SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 10 | October 2024 - Peer Reviewed Journal

A TECHNIQUE TO SECURE DATA TRANSMISSION IN WIRELESS BODY AREA NETWORKS

Joshua Auko[1], Richard Omollo[2]
[1,2] *Jaramogi Oginga Odinga University of Science & Technology*

Article DOI: https://doi.org/10.36713/epra18336
DOI No: 10.36713/epra18336

ABSTRACT

The wireless body area networks have contributed to the changes in healthcare sector by enabling continuous monitoring of biomedical parameters remotely on the patient body and offering real time data transmission. Upon collection of the vital signs, they are transmitted to the gateway node which then forwards them to the remote hospital medical servers. Here, these physiological data items are analyzed and necessary action is taken. Such physiological data include electrocardiograms (ECGs), blood pressure, body temperature, blood oxygen levels, respiratory rate, Electroencephalogram (EEG), Electromyogram (EMG), glucose levels, physical activity and Electrodermal Activity (EDA). In this paper, we develop a technique for securely transmitting this sensitive data from the body sensor unit (BSU) to the remote hospital medical server (HMS).

KEYWORDS: *Sensors, BSU, WBAN, security, privacy*

1. INTRODUCTION

Wireless body area network (WBANs) comprised of smart medical sensors that are placed inside the patient's body or located in the vicinity of the patient. The main components of a typical WBAN include the medical staff, sensors, and gateway nodes [1]. 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.

As explained in [2], WBANs collect patient medical data and forward the same to medical staff for monitoring the patient's health remotely. Thus, patients diagnosis can be done remotely using some remote clinical nano-sensors [3]. The collected data may include body temperature, ECG, sugar level and blood pressure among others [4]. WBAN presents an emerging domain that employs ubiquitous technologies such as smart sensors, cloud computing, embedded systems and wireless network technologies to boost the electronic-health care system [5]. As explained in [6] and [7], WBAN based systems represent one of the most critical technologies in the biomedical field. Basically, important patient and elderly health parameters and movements are received and forwarded to the healthcare service provider for analysis and appropriate action [2], [8]. As a result of the effectiveness and demand for WBAN, a new international communication standard IEEE 802.15.6 [9] has been developed.

In spite of the numerous merits accompanying this technology, its open nature in regard to wireless communication channels coupled with cloud computing introduce a number of security threats and vulnerabilities. As such, the privacy and integrity of the exchanged data may be compromised. 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 [10], 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 [11]. The resource-constrained nature [12] of the sensors deployed in WBAN presents some challenges with regard to execution, storage and communication complexities. Cloud computing can potentially solve these issues but it introduces its own threats and vulnerabilities [13]. According to [14] and [15], data encryption is another solution to these issues. However, some of the encryption algorithms are resource-intensive hence not suitable for the sensors. This paper makes the following contributions:

- A review of the current security techniques for WBAN is provided, including the shortcomings of these techniques.
- We develop an efficient technique to protect the data exchanged in WBANs.

- We show that it is computationally infeasible to extract the sensory data transmitted over the public channels.

The rest of this article is structured as follows: Part 2 describes the related works while Part 3 presents the adopted methodology. However, Part 4 presents the obtained results while Part 5 concludes this paper.

2. RELATED WORKS

Many security solutions have been put forward by researchers in industry as well as academia to protecting WBAN communication process. For example, the authentication protocols in [16] 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 [17] cannot uphold user anonymity [12]. These issues can be addressed by the secure and efficient approaches in [18] and [19]. Using offline signatures, a remote authentication scheme is developed in [20]. Using the physical unclonable functions (PUFs), lightweight protocols are developed in [21] and [22]. Unfortunately, the security analysis of the scheme in [21] is missing. In addition, PUF-based schemes have stability challenges. On the other hand, an energy-efficient authentication and key agreement protocol is developed [23]. Although the technique incurs less communication, memory and computation overheads, it cannot withstand many security attacks [24]. To address this challenge, many schemes have been put forward in [25], [26] and [27]. However, most of these schemes are not lightweight and cannot offer forward secrecy, untrace ability as well as resilience against key compromise impersonation attack [10]. For instance, the scheme [26] incurs extremely high communication costs. To reduce the computation and communication overheads, a secure anonymous user authentication scheme is developed in [28]. Similarly, and efficient and privacy preserving smart card-based authentication protocol is presented in [29]. However, this approach is vulnerable to offline password guessing, replay, smart card loss and forgery attacks. Similarly, the scheme in [30] is susceptible to key compromise, replay, privacy leakages and impersonation attacks [5].

