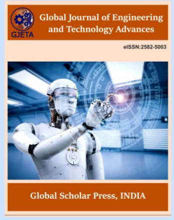
Global Journal of Engineering and Technology Advances

eISSN: 2582-5003

Cross Ref DOI: 10.30574/gjeta

Journal homepage: https://gjeta.com/



(REVIEW ARTICLE)

Check for updates

Wireless body area networks: A critical review of the state-of-the-art security schemes

Joshua Auko* and Silvance Abeka

Jaramogi Oginga, Odinga University of Science & Technology, Bondo, Kenya.

Global Journal of Engineering and Technology Advances, 2022, 12(01), 131–146

Publication history: Received on 16 June 2022; revised on 24 July 2022; accepted on 26 July 2022

Article DOI: https://doi.org/10.30574/gjeta.2022.12.1.0123

Abstract

The continued advancement of information communication technologies (ICT) has led to the adoption of internet of things in the healthcare sector. One of such application domain of ICT is the wireless body area network (WBAN), which enables remote monitoring of vital biomedical parameters on the patient or the elderly. Upon collection of these parameters, they are forwarded to the remote hospital servers where analysis and appropriate actions are taken. Obviously, the data exchanged in these networks is sensitive and private and hence can have devastating effects on the patient if leaked to the unintended parties. Consequently, many security solutions have been developed in literature. The goal of this paper is to carry out an extensive review of these security schemes in an effort to pin point their strengths and weaknesses. Based on the findings, it is evident that many of these security solutions try to attain a number of security and privacy protection. However, it is noted that these schemes still lack many of the required security goals such as anonymity, untraeability, forward key secrecy as well as resistance to many of the conventional attacks. Therefore, some recommendations for the attainment of perfect privacy and security are given towards the end of this paper.

Keywords: Security; Privacy; WBAN; Attacks; LoT; Sensors

1. Introduction

The ever increasing utilization of mobile devices, wireless sensor networks (WSNs), internet of things (IoT) and sensors has seen the healthcare sector adopting IoT devices to collect data, monitor patients and communicate with patients over wireless body area networks (WBANs) [1]. In essence, WBAN is a collection of smart medical sensors that are implanted in the patient body or placed around the patient. As shown in Figure 1, the main components of a typical WBAN include the medical staff, sensors and gateway nodes.

These sensors offer real-time monitoring and healthcare support to the patients. They may also be utilized to monitor the elderly people who need some permanent care devoid of being hospitalized. In such a scenario, the monitoring is done at home using sensors that then send the collected data to the hospital using some wireless transmission channels. In case of emergencies such as heart attack, the medical staff can initiate some immediate actions without further delays. In terms of computational capabilities, gateway nodes are more powerful than sensors and they act secure interfaces between the medical staff and the sensors.

As explained in [2], WBANs collect patient health information and forward the same to medical staff so as to monitor and control the patient's health remotely. As such, it makes it possible for patients to be diagnosed using some remote clinical nano-sensors [3]. The collected data may include body temperature, ECG, sugar level and blood pressure among

*Corresponding author: Joshua Auko

Jaramogi Oginga Odinga University of Science & Technology, Bondo, Kenya.

others [4]. WBAN presents an emerging domain that employs ubiquitous technologies such as smart sensors [5], cloud computing, embedded systems and wireless network technologies to boost the electronic-health care system [6]. As explained in [7]-[12], WBAN based systems represent one of the most critical technologies in the biomedical field. Basically, important patient and elderly health parameters and movements are perceived and forwarded to the healthcare service provider for analysis and appropriate action [2], [13]. As a result of the effectiveness and demand for WBAN, a new International communication standard IEEE 802.15.6 [14] has been developed.

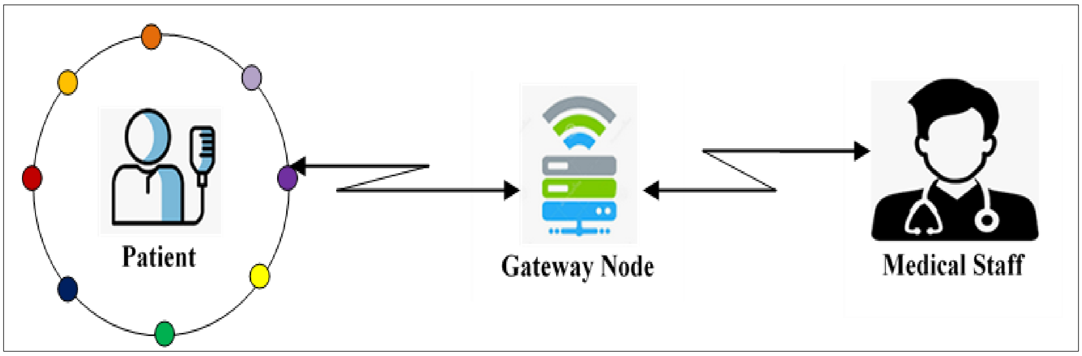


Figure 1 WBAN Communication Architecture

In spite of the numerous merits that this technology has come with, the open nature of the wireless communication channels coupled with cloud computing introduce a number of security threats and vulnerabilities [15]. As such, the privacy and integrity of the exchanged data may be compromised [16], [17]. For instance, an attacker can eavesdrop, intercept, modify, or replay the exchanged messages. In addition, the data stored in the utilized mobile devices and sensors can be retrieved. As explained in [1], attacks such as offline password guessing, privileged insider, user tracking, session key disclosure, forgery and impersonations are possible in WBANs. Since the exchanged data directly impacts on patient health and life, its confidentiality should be upheld [18]. The resource-constrained nature [19] of the devices involved in WBAN is another major issue. Although cloud computing can offload some of the processing of these devices, it introduces numerous threats and vulnerabilities that can be exploited by adversaries [20]. One way of dealing with these challenges is through data encryption [21]. This is particularly important for inter WBAN which uses internet links to connect the patient to the medical servers [22], [23].

In light of the above challenges, there is need for the development of lightweight and efficient security solutions for these networks to curb the numerous active and passive attacks [1], [3], [24], [25], [26], [27]. One of the most effective mechanisms for boosting security in wireless networks is through strong mutual authentication [28], [29]. This will go a long way in insuring that only legitimate healthcare personnel has access to the highly sensitive and confidential patient data [52]. The main contributions of this article are as follows:

- An extensive review of the current techniques for achieving security and privacy in wireless body area networks is provided.
- The challenges and strengths of the security solutions designed for wireless body area networks are identified.
- Based on the shortcomings identified in literature, recommendations for attaining perfect security and privacy are provided

The rest of this paper is organized as follows: Section 2 discusses related work while Section 3 presents the obtained results. On the other hand, Section 4 offers the recommendations emanating from this study while Section 5 concludes the paper.

2. Related work

Many security solutions have been put forward by researchers in the industry as well as academia in an effort to protect WBAN communication process. However, majority of these techniques still have security holes, while others have high complexities in terms of storage, computation and communication. For example, the authentication protocols in [30] are lightweight and incur less communication overheads but are never evaluated from the privacy and security perspectives. On the other hand, the two-factor authentication scheme in [31] cannot uphold user anonymity [19]. These issues can be addressed by the secure and efficient approaches in [32] and [33]. Using offline signatures, a remote authentication scheme is developed in [34]. However, this scheme is not suitable for high mobility and multiple server environments. Although the protocol in [35] potentially addresses this issue, it is susceptible to denial of service attack [36]. Therefore, the smart card and proximity-based authentication schemes are introduced in [37] and [38] respectively to curb this attack. To further enhance security, multi-hop channel and AES based authentication protocols are presented in [39] and [40] respectively. On the other hand, a risk-based adaptive authentication framework is developed in [41]. However, validation [42] of the proposed framework is missing.

