed out the open issues to be covered in the future schemes design and the methods that have a great opportunity to enhance authentication schemes design in the future.

### *1.4 Organization*

The rest of this paper is organized as follows. Firstly, Section 2 provides a background of various authentication concepts, types and standards. Section 3 offers authentication schemes platforms, techniques and taxonomy of them. Then, the existing schemes formal validation methods, and tools is discussed in Section 4. Also, a comparative analysis of the mentioned schemes is deliberated in Section 5. Next, the open issues are offered in Section 6. Finally, the paper conclusion followed by future work direction is given in Section 7.

## 2 Background

We must realize the WBAN schemes construction to distinguish how the system modules interconnect amongst themselves. It resides of three main objects, namely: gateway node, first-level node, and second-level node (sensor node). First, hub node advocates like a server that transmits the information composed from the sensor and distributes them to system management for treating. The hub node has high performance and storage. Second, foreign network (e.g., mobile, etc.) has less managing capabilities and power in comparison to the hub node [26]. Third, the second-level node with the lowermost performance and storage, as depicted in Fig. 2.

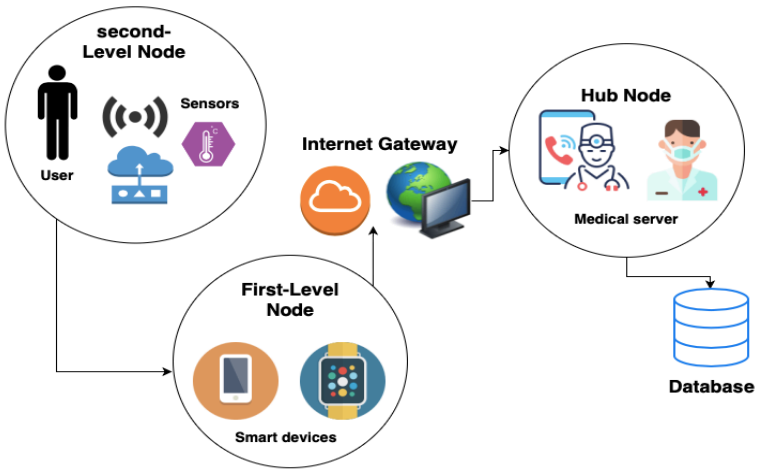


**Figure 2:** WBAN two-stage architecture

### *2.1 User Authentication Factors*

Considering the user as an important entity in the WBAN architecture as a patient, a doctor, and administrator, it is very important to authenticate the user to the server and device. Subsequently, we identified several types of user authentication.

1) Password Authentication

This type of authentication is emanating from a password from the user choice or the system choice to authorize the user. Moreover, this method is the most popular method and the lowest cost of all, but it is the weakest method because it can be broken easily.

2) Two-factor Authentication

This type of authentication is based on a one-time password with a token or a card to identify the privileged user and give him/her access to the service. Moreover, this method is used on the ATM worldwide.

3) Multi-factor Authentication

This type of authentication is based on a one-time password with a token or a card to identify the privileged user and give him/her access to the service. Moreover, this method is used on the ATM worldwide.

After mentioning the interconnected entities and the user authentication types, it showed what areas to be concerned in the WBAN environment for protection. Therefore, the WBAN environment requires to ensure the attainment of authentication between the approved interconnected objects alongside anonymity, un-traceability, integrity, and privacy [27]. Network Authentication solutions need to concentrate on particular standards to deliver a certain level of security and performance depends on the desired facility. The following section discusses different standards that lead to the creation of IEEE 802.15.6 (WBAN standard).

### *2.2 Network Authentication Standards*

In this section, we explained how a WBAN technology structure depends on small, and smart, lower power-constrained memory sensors implanted or attached to the human body. After knowing WBAN architecture, it is known that many security schemes had been represented to enhance security in different WBAN entities. As a result, plenty of security standards proposed to ensure that authentication schemes met the criteria for reliable communication like low cost, lightweight, robustness, and low power consumption [28]. Thence, we specified below the popular Ad Hoc operation mode standards used to protect WBAN architecture, besides that all of their power consumption information, network topology, and their earmark applications:

- IEEE 802.11 a/b/g/n (WiFi): This standard has a higher power consumption which is around 800 mW, infrastructure-based network topology, and it is applicable for data network not for WBAN sensor due to its power consumption.
- IEEE 802.15.1 (Bluetooth): This standard has the medium power consumption, which is around 100 mW, Ad Hoc small-based network topology, and it is applicable for voice link not for WBAN medical sensor.
- IEEE 802.15.4 (Zigbee): This standard has a low power consumption, which is around 50 mW, it supports many network topologies like Ad-hoc, Peer-to-Peer, Star, and Mesh, also it is applicable for sensor and home automation.
- IEEE 802.15.4 a (UWB): This standard has the low power consumption, which is less than 50 mW, it supports many network topologies like Ad-hoc, Peer- to-Peer, Star, and Mesh, also it is applicable for short-range and high data rates localization.
- IEEE 802.15.6 (WBANs Standard): This standard has the lower power consumption, which is around 1 mW in 1m distance, it supports many network topologies like Intra-WBAN: coordinated, uncoordinated, 1/2-hop star, and Inter-WBANs, also it is applicable for health monitoring, sports, disability assistance, body-centric application, etc.

IEEE 802.15.6 is the basic standard for WBAN medical sensors, and it includes several layers fall under the Physical layer and MAC layer as follows:

- Physical layer: It stems from different types support different needs of WBAN applications such as:
  - Human Body Communications (HBC): It creates a new channel for medical embedded devices and their communication with a frequency range between 5–50 MHz, also it contains two types of coupling captive and galvanic.

  - Narrow Band (NB): It has higher power consumption and considers the communication between many non-embedded on the body sensors. Many frequency bands depending on the application and country worldwide.
  - Ultra-Wide Band (UWB): It consists of many features for WBAN sensors such as attack resistance, performance, and low power consumption. Many frequency masks depend on the application and country worldwide.
- MAC layer: It is the main standard that helps users to have many features that stems of different types to support different needs such as hybrid Time-Division Multiple Access (TDMA), Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA), and the combination of both.

The aforementioned standards were designed to fit specific application requirements, although those criteria were not fully met their purposes like power consumption, communication range, and data rate along with their lack of supporting WBAN constrained structure [28]. Therefore, allot of security key agreement and authentication schemes had been developed over the recent years to overcome some standards issues.

### *2.3 WBAN Security and Functional Features*

Allot of security research related to our work had discussed the system security features to enable the readers from knowing the ideal WBAN system behavior, and how to implement it in their schemes. Besides, it is important to know them and analyze the schemes for weaknesses and strengths. In the table below we discussed each feature along with their acronym to simplify the terms, as depicted in Table 2.

**Table 2:** Security and functional features

| Acronym | Security requirement | Discussion |
|---|---|---|
| F1 | Integrity | The content of any message does not change during the transmission |
| F2 | Anonymity | The identity of each communication party should be hidden during communication or offline |
| F3 | Confidentiality | Preventing unauthorized people from accessing the message and make the information available for legitimate users |
| F4 | Robustness | The system is complicated enough with algorithms that make it robust against attacks |
| F5 | Authenticity | Trusting the source and destination of the message |
| F6 | Un-traceability | The attacker cannot follow the trace of the object as it moves from one participant or location to another [29] |
| F7 | Forward/backward secrecy | Assurance that the session key will not be compromised [30] |
| F8 | Non-repudiation | No one can deny sending/receiving during communication. |
| F9 | Key escrow resilience | The network operator cannot impersonate any other entities without being noticed [31] |
| F10 | Scalability | Ability to handle an increasing number of resources without degrading the performance |

### *2.4 Possible Attacks*

Several security types of research had discussed the threats that might face their system during the authentication process, to help the scheme's designers to avoid any fault could cause a breach. Also, it is a crucial task to analyze authentication schemes and find the best ways to enhance them. In Table 3, we discussed each threat along with their acronym to simplify the terms.

**Table 3:** Common threats to authentication in WBAN architecture

| Acronym | Threat | Discussion |
|---|---|---|
| A1 | Impersonation attack | Adversary disguises as a legitimate user to fool the application provider |
| A2 | Known key attack | The exposed session key should not lead the adversary to know the next session keys |
| A3 | Man in the middle (MITM) | Adversary intercepts the communication between legitimate users and application providers |
| A4 | Replay attack | Adversary intercepts messages and uses the information to repeat and get a legal application for the next session |
| A5 | Brute force attack | Adversary tries every possible combination to guess the password |
| A6 | Stolen verifier attack | Adversary steals the verification table to disguise the system as a legitimate user |
| A7 | Denial of service attack (DoS) | The adversary uses many clients to enable him/her to overwhelm the network with bogus requests |
| A8 | Privileged insider attack | Malicious insiders with privileged account credentials can pose a serious threat to other personal data in the same domain |
| A9 | Shoulder surfing attack | A social engineering type attack that enables attackers from looking over someone's shoulder to get password, identification method |
| A10 | Forgery attack | A malicious code submitted to the user and the application trusts |

### *2.5 Summarization*

To sum up, many standards with different bandwidths along with different features were employed to attain specific purpose. However, the most engaged standard in WBAN architecture is IEEE 802.15.6. Also, in any WBAN system there are several security and functional features must be considered, refer to Table 1. Lastly, multiple authentication schemes exist to levitate the system robustness against several attacks that mentioned in Table 3. In the figure below, we listed all the standards, functional security features, along with attacks refer to Fig. 3.