3. METHODOLOGY

The major communicating entities in the proposed algorithm include the Gateway Node (GWN), Hospital Medical Server (HMS) and the Body Sensor Unit (BSU) as shown in Figure 1 below.

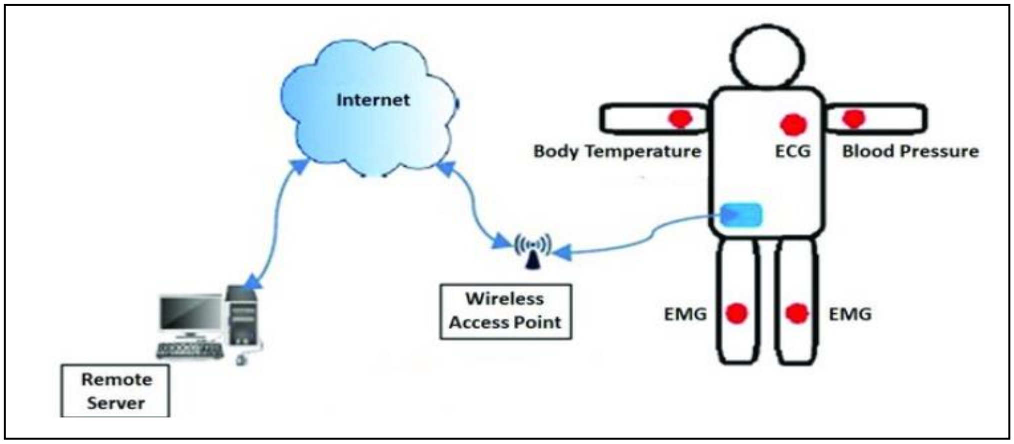


Figure 1: WBAN environment

In this environment, the BSU collects data such as body temperature, glucose levels, PR, QT, ST, QRS and RR. The PR, QT, and RR intervals represent the duration of conduction through the AV node, the duration of ventricular depolarization to repolarization, and the duration between each cardiac cycle, respectively. Basically, PR and ST segments represent the isoelectric interval between depolarization and repolarization of the atria and ventricles. On the other hand, QRS complex is a crucial part of an electrocardiogram (ECG or EKG) which represent the electrical activity associated with the depolarization of the ventricles, which are the two lower chambers of the heart. Table 1 gives a summary of these physiological data collected at the BSU.

Table 1: Physiological parameters

Physiological parameter	Description
QRS complex	Represents ventricular depolarization and consists of three main components: *Q Wave* - This is the initial downward deflection following the P wave which represents the initial depolarization of the interventricular septum. *R Wave* - This is the first upward deflection after the Q wave and it represents the depolarization of the main mass of the ventricles, primarily the left ventricle. *S Wave* - This is the downward deflection following the R wave which represents the final phase of ventricular depolarization at the base of the heart.
PR Interval	Is the time from the onset of the P wave (the start of atrial depolarization) to the beginning of the QRS complex (the start of ventricular depolarization). *Clinical Importance*: a prolonged PR interval can indicate first-degree heart block, while a shortened PR interval may suggest a pre-excitation syndrome such as Wolff-Parkinson-White (WPW) syndrome.
QT Interval	Is the time from the beginning of the QRS complex (start of ventricular depolarization) to the end of the T wave (end of ventricular repolarization). *Clinical Importance*: a prolonged QT interval can increase the risk of ventricular arrhythmias, such as Torsades de Pointes, and may indicate conditions like Long QT Syndrome. On the other hand, a shortened QT interval can be associated with hypercalcemia or Short QT Syndrome.
ST Segment	Is the flat, isoelectric section of the ECG between the end of the S wave and the beginning of the T wave. *Clinical Importance*: Elevation of the ST segment can indicate myocardial infarction (STEMI) or pericarditis. On the other hand, depression of the ST segment can suggest ischemia or non-ST elevation myocardial infarction (NSTEMI).
RR Interval	Is the time between two successive R waves, which represent consecutive ventricular depolarizations. *Clinical Importance*: Regular RR intervals indicate a regular heart rhythm while irregular RR intervals can indicate arrhythmias such as atrial fibrillation.