Using the physical unclonable functions (PUFs), lightweight protocols are developed in [43]-[47]. Unfortunately, the security analysis of the scheme in [46] is missing. In addition, PUF-based schemes have stability challenges [48]. Further, the protocol in [44] is vulnerable to denial of service attacks and cannot uphold perfect forward secrecy [49] nor can it ensure session key agreement. To prevent this attack, an energy-efficient authentication and key agreement protocol is developed in [50]. Although the technique incurs less communication, memory and computation overheads [51], it cannot withstand many security attacks [52]. To address this challenge, many schemes have been put forward in [53]-[58]. However, most of these schemes are not lightweight [59] and cannot offer forward secrecy, untraceability as well as resilience against key compromise and impersonation attacks [1], [60]. For instance, the scheme [57] incurs extremely high communication costs. To reduce the computation and communication overheads, a secure anonymous user authentication scheme is developed in [61]. Similarly, and efficient and privacy preserving smart card based authentication protocol is presented in [62]. However, this approach is vulnerable to offline password guessing, replay, smart card loss and forgery attacks. Similarly, the scheme in [63] is susceptible to key compromise, replay, privacy leakages and impersonation attacks [6].

To minimize computation and storage complexities, an ECG-based authentication scheme is introduced in [64]. However, this protocol lacks protection against Sybil, sink and wormhole attacks. To prevent these attacks, an identity-based anonymous authentication is developed in [19]. Although this approach offers mutual authentication, key agreement and user anonymity, identity-based schemes have key escrow problems [65]. The protocol in [66] can help address this issue, but it incurs high execution time at the server side. The schemes in [67] and [68] are fairly lightweight and hence can address the performance issues in [66]. Unfortunately, the approach in [68] lacks security evaluation against adversarial attacks [52]. Based on user's password, an authentication technique is developed in [69]. Unfortunately, low entropy passwords are vulnerable to brute force and dictionary attacks. Although the PUF based scheme in [70] is resilient energy-efficient, it is devoid of discussion on security features. On the other hand, a number of vulnerabilities have been discovered in [71] by the author in [72]. As such, a smart card-based secure authentication scheme has been introduced in [72] to eliminate these vulnerabilities. Unfortunately, this scheme lacks analysis is of the communication and computation costs. In addition, it lacks formal verification [73] of the offered security features. To resolve sensor impersonation and server impersonation attacks in [74], energy efficient authentication schemes are developed in [75] and [76]. However, the protocol in [76] has some security loopholes [77]. The proximity-based authentication mechanism in [78] can potentially prevent some of these security setbacks.

Using elliptic curve cryptography (ECC) and bilinear pairing operations, an authentication protocol is developed in [79]. However, these pairing operations are computationally extensive [80] for the WBAN devices. To prevent denial of service, man-in-the-middle, session hijacking and impersonation attacks, a security protocol is introduced in [81]. However, this scheme has not been analytically analyzed and is limited to ECG features. On the other hand, high computation and client impersonation attacks have been identified in [82]. Therefore, an improved protocol has been presented in [83], which is shown to offer anonymity, mutual authentication and forward secrecy. In addition, it is robust against tampering, replay and impersonation attacks. To securely pair wearable devices, a proximity-based authentication technique is presented in [84], while three-factor mutual authentication scheme is presented in [85]. Although the protocol in [85] reduces communication and computation costs, it does not consider security features such as untraceability, unlinkability and non-repudiation. To improve on this, the schemes in [86] and [87] can be utilized. However, the protocol in [86] is vulnerable to de-synchronization [88] attacks. Therefore, enhanced two-factor authentication approaches are introduced in [89]-[91] based on smart cards and passwords.

Based on ECC and certificateless cryptography, a conditional privacy-preserving authentication protocol is developed in [92]. Although this technique prevents forgery attack and incurs less computation and communication overheads, batch verification is not included. To reduce these message exchanges, an identity-based authentication and key agreement protocol is developed in [93]. Unfortunately, this scheme cannot offer unlinkability and user anonymity [94]. Similarly, the technique in [95] lacks user anonymity and is vulnerable to smart card loss, offline password guessing and credentials leakage attacks. Consequently, an improved a biometric based distributed key management protocol is developed in [96]. This approach is shown to provide confidentiality, security, authentication and resilience against different attacks and threats. Although the retina-based authentication scheme in [97] is storage efficient, it lacks evaluation against security attacks. Similarly, anonymity preserving authentication scheme in [98] is efficient and offers conditional privacy but lacks discussion on vital security attacks such as man-in-the-middle, impersonation, modification and eavesdropping. To address these issues, novel identity-based authentication protocols are developed in [99] and [100]. However, the deployed bilinear pairing operations render the scheme in [99] computationally intensive [101]. In addition, it is vulnerable to impersonation attack and does not offer mutual authentication [102]. On the other hand, the protocol in [100] lacks user anonymity [19]. Similarly, the two-factor authentication protocol in [103] is vulnerable to offline guessing attacks [1], while the protocol in [104] is susceptible to node compromise attack. To address some of these attacks, a privacy preserving certificateless scheme is introduced in [105]. Unfortunately, this scheme incurs high computation costs [106] and its resilience against security attacks is not provided. On the other hand, a pairing based authentication protocol is presented in [107]. However, this protocol cannot withstand impersonation attacks [108].

To mutually construct the session key, a lightweight authentication technique is presented in [109]. Unfortunately, this approach is vulnerable to user tracking and offline password guessing attacks. To solve these issues, a multi-hop and lightweight authentication schemes are presented in [110] and [111] respectively. Although the scheme in [111] offers untraceability, it presents some challenges in the management of a set of pseudo-IDs [112] and secret keys. Similarly, the protocols in [113] and [114] are not evaluated against security attacks. On the other hand, the approach in [115] offers security evaluation, where it is demonstrated to be robust against controller and sensor node spoofing attacks. To address the issues in [111], a novel user authentication protocol developed in [116] can be utilized. However, this scheme is susceptible to replay and spoofing attacks [117] and hence an improved scheme was put forward in [117]. Unfortunately, this scheme cannot withstand user forgery and offline password guessing attacks [118]. Similarly, the ECC based protocol in [119] cannot achieve user unlinkability [47]. Although the group device pairing protocol in [120] can potentially address this issue, it can be compromised by malicious group members [121]. This challenge is prevented by the protocol in [122], which is robust against eavesdropping, man-in-the-middle, jamming, impersonation, modification and replay attacks. Unfortunately, this protocol is never evaluated against non-repudiation. Similarly, the scheme in [123] is vulnerable to user tracking attacks [124]. Although the scheme in [125] provides conditional privacy and protection against forgery attacks, it remains susceptible to denial of service and impersonation attacks. On the other hand, the two-factor protocol in [126] offers untraceability but cannot resist session- specific temporary information threats and de-synchronization attacks [127]. It may also permit unauthorized logins. These challenges can be solved by the three factor authentication protocol developed in [128], based on passwords, smart cards and biometrics. Similarly, the protocol in [129] is efficient and offers strong forward secrecy as well as resilience against numerous attacks. As such, it can address the security issues in [126].

Chaotic cryptography has also been crucial in securing WBANs. For instance, a chaotic map based scheme is presented in [130]. This scheme is demonstrated to offer protection against information disclosure. On the other hand, a lightweight authentication protocol is presented in [131], which is shown to be energy-efficient, fast and requires less memory space during authentication procedures. As such, it can help address the inefficiency in the homomorphic encryption method developed in [132]. Although the one-to-many group authentication scheme in [133] helps establish a group key between the sensor and the PDA, it lacks resilience against key escrow [134] and non-repudiation. Similarly, the certificateless encryption and signature scheme in [135] offers scalable and anonymous remote authentication. It is also robust against chosen-plaintext attack. Unfortunately, its resilience against other attacks is not analyzed. On the other hand, authors in [136] have deployed asymmetric key generation approach for efficient and secure data transmission. However, the asymmetric key technique calls for pairs of public and private keys, which renders this algorithm slower and highly complex [137]. Similarly, in-field user authentication scheme in [138] lacks security analysis. As such, the three-phase authentication scheme in [139] and lightweight two-factor authentication scheme in [140] have been developed to offer and security analysis. In particular, the protocol in [140] is shown to be robust against session key disclosure, tracking and offline guessing attacks. However, it fails to offer forward key secrecy [1]. On the other hand an RSS based authentication scheme is presented in [141] while a certificate-less authentication protocol is developed in [142]. However, the scheme in [142] is vulnerable to impersonation attack [143] and cannot offer user anonymity [119].

To offer scalability at low computation overheads, a password-based user access control scheme is presented in [144]. Unfortunately, this approach fails to provide anonymity and has some mistakes in its formal analysis. To solve this problem, a novel pairing scheme is presented in [145]. Similarly, the protocols in [146] and [147] can address the security issues in [144]. Based on the blockchain, an authentication scheme is presented in [148], which is shown to offer privacy protection and secure storage of medical records. However, its analysis against various attacks is missing. In addition, the blockchains have high storage and computation costs [149]. These performance issues can be addressed by the protocols in [150] and [151]. Similarly, the anonymous three-factor authentication scheme in [152] and password-based authentication protocol in [153] are lightweight and can remedy the issues in [148]. Unfortunately, the protocol in [153] deploys a single shared key between gateway and sensors and hence is insecure. This issue is resolved by the remote authentication and key establishment scheme in [154] and physical layer based device pairing protocol in [155]. Although the certificateless remote authentication scheme in [156] offers anonymity and resilience against key escrow problems, it cannot withstand replay and man-in-the-middle attacks. These security problems are effectively addressed by the protocol in [157]. However, the blockchains in this scheme makes it unnecessarily extensive [158]. To solve this problem, an energy efficient and secure protocol in [159] can be utilized.

To protect against main-in-the-middle and impersonation attacks, password-based authentication technique is presented in [160], while a stable and effective fuzzy logic based authentication protocol is developed in [161]. Although the scheme in [162] is privacy-preserving, it incurs high processing cost at the hub node. On the other hand, pair-wise and group keys [163] based protocols in [164] are never validated and access to data in storage is not protected. Based on fuzzy vault, an authentication scheme is presented in [165], which is shown to offer resilience against data alteration, brute-force and impersonation. However, this protocol has high computation and communication overheads. This problem can be resolved by the anonymous authentication scheme in [166], which is demonstrated to offer untraceability at low complexities.

3. Results and Discussion

Based on the review in the previous section, numerous shortcomings have been discovered in virtually all the current security techniques. Table 1 presents a summary of the challenges experienced with the current WBAN security solutions.

Table 1 Summary of Challenges in Current Schemes

Scheme	Challenges
Liu et al. [30]	Privacy & security evaluation missing
Nikooghadam & Amintoosi [31]	Cannot uphold user anonymity
Saeed et al. [34]	Not suitable for high mobility and multiple server environments
Islam & Biswas [35]	Susceptible to denial of service attack
Mattias & Abie [42]	Validation is missing
Tan et al. [46]	Security analysis is missing
Zhao et al. [44]	Vulnerable to denial of service attacks, cannot uphold perfect forward secrecy, cannot ensure session key agreement
Wei et al. [57]	incurs extremely high communication costs
Chia-Hui & Chung [62]	Vulnerable to offline password guessing, replay, smart card loss, forgery attacks
Xu et al. [63]	Susceptible to key compromise, replay, privacy leakages, impersonation attacks
Zhang et al. [64]	Lacks protection against Sybil, sink and wormhole attacks
Kumar & Chand [19]	Has key escrow problems
Renuka et al. [66]	Incurs high execution time at the server side
Chang et al. [68]	Lacks security evaluation against adversarial attacks
Wu et al. [69]	Low entropy passwords are vulnerable to brute force and dictionary attacks
Zhang et al. [70]	Is devoid of discussion on security features
Tritilanunt [72]	Lacks analysis of the communication and computation costs
Xiong [79]	Computationally extensive
Wu et al. [82]	High computation , client impersonation attacks
Sahoo et al. [85]	Does not consider untraceability, unlinkability and non-repudiation
Ibrahim et al. [86]	Vulnerable to de-synchronization
Xie et al. [92]	Batch verification is not included

Cao et al. [93]	Cannot offer unlinkability and user anonymity
Wang [95]	Lacks user anonymity and is vulnerable to smart card loss, offline password guessing & credentials leakage attacks
Ullah et al. [97]	Lacks evaluation against security attacks
Jegadeesan et al. [98]	Devoid of discussion on vital security attacks such as man-in-the-middle, impersonation, modification and eavesdropping
Tsai & Lo [99]	Is computationally intensive, vulnerable to impersonation attack and does not offer mutual authentication
Kumar & Saxena [100]	Lacks user anonymity
Amin et al. [103]	Vulnerable to offline guessing attacks
Abina et al. [104]	Susceptible to node compromise attack
Mwitende et al. [105]	Incurs high computation costs, its resilience against security attacks is not provided
Wang & Zhang [107]	Cannot withstand impersonation attacks
Kumari & Om [109]	Vulnerable to user tracking and offline password guessing attacks
Yang et al. [111]	Has challenges in the management of a set of pseudo-IDs
Jiang et al. [116]	Susceptible to replay and spoofing attacks
Wen et al. [117]	Cannot withstand user forgery and offline password guessing attacks
Zhao [119]	Cannot achieve user unlinkability
Li et al. [120]	Can be compromised by malicious group members
Bhawna et al. [122]	Is never evaluated against non-repudiation
Farash et al. [123]	Vulnerable to user tracking attacks
Tan & Chung [125]	Susceptible to denial of service and impersonation attacks
Jiang et al. [126]	Cannot resist session- specific temporary information threats and de-synchronization attacks
Shen et al. [133]	Lacks resilience against key escrow and non-repudiation
Anwar et al. [136]	Is slower and highly complex
Debayan et al. [138]	Lacks security analysis
Wu et al. [140]	Fails to offer forward key secrecy
Liu et al. [142]	Vulnerable to impersonation attack and cannot offer user anonymity
Santanu et al. [144]	It fails to provide anonymity and has some mistakes in its formal analysis
Cheng et al. [148]	Its analysis against various attacks is missing, has high storage and computation costs
Muhammad & Kumari [153]	Deploys a single shared key between gateway and sensors and hence is insecure
Omala et al. [156]	Cannot withstand replay and man-in-the-middle attacks
Bhattacharya et al. [157]	Computationally extensive
Xu et al. [162]	It incurs high processing cost at the hub node
Drira et al. [164]	Data in storage is not protected
Hodgkiss & Djahel [165]	Has high computation and communication overheads

As shown in Table 1 above, these challenges can broadly be classified as being against privacy, security, communication costs, computation overheads, storage complexities, susceptibility to attacks as well as key escrow issues. As such, the recommendations in Section 4 below are thought to be ideal for enhanced WBAN security.

3.1. Recommendations

The messages exchanged in WBANs are sensitive, private and mission-critical. As such, any leakages, corruption or misuse can potentially lead to job losses, humiliation, incorrect medication, mental disturbance, unhealthy relationship or even improper care. As such, security and privacy are essential ingredients of WBAN systems as shown in Figure 2.

