iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VIII **Month of publication:** Aug 2023

DOI: https://doi.org/10.22214/ijraset.2023.55405

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

Security Concerns in Wireless Body Area Network

Oluwatosin Abiona[1], Abdul-Quadri Oje[2]

I. INTRODUCTION

Wireless Body Area Network (WBAN) is a rapidly growing field of wireless communication that deals with the connectivity of wireless sensors and devices in the human body. WBANs have been widely adopted in the healthcare sector for monitoring vital signs, chronic disease management, and remote diagnosis. However, the use of WBANs raises concerns about the security and privacy of patient data, as the communication between the sensors and devices is transmitted through the airwaves. This paper will discuss the security concerns in wireless body area networks, the current state of research in the field, and potential solutions to mitigate these concerns.

II. SECURITY CONCERNS IN WIRELESS BODY AREA NETWORK

A. *Unauthorized Access*

A great setback facing WBA's is the unauthorized access it has to user's data. The way the sensor works is that it forms a wireless connection with devices through the airwaves[i]. Airwaves data transmission is still vulnerable and easily accessed by hackers. When access is gained to the patient data, the patients are usually left at the mercy of the hackers. They most times carry out fraudulent activity, Identity theft, or blackmail.[ii]

B. *Interference*

Another security concern in WBANs is interference. Since the data is transmitted through the airwaves, it is susceptible to interference from other wireless devices[iii]. Interference can lead to data loss or corruption, which can compromise the accuracy of the patient data. Inaccurate patient data can lead to incorrect diagnoses, which can have serious consequences for the patient's health[iv].

C. *Data Integrity*

In WBANs, data integrity is a crucial problem. Hackers may alter patient data, resulting in misdiagnoses, therapies, or medications. By intercepting, changing, or deleting data while it is being transmitted, data integrity can be compromised. For instance, a hacker may change drug information, resulting in inaccurate dosages, or alter vital sign data, resulting in an incorrect diagnosis[v].

D. *Data Privacy*

Another security risk with WBANs is data privacy. Regarding their medical histories, vital signs, and other sensitive information, patients have a right to privacy. Hackers have the ability to intercept patient data and utilize it for bad. Additionally, without the patient's permission, healthcare professionals and insurance firms may use patient data for commercial purposes, which is against privacy laws.

III. CURRENT STATE OF RESEARCH

Researchers have been working on developing solutions to mitigate the security concerns in WBANs. The following are some of the current research efforts in the field:

A. *Encryption*

One of the main ways to address the security issues in WBANs is encryption. This is a technique that researchers have been exploring to protect patient data when it is sent. Encryption algorithms can stop hackers from accessing patient data by making it incomprehensible to them. Moreover, encryption can also prevent data tampering, maintaining the accuracy of the patient data[vi].

B. *Authentication*

Authentication is another solution to mitigate the security concerns in WBANs. Authentication ensures that only authorized personnel can access patient data. Researchers have been working on developing authentication protocols that can verify the identity of the user accessing the patient data. Authentication protocols can prevent unauthorized access to patient data by ensuring that only authorized personnel can access the data[vii].

C. Intrusion Detection

Intrusion detection is another solution to mitigate the security concerns in WBANs. Intrusion detection systems can detect and alert healthcare providers of any suspicious activity, such as unauthorized access or data manipulation. Intrusion detection can prevent data breaches by alerting healthcare providers of any security threats[viii].

D. Secure Protocols

Secure protocols are another solution to mitigate the security concerns in WBANs. Researchers have been working on developing secure protocols that can ensure the security and privacy of patient data. Secure protocols can prevent data loss or corruption by ensuring the accuracy of the patient data during transmission. Additionally, secure protocols can prevent unauthorized access to patient data by ensuring that only authorized personnel can access the data[ix].

E. Physical Security

Physical security is another solution to mitigate the security concerns in WBANs. Physical security measures, such as access control, can prevent unauthorized access to WBAN devices. Healthcare providers can limit physical access to WBAN devices to authorized personnel only, which can prevent data breaches[x].

F. Risk Assessment

Risk assessment is another solution to mitigate the security concerns in WBANs. Healthcare providers can conduct risk assessments to identify potential security threats and vulnerabilities. Risk assessments can help healthcare providers develop strategies to mitigate security risks and ensure the security and privacy of patient data[xi].

IV. POTENTIAL SOLUTIONS TO MITIGATE SECURITY CONCERNS

A. Standardization

Standardization is one potential solution to mitigate security concerns in WBANs. Standardization can ensure that all WBAN devices and sensors meet certain security standards, which can prevent security vulnerabilities. Additionally, standardization can ensure that all WBAN devices and sensors are interoperable, which can improve the efficiency and effectiveness of WBANs.