In a nutshell, in the context of the cardiac conduction system and electrocardiography (ECG or EKG), PR, QT, ST, QRS and RR intervals are critical measurements that provide valuable information about the heart's electrical activity and overall function. Table 2 presents the permissible ranges of these physiological data items.

Table 2: Physiological parameters ranges

Physiological parameter	Range
Body temperature	97°F (36.1°C) to 99°F (37.2°C).
Glucose level	70 to 99 mg/dL (3.9 and 5.5 mmol/L)
RR Interval	0.6-1.2 seconds
PR Interval	120-200 milliseconds
PR segment	50-120 milliseconds
ST Segment	80-120 milliseconds
QRS complex	80-100 milliseconds

To protect the transmitted physiological data transmitted between the BSU and HMS, a session key is setup. This session key consist of random number R_{i}, the gateway node master key M_{GW}, and the entities of both the BSU and HMS (ID_{BSU}, ID_{HMS}), which are then hashed. That is,

Session key, SK = $h\ (M_{\text{GW}}||ID_{\text{BSU}}||ID_{\text{HMS}}||R_{\text{i}})$

The collected data is then encapsulated as shown in Table 3.

Table 3: Transmitted data format

Physiological parameter	Encapsulated data
Body temperature, *body_temp*	*Trans_ body_temp = SK*⊕body_temp
Glucose level, *Gluc_lev*	*Trans_ Gluc_lev = SK*⊕Gluc_lev
RR Interval, *RR_int*	*Trans_ RR_int = SK*⊕*RR_int*
PR Interval, *PR_int*	*Trans_ PR_int = SK*⊕*PR_int*
PR segment, *PR_seg*	*Trans_ PR_seg = SK*⊕*PR_seg*
ST Segment, *ST_seg*	*Trans_ ST_seg = SK*⊕*ST_seg*
QRS complex, *QRS_com*	*Trans_ QRS_com = SK*⊕*QRS_com*

The transmitted data is therefore a concatenation of the above seven physiological data items. At the receiver end, the plaintext physiological data is recovered as shown in Table 4.

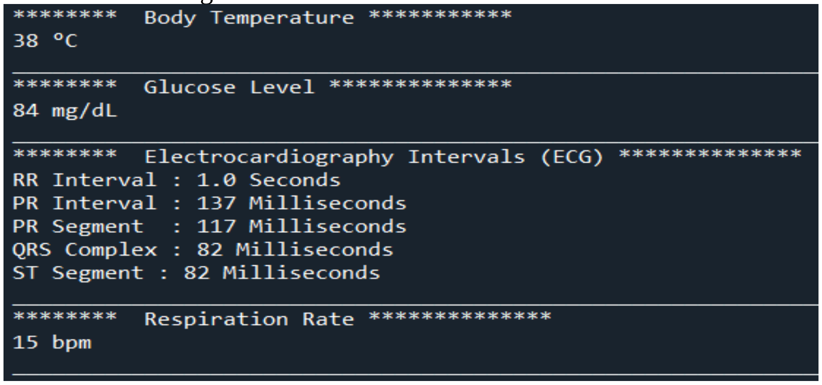
Table 4: Data recovery at HMS

Physiological parameter	Recovered data
Body temperature, *body_temp*	*SK*⊕ *Trans_ body_temp*
Glucose level, *Gluc_lev*	*SK*⊕ *Trans_ Gluc_lev*
RR Interval, *RR_int*	*SK*⊕ *Trans_ RR_int*
PR Interval, *PR_int*	*SK*⊕ *Trans_ PR_int*
PR segment, *PR_seg*	*SK*⊕*Trans_ PR_seg*
ST Segment, *ST_seg*	*SK*⊕ *Trans_ ST_seg*
QRS complex, *QRS_com*	*SK*⊕*Trans_ QRS_com*

The obtained plaintext data in Table 4 is then read and interpreted by the medical experts. Thereafter, appropriate action and medication can be recommended.

4. RESULTS AND DISCUSSION

In this sub-section, the security characteristics offered by the developed algorithm are demonstrated. After every successful mutual authentication, session key *Session key*, *SK* = *h* ($M_{GW}||ID_{BSU}||ID_{HMS}||R_i$) is setup to encipher all exchanged messages. Consider the plaintext data generated at the BSU shown in Figure 2.

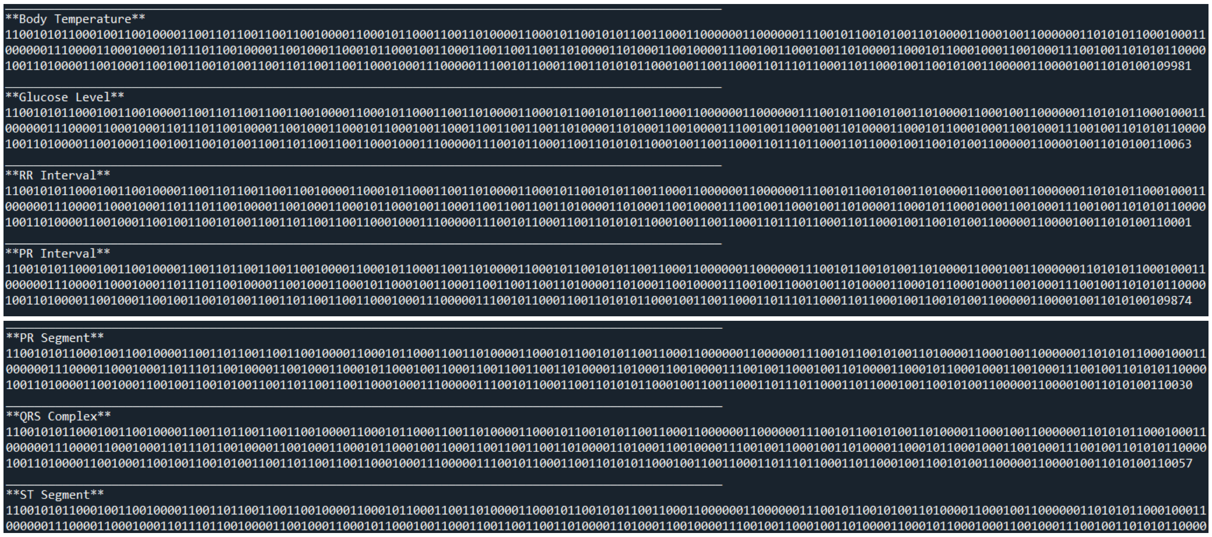


```
********  Body Temperature ***********
38 °C

********  Glucose Level **************
84 mg/dL

********  Electrocardiography Intervals (ECG) ***************
RR Interval : 1.0 Seconds
PR Interval : 137 Milliseconds
PR Segment  : 117 Milliseconds
QRS Complex : 82 Milliseconds
ST Segment : 82 Milliseconds

********  Respiration Rate **************
15 bpm
```

Figure 2: Generated BSU data

Prior to sending the above physiological data over the open wireless channels, each data item is XORed with the session key (as detailed in Table 3 above) to produce the output shown in Figure 3. Basically,

Transmitted data = session key ⊕ *plaintext data*

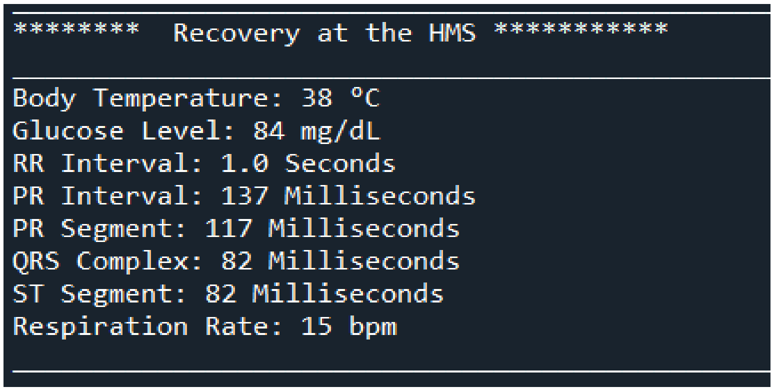


```
**Body Temperature**
110010101100010011001000011001101100110011001000011000101100011001101000011000101100101011001100011000000110000001110010110010100110100001100010011000000110101011000100011
000000111000001100010011011101100100001100100011000101100010011000110011001100110100001101000110010000111001001100010011010000110001011000100011001000111001001101010110000
10011010000110010001100100110010100110011011001100110001000111000001110010110001100110101011000100110011000110111011000110110001001100101001100000011000010011010100109981

**Glucose Level**
110010101100010011001000011001101100110011001000011000101100011001101000011000101100101011001100011000000110000001110010110010100110100001100010011000000110101011000100011
000000111000001100010011011101100100001100100011000101100010011000110011001100110100001101000110010000111001001100010011010000110001011000100011001000111001001101010110000
10011010000110010001100100110010100110011011001100110001000111000001110010110001100110101011000100110011000110111011000110110001001100101001100000011000010011010100110063

**RR Interval**
110010101100010011001000011001101100110011001000011000101100011001101000011000101100101011001100011000000110000001110010110010100110100001100010011000000110101011000100011
000000111000001100010011011101100100001100100011000101100010011000110011001100110100001101000110010000111001001100010011010000110001011000100011001000111001001101010110000
10011010000110010001100100110010100110011011001100110001000111000001110010110001100110101011000100110011000110111011000110110001001100101001100000011000010011010100110001

**PR Interval**
110010101100010011001000011001101100110011001000011000101100011001101000011000101100101011001100011000000110000001110010110010100110100001100010011000000110101011000100011
000000111000001100010011011101100100001100100011000101100010011000110011001100110100001101000110010000111001001100010011010000110001011000100011001000111001001101010110000
10011010000110010001100100110010100110011011001100110001000111000001110010110001100110101011000100110011000110111011000110110001001100101001100000011000010011010100109874

**PR Segment**
110010101100010011001000011001101100110011001000011000101100011001101000011000101100101011001100011000000110000001110010110010100110100001100010011000000110101011000100011
000000111000001100010011011101100100001100100011000101100010011000110011001100110100001101000110010000111001001100010011010000110001011000100011001000111001001101010110000
10011010000110010001100100110010100110011011001100110001000111000001110010110001100110101011000100110011000110111011000110110001001100101001100000011000010011010100110030

**QRS Complex**
110010101100010011001000011001101100110011001000011000101100011001101000011000101100101011001100011000000110000001110010110010100110100001100010011000000110101011000100011
000000111000001100010011011101100100001100100011000101100010011000110011001100110100001101000110010000111001001100010011010000110001011000100011001000111001001101010110000
10011010000110010001100100110010100110011011001100110001000111000001110010110001100110101011000100110011000110111011000110110001001100101001100000011000010011010100110057

**ST Segment**
110010101100010011001000011001101100110011001000011000101100011001101000011000101100101011001100011000000110000001110010110010100110100001100010011000000110101011000100011
000000111000001100010011011101100100001100100011000101100010011000110011001100110100001101000110010000111001001100010011010000110001011000100011001000111001001101010110000
```

Figure 3: Data in transit over the communication channel

Suppose that an adversary acting as man-in-the-middle (MitM) between the BSU and the HM launches an eavesdropping attack. However, due to the one-way hashing operations, the adversary is unable to recover identities ID_{BSU} and ID_{HMS}. As such, anonymity is preserved. In addition, we include random number R_i in each communication session. Therefore, the derived session key is different for each session, mitigating against tracking attacks. At the HMS, the plaintext data is recovered as follows in Figure 4. Basically,

Plaintext data = session key $\oplus$ *transmitted data*



```
********  Recovery at the HMS ***********

Body Temperature: 38 °C
Glucose Level: 84 mg/dL
RR Interval: 1.0 Seconds
PR Interval: 137 Milliseconds
PR Segment: 117 Milliseconds
QRS Complex: 82 Milliseconds
ST Segment: 82 Milliseconds
Respiration Rate: 15 bpm
```

Figure 4: Data at the HMS

As shown in Figure 4, the obtained values at the HMS have been successfully recovered. Basically, they are equivalent to the values appearing at the BSU in Figure 2 presented earlier on.

5. CONCLUSION

The ever-increasing utilization of mobile devices, wireless networks, Internet of Things (IoT) and sensors has seen the healthcare sector adopting numerous mobile devices to collect data, monitor patients and communicate the data over WBANs. 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 spite of the numerous merits accompanying this technology, its open nature in regard to wireless communication channels coupled with cloud computing introduce a number of security threats and vulnerabilities . As such, the privacy and integrity of the exchanged data may be compromised. In this paper, we have presented a technique that can potentially help address these security and privacy issues.

REFERENCES

1. *Prajapat, S., Kumar, P., & Kumar, S. (2024). A privacy preserving quantum authentication scheme for secure data sharing in wireless body area networks. Cluster Computing, 1-17.*
2. *M. Salayma, A. Al-Dubai, I. Romdhani, andY. Nasser,"Wireless body area network(WBAN):Asurvey on reliability, fault tolerance, and technologies coexistence," ACM Comput. Surv., vol. 50, no. 1, pp. 1–38, 2017.*
3. *Jabeen, T., Ashraf, H., & Ullah, A. (2021). A survey on healthcare data security in wireless body area networks. Journal of ambient intelligence and humanized computing, 12(10), 9841-9854.*
4. *S. Ali, H. Ashraf, and M. S. Ramazan, "An efficient cryptographic technique using modified DifeHellman in wireless sensor networks,'' Int. J. Distrib. Sensor Netw., vol. 16, no. 6, p. 24, 2020.*
5. *Alzahrani, B. A., Irshad, A., Albeshri, A., & Alsubhi, K. (2021). A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks. Wireless Personal Communications, 117(1), 47-69.*
6. *Ren Y, Leng Y, Zhu F, Wang J, Kim H-J (2019) Data storage mechanism based on blockchain with privacy protection in wireless body area network. Sensors 19(10):2395*
7. *Sandhu A, Malik A (2020) PAP: priority aware protocol for healthcare application in wireless body area network. Int J Recent Technol Eng (IJRTE) 8(5):7*
8. *Abidi, B., Jilbab, A., & Mohamed, E. H. (2020). Wireless body area networks: a comprehensive survey. Journal of Medical Engineering & Technology, 1-11.*
9. *Nabila, A. (2019, April). 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) (pp. 1-5). IEEE.*
10. *Fotouhi, M., Bayat, M., Das, A. K., Far, H. A. N., Pournaghi, S. M., & Doostari, M. A. (2020). A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. Computer Networks, 177, 107333.*
11. *A. Bashir and A. H. Mir, ``Securing communication in MQTT enabled Internet of Things with lightweight security protocol,'' EAI Endorsed Trans. Internet Things, vol. 3, no. 12, pp. 1-6, Apr. 2018.*
12. *Kumar, M., & Chand, S. (2020). A lightweight cloud-assisted identity-based anonymous authentication and key agreement protocol for secure wireless body area network. IEEE Systems Journal, 15(2), 2779-2786.*
13. *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; 21(1):49–60.*
14. *Farooq S, Prashar D, Jyoti K (2018) Hybrid encryption algorithm in wireless body area network (WBAN). In: Rajesh S, Sushabhan C, Anita G (eds) Intelligent communication control and devices. Springer Nature, Singapore, p 10*
15. *Al-Janabi S, Al-Shourbaji I, Shojafar M, Shamshirband S (2016) Survey of main challenges (security and privacy) in wireless body area network for Healthcare Application. Egypt Inform J 18(2):113–122*
16. *Liu, J., Li, Q., Yan, R., & Sun, R. (2015). Efficient authenticated key exchange protocols for wireless body area networks. EURASIP Journal on Wireless Communications and Networking, 2015(1), 1-11.*
17. *M. Nikooghadam and H. Amintoosi, "A secure and robust elliptic curve cryptography-based mutual authentication scheme for session initiation protocol," Secur. Privacy, vol. 3, no. 1, pp. 165–178, 2020.*
18. *Shuming Qiu, Guoai Xu, Haseen Ahmad and Licheng Wang, "A Robust Mutual Authentication Scheme Based on Elliptic Curve Cryptography for Telecare Medical Information Systems," IEEE Access, vol. 6, pp. 7452-7463, December 2017.*
19. *Osman Salem, Alexey Guerassimov, Ahmed Mehaoua, Anthony Marcus and Borko Furht, "Anomaly Detection in Medical Wireless Sensor Networks using SVM and Linear Regression Models," International Journal of E-Health and Medical Communications, vol. 5, no. 1, pp. 20-45, January 2014.*
20. *Saeed, M. E. S., Liu, Q. Y., Tian, G., Gao, B., & Li, F. (2018). Remote authentication schemes for wireless body area networks based on the Internet of Things. IEEE Internet of Things Journal, 5(6), 4926-4944.*
21. *Tan, H., & Chung, I. (2019). Secure Authentication and Group Key Distribution Scheme for WBANs Based on Smartphone ECG Sensor. IEEE Access, 7, 151459-151474.*
22. *Wang, W., Shi, X., & Qin, T. (2019). Encryption-free Authentication and Integrity Protection in Body Area Networks through Physical Unclonable Functions. Smart Health, 12, 66-81.*
23. *Iqbal, J., Umar, A. I., ul Amin, N., & Din, N. (2017). Efficient Key Agreement and Nodes Authentication Scheme for Body Sensor Networks. International Journal Of Advanced Computer Science And Applications, 8(7), 180-187.*
24. *Narwal, B., & Mohapatra, A. K. (2021). A survey on security and authentication in wireless body area networks. Journal of Systems Architecture, 113, 101883.*
25. *Srinivas J, Mishra D, Mukhopadhyay S. A mutual authentication framework for wireless medical sensor networks. Journal of medical systems 2017; 41(5):80.*
26. *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; 65:322–31.*
27. *Wazid M, Das AK, Vasilakos AV. Authenticated key management protocol for cloud-assisted body area sensor networks. Journal of Network and Computer Applications 2018; 123:112–26.*

28. *Y. Kirsal Ever, "Secure-Anonymous User Authentication Scheme for e-Healthcare Application Using Wireless Medical Sensor Networks," in IEEE Systems Journal, vol. 13, no. 1, pp. 456-467, March 2019*
29. *Chia-Hui Liu and Yu-Fang Chung, "Secure user authentication scheme for wireless healthcare sensor networks," Journal of Computers and Electrical Engineering, vol. 59, pp. 250-261, February 2016.*
30. *Xu J., Meng X., Liang W., Peng L., Xu Z., Li KC. (2020) A Hybrid Mutual Authentication Scheme Based on Blockchain Techno logy for WBANs. In: Zheng Z., Dai HN., Tang M., Chen X. (eds) Blockchain and Trustworthy Systems. BlockSys 2019. Communications in Computer and Information Science, vol 1156. Springer, Singapore.*