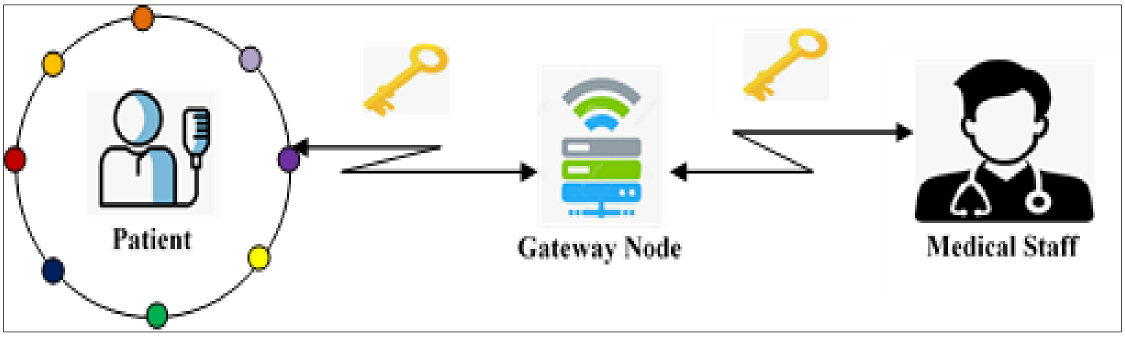


Figure 2 Proposed Communication Architecture

As shown in Figure 2, all the transmitted data need to be enciphered using strong encryption algorithms. Although numerous data security [167] schemes have been developed over the recent past, they have been shown to have a number of security and privacy issues. For instance, techniques such as digital signatures, Advanced Encryption Standards (AES), public key infrastructure (PKI) and elliptic curve cryptography point multiplications may be inefficient for the resource limited WBAN devices. Particularly, the management of digital certificates in PKI-based authentication protocols is inefficient [168]. In addition, high computational primitives such as ECC and identity-based bilinear operations [169]-[174] have led to the deployment of lightweight crypto-primitives such as hash functions and XOR functions for the design of more efficient security protocols. Besides performance, communication sessions unlinkability, mutual authentication and anonymity [175] must be upheld in WBAN security frameworks. In this regard, an ideal WBAN security solution must fulfill the following requirements:

- Efficiency –the security schemes must not overburden the WBAN devices in terms of processing power, communication bandwidth and storage requirements.
- Perfect forward secrecy – the adversary who manages to capture the current session key should be unable to correctly derive the session key for the subsequent session.
- User untraceability and anonymity - the attacker eavesdropping the communication channel should be incapable of associating any communication session to a particular communicating entity.
- Mutual authentication – before any access to the sensed data can be granted, the requesting device should be sufficiently validated.
- Revocability – it should be easy to identify and retract any secret tokens or privileges accorded to the communicating entities once they are compromised.
- Resilience against – the security systems should be capable of withstanding typical WBAN attack vectors such as denial of services, man-in-the-middle, de-synchronization, packet replays among others.

A scheme with all of the above requirements offers strong security at low overheads. These are the bare minimum for the success and large scale adoption of the WBANs in the healthcare sector.

4. Conclusion

Wireless body area networks have become part and parcel of the electronic health systems where they facilitate remote monitoring of the patients as well as the elderly. Therefore, massive volumes of sensitive and private data flows between the patients and the hospital medical staff. Since the transmission of the collected data from the patients is over open wireless channels, many attacks are possible. To curb these attacks, numerous security solutions have been presented in literature. However, this review has identified many security, privacy and performance gaps that need to be filled. As such, a number of recommendations have been presented that can potentially improve on the wireless body networks security posture.

Future work

Future work involves putting these recommendations into practice in form of algorithms that can then be analyzed to showcase their resilience and performance.

Compliance with ethical standards

Acknowledgments

The authors would like to acknowledge all the colleagues who contributed in one way or the other towards the completion of this paper.

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.

References

[1] Fotouhi M, Bayat M, Das AK, Far HA, Pournaghi SM, Doostari MA. A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. Computer Networks. 2020 Aug 4; 177:107333.

[2] Salayma M, Al-Dubai A, Romdhani I, Nasser Y. Wireless body area network (WBAN) a survey on reliability, fault tolerance, and technologies coexistence. ACM Computing Surveys (CSUR). 2017 Mar 10; 50(1):1-38.

[3] Jabeen T, Ashraf H, Ullah A. A survey on healthcare data security in wireless body area networks. Journal of ambient intelligence and humanized computing. 2021 Oct; 12(10):9841-54.

[4] Ali S, Humaria A, Ramzan MS, Khan I, Saqlain SM, Ghani A, Zakia J, Alzahrani BA. An efficient cryptographic technique using modified Diffie–Hellman in wireless sensor networks. International journal of distributed sensor networks. 2020 Jun; 16(6):1550147720925772.

[5] Nyangaresi VO, Ogundoyin SO. Certificate Based Authentication Scheme for Smart Homes. In 2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 202-207). IEEE.

[6] Alzahrani BA, Irshad A, Albeshri A, Alsubhi K. A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks. Wireless Personal Communications. 2021 Mar; 117(1):47-69.

[7] Latré B, Braem B, Moerman I, Blondia C, Demeester P. A survey on wireless body area networks. Wireless networks. 2011 Jan; 17(1):1-8.

[8] Zhang P, Ma J. Channel characteristic aware privacy protection mechanism in WBAN. Sensors. 2018 Jul 24; 18(8):2403.

[9] Tariq MB, Abbas K. Threats, challenges, security of wireless body area network (WBAN) using IEEE 802154/ZIGBEE. Int J Sci Eng. 2017; 8(5):878-84.

[10] Ren Y, Leng Y, Zhu F, Wang J, Kim HJ. Data storage mechanism based on blockchain with privacy protection in wireless body area network. Sensors. 2019 May 25; 19(10):2395.

[11] Sandhu, A., & Malik, A. PAP: priority aware protocol for healthcare application in wireless body area network. Int J Recent TechnolEng (IJRTE). 2020 Aug; 8(5):7

[12] Nyangaresi VO, Abduljabbar ZA, Ma J, Al Sibahee MA. Verifiable Security and Privacy Provisioning Protocol for High Reliability in Smart Healthcare Communication Environment. In 2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 569-574). IEEE.

[13] Abidi B, Jilbab A, Mohamed EH. Wireless body area networks: a comprehensive survey. Journal of Medical Engineering & Technology. 2020 Apr 2; 44(3):97-107.

[14] Nabila A. 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 Apr 3 (pp. 1-5). IEEE.

[15] Crosby GV, Ghosh T, Murimi R, Chin CA. Wireless body area networks for healthcare: A survey. International Journal of Ad Hoc, Sensor & Ubiquitous Computing. 2012 Jun 1; 3(3):1.

[16] Lin H, Shao J, Zhang C, Fang Y. CAM: cloud-assisted privacy preserving mobile health monitoring. IEEE Transactions on Information Forensics and Security. 2013 Mar 29; 8(6):985-97.

[17] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In 2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[18] Bashir A, Hussain Mir A. Securing Communication in MQTT enabled Internet of Things with Lightweight security protocol. EAI Endorsed Transactions on internet of things. 2018; 3(12).

[19] 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 May 22; 15(2):2779-86.

[20] He D, Zeadally S, Kumar N, Lee JH. Anonymous authentication for wireless body area networks with provable security. IEEE Systems Journal. 2016 Apr 22; 11(4):2590-601.

[21] Farooq S, Prashar D, Jyoti K. Hybrid encryption algorithm in wireless body area networks (WBAN). In Intelligent communication, control and devices 2018 (pp. 401-410). Springer, Singapore.

[22] Al-Janabi S, Al-Shourbaji I, Shojafar M, Shamshirband S. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egyptian Informatics Journal. 2017 Jul 1; 18(2):113-22.

[23] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Sep; 3(5):1-6.

[24] Prameela S, Ponmuthuramalingam P. A robust energy efficient and secure data dissemination protocol for wireless body area networks. In 2016 IEEE International Conference on Advances in Computer Applications (ICACA) 2016 Oct 24 (pp. 131-134). IEEE.

[25] Vishwakarma R, Mohapatra RK. A secure three-party authentication protocol for wireless body area networks. In 2017 Third International Conference on Sensing, Signal Processing and Security (ICSSS) 2017 May 4 (pp. 99-103). IEEE.

[26] Al Shayokh M, Abeshu A, Satrya GB, Nugroho MA. Efficient and secure data delivery in software defined WBAN for virtual hospital. In 2016 international conference on control, electronics, renewable energy and communications (ICCEREC) 2016 Sep 13 (pp. 12-16). IEEE.

[27] Narwal B, Mohapatra AK, Usmani KA. Towards a taxonomy of cyber threats against target applications. Journal of Statistics and Management Systems. 2019 Feb 17; 22(2):301-25.

[28] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. In International Conference on Internet of Things as a Service 2022 (pp. 3-18). Springer, Cham.

[29] Ferrag MA, Maglaras LA, Janicke H, Jiang J, Shu L. Authentication protocols for internet of things: a comprehensive survey. Security and Communication Networks. 2017 Nov 6; 2017.

[30] Liu J, Li Q, Yan R, Sun R. Efficient authenticated key exchange protocols for wireless body area networks. EURASIP Journal on Wireless Communications and Networking. 2015 Dec; 2015(1):1-1.

[31] Nikooghadam M, Amintoosi H. A secure and robust elliptic curve cryptography-based mutual authentication scheme for session initiation protocol. Security and Privacy. 2020 Jan;3(1):e92, 165–178

[32] Qiu S, Xu G, Ahmad H, Wang L. A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems. IEEE access. 2017 Dec 8; 6:7452-63.

[33] Salem O, Guerassimov A, Mehaoua A, Marcus A, Furht B. Anomaly detection in medical wireless sensor networks using SVM and linear regression models. International Journal of E-Health and Medical Communications (IJEHMC). 2014 Jan 1; 5(1):20-45.

[34] Saeed ME, Liu QY, Tian G, Gao B, Li F. Remote authentication schemes for wireless body area networks based on the Internet of Things. IEEE Internet of Things Journal. 2018 Oct 18; 5(6):4926-44.

[35] Islam SH, Biswas GP. A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. Journal of Systems and Software. 2011 Nov 1; 84(11):1892-8.

[36] Nyangaresi VO. ECC based authentication scheme for smart homes. In 2021 International Symposium ELMAR 2021 Sep 13 (pp. 5-10). IEEE.

[37] Radhakrishnan N, Karuppiah M. An efficient and secure remote user mutual authentication scheme using smart cards for Telecare medical information systems. Informatics in Medicine Unlocked. 2019 Jan 1; 16:100092.

[38] Varshavsky A, Scannell A, LaMarca A, Lara ED. Amigo: Proximity-based authentication of mobile devices. In International Conference on Ubiquitous Computing 2007 Sep 16 (pp. 253-270). Springer, Berlin, Heidelberg.

[39] Shi L, Li M, Yu S, Yuan J. BANA: Body area network authentication exploiting channel characteristics. IEEE Journal on selected Areas in Communications. 2013 Aug 23; 31(9):1803-16.

[40] Chowdhury FS, Istiaque A, Mahmud A, Miskat M. An implementation of a lightweight end-to-end secured communication system for patient monitoring system. In 2018 Emerging Trends in Electronic Devices and Computational Techniques (EDCT) 2018 Mar 8 (pp. 1-5). IEEE.

[41] Gebrie MT, Abie H. Risk-based adaptive authentication for internet of things in smart home eHealth. In Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings 2017 Sep 11 (pp. 102-108).

[42] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In 2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[43] Aman MN, Chua KC, Sikdar B. A light-weight mutual authentication protocol for IoT systems. In GLOBECOM 2017-2017 IEEE Global Communications Conference 2017 Dec 4 (pp. 1-6). IEEE.

[44] Zhao M, Yao X, Liu H, Ning H. Physical unclonable function based authentication protocol for unit IoT and ubiquitous IoT. In 2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI) 2016 Oct 20 (pp. 179-184). IEEE.

[45] Xie L, Wang W, Shi X, Qin T. Lightweight mutual authentication among sensors in body area networks through physical unclonable functions. In 2017 IEEE International Conference on Communications (ICC) 2017 May 21 (pp. 1-6). IEEE.

[46] Tan X, Zhang J, Zhang Y, Qin Z, Ding Y, Wang X. A PUF-based and cloud-assisted lightweight authentication for multi-hop body area network. Tsinghua Science and Technology. 2020 Jun 19; 26(1):36-47.

[47] Wang W, Shi X, Qin T. Encryption-free authentication and integrity protection in body area networks through physical unclonable functions. Smart Health. 2019 Apr 1; 12:66-81.

[48] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In 2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[49] Li X, Niu J, Kumari S, Wu F, Choo KK. A robust biometrics based three-factor authentication scheme for global mobility networks in smart city. Future Generation Computer Systems. 2018 Jun 1; 83:607-18.

[50] Iqbal J, ul Amin N, Umar AI, Din N. Efficient key agreement and nodes authentication scheme for body sensor networks. International Journal of Advanced Computer Science and Applications. 2017; 8(7):180-187

[51] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably Secure and Fast Color Image Encryption Algorithm Based on S-Boxes and Hyperchaotic Map. IEEE Access. 2022 Feb 11; 10:26257-70.

[52] Narwal B, Mohapatra AK. A survey on security and authentication in wireless body area networks. Journal of Systems Architecture. 2021 Feb 1; 113:101883.

[53] Gope P, Hwang T. A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks. IEEE Transactions on industrial electronics. 2016 Jun 27; 63(11):7124-32.

[54] Kumari S, Li X, Wu F, Das AK, Arshad H, Khan MK. A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps. Future Generation Computer Systems. 2016 Oct 1; 63:56-75.

[55] Srinivas J, Mishra D, Mukhopadhyay S. A mutual authentication framework for wireless medical sensor networks. Journal of medical systems. 2017 May; 41(5):1-9.

[56] He D, Zeadally S, Wu L. Certificateless public auditing scheme for cloud-assisted wireless body area networks. IEEE Systems Journal. 2015 May 21; 12(1):64-73.

[57] Wei F, Vijayakumar P, Shen J, Zhang R, Li L. A provably secure password-based anonymous authentication scheme for wireless body area networks. Computers & Electrical Engineering. 2018 Jan 1; 65:322-31.

[58] Wazid M, Das AK, Vasilakos AV. Authenticated key management protocol for cloud-assisted body area sensor networks. Journal of Network and Computer Applications. 2018 Dec 1; 123:112-26.

[59] Al Sibahee MA, Abdulsada AI, Abduljabbar ZA, Ma J, Nyangaresi VO, Umran SM. Lightweight, Secure, Similar-Document Retrieval over Encrypted Data. Applied Sciences. 2021 Dec 17; 11(24):12040.

[60] Nyangaresi VO. Provably Secure Protocol for 5G HetNets. In 2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[61] Ever YK. Secure-anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks. IEEE systems journal. 2018 Sep 20; 13(1):456-67.

[62] Liu CH, Chung YF. Secure user authentication scheme for wireless healthcare sensor networks. Computers & Electrical Engineering. 2017 Apr 1; 59:250-61.

[63] Xu Z, Xu C, Chen H, Yang F. A lightweight anonymous mutual authentication and key agreement scheme for WBAN. Concurrency and computation: Practice and experience. 2019 Jul 25; 31(14):e5295.