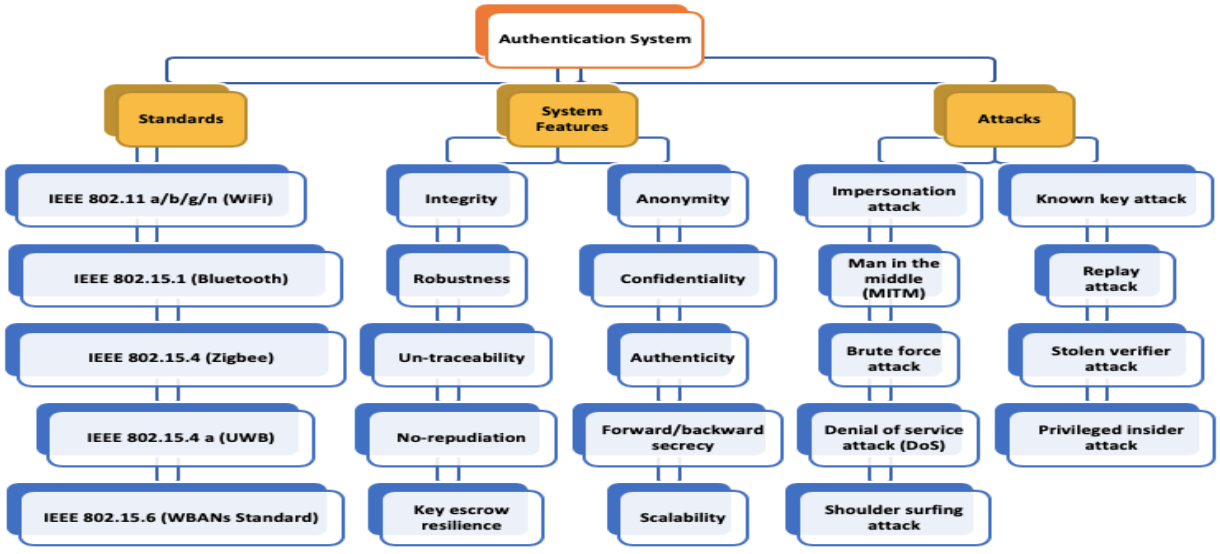


**Figure 3:** Authentication system standards and attacks

Moreover, knowing background information about the standards, security features and threats helps to direct the reader into the following section, in order to categorize the proposed authentication schemes in WBAN and analyze them.

## 3 Authentication in WBAN

In precedence to the discussion about WBAN architecture, we clarified in detail the techniques used to authenticate the data and the sensor. Firstly, we created a taxonomy of the techniques and platforms used in the WBAN architecture refer to Fig. 4. Then, we divided authentication techniques to symmetric, asymmetric, emerging technologies. Also, we categorize the techniques based on the platform that employed them in the following sections: Section 3.1, Section 3.2, and Section 3.3.

### *3.1 Asymmetric Cryptography*

WBAN architecture contains very essential private information for the patient that needs to be hidden and saved from any harmful attack. While patient data is transmitted over insecure communication channels, then it is a necessity to propose authentication schemes to intensify the user protection [23]. Numerous of schemes focused on the enhancement of the forward secrecy, privacy, anonymity, etc. But they neglect strengthening of the authentication model along with its authentication key. In the following, we identified the asymmetric authentication in both mobile and cloud platforms.

#### *3.1.1 Asymmetric Cryptography in Mobile Platform*

WBAN mobile platform is very popular in creating authentication schemes and the following schemes are based on asymmetric cryptography in a mobile platform. Liu et al. [32] proposed an authentication scheme based on bilinear pairing for user authentication in a mobile platform where the identity of the user, public key, and private keys protected by random number and timestamp from the network manager (NM). Their scheme is simulated through the oracle model and proved it has F2. Thus, Li et al. [33] analyzed protocol and found that it is vulnerable to A1, A6, and A7. Then, they proposed an authentication scheme based on the elliptic curve cryptography to authenticate the mobile user to the application server in the WBAN. It includes creating asymmetric keys to the user based on the randomness and complexity of the elliptic curve problem. ECC applies to small constraint devices due to its shorter key size and the random points that added continuously to the generated key.

In [33] scheme, the user chooses his/her user name and id, sends it to the network manager for authentication with the application provider. They conducted a BAN logic formal proof for the scheme and stated that the scheme is resistant to A1, A4, A6, A7, A8, and A10. On the other hand, Sowjanya et al. [8] analyzed and found that it has drawbacks in F7 along with the problem of key control and harmonization. The system generates a public key and private key through ECC and hashes to secure the pair.

Furthermore, the scheme in [8] allows the application server (AS) to select key pairs and the user can sort the first interaction in an insecure network to register.

Also, NM verifies the identity of the client to authenticate it and direct it to the application provider. Their scheme formally proved by BAN logic along with Automated Validation of Internet Security Protocols and Applications (AVISPA) tool and proved that the scheme is robust against A1, A3, A4, A7 and it has weakness in F7.

Chang et al. [34,35] had proposed an authentication scheme between the user node and the GW node to authenticate each other by applying a honeyword checker. Also, their scheme used random number generation from the Elliptic curve along with a hash function right before sending the authentication request in the insecure channel. Consequently, Wang et al. [36] had cryptanalyzed both schemes and exposed their lack of F2 and their vulnerability to A2, and A8. Therefore, Wang et al. [36] proposed an improved anonymity three-factor authentication scheme employing an Elliptic curve cryptosystem (ECC) for Wireless Sensor Network (WSN). The scheme counted on the biometric fuzzy extractor method to

enhance scheme security against password guessing and A1. Unfortunately, their scheme suffered from F2 issues when the user loses his/her smartcard and due to some parameters lack protection.

Similarly, Challa et al. [37] proposed a three-factor authentication scheme in WBAN architecture based on the public key and Elliptic curve structure to create a secure system. They claimed that their scheme is robust versus numerous types of attacks such as A8, password guessing, A6, A7, A2, A1, A3, and A4. But their scheme lacked F2 of the user and second-level node identities. Also, the weak protection to the public key by the user phone and temporary identity made the scheme weak toward F2 and guessing attack due to the exposure of random parameters in an open channel. It cannot withstand A2. Mo et al. [38] had analyzed the security flaws in the proposed three-factor scheme in WSN by Lu et al. [39] and found that their protocol is suspectable to offline password guessing, A2, and lack of F7. Therefore, Mo et al. [38] had proposed a three-factor authentication scheme based on the biometric, smart card and password where they used hash function and Elliptic curve to protect the passwords and security parameters. But the issue is the user F2 might be compromised because the user identity is only protected by random number and biometric which both might be easily guessed and spoofed by the intruder. Also, their scheme suffered from various security outbreaks, such as session key exposure, A1, and cannot ensure F2, F5, and F6.

Therefore, Ali et al. [40] had offered a lightweight and secure three-factor authentication procedure for WBAN by employing the Elliptic curve cryptography, and bilinear pairing to resolve the issues in these schemes [37,41]. Although their scheme is guarded against A1, A8, offline password guessing, A6, and A4, but it still has high computation cost and delays in communication due to extensive cryptographic operations.

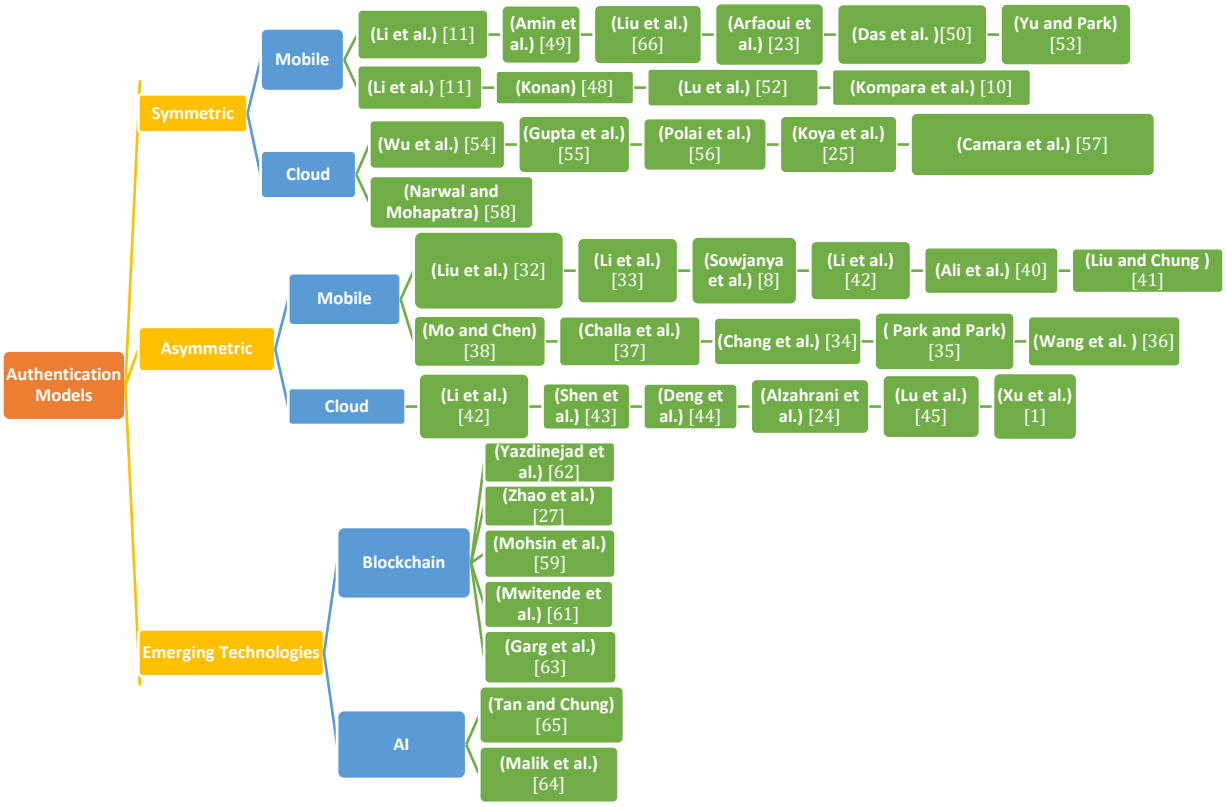


**Figure 4:** Taxonomy of authentication in WBAN

*3.1.2 Asymmetric Cryptography in Cloud Platform*

WBAN cloud platform is a very sophisticated and strong platform to create powerful authentication schemes on the network and the following schemes employ asymmetric cryptography in the cloud. Li et al. [42] employed bilinear pairing cryptography and hash function to create a lightweight and efficient public auditing scheme (LEPA). In their scheme, they shifted the integrity check from the user side into the cloud server-side to reduce the computational complexity. Also, the oracle model used to formally prove the system's robustness against A5 and A10. The scheme has issues in F10 because it did not include system parameter estimation in a real environment or real scenario. Likewise, Shen et al. [43] had offered a scheme to assist the client in connecting secretly in the cloud ecosystem by adopting message authentication code and asymmetric encryption for F1. The proposed scheme in [43] has issues which are the latency, and the secret arbitrary number is weakly protected since its encoded through using the current time as a key. Another scheme suggested by Deng et al. [44] had proposed asymmetric encryption system where its data can be restored from the cloud.

Also, Alzahrani et al. [24] had cryptanalyzed the scheme in [45] and exposed that it has limitations in F6, and F10. Alzahrani et al. [24] focused on securing the home-based network facilities by employing the elliptic curve based on the elliptic curve discrete logarithm and elliptic curve Diffie Hellman (ECCDH) to secure the F2 in first-level node and isolated area. Although that [24] scheme had achieved F2, F6, and defense versus A8, the scheme is susceptible to A7 due to intense computations and influences from the foreign network node, that permit the attacker from creating bogus arguments during the interaction. Other schemes do not engage the user to choose the secure password and identity during registration and initialization like Xu et al. [1] who worked on improving the strategy [46] by using ECC and Xoring the point from the curve to strengthen the shared key in the initialization phase. Furthermore, ECC is public-key cryptography with a key size 256 bits to prevent A5 and collision attacks [47].

Therefore, according to Konan et al. [48] who proposed authentication scheme based SHA- 2 hash function family with key sizes: 224 bit and above to resist the collision. While their system is formally proven by Proverif to prove its security against A1, A3, and A6, also it has poorer proficiency in contrast to [46] and F2 drawback for access point id.

***3.2 Symmetric Cryptography***

There is a necessity for protecting the data and sensors of the WBAN platform through encryption and hash function [23]. In the following, we identified the symmetric authentication in both mobile and cloud platforms.

*3.2.1 Symmetric Cryptography in Mobile Platform*

Mobile platform authentication schemes in WBAN are in development recently and the following schemes utilized symmetric cryptography in the mobile platform. Li et al. [11] recommended a WBAN authentication scheme based on the hash function and it is verified by BAN logic along with AVISPA tool to guarantee the scheme is robust *vs.* A1, A3, A5, and A6. Similarly, Amin et al. [49] had offered an authentication scheme built upon a hash function, and password for a mobile device. The user registers to the service by choosing a username, password and send them hashed together via a secure channel to the gateway (GW). Their scheme formally proved by BAN logic along with AVISPA tool, also it confirmed that the system achieved F6 and it is protected versus A6. Liu et al. [27] investigated the former scheme and proved that the scheme is susceptible to A9. Liu et al. [27] had utilized smartcard, biometric, and a changing password for user authentication. The scheme used hash function in a mobile device as GW for user validation and authentication along with the implementation of the IEEE 802.15.6 standard. The scheme had attained numerous security features like F1, F2, and security against A4, but regarding Arfaoui et al. [23] did not employ received signal strength indicator (RSSI) amongst nodes to safeguard the user biometric which affected badly on their scheme robustness to A1.

Furthermore, Das et al. [50] had suggested a biometric authentication scheme concerning mobile and wearable devices that applied a cryptographic hash function to safeguard the system arguments. Their scheme engaged AVISPA and random oracle to properly verify the system security regarding A1, A2, A4, and A3. Their scheme is protected against many attacks, but it has a lack of performance. Collection of authentication schemes were offered in [50,51] to condense the interaction operating cost in 5G networks and WBAN. Likewise, Kompara et al. [10] recommended a lightweight structure to solve the sensor A1, A3, and F6 issues in [46] by allowing the scheme to save the newest dual session keys and preserve the old keys. Their scheme is formally verified by BAN logic and AVISPA tool to confirm the system security against A1, A3, and achieves F7. Furthermore, Konan et al. [48] stated that the scheme in [10] had increased storage space problems. Lu et al. [52] proposed an authentication scheme in WBAN for symmetric session key and used Tamarin prover to confirm that their scheme can counterattack A3 and A7.

Recently, Yu et al. [53] proposed SLUA-WSN which is a lightweight three-factor authentication scheme with escalated user authentication system security against attacks and protects user anonymity by employing symmetric and hash function along with fuzzy extractor for the user biometric feature. Their scheme is the best communication and computation cost of all the previous schemes in the state-of-art in the matter of robustness against sensor node capture, A4, A8, and A1, also it ensures F5, and F6. Thus, SLUA-WSN is suitable for practical WBAN environments because it is more secure and efficient than related schemes. Their scheme suffers from A6 and shared secret key guessing because when the secret value is guessed, the system faces a major breach toward all the parameters security and F2.

*3.2.2 Symmetric Cryptography in Cloud Platform*

The following scheme enabled the user from choosing the initial authentication password like Wu et al. [54] who had operated the power of cryptographic hash function to guard the user password and id in the WBAN environment. Their scheme permitted the wearable device to produce time, password, id, and random nonce to be directed to the mobile while the cloud server preserves the latest used password and ID in the system. Their scheme used plenty of hashes to increase confusion to the produced arguments in every stage. Their scheme formally verified by the Proverif tool to confirm scheme robustness versus A4, and F10. Correspondingly, Gupta et al. [55] offered a user authentication scheme for mobile application thorough hash function, time, and random nonce. The user utilized his/her mobile phone to register in the medicinal WBAN application to demand the service and construct an account with an exclusive key and user ID. Thence, after correct registering and swapping arguments in a protected medium, the system validated the user by producing an arbitrary nonce and time stamp in all the collaborative units: sensor, mobile, and the server. Accordingly, this scheme properly verified by BAN logic along with the AVISPA tool and it can counterattack A1, A3, A4, A5, and A8. Both schemes have a shortage of performance effectiveness due to enormous parameterization and computations.

Other schemes do not engage users to choose the secure password and identity during registration and initialization like Polai et al. [56] had suggested a lightweight protocol for authentication in WBAN with twenty-four of hashes, an arbitrary value, and three secret values. They confirm the scheme security by implementing the scheme on AVISPA tool and BAN logic. Their scheme has two collaborating units' hubs with the sensor which makes it protected versus A7, but it is slow and unguarded to A4. Likewise, Arfaoui et al. [23] recommended two authentication procedures with miner sensor nodes and main connected nodes to gather the vital signs of human body and direct them to the manager node for nodes verification. Their structure accomplished F2 for the nodes by operating an arbitrary nonce, a one-way hash function, and sequence number to counterattack A4.