B. Education and Training

Education and training are another potential solution to mitigate security concerns in WBANs. Healthcare providers and personnel can be trained on the best practices for securing patient data in WBANs. Additionally, patients can be educated on the importance of data privacy and security.

C. Regulatory Compliance

Regulatory compliance is another potential solution to mitigate security concerns in WBANs. Healthcare providers and personnel can comply with regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), which ensure the security and privacy of patient data. Compliance with regulations can prevent data breaches and ensure the security and privacy of patient data.

V. CONCLUSION

Wireless Body Area Network (WBAN) is a rapidly growing field of wireless communication that deals with the connectivity of wireless sensors and devices in the human body. However, the use of WBANs raises concerns about the security and privacy of patient data, as the communication between the sensors and devices is transmitted through the airwaves. Security concerns in WBANs include unauthorized access, interference, data integrity, and data privacy. Researchers have been working on developing solutions to mitigate the security concerns in WBANs, such as encryption, authentication, intrusion detection, secure protocols, physical security, and risk assessment. Potential solutions to mitigate security concerns include standardization, education and training, and regulatory compliance. Ultimately, ensuring the security and privacy of patient data in WBANs is crucial to the success of WBANs in the healthcare sector. As WBANs become more widely adopted in healthcare settings, it is essential to address the security concerns that may arise. With the proper measures in place, WBANs have the potential to revolutionize healthcare delivery by providing real-time data on patient health, allowing for better diagnosis and treatment. However, without adequate security measures, these benefits may be overshadowed by potential risks to patient data.

The solutions presented in this paper, such as encryption, authentication, intrusion detection, secure protocols, physical security, and risk assessment, can mitigate security concerns in WBANs. Additionally, potential solutions such as standardization, education and training, and regulatory compliance can help ensure the security and privacy of patient data.

It is crucial for healthcare providers to take a proactive approach to security in WBANs. This includes implementing security measures, complying with regulations, educating personnel, and conducting risk assessments. By doing so, healthcare providers can ensure the security and privacy of patient data in WBANs and provide high-quality healthcare services.

In conclusion, WBANs have the potential to transform healthcare delivery by providing real-time data on patient health. However, security concerns in WBANs must be addressed to ensure the security and privacy of patient data. Researchers and healthcare providers must continue to develop and implement security solutions to mitigate the risks associated with WBANs. By doing so, healthcare providers can provide high-quality healthcare services while ensuring the security and privacy of patient data.

REFERENCES

[1] K. Opasjumruskit et al., "Self-powered wireless temperature sensors exploit RFID technology," in IEEE Pervasive Computing, vol. 5, no. 1, pp. 54-61, Jan.-March 2006, doi: 10.1109/MPRV.2006.15.

[2] Tao, Hai, et al. "Economic perspective analysis of protecting big data security and privacy." *Future Generation Computer Systems* 98 (2019): 660-671.

[3] Kothari, Ashwin. (2017). Interference Analysis and Mitigation Techniques in Wireless Body Area Networks. Wireless Personal Communications. 96. 10.1007/s11277-017-4071-0.

[4] Ananthi, J.V., Jose, P.S.H. A Perspective Review of Security Challenges in Body Area Networks for Healthcare Applications. *Int J Wireless Inf Networks* **28**, 451–466 (2021). https://doi.org/10.1007/s10776-021-00538-3

[5] Alsafi, H., Elhoseny, M., & Menouar, H. (2018). Security and privacy in wireless body area networks: Challenges and solutions. Journal of Medical Systems, 42(9), 1-18. https://doi.org/10.1007/s10916-018-1026-5

[6] Y. Zhang, X. Li, J. Wang and Y. Zhang, "A New Asymmetrical Encryption Algorithm Based on Semitensor Compressed Sensing for WBANs," 2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), Chongqing, China, 2019, pp. 1226-1230, doi: 10.1109/ITAIC.2019.8901170