[64] Zhang Z, Wang H, Vasilakos AV, Fang H. ECG-cryptography and authentication in body area networks. IEEE Transactions on Information Technology in Biomedicine. 2012 Jun 26; 16(6):1070-8.

[65] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Jun 25:100210.

[66] Renuka K, Kumari S, Li X. Design of a secure three-factor authentication scheme for smart healthcare. Journal of medical systems. 2019 May; 43(5):1-2.

[67] Toqeer A, Nauman M, Jan S. Trust in IoT: dynamic remote attestation through efficient behavior capture. Cluster Computing. 2018 Mar; 21(1):409-21.

[68] Chang CC, Lee JS, Wu JS. An energy conservation authentication scheme in wireless body area network. Communications of the CCISA. 2017 Oct 1; 23(4):37-54.

[69] Wu ZY, Lee YC, Lai F, Lee HC, Chung Y. A secure authentication scheme for telecare medicine information systems. Journal of medical systems. 2012 Jun; 36(3):1529-35.

[70] Zhang W, Qin T, Mekonen M, Wang W. Wireless body area network identity authentication protocol based on physical unclonable function. In 2018 International Conference on Sensor Networks and Signal Processing (SNSP) 2018 Oct 28 (pp. 60-64). IEEE.

[71] Chunyi C, Jung J, Kim J, Sun Q, Lee D, Won D. Cryptanalysis and improvement of a biometric and smart card based remote user authentication scheme. In Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication 2017 Jan 5 (pp. 1-8).

[72] Tritilanunt S. A biometric smart card based remote user authentication for telecare medicine information system. In Proceedings of the 2019 4th International Conference on Cloud Computing and Internet of Things 2019 Sep 20 (pp. 59-65).

[73] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In 2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[74] Li X, Ibrahim MH, Kumari S, Sangaiah AK, Gupta V, Choo KK. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. Computer Networks. 2017 Dec 24; 129:429-43.

[75] Chen CM, Xiang B, Wu TY, Wang KH. An anonymous mutual authenticated key agreement scheme for wearable sensors in wireless body area networks. Applied Sciences. 2018 Jul 2; 8(7):1074.

[76] Li X, Peng J, Kumari S, Wu F, Karuppiah M, Choo KK. An enhanced 1-round authentication protocol for wireless body area networks with user anonymity. Computers & Electrical Engineering. 2017 Jul 1; 61:238-49.

[77] Nyakomitta PS, Nyangaresi VO, Ogara SO. Efficient Authentication Algorithm for Secure Remote Access in Wireless Sensor Networks. Journal of Computer Science Research. 2021 June; 3(4): 43-50.

[78] Rasmussen KB, Castelluccia C, Heydt-Benjamin TS, Capkun S. Proximity-based access control for implantable medical devices. In Proceedings of the 16th ACM conference on Computer and communications security 2009 Nov 9 (pp. 410-419).

[79] Xiong H. Cost-effective scalable and anonymous certificateless remote authentication protocol. IEEE Transactions on Information Forensics and Security. 2014 Oct 16; 9(12):2327-39.

[80] Nyangaresi VO, Rodrigues AJ, Al Rababah AA. Secure Protocol for Resource-Constrained IoT Device Authentication. International Journal of Interdisciplinary Telecommunications and Networking (IJITN). 2022 Jan 1; 14(1):1-5.

[81] Zebboudj S, Cherifi F, Mohammedi M, Omar M. Secure and efficient ECG-based authentication scheme for medical body area sensor networks. Smart Health. 2017 Sep 1;3:75-84.

[82] Wu L, Zhang Y, Li L, Shen J. Efficient and anonymous authentication scheme for wireless body area networks. Journal of medical systems. 2016 Jun; 40(6):1-2.

[83] Chen R, Peng D. Analysis and improvement of a mutual authentication scheme for wireless body area networks. Journal of medical Systems. 2019 Feb; 43(2):1-0.

[84] Kalamandeen A, Scannell A, de Lara E, Sheth A, LaMarca A. Ensemble: cooperative proximity-based authentication. In Proceedings of the 8th international conference on Mobile systems, applications, and services 2010 Jun 15 (pp. 331-344).

[85] Sahoo SS, Mohanty S, Majhi B. A secure three factor based authentication scheme for health care systems using IoT enabled devices. Journal of Ambient Intelligence and Humanized Computing. 2021 Jan; 12(1):1419-34.

[86] Ibrahim MH, Kumari S, Das AK, Wazid M, Odelu V. Secure anonymous mutual authentication for star two-tier wireless body area networks. Computer methods and programs in biomedicine. 2016 Oct 1; 135:37-50.

[87] Mathur S, Miller R, Varshavsky A, Trappe W, Mandayam N. Proximate: proximity-based secure pairing using ambient wireless signals. In Proceedings of the 9th international conference on Mobile systems, applications, and services 2011 Jun 28 (pp. 211-224).

[88] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. In International Conference for Emerging Technologies in Computing 2021 Aug 18 (pp. 3-20). Springer, Cham.

[89] 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. Multimedia Systems. 2015 Feb; 21(1):49-60.

[90] Odelu V, Das AK, Goswami A. An efficient ECC-based privacy-preserving client authentication protocol with key agreement using smart card. Journal of Information Security and Applications. 2015 Apr 1; 21:1-9.

[91] Li X, Niu J, Karuppiah M, Kumari S, Wu F. Secure and efficient two-factor user authentication scheme with user anonymity for network based e-health care applications. Journal of medical systems. 2016 Dec; 40(12):1-2.

[92] Xie Y, Zhang S, Li X, Li Y, Chai Y. Cascp: efficient and secure certificateless authentication scheme for wireless body area networks with conditional privacy-preserving. Security and Communication Networks. 2019 Jun 4; 2019.

[93] Cao X, Kou W, Du X. A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges. Information Sciences. 2010 Aug 1; 180(15):2895-903.

[94] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In 2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[95] Wang L. Analysis and enhancement of a password authentication and update scheme based on elliptic curve cryptography. Journal of Applied Mathematics. 2014 Jan 1; 2014.

[96] Roy M, Chowdhury C, Kundu A, Aslam N. Secure lightweight routing (SLR) strategy for wireless body area networks. In 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) 2017 Dec 17 (pp. 1-4). IEEE.

[97] Ullah MG, Chowdhary BS, Rajput AQ, Baloch AK, Ursani AA, Latif S. Wireless body area sensor network authentication using voronoi diagram of retinal vascular pattern. Wireless personal communications. 2014 Jun;76(3):579-89.

[98] Jegadeesan S, Azees M, Babu NR, Subramaniam U, Almakhles JD. EPAW: Efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs). IEEE Access. 2020 Mar 3; 8:48576-86.

[99] Tsai JL, Lo NW. A privacy-aware authentication scheme for distributed mobile cloud computing services. IEEE systems journal. 2015 May 21; 9(3):805-15.

[100] Kumar M, Saxena P C. Pairing-free authenticated identity-based two-party key agreement protocol for resource-constraint devices. In Proc. Futuristic Trends Netw. Commun. Technol. 2020 May 22 (pp. 425-440).

[101] Nyangaresi VO, Moundounga AR. Secure Data Exchange Scheme for Smart Grids. In 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[102] Jiang Q, Ma J, Wei F. On the security of a privacy-aware authentication scheme for distributed mobile cloud computing services. IEEE systems journal. 2016 Jun 23; 12(2):2039-42.

[103] Amin R, Islam SH, Biswas GP, Khan MK, Kumar N. A robust and anonymous patient monitoring system using wireless medical sensor networks. Future Generation Computer Systems. 2018 Mar 1; 80:483-95.

[104] Abina P, Dhivyakala K, Suganya L, Praveena SM. Biometric authentication system for body area network. Int. J. Adv. Res. Electr. 2014; 3(3):7954-64.

[105] Mwitende G, Ye Y, Ali I, Li F. Certificateless authenticated key agreement for blockchain-based WBANs. Journal of Systems Architecture. 2020 Nov 1; 110:101777.

[106] Nyangaresi VO, Morsy MA. Towards Privacy Preservation in Internet of Drones. In 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[107] Wang C, Zhang Y. New authentication scheme for wireless body area networks using the bilinear pairing. Journal of medical systems. 2015 Nov; 39(11):1-8.

[108] Jiang Q, Lian X, Yang C, Ma J, Tian Y, Yang Y. A bilinear pairing based anonymous authentication scheme in wireless body area networks for mHealth. Journal of medical systems. 2016 Nov; 40(11):1-0.

[109] Kumari S, Om H. Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines. Computer Networks. 2016 Jul 20; 104:137-54.

[110] Shi L, Yuan J, Yu S, Li M. ASK-BAN: Authenticated secret key extraction utilizing channel characteristics for body area networks. In Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks 2013 Apr 17 (pp. 155-166).

[111] Yang X, Huang X, Liu JK. Efficient handover authentication with user anonymity and untraceability for mobile cloud computing. Future Generation Computer Systems. 2016 Sep 1; 62:190-5.

[112] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In 2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[113] Pirbhulal S, Zhang H, Mukhopadhyay SC, Li C, Wang Y, Li G, Wu W, Zhang YT. An efficient biometric-based algorithm using heart rate variability for securing body sensor networks. Sensors. 2015 Jun 26; 15(7):15067-89.

[114] Peter S, Pratap Reddy B, Momtaz F, Givargis T. Design of secure ECG-based biometric authentication in body area sensor networks. Sensors. 2016 Apr 22; 16(4):570.

[115] Narwal B, Mohapatra AK. SEEMAKA: Secured energy-efficient mutual authentication and key agreement scheme for wireless body area networks. Wireless Personal Communications. 2020 Aug; 113(4):1985-2008.

[116] Jiang Q, Ma J, Li G, Yang L. An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks. Wireless personal communications. 2013 Feb; 68(4):1477-91.

[117] Wen F, Susilo W, Yang G. A secure and effective anonymous user authentication scheme for roaming service in global mobility networks. Wireless personal communications. 2013 Dec; 73(3):993-1004.

[118] Gope P, Hwang T. Enhanced secure mutual authentication and key agreement scheme preserving user anonymity in global mobile networks. Wireless Personal Communications. 2015 Jun; 82(4):2231-45.

[119] Zhao Z. An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem. Journal of medical systems. 2014 Feb; 38(2):1-7.

[120] Li M, Yu S, Lou W, Ren K. Group device pairing based secure sensor association and key management for body area networks. In2010 Proceedings IEEE INFOCOM 2010 Mar 14 (pp. 1-9). IEEE.

[121] Nyangaresi VO, Abd-Elnaby M, Eid MM, Nabih Zaki Rashed A. Trusted authority based session key agreement and authentication algorithm for smart grid networks. Transactions on Emerging Telecommunications Technologies. 2022 May 6:e4528.

[122] Bhawna N, Mohapatra AK. SALMAKA: secured, anonymity preserving and lightweight mutual authentication and key agreement scheme for WBAN. International Journal of Sensors Wireless Communications and Control. 2021 May 1; 11(4):374-84.

[123] Farash MS, Chaudhry SA, Heydari M, Sajad Sadough SM, Kumari S, Khan MK. A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security. International Journal of Communication Systems. 2017 Mar 10; 30(4):e3019.

[124] Wu F, Xu L, Kumari S, Li X, Das AK, Khan MK, Karuppiah M, Baliyan R. A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks. Security and Communication Networks. 2016 Nov 10; 9(16):3527-42.

[125] Tan H, Chung I. Secure authentication and group key distribution scheme for WBANs based on smartphone ECG sensor. IEEE Access. 2019 Oct 18; 7:151459-74.

[126] Jiang Q, Ma J, Wei F, Tian Y, Shen J, Yang Y. An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks. Journal of Network and Computer Applications. 2016 Dec 1; 76:37-48.

[127] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. In The Fifth International Conference on Safety and Security with IoT 2023 (pp. 81-99). Springer, Cham.

[128] Qi J, Wei F, Fu S, Ma J, Li G, Alelaiwi A. Robust extended chaotic maps-based three-factor authentication scheme preserving biometric template privacy. Nonlinear Dynamics. 2016 Mar; 83(4):2085-101.

[129] He D, Zeadally S. Authentication protocol for an ambient assisted living system. IEEE Communications Magazine. 2015 Jan 16; 53(1):71-7.

[130] Gupta R, Tanwar S, Tyagi S, Kumar N, Obaidat MS, Sadoun B. HaBiTs: Blockchain-based telesurgery framework for healthcare 4.0. In 2019 international conference on computer, information and telecommunication systems (CITS) 2019 Aug 28 (pp. 1-5). IEEE.

[131] Ma L, Ge Y, Zhu Y. TinyZKP: a lightweight authentication scheme based on zero-knowledge proof for wireless body area networks. Wireless personal communications. 2014 Jul; 77(2):1077-90.

[132] Hathaliya J, Sharma P, Tanwar S, Gupta R. Blockchain-based remote patient monitoring in healthcare 4.0. In 2019 IEEE 9th international conference on advanced computing (IACC) 2019 Dec 13 (pp. 87-91). IEEE.

[133] Shen J, Chang S, Shen J, Liu Q, Sun X. A lightweight multi-layer authentication protocol for wireless body area networks. Future generation computer systems. 2018 Jan 1; 78:956-63.

[134] Nyangaresi VO, Abduljabbar ZA, Refish SH, Al Sibahee MA, Abood EW, Lu S. Anonymous Key Agreement and Mutual Authentication Protocol for Smart Grids. In International Conference on Cognitive Radio Oriented Wireless Networks, International Wireless Internet Conference 2022 (pp. 325-340). Springer, Cham.

[135] Xiong H, Qin Z. Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks. IEEE transactions on information forensics and security. 2015 Mar 18; 10(7):1442-55.

[136] Anwar M, Abdullah AH, Butt RA, Ashraf MW, Qureshi KN, Ullah F. Securing data communication in wireless body area networks using digital signatures. Technical Journal. 2018 Jun 29; 23(02):50-5.

[137] Nyangaresi VO, Abduljabbar ZA, Abduljabbar ZA. Authentication and Key Agreement Protocol for Secure Traffic Signaling in 5G Networks. In 2021 IEEE 2nd International Conference on Signal, Control and Communication (SCC) 2021 Dec 20 (pp. 188-193). IEEE.

[138] Debayan D, Maity S, Chatterjee B, Sen S. In-field remote fingerprint authentication using human body communication and on-hub analytics. In 2018 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC) 2018 Jul 18 (pp. 5398-5401). IEEE.

[139] Bu G, Potop-Butucaru M. Ban-gzkp: Optimal zero knowledge proof based scheme for wireless body area networks. Ad Hoc Networks. 2018 Aug 1; 77:28-41.

[140] Wu F, Li X, Sangaiah AK, Xu L, Kumari S, Wu L, Shen J. A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. Future Generation Computer Systems. 2018 May 1; 82:727-37.

[141] Wu Y, Wang K, Sun Y, Ji Y. R 2 NA: Received Signal Strength (RSS) Ratio-Based Node Authentication for Body Area Network. Sensors. 2013 Dec 2;13(12):16512-32.

[142] Liu J, Zhang Z, Chen X, Kwak KS. Certificateless remote anonymous authentication schemes for wireless body area networks. IEEE Transactions on parallel and distributed systems. 2013 May 23; 25(2):332-42.

[143] Nyangaresi VO, Abduljabbar ZA, Sibahee MA, Abood EW, Abduljaleel IQ. Dynamic Ephemeral and Session Key Generation Protocol for Next Generation Smart Grids. In Ad Hoc Networks and Tools for IT 2021 Dec 6 (pp. 188-204). Springer, Cham.

[144] Santanu C, Das AK, Sing JK. A novel and efficient user access control scheme for wireless body area sensor networks. Journal of King Saud University-Computer and Information Sciences. 2014 Jul 1; 26(2):181-201.

[145] Schürmann D, Brüsch A, Sigg S, Wolf L. BANDANA—Body area network device-to-device authentication using natural gAit. In2017 IEEE International Conference on Pervasive Computing and Communications (PerCom) 2017 Mar 13 (pp. 190-196). IEEE.

[146] Raza SF, Naveen C, Satpute VR, Keskar AG. A proficient chaos based security algorithm for emergency response in WBAN system. In 2016 IEEE Students' Technology Symposium (TechSym) 2016 Sep (pp. 18-23). IEEE.

[147] Koya AM, Deepthi PP. Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network. Computer Networks. 2018 Jul 20; 140:138-51.

[148] Cheng X, Chen F, Xie D, Sun H, Huang C, Qi Z. Blockchain-based secure authentication scheme for medical data sharing. In International Conference of Pioneering Computer Scientists, Engineers and Educators 2019 Sep 20 (pp. 396-411). Springer, Singapore.

[149] Nyangaresi VO, Ibrahim A, Abduljabbar ZA, Hussain MA, Al Sibahee MA, Hussien ZA, Ghrabat MJ. Provably Secure Session Key Agreement Protocol for Unmanned Aerial Vehicles Packet Exchanges. In 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET) 2021 Dec 9 (pp. 1-6). IEEE.

[150] Reddy AG, Das AK, Yoon EJ, Yoo KY. A secure anonymous authentication protocol for mobile services on elliptic curve cryptography. IEEE access. 2016 Jul 29; 4:4394-407.

[151] Jiang Q, Chen Z, Ma J, Ma X, Shen J, Wu D. Optimized fuzzy commitment based key agreement protocol for wireless body area network. IEEE Transactions on Emerging Topics in Computing. 2019 Oct 23; 9(2):839-53.

[152] Li X, Niu J, Kumari S, Wu F, Sangaiah AK, Choo KK. A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. Journal of Network and Computer Applications. 2018 Feb 1; 103:194-204.

[153] Muhammad KK, Kumari S. An improved user authentication protocol for healthcare services via wireless medical sensor networks. International Journal of Distributed Sensor Networks. 2014 Apr 26; 10(4):347169.

[154] Barman S, Shum HP, Chattopadhyay S, Samanta D. A secure authentication protocol for multi -server-based e-healthcare using a fuzzy commitment scheme. IEEE Access. 2019 July 10; 7:12557-12574.

[155] Javali C, Revadigar G, Libman L, Jha S. SeAK: Secure authentication and key generation protocol based on dual antennas for wireless body area networks. In International Workshop on Radio Frequency Identification: Security and Privacy Issues 2015 Jun 23 (pp. 74-89). Springer, Cham.

[156] Omala AA, Kibiwott KP, Li F. An efficient remote authentication scheme for wireless body area network. Journal of medical systems. 2017 Feb; 41(2):1-9.

[157] Bhattacharya P, Tanwar S, Bodkhe U, Tyagi S, Kumar N. Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications. IEEE Transactions on Network Science and Engineering. 2019 Dec 25; 8(2):1242-55.

[158] Nyangaresi VO, Abduljabbar ZA, Al Sibahee MA, Abduljaleel IQ, Abood EW. Towards Security and Privacy Preservation in 5G Networks. In 2021 29th Telecommunications Forum (TELFOR) 2021 Nov 23 (pp. 1-4). IEEE.

[159] Gowtham M, Ahila SS. Privacy enhanced data communication protocol for wireless body area network. In 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS) 2017 Jan 6 (pp. 1-5). IEEE.

[160] Jie Z, Huang X, Craig P, Marshall A, Liu D. An improved protocol for the password authenticated association of IEEE 802.15. 6 standard that alleviates computational burden on the node. Symmetry. 2016 Nov 17; 8(11):131.

[161] Mahendran RK, Velusamy P. A secure fuzzy extractor based biometric key authentication scheme for body sensor network in Internet of Medical Things. Computer Communications. 2020 Mar 1; 153:545-52.

[162] Xu J, Meng X, Liang W, Peng L, Xu Z, Li KC. A hybrid mutual authentication scheme based on blockchain technology for WBANs. In International Conference on Blockchain and Trustworthy Systems 2019 Dec 7 (pp. 350-362). Springer, Singapore.

[163] Nyangaresi VO, Abood EW, Abduljabbar ZA, Al Sibahe MA. Energy Efficient WSN Sink-Cloud Server Authentication Protocol. In 2021 5th International Conference on Information Systems and Computer Networks (ISCON) 2021 Oct 22 (pp. 1-6). IEEE.

[164] Drira W, Renault É, Zeghlache D. A hybrid authentication and key establishment scheme for wban. In 2012 IEEE 11th international conference on trust, security and privacy in computing and communications 2012 Jun 25 (pp. 78-83). IEEE.

[165] Hodgkiss J, Djahel S. Securing fuzzy vault enabled authentication in body area networks based smart healthcare. IEEE Consumer Electronics Magazine. 2020 May 7.

[166] Seulgi S, Lee SW, Kim H. Authentication protocol for healthcare services over wireless body area networks. International Journal of Computer and Communication Engineering. 2016 Jan 1; 5(1):50.

[167] Abood EW, Abdullah AM, Al Sibahe MA, Abduljabbar ZA, Nyangaresi VO, Kalafy SA, Ghrabta MJ. Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics. 2022 Feb 1; 11(1):185-94.

[168] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV Computing-Assisted Search and Rescue Mission Framework for Disaster and Harsh Environment Mitigation. Drones. 2022 Jun 22; 6(7):154.

[169] Amin R, Islam SH, Kumar N, Choo KK. An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks. Journal of network and computer applications. 2018 Feb 15; 104:133-44.

[170] Irshad A, Sher M, Chaudhry SA, Xie Q, Kumari S, Wu F. An improved and secure chaotic map based authenticated key agreement in multi-server architecture. Multimedia Tools and Applications. 2018 Jan; 77(1):1167-204.

[171] Azeem I, Chaudhry SA, Kumari S, Usman M, Mahmood K, Faisal MS. An improved lightweight multiserver authentication scheme. International Journal of Communication Systems. 2017 Nov 25; 30(17):e3351.

[172] Azeem I, Chaudhry SA, Xie Q, Li X, Farash MS, Kumari S, Wu F. An enhanced and provably secure chaotic map-based authenticated key agreement in multi-server architecture. Arabian Journal for Science and Engineering. 2018 Feb; 43(2):811-28.

[173] Irshad A, Sher M, Chaudhry SA, Kumari S, Sangaiah AK, Li X, Wu F. A secure mutual authenticated key agreement of user with multiple servers for critical systems. Multimedia Tools and Applications. 2018 May; 77(9):11067-99.

[174] Irshad A, Sher M, Nawaz O, Chaudhry SA, Khan I, Kumari S. A secure and provable multi-server authenticated key agreement for TMIS based on Amin et al. scheme. Multimedia Tools and Applications. 2017 Aug; 76(15):16463-89.

[175] Nyakomitta SP, Omollo V. Biometric-Based Authentication Model for E-Card Payment Technology. IOSR Journal of Computer Engineering (IOSRJCE). 2014;16(5):137-44.