Likewise, Koya et al. [25] had amended the scheme [46] by enhancing it with smart cards along with user biometric in the first-level node [25]. Their scheme is strong versus A1 and F9 limitations, but it is susceptible to A1, A4, F6 concerns according to [10] and F2 drawback. Camara et al. [57] specified that the scheme in [25] has a weakness versus A5 that an adversary can effortlessly predict the protected arguments easily to acquire the following session key by the sensor. Bhawna Narwal et al. [58] had offered a structure to improve the security of [25] but it slow.

### *3.3 Emerging Technologies*

Since 2009, the Bitcoin technology arises worldwide, the necessity of blockchain technology was important to protect any transaction data. Blockchain grabbed huge attention in many fields especially IoT to create a decentralized system, because it eliminates the need for authorization from the third party. This technology is applied due to its high security against IP spoofing attacks or IP address falsification. Therefore, altering blockchains is challenging; nodes cannot join a network by themselves via inserting fake signatures into the record as camouflage [59]. Furthermore, Zhao et al. [60] applied blockchain to retrieve the session key in WBAN design. Their scheme used cryptography or the blockchain blocks to protect the data and administer the key adequately. Also, Mohsin et al. [59] proposed a decentralized authentication based on randomization of radio frequency identification (RFID) and finger vein (FV) protection scheme with the help of blockchain, hash function, steganography, and symmetric encryption AES. Their scheme extracts user features from the biometric image with two copies one is hashed for integrity and another copy is encrypted by AES to be sent to the server as a blockchain. The blockchain copy stored and steganography applied along with hash the steganographic value for F1. The scheme achieved F1, F2, and F3 for security. The issue in the blockchain is that the implementation and simulation costs are high that is why they cannot verify the suggested scheme if it is secure or efficient.

On the other hand, Mwitende et al. [61] utilized a blind identity-based signature to back up the message that is encrypted by blockchain technology. The blockchain used on the nodes and the encrypted session key with symmetric and asymmetric encryption. Their scheme was formally proofed by random oracle alongside simulated by JPBC pairing and it proved that it has F2, immutability, key compromise security, key control security, verifiability of the scheme, and more efficient in the limited bandwidth. Yazdinejad et al. [62] proposed a blockchain architecture for the distributed network over cooperated hospitals to enable patients from communication remotely to any near hospital regarding his/ her geographic location. Their scheme employed new algorithms for calculating patient information in the block and verifying the validity of the transferred block to the medical station. Moreover, it used a decentralized blockchain authentication scheme to reduce the operations overhead and utilize asymmetric cryptography for transaction validation and symmetric cryptography to encrypt the block information. Most of the distributed architectures are facing A7 due to a malicious node or cooperated hospital addition. Their work is simulated by the NS-2 V2.35 simulator to check the F4 of their scheme against attacks and it proved it can highly detect the previous attacks along its resistance to spoofing and info tampering.

Moreover, to deal with sensitivity of data issue, Garg et al. [63] proposed a scheme based on the Elliptic curve, signature, and blockchain for WBAN to increase the security of data transmitted through an insecure channel and protect the F2. Their scheme included the identity of the trusted authority as an additional secure parameter to authenticate between the communicated nodes. They included the pre-deployment phase, registration phase, login phase, authentication phase, password change, secure nodes addition, and secure data transmission blocks between GW and foreign network. Although that their scheme deployed a great combination of cryptographic and blockchain emerging technology to protect the data, it might face A7 and communication delay between the nodes, because of the heavy computation along with high storage cost.

Whereas Malik et al. [64] proposed an authentication scheme “ADLAuth” on the mobile platform based on artificial intelligence algorithms to authenticate the users from the dataset of their daily activities whether static, dynamic, or transition between them. The scheme implemented three classifiers support vector machine (SVM), decision tree (DT), and random forest (RF), along with three types of evaluations: HAR: Human Activity Recognition using smartphone dataset with mobile on waist sensor, accelerometer, and gyroscope which shows better recognition accuracy in recognizing dynamic activities more than static activities. Another type of evaluation was MobiAct and contains three sensors accelerometer, gyroscope, and magnetometer and it shows better performance than HAR in recognizing the dynamic feature recognition, but lower accuracy in recognizing static activity recognition. Lastly, PAMAP2: Physical Activity Monitoring Dataset that contains three sensors types and it performed the best in the dynamic feature activity recognition, but it has the lowest accuracy in recognizing static activity.

Also Tan et al. [65] proposed a certificateless biometric authentication scheme in mobile platforms and 5G network protected by a hash function. Their scheme utilized electrocardiogram (ECG) signals used by [66] as an AI technique in support vector to collect sensor data and communicate with the user smartphones. Their scheme is formally proved by the forking lemma that it is resistant to chosen message attack (CMA), A4, and F10 along with its improved efficiency in comparison to the schemes in their literature.

## 4 Authentication Scheme Validation Method

In this section, we discussed tools and proofs that were used to verify the authentication protocols formally and ensure that the protocols achieve a certain level of security, as summarized in Fig. 5. Also, formal proofs confirm that the protocol accomplished mutual authentication and key agreement. Likewise, formal verification simulation tools used to extract the syntax of protocols in simple syntaxes and run them on the machine to analyze the protocol security [67]. First, Section 4.1 explains the formal proof methods. Then, Section 4.2 provides the simulation tools used in protocol verification.

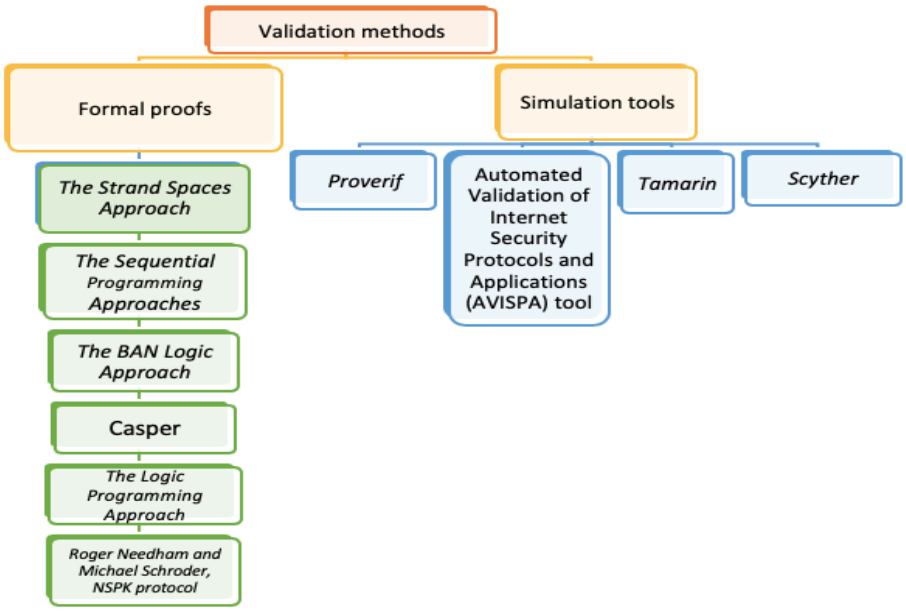


**Figure 5:** Validation methods diagram

### *4.1 Authentication Formal Proofs Method*

This section introduced the formal mathematical proofs to validate the protocols authentication and key agreement as follows:

1) Roger and Michael Schroder, NSPK protocol

This proof is offered by Roger Needham and Michael Schroder to enable mutual authentication and key agreement between two entities. This protocol uses different symbols to point each unit participated in the protocol such as S as a server, A, and B for communicating parties Kax and Kbx as shared secret key.

**Protocol overview:**

A and B are client's identities.

Kax is a secret key known only to clientA and the server.

Kbx is a secret key known only to clientB and the server.

Na and Nb are random numbers created by A and B.

Kab is a secret shared key to be used as a session key in the symmetric communication [68]. So, these symbols should represent the communication scenario between entities A and B to ensure the

scheme authenticity. Although this protocol is easy to conduct and used in various schemes, it is vulnerable to a replay attack [67].

2) The Strand Spaces Approach

Authors in [69] suggests this method, which consists of an equation framework for the proof of authentication schemes. It depends on the sequential information which is transmitted between the interacting entities. It is a comprehensive description to show well-performance of the authentication scheme with several symbols to identify each object along with device behavior.

**Protocol overview:**

A: a set to define: T as a collection of text messages and K as a collection of cryptographic keys K-1 for decryption. The key is used to encrypt and decrypt of sent message between entities to prove the authentication and key agreement between communicators.

3) The Logic Programming Approach

This approach uses Action Language for Security Protocols (ALSP) that is based on Logic Programming with Stable Model Semantics (LPSM) to be used as formal proof for NSPK. It is a formal proof language to analyze protocols security and authenticity. Furthermore, it is a great approach to see the protocol security violation and the results from running a specific authentication protocol.

**Protocol overview:**

P is the logic plug-in with S as a key set for q. Then the rule interpreted as if S and p fit to the key set S then q also fits to S.

4) The sequential Programming Approach

This approach is based on CSP (Communicating Sequential Process) which is a process of mathematical symbols to interpret the communication between entities and their events in the network environment. Furthermore, this approach uses Failure Divergence Refinement (FDR) to verify the CSP process and execute the output from the protocol implementation on CSP notation. FDR investigates the protocol sequence for malicious weak points that might jeopardize scheme security. It is created to fix the breach in NSPK.

**Protocol overview:**

L and R are communicating entities and they chose different deterministic decisions such as c, d, and the decisions execute different outputs like j, and z. Also the protocol run consists of stop, kill, and comm.v processes. Although this approach is providing a detailed process, it is still error-prone and time-consuming. Therefore, the Casper tool developed by [70] to overcome CSP issues.

5) Casper

It is a mathematical modelling tool to provide detailed expression into CSP code. Casper contains two items in its input file one is the generic definition which describes how protocol runs and detailed description for the system for checking. Also, those parts always start the description with '#' and have their Variables, Adversary Details, Protocol explanation, Specification, System, etc.

**Protocol overview:**

Message 0, sender identity C, receiver identity D, and the public key (PK) to encrypt sender and receiver identity during the communication.

6) The BAN Logic Approach

This approach was proposed by [71] to formally proof authentication and key agreement protocol based on belief logic. It depends on two entities believe each other's and communicate among themselves to achieve protocol goals securely. It is the preferable tool in proofing to avoid time consumption in previous approaches and to simplify protocol checking.

**Protocol overview:**

B and D both are communicators that believe and trust each other to share keys, messages, and nonce in a secure channel. Different symbols are used to clarify the status of the entity or message like (#) for fresh message, ≡ for the trust between communicators, ⟺ both entities recognize each other, and ↔ so both communicators can share message m or random nonce.

### *4.2 Authentication Simulation Tools*

As it is not enough to formally write mathematical assumptions to run any authentication protocol to model its behavior and communicating entities. Therefore, it is very important to simulate the protocol in a programmable environment. Thus, the programmable environment contains the logical behavior of the system, the communication channel, the process undertaken by the protocol, and the potential attacker malicious activities. In this subsection, we explained different authentication protocol simulation tools with a comparison between them as follows:

1) Scyther

This simulation tool is based on the Security Protocol Description Language Scyther (SPDL), and it is used to verify the authentication protocol security. It provides a library to allow users from applying their function, communicating entities, and simulate attacks either syntactically or graphical user interface. Moreover, it validates the correctness of any cryptographic function and the protocol robustness against the attacks according to the claim mentioned. Lastly, this tool checks the validity of symmetric, hash function, and asymmetric cryptographic protocols.

2) Proverif

It is a software simulation tool that runs security cryptographic protocols and checks their robustness along with security against the claimed attacks. This tool was developed as computer software with a graphical user interface or web simulation page to verify the protocols in syntax. Also, two ways modelling to extract the input are Horn clauses or Pi calculus, and the same output produced in both ways. Lastly, the developer can specify the condition of the attack active/passive, and the explicit modelling of the attacker is not required [72].

3) Tamarin

It is a simulation tool that provides symbolic modelling and syntax analysis of the protocol. By default, Tamarin has a Dolev-Yao adversary network model, and by using this, it can confirm or deny stated properties (lemmas) stems from a scheme. The attack explicit modelling is required in this tool to allow it from updating or deleting the old values. Tamarin uses rephrase rubrics on groups of evidence to shape procedures, i.e., Input/output behavior, long-range keys, short-range keys, etc. A fact F(t1,...,tk) consists of a fact symbol F of degree k and terms t1,...,tk. A set of earmarked evidence symbols is used to indicate freshness info (Fr) and communications to the network (In and Out). The rubrics contain of premises l, activities a and terminations r, and attackers are identified using an expressive language stems from multiset redrafting rules Tamarin prover can be used to demonstrate the security of cryptographic protocols, hash functions, and blockchain schemes [73].

4) Automated Validation of Internet Security Protocols and Applications (AVISPA)

It is used to verify the authentication schemes security by using High-Level Protocol Specification Language (HLPSL). This tool used CAS+ to convert SPAN into HLPSL notations, and to prove the security scheme procedure, which similarly permits us to indicate the procedure security features verification. Moreover, it supports many backends such as the On-the-fly-Model-Checker (OFMC), Constraint-Logic-based-Attack-Searcher (CLAtSe), Satisfiability-based-Model-Checker (SATMC) and Tree-Automata-based-on-Automatic- Approximations for the Analysis of Security Protocols (TA4SP) to check the HSPSL requirements were met. These backends repeat the protocol many times until it proofs that it is safe. Finally, this protocol is invoked in two ways as default commands or as a graphical user interface by using Security Protocol Animator (SPA) [74].

As discussed, in the aforementioned tools [75] considered the best applications for formal authentication security proofs are Tamarin and AVISPA, due to their implementation of ISO 9798 standard and due to the sensitivity of the patient medical data in the authentication scheme. This survey contained statistics of the most used formal methods in proving schemes validity between 2016 and 2020.

## 5 Comparison Amongst Existing WBAN Authentication Schemes

WBAN platform deals with confidential patient data that is vital to be safeguarded versus threats. Meanwhile, the patient data rambles through vulnerable channels, various schemes were crafted to improve user authentication protocols [26]. Several schemes compared in Table 4 and summarized in Figs. 6–8, to illustrate the most popular authentication types, formal proofs, simulation tools, and authentication models.

Fig. 6 showed that the most used authentication type is password, followed by three-factor authentication. Password authentication is used due to its lightweight feature which makes it fit in the WBAN architecture. Moreover, three-factor technique is the second most used type of authentication due to its high security, blockchain technology is favorable over AI because of its lower power consumption compared to AI. Fig. 7 showed that the BAN logic is the most used formal mathematical model by 72%, due to its low time consumption and simplicity of the notations. Fig. 8 presented that AVISPA tool is the most used tool for simulation by 61% due to the simplicity of the commands, its support to the graphical user interface by SPAN, and its compatibility to many operating systems.

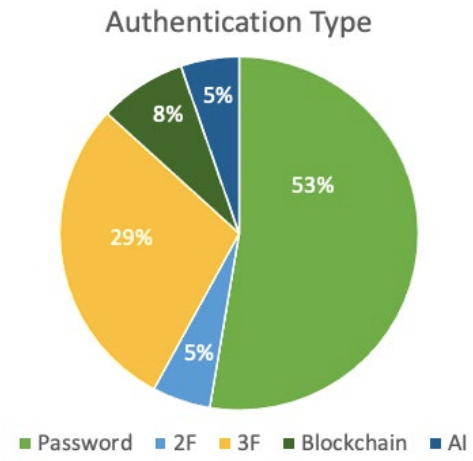


**Figure 6:** Authentication types used in schemes (2016–2020)

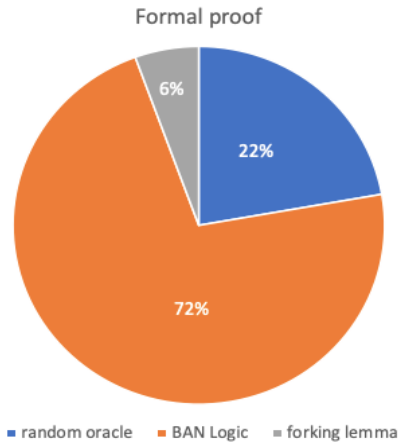


**Figure 7:** Authentication formal proof tools used in schemes (2016–2020)

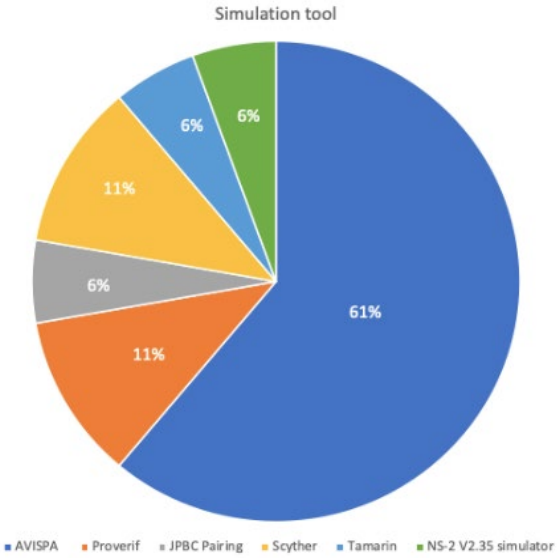


**Figure 8:** Authentication schemes simulation tools (2016–2020)

## 6 Open Issues in WBAN Authentication Schemes

In this section, we will discuss the open issues in the WBAN platform to highlight the areas of concern and build the bridge for the interested research and leaders. From the tables below Table 4 and Table 5, respectively, we discovered the weaknesses of the most authentication schemes that need to be considered first whenever engineers want to design an authentication scheme in WBAN. Thus, Tab. 6 showed WBAN schemes still vulnerable to privileged insider and DoS attacks. Furthermore, it demonstrated the schemes robustness against various security attacks, and it identified the most attack that authentication schemes resist which is the replay attack. Also, the most attack that threaten most of the schemes which is DoS attack. Moreover, the approach in [8] had achieved a higher security in comparison to other schemes regarding attack resistance. From Table 6, we discovered that most of the WBAN authentication schemes have problems in key escrow resilience, forward/backward secrecy, and non-repudiation. The open issues in WBAN authentication schemes can be summarized as follows:

1) **Scalability:** The newly designed authentication schemes need to ensure scalability between the amount of transferred information, the number of added nodes to the architecture, and time slots less than the nodes number. Thus, the system either is overwhelmed with operations and stops functioning or causes operations delay.
2) **Security:** The schemes creators need to pay attention to security aspect due to the amount and type of sensitive information which might cause risk on user life when they got exposes. Due to that, the system needs to provide such as privacy, integrity, confidentiality, authenticity, un-traceability, and non-repudiation. All these security aspects need to be assured through simulation and mathematical proofs to ensure the scheme is secure for sensitive shared user information.
3) **Performance efficiency:** WBANs' are known for their constrained memory and low processing capabilities, which makes them very important to choose a lightweight authentication secure scheme. Thence, the schemes need to have a tradeoff between security and performance efficiency along with their adaptability of platform change, memory size change, or algorithm sophistication.
4) **Enhanced algorithms:** Developing algorithms that are sufficient for WBAN technology is very hard and challenging. There must be proper encouragement and support from the ventures to the developer to increase contribution in this area.
5) **Compatibility:** The heterogeneity of the sensors in WBAN architecture causes a problem in implementing unified security architecture to fit them all. Furthermore, the incompatibility in

security standards among devices or wireless technologies that can cause interference between those standards in nodes, network, and sensors, could lead to signal degradation.

6) **Availability:** From Table 6, it showed that most of the WBAN architectures have vulnerability against Dos attack protection which affects the availability of the resources in the network, and the efficiency of the service.

**Table 4:** Comparison between authentication schemes in the literature

| Scheme | Authentication type | Formal proof | Simulation | Technique | Cons |
|---|---|---|---|---|---|
| [32] | Password | Random oracle | - | Asymmetric on mobile platform | Vulnerable to A1, A6, and A7 |
| [33] | Password | BAN logic | - | ECC on mobile platform | Weakness in F7 along with issue of key control and synchronization |
| [8] | Password | BAN logic | AVISPA | ECC on mobile platform | Weakness in F7 |
| [42] | Password | Random oracle | - | Asymmetric on cloud platform | Weakness in F10 |
| [43] | Password | - | - | Asymmetric on cloud platform | Slow due to the high computation and weak security for the secret random value |
| [44] | Password | - | - | Asymmetric on cloud platform | High computational complexity |
| [27] | Password | BAN logic | AVISPA | ECC on cloud platform | Vulnerable to A7 |
| [1] | Password | - | Proverif | ECC on cloud platform | F2 problem and high computational complexity |
| [11] | Password | BAN logic | AVISPA | Symmetric on mobile platform | Vulnerable to A9 |
| [49] | Password | BAN logic | AVISPA | Symmetric on mobile platform | Vulnerable to A9 |
| [30] | 3F | BAN logic | AVISPA | Symmetric on mobile platform | Vulnerable to A1 |
| [50] | 2F | Random oracle | AVISPA | Symmetric on mobile platform | High computational complexity |
| [10] | Password | BAN logic | AVISPA | Symmetric on mobile platform | Increased storage, and vulnerable to A4 |
| [54] | Password | - | Proverif | Symmetric on cloud platform | High computational complexity |
| [55] | Password | BAN logic | AVISPA | Symmetric on cloud platform | High computational complexity |
| [56] | Password | BAN logic | AVISPA | Symmetric on cloud platform | High computation time and vulnerable to A4 |
| [26] | Password | BAN logic | Scyther | Symmetric on cloud platform | High computational complexity |
| [28] | 3F | BAN logic | AVISPA | Symmetric on cloud platform | Vulnerable to A1, A4, and F6 problem |
| [58] | Password | BAN logic | AVISPA | Symmetric on cloud platform | High computational complexity |
| [60] | Password | - | - | Symmetric/Asymmetric in Blockchain | High cost simulation and implementation |
| [59] | 3F | - | - | Symmetric in Blockchain | High cost simulation and implementation |
| [61] | Password | Random oracle | JPBC | Asymmetric | Might face vulnerability in A7 with high data load |
| [62] | Password | - | NS-2 V2.35 simulator | Symmetric and Asymmetric in Blockchain | High computational complexity |
| [64] | 3F | - | - | Artificial intelligence | High computational complexity in comparison to symmetric cryptography |

| | | | | | |
|---|---|---|---|---|---|
| [65] | 3F | Forking lemme | - | Symmetric on mobile platform in Artificial intelligence | High computational complexity in comparison to symmetric cryptography |
| [52] | Password | BAN Logic | Tamarin and Scyther | Symmetric on mobile platform | F2 issue |
| [34], [35] | 2F | BAN Logic | - | ECC in mobile | Vulnerability to A2, and A8 |
| [36] | 3F | BAN Logic | - | ECC in mobile | Suffered from F2 |
| [37] | 3F | BAN Logic | AVISPA | ECC in mobile | Weak toward F2 and guessing attack, A2 |
| [38] | 3F | Random Oracle | Proverif | ECC in mobile | Suffered from session key exposure, A1, and cannot ensure F2, F5, and F6. |
| [40] | 3F | BAN Logic | AVISPA | ECC in mobile | High computation cost and delays in communication |
| [63] | 3F | - | AVISPA | Blockchain and ECC in cloud | Weak towards A7 and communication delay between the nodes |
| [53] | 3F | BAN Logic | AVISPA | Hash function symmetric in mobile | Suffered from A6, shared secret key guessing, and F2. |

**Table 5:** Security attacks of authentication schemes in the literature

| **Scheme** | **Resist replay attack** | **Resist brute force** | **Resist MITM** | **Resist impersonation attack** | **Resist stolen verifier** | **Resist privileged insider** | **Resist DoS attack** |
|---|---|---|---|---|---|---|---|
| [32] | × | ✓ | × | × | × | × | × |
| [33] | ✓ | × | ✓ | ✓ | ✓ | × | × |
| [8] | ✓ | × | ✓ | ✓ | ✓ | ✓ | ✓ |
| [42] | × | × | × | × | ✓ | × | × |
| [43] | ✓ | - | × | - | ✓ | × | × |
| [27] | ✓ | - | × | ✓ | ✓ | ✓ | × |
| [1] | ✓ | ✓ | - | ✓ | × | × | × |
| [11] | ✓ | ✓ | ✓ | ✓ | ✓ | × | × |
| [49] | ✓ | ✓ | × | ✓ | ✓ | × | × |
| [30] | ✓ | ✓ | × | × | ✓ | ✓ | × |
| [50] | ✓ | × | ✓ | ✓ | ✓ | × | × |
| [10] | × | × | ✓ | ✓ | ✓ | × | × |
| [54] | ✓ | - | - | × | × | × | × |
| [55] | ✓ | ✓ | ✓ | ✓ | × | × | × |
| [56] | × | × | × | ✓ | ✓ | ✓ | ✓ |
| [26] | ✓ | - | ✓ | ✓ | × | × | × |
| [28] | × | × | ✓ | × | ✓ | × | × |
| [60] | ✓ | ✓ | ✓ | × | ✓ | × | ✓ |
| [59] | ✓ | ✓ | ✓ | × | ✓ | × | ✓ |
| [61] | ✓ | ✓ | ✓ | ✓ | × | × | × |
| [65] | ✓ | ✓ | × | × | × | × | × |
| [34,35] | ✓ | ✓ | × | × | × | × | × |
| [36] | ✓ | ✓ | × | × | × | ✓ | - |
| [37] | ✓ | × | × | × | × | ✓ | × |
| [38] | ✓ | × | × | | × | ✓ | - |
| [40] | ✓ | × | ✓ | ✓ | × | ✓ | ✓ |
| [63] | ✓ | ✓ | × | ✓ | ✓ | ✓ | × |
| [53] | ✓ | × | × | × | × | ✓ | - |

**Table 6:** Security and functional features of authentication schemes

| Scheme | Anonymity | Integrity | Un-traceability | key escrow resilience | Forward/backward secrecy | No-repudiation | Mutual authentication |
|---|---|---|---|---|---|---|---|
| [32] | ✓ | × | × | - | ✓ | ✓ | ✓ |
| [33] | ✓ | ✓ | × | - | × | - | ✓ |
| [8] | ✓ | - | ✓ | | × | - | ✓ |
| [42] | × | ✓ | × | - | × | × | - |
| [43] | ✓ | ✓ | - | - | ✓ | ✓ | ✓ |
| [27] | ✓ | ✓ | ✓ | × | ✓ | × | ✓ |
| [1] | × | × | ✓ | × | ✓ | × | ✓ |
| [11] | ✓ | × | × | × | ✓ | × | ✓ |
| [49] | ✓ | × | ✓ | × | × | × | ✓ |
| [30] | ✓ | ✓ | ✓ | × | × | ✓ | ✓ |
| [50] | ✓ | × | ✓ | × | × | × | ✓ |
| [10] | ✓ | ✓ | × | × | ✓ | × | ✓ |
| [54] | ✓ | × | ✓ | × | × | × | ✓ |
| [55] | ✓ | - | ✓ | × | ✓ | × | ✓ |
| [56] | ✓ | × | × | × | ✓ | × | ✓ |
| [26] | ✓ | × | ✓ | × | ✓ | × | ✓ |
| [28] | ✓ | × | × | ✓ | ✓ | × | ✓ |
| [60] | ✓ | ✓ | × | - | - | ✓ | ✓ |
| [59] | ✓ | ✓ | × | - | - | ✓ | ✓ |
| [61] | ✓ | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| [65] | ✓ | × | ✓ | ✓ | × | × | ✓ |
| [34,35] | × | ✓ | ✓ | - | ✓ | ✓ | ✓ |
| [36] | × | ✓ | ✓ | - | ✓ | ✓ | ✓ |
| [37] | × | ✓ | ✓ | - | ✓ | ✓ | ✓ |
| [38] | ✓ | ✓ | × | - | ✓ | ✓ | ✓ |
| [40] | ✓ | ✓ | ✓ | - | ✓ | ✓ | ✓ |
| [63] | ✓ | ✓ | ✓ | - | ✓ | ✓ | ✓ |
| [53] | × | ✓ | × | - | ✓ | - | ✓ |

## 7 Conclusion

WBAN sensors attracted many people in the medical environment recently, due to its huge role in the facilitation of service and accuracy of processing the patient health information. Although WBAN receives patient and doctor's satisfaction regarding its speed and convenience, it is forming a huge risk to users' privacy and info security. Many secure authentication schemes were designed to authenticate the user and protect user data. However, we surveyed the recent authentication schemes and showed their weaknesses in the protection of the user private information. Furthermore, we stated the popular techniques used in them, which are the password and symmetric key encryption due to their efficiency in the WBAN structure. Also, we identified DoS and privileged insider attacks as the most popular attacks in WBAN schemes to be mitigated in any authentication scheme design. Thus, the most used formal method to validate schemes were BAN Logic and AVISPA tool due to their simplicity. Also, new techniques that might attract interested engineers in building authentication schemes are blockchain and artificial intelligence to increase efficiency and improve security. To conclude, our survey pointed out the open challenges to be considered during any scheme proposal.

**Funding Statement:** There is no specific funding to support the research.

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

## References


[1] Z. Xu, C. Xu, W. Liang, J. Xu and H. Chen, "A lightweight mutual authentication and key agreement scheme for medical Internet of Things," *IEEE Access*, vol. 7, pp. 53922–53931, 2019.

[2] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen *et al.,* "Efficient end-to-end authentication protocol for wearable health monitoring systems," *Computers and Electrical Engineering*, vol. 63, pp. 182–195, 2017.

[3] G. K Ragesh and K. Baskaran, "A survey on futuristic health care system: WBANs," *Procedia Engineering*, vol. 30, pp. 889–896, 2012.

[4] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant *et al.,* "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Future Generation Computer Systems*, vol. 78, pp. 659–676, 2018.

[5] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal *et al.,* "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[6] B. A. Alzahrani, A. Irshad, A. Albeshri and K. Alsubhi, "A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks," *Wireless Personal Communications*, vol. 117, pp. 47–69, 2020.

[7] P. Vijayakumar, M. S. Obaidat, M. Azees, S. H. Islam and N. Kumar, "Efficient and secure anonymous authentication with location privacy for IoT–based WBANs," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, pp. 2603–2611, 2020.

[8] K. Sowjanya, M. Dasgupta and S. Ray, "An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems," *International Journal of Inforamtion Security*, vol. 19, no. 1, pp. 129–146, 2020.

[9] S. Deng, Z. Xiang, J. Yin, J. Taheri and A. Y. Zomaya, "Composition–driven IoT service provisioning in distributed edges," *IEEE Access*, vol. 6, pp. 54258–54269, 2018.

[10] M. Kompara, S. K. H. Islam and M. Hölbl, "A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs," *Computer Networks*, vol. 148, pp. 196–213, 2019.

[11] X. Li, M. H. Ibrahim, S. Kumari and R. Kumar, "Secure and efficient anonymous authentication scheme for three-tier mobile healthcare systems with wearable sensors," *Telecommunication systems: Modeling, Analysis, Design and Management*, vol. 67, no. 2, pp. 323–348, 2018.

[12] P. K. Sahoo, "Efficient security mechanisms for mhealth applications using wireless body sensor networks," *Sensors*, vol. 12, no. 9, pp. 1–28, 2012.

[13] F. Sulak, O. Kocak, E. Saygi, M. Ogunc and B. Bozdemir, "A second pre-image attack and a collision attack to cryptographic hash function LUX," *Communications Faculty of Sciences University of Ankara Series A1 Mathematics and Statistics*, vol. 66, no. 1, pp. 254–266, 2017.

[14] M. Hussain, A. Mehmood, S. Khan, M. A. Khan and Z. Iqbal, "Authentication techniques and methodologies used in wireless body area networks," *Journal of System Architecture*, vol. 101, pp. 1–15, 2019.

[15] Y. Yao, X. Chang, J. Mišić and V. B. Mišić, "Lightweight batch AKA scheme for user-centric ultra-dense networks," *IEEE Transcations on Cognitive Communications*, vol. 6, no. 2, pp. 597–606, 2020.

[16] B. S. Abdullah and M. Almuhaideb, "Authentication in ubiquitous networking," *International Journal of Information Security and Privacy*, vol. 9, no. 3, pp. 1–27, 2015.

[17] W. Meng, D. S. Wong, S. Furnell and J. Zhou, "Surveying the development of biometric user authentication on mobile phones," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 3, pp. 1268–1293, 2015.

[18] A. Sundararajan, A. I. Sarwat and A. Pons, "A survey on modality characteristics, performance evaluation metrics, and security for traditional and wearable biometric systems," *ACM Computing Surveys*, vol. 52, no. 2, pp. 1–39, 2019.

[19] M. Masdari and S. Ahmadzadeh, "Comprehensive analysis of the authentication methods in wireless body area networks," *Security and Communication Networks*, vol. 9, no. 17, pp. 4777–4803, 2016.

[20] M. Kompara and M. Hölbl, "Survey on security in intra-body area network communication," *Ad Hoc Networks*,

vol. 70, pp. 1–42, 2017.

[21] B. Narwal and A. K. Mohapatra, "A review on authentication protocols in wireless body area networks (WBAN)," in *3rd Int. Conf. on Contemporary Computing and Informatics (IC3I)*, pp. 227–232, 2018.

[22] M. Dhanvijay and S. Patil, "Internet of Things: A survey of enabling technologies in healthcare and its applications," *Computer Networks*, vol. 153, pp. 113–131, 2019.

[23] G. Bleumer, "Untraceability," in *Encyclopedia of Cryptography and Security*, pp. 1351–1352, 2011.

[24] K. Renuka, S. Kumari and X. Li, "Design of a secure three-factor authentication scheme for smart healthcare," *Journal of Medical Systems*, vol. 43, no. 113, pp. 1–12, 2019.

[25] D. Fang, Y. Qian and R. Q. Hu, "A flexible and efficient authentication and secure data transmission scheme for IoT applications," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3474–3484, 2020.

[26] A. Arfaoui, A. Kribeche and S. M. Senouci, "Context-aware anonymous authentication protocols in the Internet of Things dedicated to e–health applications," *Computer Networks*, vol. 159, pp. 23–36, 2019.

[27] B. A. Alzahrani, S. A. Chaudhry, A. Barnawi, A. Al–Barakati and M. H. Alsharif, "A privacy preserving authentication scheme for roaming in IoT–based wireless mobile networks," *Symmetry*, vol. 12, no. 2, pp. 1–18, 2020.

[28] A. M. Koya and P. P. Deepthi, "Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network," *Computer Networks*, vol. 140, pp. 138–151, 2018.

[29] Y. Y. Deng, C. L. Chen, T. W. Jiunn, Y. W. Tang and J. H. Chen, "Internet of Things (IoT) based design of a secure and lightweight body area network (BAN) healthcare system," *Sensors*, vol. 17, no. 12, pp. 1–18, 2017.

[30] X. Liu, R. Zhang and M. Zhao, "A robust authentication scheme with dynamic password for wireless body area networks," *Computer Networks*, vol. 161, pp. 220–234, 2019.

[31] M. M. Alam, E. B. Hamida, "Surveying wearable human assistive technology for life and safety critical applications: Standards, challenges and opportunities," *Sensors*, vol. 14, no. 5, pp. 9153–9209, 2014.

[32] J. Liu, L. Zhang and R. Sun, "1-RAAP: An efficient 1-round anonymous authentication protocol for wireless body area networks," *Sensors*, vol. 16, no. 5, pp. 1–16, 2016.

[33] X. Li, J. Peng, S. Kumari, F. Wu, M. Karuppiah *et al.,* "An enhanced 1-round authentication protocol for wireless body area networks with user anonymity," *Computer and Electrical Engineering*, vol. 61, pp. 238–249, 2017.

[34] I. P. Chang, L. T. Fu, T. H. Lin and C. M. Liu, "Enhanced two-factor authentication and key agreement using dynamic identities in wireless sensor networks," *Sensors*, vol. 15, no. 12, pp. 29841–29854, 2015.

[35] Y. Park and Y. H. Park, "Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks," *Sensors*, vol. 16, no. 12, pp. 1–17, 2016.

[36] C. Wang, G. Xu and J. Sun, "An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks," *Sensors*, vol. 17, no. 12, pp. 1–20, 2017.

[37] S. Challa, A. K. Das, V. Odelu, N. Kumar and A. V. Vasilakos, "An efficient ECC–based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Computers and Electrical Engineering*, vol. 69, pp. 534–554, 2018.

[38] J. Mo and H. Chen, "A lightweight secure user authentication and key agreement protocol for wireless sensor networks," *Security and Communication Networks*, vol. 21, pp. 1–17, 2019.

[39] Y. Lu, G. Xu, L. Li and Y. Yang, "Anonymous three-factor authenticated key agreement for wireless sensor networks," *Wireless Networks*, vol. 25, no. 4, pp. 1461–1475, 2019.

[40] Z. Ali, A. Ghani, I. Khan, S. A. Chaudhry, S. K. H. Islam *et al.,* "A robust authentication and access control protocol for securing wireless healthcare sensor networks," *Journal of Information Security and Applications*, vol. 52, pp. 1–14, 2020.

[41] C. H. Liu and Y. F. Chung, "Secure user authentication scheme for wireless healthcare sensor networks," *Computer and Electrical Engineering*, vol. 59, pp. 250–261, 2017.

[42] S. Li, J. Cui, H. Zhong, Y. Zhang and Q. He, "LEPA: A lightweight and efficient public auditing scheme for cloud–assisted wireless body sensor networks," *Security and Communication Networks*, vol. 43, pp. 1–16, 2017.

[43] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan *et al.,* "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *Journal of Network and Computer Applications*, vol. 106, pp. 117–123, 2018.

[44] S. Deng, L. Huang, Y. Li, H. Zhou, Z. Wu *et al.,* "Toward risk reduction for mobile service composition," *IEEE Transactions on Cybernetics*, vol. 46, no. 8, pp. 1807–1816, 2016.

[45] Y. Lu, G. Xu, L. Li and Y. Yang, "Robust privacy-preserving mutual authenticated key agreement scheme in roaming service for global mobility networks," *IEEE Systems Journal*, vol. 13, no. 2, pp. 1454–1465, 2019.

[46] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta *et al.,* "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Computer Networks*, vol. 129, pp. 429–443, 2017.

[47] A. Braeken, "Highly efficient symmetric key based authentication and key agreement protocol using keccak," *Sensors*, vol. 20, no. 8, pp. 1–15, 2020.

[48] M. Konan and W. Wang, "A secure mutual batch authentication scheme for patient data privacy preserving in WBAN," *Sensors*, vol. 19, no. 7, pp. 1–16, 2019.

[49] R. Amin, S. K. H. Islam, G. P. Biswas, M. K. Khan and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Generations Computer Systems*, vol. 80, pp. 483–495, 2018.

[50] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K. R. Choo *et al.,* "Design of secure and lightweight authentication protocol for wearable devices environment," *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 4, pp. 1310–1322, 2018.

[51] A. Gupta, M. Tripathi and A. Sharma, "A provably secure and efficient anonymous mutual authentication and key agreement protocol for wearable devices in WBAN," *Computer Communications*, vol. 160, pp. 311–325, 2020.

[52] B. Lu, R. Cao, Y. Lu and X. Luo, "Design and formal analysis of an authentication protocol, eWMDP on wearable devices," *IEEE Access*, vol. 7, pp. 97771–97783, 2019.

[53] S. Yu and Y. Park, "SLUA-WSN: Secure and lightweight three-factor-based user authentication protocol for wireless sensor networks," *Sensors*, vol. 20, no. 15, pp. 1–26, 2020.

[54] F. Wu, X. Li, L. Xu, S. Kumari, M. Karuppiah *et al.,* "A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server," *Computers and Electrical Engineering*, vol. 63, pp. 168–181, 2017.

[55] A. Gupta, M. Tripathi, T. J. Shaikh and A. Sharma, "A lightweight anonymous user authentication and key establishment scheme for wearable devices," *Computer Networks*, vol. 149, pp. 29–42, 2019.

[56] M. Polai, S. Mohanty and S. S. Sahoo, "A lightweight mutual authentication protocol for wireless body area network," in *6th Int. Conf. on Signal Processing and Integrated Networks*, pp. 760–765, 2019.

[57] C. Camara, H. Martín, P. P. Lopez and M. Naser, "Design and analysis of a true random number generator based on GSR signals for body sensor networks," *Sensors*, vol. 9, pp. 1–15, 2019.

[58] B. Narwal and A. K. Mohapatra, "SEEMAKA: Secured energy-efficient mutual authentication and key agreement scheme for wireless body area networks," *Wireless Personal Communications*, vol. 113, pp. 1985–2008, 2020.

[59] A. H. Mohsin, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, A. S. Albahri *et al.,* "Based medical systems for patient's authentication: Towards a new verification secure framework using CIA standard," *Journal of Medical Systems*, vol. 43, no. 7, pp. 1–34, 2019.

[60] H. Zhao, P. Bai, Y. Peng and R. Xu, "Efficient key management scheme for health blockchain," *CAAI Transcations on Intelligence Technology*, vol. 3, pp. 114–118, 2018.

[61] G. Mwitende, I. Ali, N. Eltayieb, B. Wang and F. Li, "Authenticated key agreement for blockchain–based WBAN," *Telecommunication Systems:Modelling, Analysis, Design and Management*, vol. 74, no. 3, pp. 347–365, 2020.

[62] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K. R. Choo *et al.,* "Decentralized authentication of distributed patients in hospital networks using blockchain," *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 8, pp. 2146–2156, 2020.

[63] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. P. C. Rodrigues *et al.,* "BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment," *IEEE Access*, vol. 8, pp. 95956–95977, 2020.

[64] M. N. Malik, M. A. Azam, M. Ehatisham–Ul–Haq, W. Ejaz and A. Khalid, "ADLAuth: Passive authentication based on activity of daily living using heterogeneous sensing in smart cities," *Sensors*, vol.

19, no. 11, pp. 1–23, 2019.

[65] H. Tan and I. Chung, "Secure authentication and group key distribution scheme for WBANs based on smartphone ECG sensor," *IEEE Access*, vol. 7, pp. 151459–151474, 2019.

[66] M. Hammad, Y. Liu and K. Wang, "Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint," *IEEE Access*, vol. 7, pp. 26527–26542, 2019.

[67] M. Henzi and P. Hanacek, "A Security formal verification method for protocols using cryptographic contactless smart cards," *Radioengineering*, vol. 25, no. 1, pp. 132–139, 2015.

[68] S. Szymoniak, O. S. Lamch and M. Kurkowski, "SAT–based verification of NSPK protocol including delays in the network," in *IEEE 14th Int. Scientific Conf. on Informatics*, pp. 388–393, 2017.

[69] F. J. T. Fabrega, J. C. Herzog and J. D. Guttman, "Strand spaces: Why is a security protocol correct?," in *Proc. 1998 IEEE Sym. on Security and Privacy*, pp. 160–171, 1998.

[70] G. Lowe, "Casper: A compiler for the analysis of security protocols," in *Proc. 10th Computer Security Foundations Workshop*, vol. 6, no. 1, pp. 18–30, 1998.

[71] M. Burrows, M. Abadi and R. Needham, "A logic of authentication," in *Proc. of the Royal Society A Mathematical*, vol. 23, no. 5, pp. 1–13, 1989.

[72] R. Patel, B. Borisaniya, A. Patel, D. Patel, M. Rajarajan *et al.,* "Comparative Analysis of formal model checking tools for security protocol verification," in *Int. Conf. on Network Security and Applications*, pp. 152–163, 2010.

[73] A. J. M. Milne, A. Beckmann and P. Kumar, "Cyber-physical trust systems driven by blockchain," *IEEE Access*, vol. 8, pp. 66423–66437, 2020.

[74] R. Patil and S. Devane, "Formal verification of secure evidence collection protocol using BAN logic and AVISPA," *Procedia Computer Science*, vol. 167, pp. 1334–1344, 2020.

[75] D. Sas and P. Avgeriou, "Quality attribute trade-offs in the embedded systems industry: An exploratory case study," *Software Quality Journal*, vol. 28, no. 7, pp. 505–534, 2020.