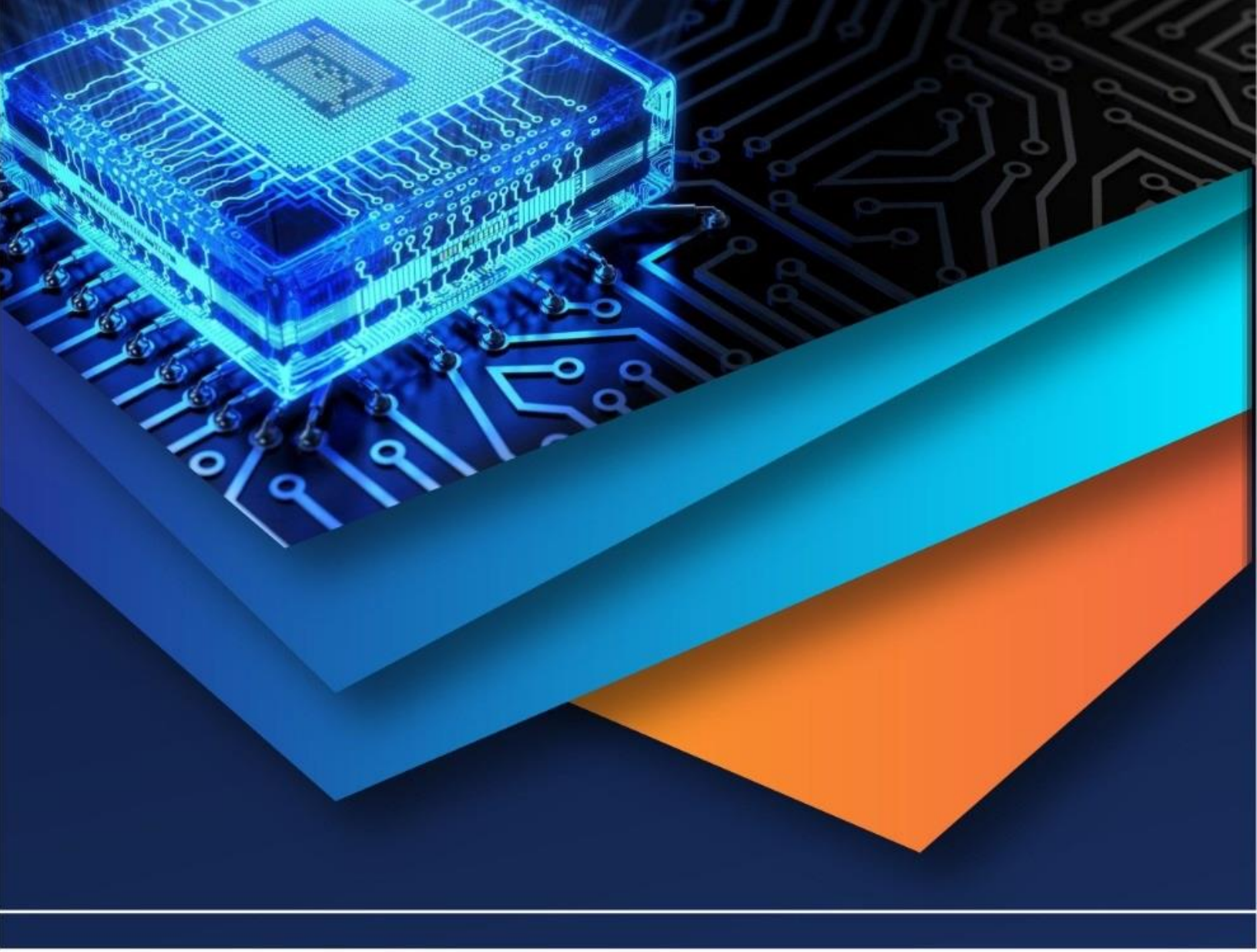
[7] J. Zhang, Q. Zhang, Z. Li, X. Lu and Y. Gan, "A Lightweight and Secure Anonymous User Authentication Protocol for Wireless Body Area Networks," in Security and Communication Networks, vol. 2021, Article ID 4939589, July 2021, doi: 10.1155/2021/4939589.

[8] A. Odesile and G. Thamilarasu, "Distributed Intrusion Detection Using Mobile Agents in Wireless Body Area Networks," 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, 2017, pp. 216-221, doi: 10.1109/UEMCON.2017.8249029.

[9] Y. Wang, J. Zhang, X. Li, Z. Li and Y. Zhang, "A Secure Framework for Data Sharing in Private Blockchain-Based WBANs," in IEEE Access, vol. 8, pp. 153956-153968, 2020, doi: 10.1109/ACCESS.2020.3018119.

[10] M. Asam, T. Jamal, A. Ajaz, Z. Haider and S. Butt, "Security Issues in WBANs," arXiv preprint arXiv:1911.04330, 2019.

[11] C. A. Tavera, J. H. Ortiz, O. I. Khalaf, D. F. Saavedra and T. H. H. Aldhyani, "Wearable Wireless Body Area Networks for Medical Applications," in Computational and Mathematical Methods in Medicine, vol. 2021, Article ID 5574376, 2021, doi: 10.1155/2021/5574376.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY