World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Current security and privacy posture in wireless body area networks

Joshua Auko *

Jaramogi Oginga Odinga University of Science & Technology, Kenya.

World Journal of Advanced Research and Reviews, 2023, 18(03), 1185–1206

Publication history: Received on 15 May 2023; revised on 22 June 2023; accepted on 24 June 2023

Article DOI: https://doi.org/10.30574/wjarr.2023.18.3.1240

Abstract

Wireless Body Area Networks (WBANs) have emerged as a promising technology for remote health monitoring and healthcare applications. However, ensuring the security and privacy of sensitive health data in WBANs is crucial to foster user trust and prevent unauthorized access or data breaches. This paper provides an overview of the key challenges, techniques, and research gaps in WBAN security and privacy. The findings indicate that the challenges in WBAN security and privacy include resource constraints, compatibility issues, privacy concerns, dynamic network environments, security and usability trade-offs, emerging threat landscape, and user awareness and education. To address these challenges, various security techniques have been developed, such as authentication and authorization mechanisms, encryption, access control, secure communication protocols, intrusion detection systems, and privacy-preserving data handling techniques. Despite the progress made, there are research gaps that require further investigation. These research gaps include the development of secure and lightweight authentication mechanisms, privacy-preserving data analysis techniques, trust and security management frameworks, resilience to insider threats, security of data aggregation and fusion, user-centric security designs, and addressing legal and ethical considerations. Addressing these research gaps and challenges requires collaboration between researchers, device manufacturers, policymakers, and end-users. Ongoing research and innovation are necessary to develop robust security techniques, privacy-enhancing technologies, and user-friendly solutions tailored for WBANs. Additionally, compliance with privacy regulations, user education, and awareness are critical for responsible and ethical use of WBANs.

Keywords: Attacks; Threats; Security; WBAN; Vulnerabilities; Privacy

1. Introduction

Wireless Body Area Networks (WBANs) are a specialized form of wireless networks that involve the use of small, low-power sensors placed on or inside the human body to monitor various physiological parameters [1]-[4]. WBANs have gained significant attention in recent years due to their potential applications in healthcare, sports monitoring, and wellness tracking. According to [5], WBANs are specialized wireless networks that involve the use of small, low-power sensors placed on or inside the human body to monitor physiological parameters. These networks have gained significant attention in various fields, including healthcare, sports monitoring, and assisted living. They enable real-time, continuous monitoring of vital signs and other health-related data, providing valuable insights for medical professionals, athletes, and individuals seeking to enhance their well-being [6].

However, the widespread adoption of WBANs faces challenges that include power management, ensuring reliability and quality of service, data security and privacy, and interoperability [7]-[9]. Power-efficient designs and energy harvesting techniques are crucial for prolonging the battery life of sensors. Reliable communication and maintaining quality of service are essential for critical healthcare applications. Robust data security measures are necessary to protect sensitive health information, and standardization efforts are required for interoperability among different WBAN devices [10], [11]. Nonetheless, with ongoing advancements in technology, including miniaturization, artificial

*Corresponding author: Joshua Auko

intelligence, and edge computing, the future of WBANs holds great potential for personalized healthcare and real-time monitoring.

By focusing on WBAN security and privacy, we can enhance the trust and reliability of WBAN applications, enabling the widespread adoption of this technology in healthcare and improving patient care [12]. The paper provides insights into the importance of WBAN security and privacy, highlights the challenges, outlines existing techniques, and identifies areas for future research to promote secure and privacy-preserving WBAN deployments.

2. Architecture of Wireless Body Area Networks

The architecture of WBANs typically consists of body sensors, wireless communication, a central unit (such as a Personal Server or Base Station), and a remote server for data storage and analysis as shown in Figure 1. The body sensors collect data, which is wirelessly transmitted to the central unit and then forwarded to a remote server for further processing [13]-[15]. WBANs find applications in remote patient monitoring, sports and fitness monitoring, assisted living, and military scenarios, among others [16]. They facilitate early detection of health abnormalities, enable timely interventions, and enhance performance optimization.

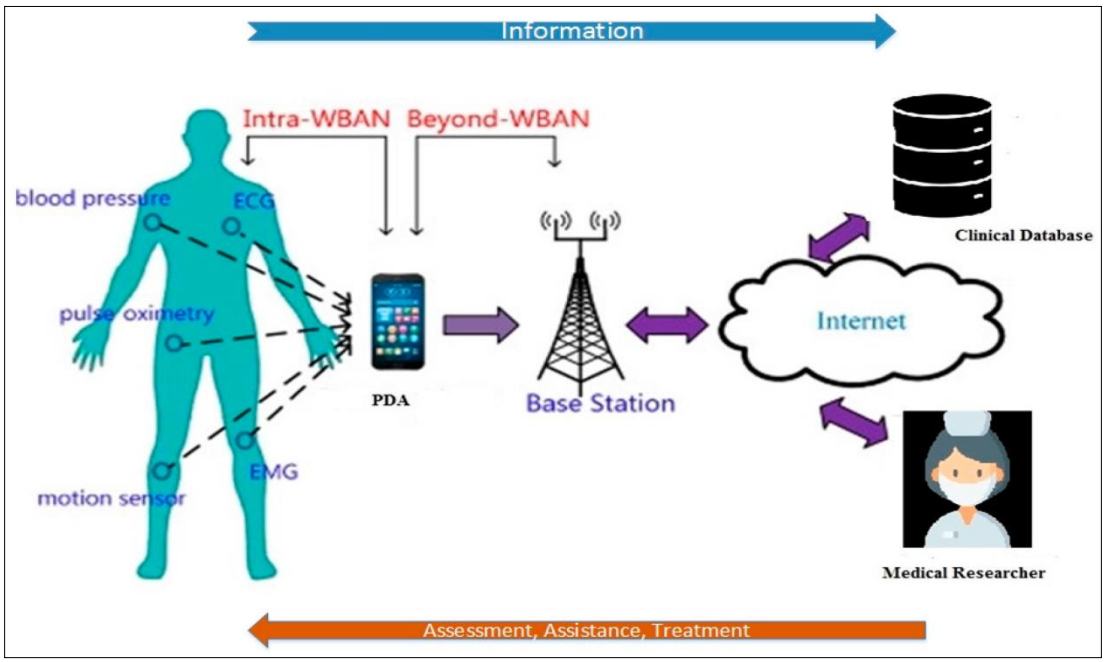

Figure 1 WBAN architecture

However, according to [17], a typical WBAN consists of the following components body sensors, wireless communication, personal server/base station and remote server. The body sensors are small, lightweight devices equipped with sensors that are either attached to the body or implanted inside it. These sensors can monitor vital signs, such as heart rate, blood pressure, body temperature, glucose levels, and even muscle activity. On the other hand, the body sensors communicate wirelessly with a central unit, referred to as the Personal Server (PS) or Base Station (BS). Communication can be achieved through short-range wireless technologies such as Bluetooth, Zigbee, or ultra-wideband (UWB) [18]. The PS or BS acts as a gateway between the body sensors and the external network. It collects the data from the sensors, performs processing if required, and transmits the data to a remote server or a healthcare professional's device for further analysis. On its part, the remote server is responsible for storing, processing, and analyzing the data received from multiple WBANs. It may utilize advanced algorithms and machine learning techniques [21] to derive meaningful insights and provide healthcare professionals with valuable information.

3. Applications of Wireless Body Area Networks

WBANs have a wide range of applications in various fields. Some of these applications include healthcare and remote patient monitoring, sports and fitness monitoring, Assisted Living and Ambient Assisted Living (AAL), military and tactical applications, wellness and lifestyle tracking, emergency medical services, research and clinical trials. According

to [22], WBANs play a crucial role in healthcare by enabling remote patient monitoring. They allow healthcare professionals to continuously monitor patients' vital signs and physiological parameters in real-time. WBANs can be used for monitoring patients with chronic conditions, post-surgical care, and elderly individuals. They facilitate early detection of health abnormalities, timely interventions, and reduced hospital visits. WBANs enable continuous and real-time monitoring of patients' vital signs, allowing healthcare providers to remotely monitor patients with chronic conditions or those recovering from surgeries [23]-[25]. This helps in early detection of abnormalities [26], timely interventions, and reduces hospital visits.

WBANs have also been extensively used in sports and fitness applications [26], [27]. Athletes and fitness enthusiasts can wear WBAN sensors to monitor their heart rate, body temperature, oxygen saturation, muscle activity, and other relevant parameters as shown in Figure 2. This data helps athletes optimize their performance, prevent injuries, and track their progress during training and competitions. WBANs are used for monitoring athletes' performance and health parameters during training or competitive events [28]-[30]. They provide valuable data on heart rate, body temperature, oxygen saturation, and activity levels, helping athletes optimize their performance and prevent injuries.

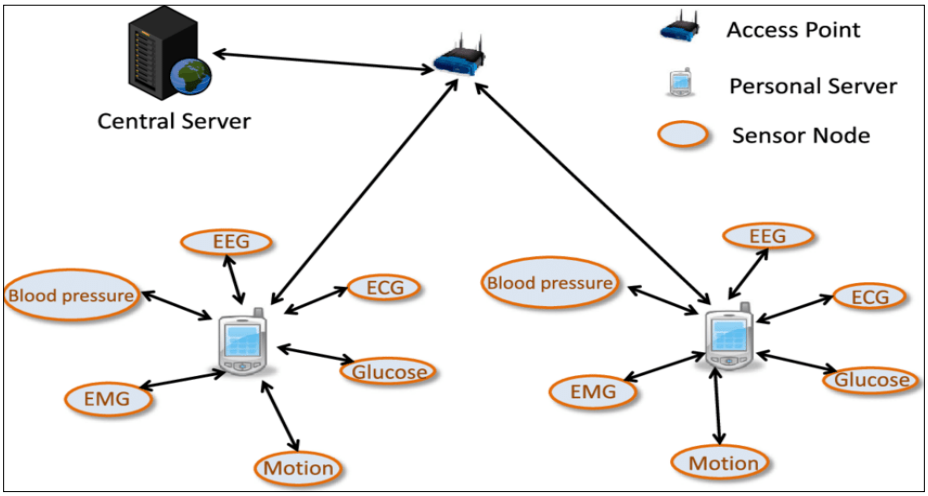

Figure 2 WBAN sensor communication

As explained in [31], WBANs are employed in assisted living environments for the elderly and individuals with disabilities. They provide continuous monitoring of vital signs, fall detection, activity tracking, and emergency alerts [32]. WBANs enhance the safety, well-being, and independence of individuals requiring assistance by enabling caregivers to remotely monitor their health status. WBANs can be used to monitor the health and well-being of elderly individuals or people with disabilities. They can detect falls, track activity levels, monitor vital signs, and trigger alerts in case of emergencies, ensuring timely assistance. In addition, WBANs find applications in military scenarios to monitor soldiers' health, performance, and well-being [33]-[36]. WBAN sensors can monitor vital signs, hydration levels, body temperature, and detect fatigue or stress. This data helps military personnel optimize their performance, prevent injuries, and ensure the well-being of soldiers in challenging environments. WBANs find applications in military scenarios where soldiers' health and performance need to be monitored continuously. It helps in detecting fatigue, heat stress, and injuries, thereby improving soldier safety and performance.

According to [37], WBANs have been used for general wellness tracking and lifestyle monitoring. Individuals can wear WBAN sensors to track their daily activity levels, sleep patterns, stress levels, and other relevant parameters. This data provides insights into their overall well-being, helps in making informed lifestyle choices, and promotes a healthier lifestyle. In addition, WBANs can be utilized in emergency medical services to provide immediate assistance and accurate assessment of patients' conditions. WBAN sensors can transmit vital signs and relevant health data [38] to emergency responders, enabling them to provide timely and appropriate medical interventions. As discussed in [39], WBANs are valuable tools for researchers and clinical trials. They enable the collection of continuous and real-time data from participants, which can be used for medical research, drug efficacy studies, and the development of personalized healthcare approaches [40]-[42].

These are just a few examples of the diverse applications of WBANs. With ongoing advancements in technology and increasing integration of WBANs into healthcare and other fields, their potential for improving monitoring, healthcare delivery, and overall well-being is continuously expanding.

4. Vulnerabilities in Wireless Body Area Networks

Wireless Body Area Networks (WBANs) are susceptible to various vulnerabilities that can be exploited by attackers [43]. Understanding these vulnerabilities is essential for developing effective security measures. Table 1 presents some of the most common vulnerabilities in WBANs.

Table 1 Common vulnerabilities in WBANs

Vulnerability	Explanation
Weak authentication and authorization	Weak authentication mechanisms or improper authorization practices can expose WBANs to unauthorized access [44]-[47]. If attackers can bypass or crack passwords, PINs, or other authentication methods, they can gain unauthorized control over WBAN devices or access sensitive data [48]. It is crucial to implement strong authentication protocols, such as two-factor authentication or biometric authentication, and enforce proper authorization controls.
Lack of encryption	Without proper encryption, data transmitted over the wireless communication channels of WBANs can be intercepted and accessed by unauthorized individuals [49]-[53]. This puts sensitive health data at risk of exposure. Implementing strong encryption algorithms, such as AES, to protect data in transit is necessary to prevent eavesdropping and data breaches.
Insecure wireless communication	The wireless communication protocols used in WBANs, such as Bluetooth or Zigbee, can have vulnerabilities that attackers can exploit. Weak encryption schemes, lack of mutual authentication, or outdated protocols can be targeted [54]-[58]. It is important to keep the wireless communication protocols up to date, follow best practices for secure configurations, and implement secure pairing mechanisms.
Physical access to devices	WBAN devices are vulnerable to physical attacks when they are unattended or easily accessible [59]. Attackers can tamper with the devices, extract sensitive data, or inject malicious code. Implementing physical security measures such as tamper-resistant packaging, secure device placement, and access control to WBAN infrastructure can mitigate these risks [60], [61].
Insufficient software security	Inadequate software security practices can leave WBAN devices vulnerable to exploitation [62]. Outdated firmware, lack of software updates, and unpatched vulnerabilities can be exploited by attackers [63]. Regular software updates, vulnerability assessments, and secure coding practices are crucial to minimize software-related vulnerabilities.
Privacy concerns	WBANs collect sensitive health data, and improper handling of this data can lead to privacy breaches. Insufficient data anonymization, inadequate consent mechanisms, or unauthorized data sharing can compromise the privacy of individuals [64]-[68]. It is essential to implement strict privacy policies, ensure data anonymization, and obtain informed consent from users.
Resource constraints	WBAN devices are often resource-constrained due to their small size and limited power. This constraint can make it challenging to implement robust security measures [69]-[73]. Attackers may exploit these limitations to launch attacks or compromise the functionality of the devices. Implementing lightweight security protocols, efficient cryptographic algorithms, and energy-efficient security mechanisms can help address these vulnerabilities.

Addressing these vulnerabilities requires a holistic approach to WBAN security. It involves implementing strong authentication and encryption mechanisms, conducting regular security audits, maintaining up-to-date firmware, educating users about security best practices, and adopting privacy-aware policies. Additionally, continuous research and development are necessary to address emerging vulnerabilities and threats in WBANs.

5. Security and threats Issues

WBANs face several security attacks and threats that need to be addressed to ensure the privacy, integrity, and availability of sensitive data [74]-[78]. Some common security attacks and threats in WBANs include eavesdropping, data tampering, unauthorized access, Denial of Service (DoS), Physical Attacks, and malicious software.

Eavesdropping refers to the unauthorized interception and monitoring of wireless communications between WBAN devices [79], [80]. Attackers can attempt to capture and analyze the transmitted data, which may include sensitive health information. Encryption techniques such as AES or TLS can help protect against eavesdropping by ensuring that the data is transmitted in an encrypted form [81]-[83]. On the other hand, data tampering involves unauthorized modification, deletion, or insertion of data within the WBAN network [84]. Attackers can intercept and alter the transmitted data, leading to incorrect diagnoses, false alarms, or wrong medication decisions. Techniques like data integrity checks, digital signatures, and hash functions can help detect and prevent data tampering [85]-[88]. However, anauthorized access refers to the attempt by an unauthorized entity to gain access to the WBAN network or its resources [89], [90]. Attackers may try to exploit vulnerabilities in the network infrastructure or compromise weak authentication mechanisms to gain unauthorized access. Strong authentication protocols, access control mechanisms, and secure communication channels can help mitigate the risk of unauthorized access [91]-[93].

A DoS attack aims to disrupt or disable the operation of the WBAN network by overwhelming it with a flood of malicious traffic or resource depletion as shown in Figure 3. This can lead to the unavailability of vital services, delayed data transmission, or failure to receive critical alerts [94], [95]. Implementing intrusion detection systems, traffic filtering, and rate limiting techniques can help detect and mitigate DoS attacks [96]-[98].

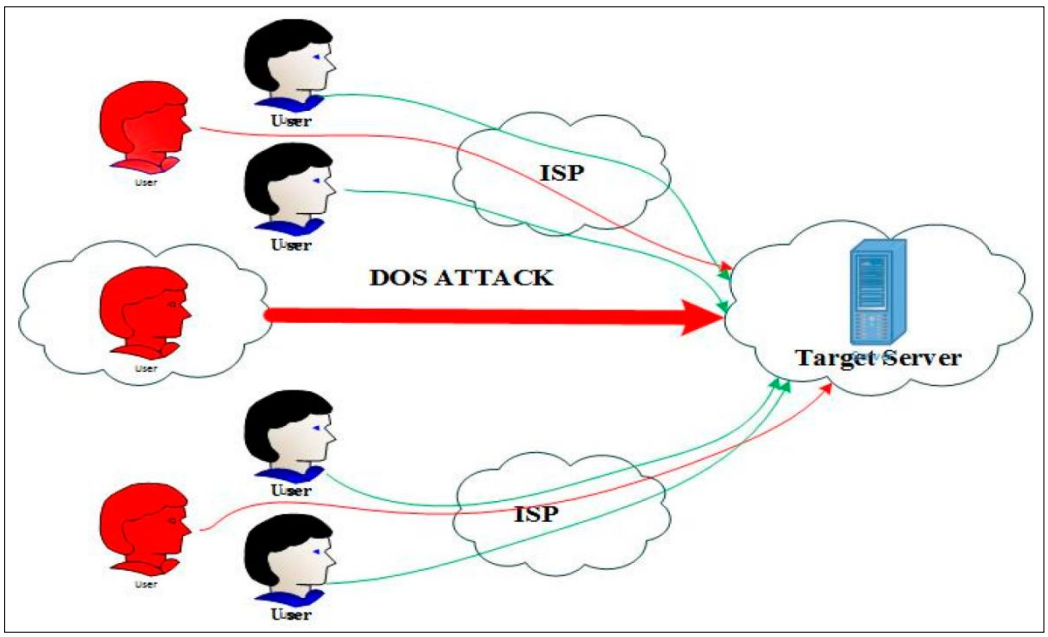

Figure 3 DoS attack in WBAN

On the other hand, physical attacks involve physical tampering or unauthorized access to WBAN devices or infrastructure [99]. Attackers may attempt to tamper with sensors, extract sensitive information, or interfere with the functionality of the network. Physical security measures, such as secure device placement, tamper-resistant packaging, and access control to the WBAN infrastructure, are essential to mitigate physical attacks [100]-[103]. However, malicious software pose a significant threat to WBANs [104]. Malicious software can infect WBAN devices, compromising their functionality, stealing sensitive data, or facilitating unauthorized access. Implementing robust security measures, including regularly updating firmware, using antivirus software, and validating software integrity, can help prevent malware attacks [105]-[108].

To address these security attacks and threats, a comprehensive security framework should be adopted for WBANs. It should include measures such as encryption, authentication, access control, intrusion detection systems, secure communication protocols, regular software updates, and user awareness and education. Ongoing monitoring, vulnerability assessments, and adherence to security best practices are also crucial to ensure the security and privacy of WBANs.

6. Security techniques for Wireless Body Area Networks

To enhance the security of Wireless Body Area Networks (WBANs), several techniques and practices can be implemented. These security techniques aim to protect sensitive data, ensure privacy, and prevent unauthorized access. Some key security techniques for WBANs include authentication and authorization, encryption, access control, secure communication protocols, Intrusion Detection and Prevention Systems (IDPS), secure software development lifecycle, privacy protection, physical security measures, user education and awareness. Figure 4 shows the implementation of some of these security mechanisms.

As explained in [109], strong authentication mechanisms should be employed to verify the identity of WBAN devices and users. This includes techniques such as password-based authentication, biometric authentication, or two-factor authentication. Authorization controls should be implemented to ensure that only authorized users can access and interact with the WBAN [110]-[113].

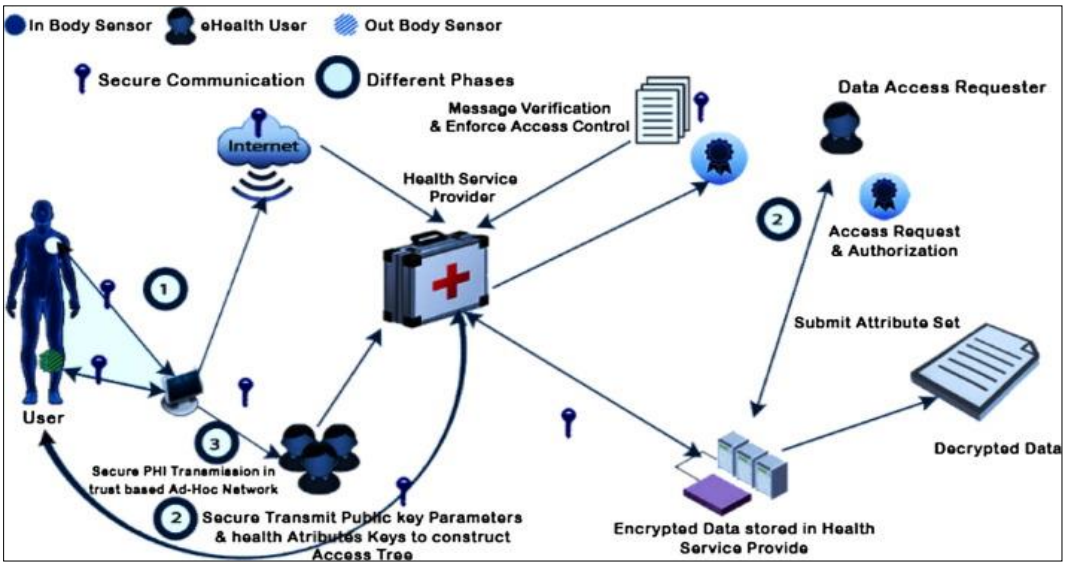

Figure 4 WBAN security mechanisms

According to [114], encryption is essential for protecting the confidentiality and integrity of data transmitted over WBANs. Data encryption techniques, such as Advanced Encryption Standard (AES), should be used to encrypt sensitive data both in transit and at rest. This prevents unauthorized access and eavesdropping of data [115]-[118]. On the other hand, access control mechanisms play a crucial role in preventing unauthorized access to WBANs. Role-based access control (RBAC) or attribute-based access control (ABAC) can be implemented to ensure that only authorized users can access specific data or perform certain operations within the WBAN [119]-[123]. Access control policies should be regularly reviewed and updated as needed. As explained in [124], secure communication protocols, such as Transport Layer Security (TLS) or Secure Shell (SSH), should be utilized to establish secure and encrypted communication channels between WBAN devices and other network components as shown in Figure 5. These protocols provide confidentiality, integrity, and authentication of the communication channels [125]-[128]. On the other hand, IDPS can be deployed within the WBAN to monitor network traffic, detect suspicious activities, and prevent or mitigate potential attacks [129]-[133]. Intrusion detection techniques, including anomaly detection or signature-based detection, can be used to identify potential security breaches and trigger appropriate responses [134], [135].

According to [136], secure software development practices should be followed during the development of WBAN devices and applications. This includes incorporating security considerations from the initial design phase, conducting security testing and code reviews, and ensuring timely software updates and patches to address vulnerabilities [137]-[138]. To protect the privacy of users, privacy-aware practices should be implemented [139]. This includes data anonymization techniques, informed consent processes, and adherence to privacy regulations and standards [140]-[143]. Minimizing the collection of personally identifiable information (PII) and implementing privacy-preserving data handling practices are essential. As explained in [144], physical security measures are crucial to protect WBAN devices from physical tampering or unauthorized access. This includes secure packaging, tamper-evident mechanisms, and physical access controls to ensure the physical integrity and confidentiality of the WBAN devices [145]-[148]. In addition, users of WBANs should be educated about the importance of security practices and potential risks. This

includes promoting strong password management, recognizing phishing attempts, and providing guidelines on secure usage and handling of WBAN devices [149]-[153].

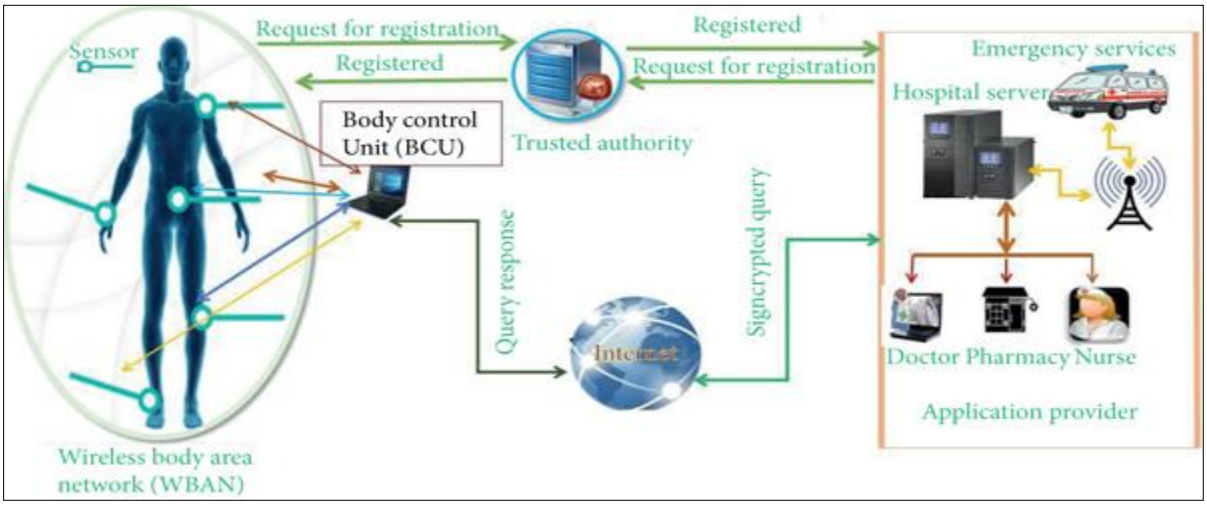

Figure 5 Secure communication in WBAN

Implementing a combination of these security techniques can significantly enhance the security posture of WBANs, safeguard sensitive data, and ensure the privacy and integrity of the network. It is important to regularly assess and update the security measures as new threats and vulnerabilities emerge.

7. Challenges of current security techniques for WBANs

While security techniques for Wireless Body Area Networks (WBANs) are designed to protect the network and its users, there are still several challenges that need to be addressed. Table 2 presents some of these challenges.

Table 2 Challenges of current WBANs security solutions

Challenge (s)	Discussion
Security and usability trade-off	There is often a trade-off between security and usability in WBANs. Strong security measures, such as complex authentication processes or frequent re-authentication, can negatively impact the usability and user experience [154]-[158]. Striking the right balance between security and usability is crucial to ensure that security measures do not hinder the practicality and acceptance of WBANs.
Privacy concerns	WBANs deal with sensitive health data, raising privacy concerns for users [159], [160]. Ensuring the privacy of health data while providing necessary access for authorized entities is a challenging task. Implementing effective privacy-preserving techniques, such as data anonymization and secure data storage and transmission, requires careful consideration and adherence to privacy regulations and standards [161]-[163].
Emerging threat landscape	The security landscape is continuously evolving, with new threats and attack vectors emerging regularly [164]. Hackers and attackers are constantly looking for vulnerabilities to exploit. Keeping up with the evolving threat landscape and promptly addressing new security challenges requires ongoing research and development efforts [165]-[168].
Resource constraints	WBAN devices often have limited resources in terms of processing power, memory, and energy. This poses challenges for implementing robust security techniques that require computational overhead or energy-intensive operations [169]-[174]. Security protocols and algorithms need to be optimized for resource-constrained WBAN devices to ensure efficient operation without draining the device's battery quickly.
Compatibility and interoperability	WBANs may consist of devices from different manufacturers, using different protocols and standards. Achieving compatibility and interoperability among these devices can be

	challenging, as security mechanisms and protocols need to be standardized and adopted uniformly [175]-[178]. Lack of standardization can lead to security vulnerabilities and difficulties in integrating devices into a secure WBAN environment.
User awareness and education	The success of security techniques in WBANs depends on user awareness and education [179]. Users need to be informed about potential security risks, trained in secure usage practices, and encouraged to follow best practices. Lack of user awareness and adherence to security guidelines can undermine the effectiveness of implemented security techniques [180]-[182].
Dynamic nature of WBANs	WBANs are dynamic in nature, with devices continuously joining or leaving the network. This dynamic environment introduces challenges in maintaining secure communication channels and managing authentication and authorization [183]-[188]. Security techniques need to be flexible and adaptable to handle the changing network topology and device configurations effectively.

Addressing these challenges requires a comprehensive approach involving collaboration among stakeholders, including device manufacturers, researchers, policymakers, and users. Continuous research, development, and standardization efforts are necessary to enhance the security techniques for WBANs and ensure the privacy and integrity of the network and its data [189]-[193].

8. Future Prospects for WBANs

The future of WBANs holds great potential for advancements and innovations. Some areas that researchers and technologists are exploring include the following:

Miniaturization and Wearability: Advances in nanotechnology and flexible electronics are driving the development of even smaller, more comfortable, and unobtrusive sensors that can be seamlessly integrated into clothing or worn as wearable accessories [194]-[197].
Artificial Intelligence and Machine Learning: Leveraging AI and machine learning techniques can enable more accurate analysis and interpretation of data collected from WBANs [198]-[202]. It can help in early detection of anomalies, personalized healthcare recommendations, and predictive analytics.

Edge Computing: By performing data processing and analysis at the edge of the network, closer to the WBAN sensors, edge computing reduces latency, enhances real-time decision-making, and minimizes the need for constant data transmission to remote servers [203]-[207].

Wireless Power Transfer: Research on wireless power transfer technologies, such as inductive charging or radio frequency energy harvesting, could eliminate the need for frequent battery replacements, thus improving the overall usability and maintenance of WBANs [208]-[212].

Evidently, Wireless Body Area Networks (WBANs) have the potential to revolutionize healthcare and monitoring applications by providing continuous, personalized, and non-intrusive monitoring of physiological parameters. While there are challenges to overcome, ongoing advancements and research in areas like power management, data security, and AI-driven analytics are paving the way for a promising future for WBANs [213]-[217].

9. Research gaps

While significant progress has been made in the security and privacy of Wireless Body Area Networks (WBANs), several research gaps still exist. These research gaps highlight areas where further investigation and development are needed to address the evolving challenges and requirements of WBAN security and privacy. Some key research gaps include:

9.1. Secure and Lightweight Authentication

Developing secure and lightweight authentication mechanisms tailored specifically for resource-constrained WBAN devices remains a challenge. Research is needed to explore novel authentication techniques that provide a balance between security, usability, and efficiency in the context of WBANs [218]-[223]. This includes exploring biometric authentication, context-aware authentication, and multi-factor authentication methods suitable for WBANs.

9.2. Privacy-Preserving Data Analysis

While ensuring privacy is crucial in WBANs, there is a need for effective techniques to perform privacy-preserving data analysis. Research is required to develop privacy-enhancing technologies that enable accurate analysis of health data without compromising individual privacy [224]-[228]. Techniques such as secure multiparty computation, differential privacy, and homomorphic encryption can be explored to enable privacy-preserving data analysis in WBANs.

9.3. Trust and Security Management

Trust management in WBANs is crucial to establish secure communication and collaboration among devices and entities. Research is needed to develop robust trust management frameworks and mechanisms that can dynamically assess the trustworthiness of WBAN devices and facilitate secure interactions [229]-[233]. This includes techniques for trust establishment, trust evaluation, and trust-based access control in dynamic WBAN environments.

9.4. Resilience to Insider Threats

Insider threats, where authorized users with malicious intent exploit their privileges, are a significant concern in WBANs. Research is required to develop techniques that can detect and mitigate insider threats, such as unauthorized access or data leakage, within WBANs [234]-[239]. This includes anomaly detection, behavior analysis, and secure user management mechanisms to identify and respond to insider threats effectively.

9.5. Security of WBAN Data Aggregation and Fusion

In WBANs, data from multiple sensors and devices are often aggregated and fused to provide a comprehensive view of an individual's health [240]-[242]. However, ensuring the security and integrity of the aggregated data poses challenges. Research is needed to develop secure data aggregation and fusion techniques that protect against data tampering, false data injection, and privacy breaches during the data fusion process [243].

9.6. Usability and User-Centric Security

Enhancing the usability of security mechanisms in WBANs is crucial for user acceptance and adherence to security practices [244]-[248]. Research is required to develop user-centric security designs and techniques that are intuitive, easy to use, and seamlessly integrated into the user's daily life. This includes user-friendly authentication mechanisms, effective security education, and user-aware privacy controls.

9.7. Legal and Ethical Considerations

As WBANs collect and transmit sensitive health data, there are legal and ethical considerations surrounding data ownership, consent, and accountability [249], [250]. Research is needed to explore legal frameworks, regulations, and ethical guidelines that address these considerations and ensure the responsible and ethical use of WBAN data.

Addressing these research gaps will contribute to the development of robust security and privacy solutions for WBANs, enabling their widespread adoption in healthcare and other domains [251]-[253]. Continued collaboration between academia, industry, policymakers, and end-users is essential to drive research and innovation in WBAN security and privacy.

10. Conclusion

The security and privacy of WBANs are of paramount importance to ensure the confidentiality, integrity, and availability of sensitive health data. Over the years, significant progress has been made in developing security techniques and privacy-preserving measures for WBANs. However, challenges and research gaps still exist that need to be addressed to enhance the overall security and privacy posture of WBANs. It has been shown that the challenges in WBAN security and privacy include resource constraints, compatibility issues, privacy concerns, dynamic network environments, security and usability trade-offs, emerging threat landscape, and user awareness and education. These challenges call for further research and development efforts to overcome the limitations and design effective security and privacy solutions tailored for WBANs. Research gaps in WBAN security and privacy include the development of secure and lightweight authentication mechanisms, privacy-preserving data analysis techniques, trust and security management frameworks, resilience to insider threats, security of data aggregation and fusion, user-centric security designs, and addressing legal and ethical considerations. Addressing these research gaps and challenges requires interdisciplinary collaboration among researchers, device manufacturers, policymakers, and end-users. Ongoing research and innovation are essential to develop robust security techniques, privacy-enhancing technologies, and user-friendly solutions for WBANs. Additionally, adherence to privacy regulations and standards, along with user education and awareness, are

critical to ensuring the responsible and ethical use of WBANs and protecting the privacy rights of individuals. By advancing the security and privacy of WBANs, we can unlock the full potential of these networks in transforming healthcare delivery, improving patient monitoring, and enabling innovative applications. The continuous focus on enhancing WBAN security and privacy will contribute to building trust, fostering widespread adoption, and realizing the benefits of this transformative technology in improving human health and well-being.

Compliance with ethical standards

Acknowledgments

I would like to appreciate my colleagues who assisted me when writing this article.

References

[1] Attir A, Naït-Abdesselam F, Faraoun KM. Lightweight anonymous and mutual authentication scheme for wireless body area networks. Computer Networks. 2023 Apr 1;224:109625.

[2] Kiran MV, Nithya B. Stable and energy-efficient next-hop router selection (SE-NRS) for wireless body area networks. International Journal of Information Technology. 2023 Feb;15(2):1189-200.

[3] Mokhtar B, Kandas I, Gamal M, Omran N, Hassanin AH, Shehata N. Nano-Enriched Self-Powered Wireless Body Area Network for Sustainable Health Monitoring Services. Sensors. 2023 Feb 27;23(5):2633.

[4] Chen Y, Han S, Chen G, Yin J, Wang KN, Cao J. A deep reinforcement learning-based wireless body area network offloading optimization strategy for healthcare services. Health Information Science and Systems. 2023 Jan 28;11(1):8.

[5] Alqahtani AS, Changalasetty SB, Parthasarathy P, Thota LS, Mubarakali A. Effective spectrum sensing using cognitive radios in 5G and wireless body area networks. Computers and Electrical Engineering. 2023 Jan 1;105:108493.

[6] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1;142:103117.

[7] Liu Q, Mkongwa KG, Zhang C. Performance issues in wireless body area networks for the healthcare application: A survey and future prospects. SN Applied Sciences. 2021 Feb;3:1-9.

[8] Dhanvijay MM, Patil SC. Internet of Things: A survey of enabling technologies in healthcare and its applications. Computer Networks. 2019 Apr 22;153:113-31.

[9] Karunarathne SM, Saxena N, Khan MK. Security and privacy in IoT smart healthcare. IEEE Internet Computing. 2021 Jan 18;25(4):37-48.

[10] Abbas A, Khan SU. E-health cloud: privacy concerns and mitigation strategies. Medical Data Privacy Handbook. 2015:389-421.

[11] Hussien, Z. A., Abdulmalik, H. A., Hussain, M. A., Nyangaresi, V. O., Ma, J., Abduljabbar, Z. A., & Abduljaleel, I. Q. (2023). Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences, 13(2), 691.

[12] Mehmood G, Khan MZ, Waheed A, Zareei M, Mohamed EM. A trust-based energy-efficient and reliable communication scheme (trust-based ERCS) for remote patient monitoring in wireless body area networks. IEEE Access. 2020 Jul 6;8:131397-413.

[13] Al Barazanchi I, Hashim W, Alkahtani AA, Abbas HH, Abdulshaheed HR. Overview of WBAN from literature survey to application implementation. In2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI) 2021 Oct 20 (pp. 16-21). IEEE.

[14] Pramanik PK, Nayyar A, Pareek G. WBAN: Driving e-healthcare beyond telemedicine to remote health monitoring: Architecture and protocols. InTelemedicine technologies 2019 Jan 1 (pp. 89-119). Academic Press.

[15] Khssibi S, Van Den Bossche A, Idoudi H, Azouz Saidane L, Val T. Enhancement of the traffic differentiation architecture for WBAN based on IEEE 802.15. 4. Wireless Personal Communications. 2018 Aug;101:1519-37.

[16] Nyangaresi, V. O., & Ma, J. (2022, June). A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In 2022 IEEE World Conference on Applied Intelligence and Computing (AIC) (pp. 416-422). IEEE.

[17] Kong D, Dong H, Li H, Zhang B. Research on Data Security of Wireless Body Area Network. In2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE) 2020 Jun 12 (pp. 132-135). IEEE.

[18] Lin CY, Liang CP, Tarng JH, Chung SJ. Compact composite noise-reduction LNA for UWB WPAN and WBAN applications. IET Microwaves, Antennas & Propagation. 2018 May;12(6):903-8.

[19] Niu Y, Nazeri S, Hashim W, Alkahtani AA, Abdulshaheed HR. A survey on short-range WBAN communication; technical overview of several standard wireless technologies. Periodicals of Engineering and Natural Sciences. 2021 Nov 3;9(4):877-85.

[20] Al-Barazanchi I, Abdulshaheed HR, Sidek MS. A Survey: Issues and challenges of communication technologies in WBAN. Sustainable Engineering and Innovation. 2019 Dec 30;1(2):84-97.

[21] Ghrabat MJ, Hussien ZA, Khalefa MS, Abduljabba ZA, Nyangaresi VO, Al Sibahee MA, Abood EW. Fully automated model on breast cancer classification using deep learning classifiers. Indonesian Journal of Electrical Engineering and Computer Science. 2022 Oct;28(1):183-91.

[22] Kaur H, Jameel R, Alam MA, Alankar B, Chang V. Securing and managing healthcare data generated by intelligent blockchain systems on cloud networks through DNA cryptography. Journal of Enterprise Information Management. 2023 Mar 9.

[23] Pirmoradian F, Safkhani M, Dakhilalian SM. ECCPWS: An ECC-based protocol for WBAN systems. Computer Networks. 2023 Apr 1;224:109598.

[24] Dang VA, Vu Khanh Q, Nguyen VH, Nguyen T, Nguyen DC. Intelligent Healthcare: Integration of Emerging Technologies and Internet of Things for Humanity. Sensors. 2023 Apr 22;23(9):4200.

[25] Memon S, Wang J, Ahmed A, Rajab A, Al Reshan MS, Shaikh A, Rajput MA. Enhanced Probabilistic Route Stability (EPRS) Protocol for Healthcare Applications of WBAN. IEEE Access. 2023 Jan 10;11:4466-77.

[26] Nyangaresi VO, El-Omari NK, Nyakina JN. Efficient Feature Selection and ML Algorithm for Accurate Diagnostics. Journal of Computer Science Research. 2022 Jan 25;4(1):10-9.

[27] Asif A, Sumra IA. Applications of wireless body area network (wban): A survey. Engineering science and technology international research journal. 2017 Apr:64-71.

[28] Li R, Lai DT, Lee W. A survey on biofeedback and actuation in wireless body area networks (WBANs). IEEE reviews in biomedical engineering. 2017 Aug 10;10:162-73.

[29] Poongodi T, Rathee A, Indrakumari R, Suresh P. IoT sensing capabilities: Sensor deployment and node discovery, wearable sensors, wireless body area network (WBAN), data acquisition. Principles of internet of things (IoT) ecosystem: Insight paradigm. 2020:127-51.

[30] Al-Turjman F, Baali I. Machine learning for wearable IoT-based applications: A survey. Transactions on Emerging Telecommunications Technologies. 2022 Aug;33(8):e3635.

[31] Isravel DP, Silas S, Rajsingh EB. SDN-based traffic management for personalized ambient assisted living healthcare system. InIntelligence in Big Data Technologies—Beyond the Hype: Proceedings of ICBDCC 2019 2021 (pp. 379-388). Springer Singapore.

[32] Al Sibahee, M. A., Nyangaresi, V. O., Ma, J., & Abduljabbar, Z. A. (2022, July). Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. In IoT as a Service: 7th EAI International Conference, IoTaaS 2021, Sydney, Australia, December 13–14, 2021, Proceedings (pp. 3-18). Cham: Springer International Publishing.

[33] Indrakumari R, Pradhan N, Sagar S, Singh K. IoT for Health, Safety, Well-Being, Inclusion, and Active Aging. Cognitive Intelligence and Big Data in Healthcare. 2022 Sep 8:97-119.

[34] Rameshkumar C, Ganeshkumar T. A Novel of Survey: In Healthcare System for Wireless Body-Area Network. InApplications of Computational Methods in Manufacturing and Product Design: Select Proceedings of IPDIMS 2020 2022 May 4 (pp. 591-609). Singapore: Springer Nature Singapore.

[35] Jose JM, Jose JV, Vijaykumar Mahamuni C. Multi-Biosensor based Wireless Body Area Networks (WBAN) for Critical Health Monitoring of Patients in Mental Health Care Centers: An Interdisciplinary Study. International Journal of Research in Engineering, Science and Management. 2020 Aug 7;3.

[36] Demrozi F, Turetta C, Kindt PH, Chiarani F, Bacchin R, Valè N, Pascucci F, Cesari P, Smania N, Tamburin S, Pravadelli G. A Low-Cost Wireless Body Area Network for Human Activity Recognition in Healthy Life and Medical Applications. IEEE Transactions on Emerging Topics in Computing. 2023 May 12.

[37] Petäjäjärvi J, Mikhaylov K, Yasmin R, Hämäläinen M, Iinatti J. Evaluation of LoRa LPWAN technology for indoor remote health and wellbeing monitoring. International Journal of Wireless Information Networks. 2017 Jun;24:153-65.

[38] Yenurkar GK, Mal S, Nyangaresi VO, Hedau A, Hatwar P, Rajurkar S, Khobragade J. Multifactor data analysis to forecast an individual's severity over novel COVID-19 pandemic using extreme gradient boosting and random forest classifier algorithms. Engineering Reports. 2023:e12678.

[39] Khalilian R, Rezai A. Wireless Body Area Network (WBAN) Applications Necessity in Real Time Healthcare. In2022 IEEE Integrated STEM Education Conference (ISEC) 2022 Mar 26 (pp. 371-374). IEEE.

[40] Mohammed MS, Sendra S, Lloret J, Bosch I. Systems and WBANs for controlling obesity. Journal of healthcare engineering. 2018 Feb 1;2018.

[41] Qu Y, Zheng G, Ma H, Wang X, Ji B, Wu H. A survey of routing protocols in WBAN for healthcare applications. Sensors. 2019 Apr 5;19(7):1638.

[42] El-Bendary MA, Kasban H, Haggag A, El-Tokhy MA. Investigating of nodes and personal authentications utilizing multimodal biometrics for medical application of WBANs security. Multimedia Tools and Applications. 2020 Sep;79:24507-35.

[43] Nyangaresi, V. O. (2023). Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. In Computer Vision and Robotics: Proceedings of CVR 2022 (pp. 503-516). Singapore: Springer Nature Singapore.

[44] Almuhaideb AM. Re-AuTh: Lightweight re-authentication with practical key management for wireless body area networks. Arabian Journal for Science and Engineering. 2021 Sep;46(9):8189-202.

[45] 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.

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

[47] Shrivastava V, Namdev M. A Review on Security and Privacy Issues in Wireless Body Area Networks for Healthcare Applications. IJO-SCIENCE. 2019 Nov;5(11).

[48] Al-Chaab W, Abduljabbar ZA, Abood EW, Nyangaresi VO, Mohammed HM, Ma J. Secure and Low-Complexity Medical Image Exchange Based on Compressive Sensing and LSB Audio Steganography. Informatica. 2023 May 31;47(6).

[49] Das D, Maity S, Chatterjee B, Sen S. Enabling covert body area network using electro-quasistatic human body communication. Scientific reports. 2019 Mar 11;9(1):4160.

[50] Peng H, Tian Y, Kurths J, Li L, Yang Y, Wang D. Secure and energy-efficient data transmission system based on chaotic compressive sensing in body-to-body networks. IEEE transactions on biomedical circuits and systems. 2017 May 19;11(3):558-73.

[51] Umar M, Wu Z, Liao X. Mutual authentication in body area networks using signal propagation characteristics. IEEE Access. 2020 Apr 2;8:66411-22.

[52] Vyas A, Pal S. Preventing security and privacy attacks in WBANs. Handbook of Computer Networks and Cyber Security: Principles and Paradigms. 2020:201-25.

[53] Nyangaresi, V. O., & Moundounga, A. R. A. (2021, September). Secure data exchange scheme for smart grids. In 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) (pp. 312-316). IEEE.

[54] Lonzetta AM, Cope P, Campbell J, Mohd BJ, Hayajneh T. Security vulnerabilities in Bluetooth technology as used in IoT. Journal of Sensor and Actuator Networks. 2018 Jul 19;7(3):28.

[55] Kang JJ. Systematic analysis of security implementation for internet of health things in mobile health networks. Data Science in Cybersecurity and Cyberthreat Intelligence. 2020:87-113.

[56] Yaqoob T, Abbas H, Atiquzzaman M. Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review. IEEE Communications Surveys & Tutorials. 2019 Apr 30;21(4):3723-68.

[57] Brito C, Pinto L, Marinho V, Paiva S, Pinto P. A review on recent advances in implanted medical devices security. In2021 16th Iberian Conference on Information Systems and Technologies (CISTI) 2021 Jun 23 (pp. 1-6). IEEE.

[58] Abduljabbar, Z. A., Omollo Nyangaresi, V., Al Sibahee, M. A., Ghrabat, M. J. J., Ma, J., Qays Abduljaleel, I., & Aldarwish, A. J. (2022). Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks, 11(3), 55.

[59] Ning H, Farha F, Ullah A, Mao L. Physical unclonable function: Architectures, applications and challenges for dependable security. IET Circuits, Devices & Systems. 2020 Jul;14(4):407-24.

[60] Khan S, Iqbal W, Waheed A, Mehmood G, Khan S, Zareei M, Biswal RR. An efficient and secure revocation-enabled attribute-based access control for eHealth in smart society. Sensors. 2022 Jan;22(1):336.

[61] Arfaoui A, Boudia OR, Kribeche A, Senouci SM, Hamdi M. Context-aware access control and anonymous authentication in WBAN. Computers & Security. 2020 Jan 1;88:101496.

[62] Paul PC, Loane J, McCaffery F, Regan G. Towards Design and Development of a Data Security and Privacy Risk Management Framework for WBAN Based Healthcare Applications. Applied System Innovation. 2021 Oct 12;4(4):76.

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

[64] Punj R, Kumar R. Technological aspects of WBANs for health monitoring: a comprehensive review. Wireless Networks. 2019 Apr 15;25:1125-57.

[65] Taleb H, Nasser A, Andrieux G, Charara N, Motta Cruz E. Wireless technologies, medical applications and future challenges in WBAN: A survey. Wireless Networks. 2021 Nov;27:5271-95.

[66] Malik MS, Ahmed M, Abdullah T, Kousar N, Shumaila MN, Awais M. Wireless body area network security and privacy issue in e-healthcare. International Journal of Advanced Computer Science and Applications. 2018;9(4).

[67] Guo C, Tian P, Choo KK. Enabling privacy-assured fog-based data aggregation in E-healthcare systems. IEEE Transactions on Industrial Informatics. 2020 May 19;17(3):1948-57.

[68] Abduljabbar, Z. A., Nyangaresi, V. O., Ma, J., Al Sibahee, M. A., Khalefa, M. S., & Honi, D. G. (2022, September). MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones. In Future Access Enablers for Ubiquitous and Intelligent Infrastructures: 6th EAI International Conference, FABULOUS 2022, Virtual Event, May 4, 2022, Proceedings (pp. 16-36). Cham: Springer International Publishing.

[69] Alam MM, Hamida EB, Berder O, Menard D, Sentieys O. A heuristic self-adaptive medium access control for resource-constrained WBAN systems. IEEE Access. 2016;4:1287-300.

[70] Prasitsupparote A, Watanabe Y, Sakamoto J, Shikata J, Matsumoto T. Implementation and analysis of fully homomorphic encryption in resource-constrained devices. International Journal of Digital Information and Wireless Communications. 2018 Oct 1;8(4):288-304.

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

[72] 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.

[73] Nyangaresi, V. O., & Ogundoyin, S. O. (2021, October). Certificate based authentication scheme for smart homes. In 2021 3rd Global Power, Energy and Communication Conference (GPECOM) (pp. 202-207). IEEE.

[74] Gaikwad VD, Ananthakumaran S. A Review: Security and Privacy for Health Care Application in Wireless Body Area Networks. Wireless Personal Communications. 2023 Mar 21:1-9.

[75] Sowmiya L, Rajasekaran AS, Suganyadevi S, Sureshkumar S, Subramaniam G, Jaazieliah R. A Secure Authenticated Message Transfer in Healthcare Application. In2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS) 2023 Feb 24 (pp. 1-6). IEEE.

[76] Peng S, Tang X, Xiong L, Zhu H. LGAAFS--A Lightweight Group Anonymous mutual Authentication and Forward Security scheme for wireless body area networks.

[77] Saeed MM, Ali ES, Saeed RA. Data-Driven Techniques and Security Issues in Wireless Networks. Data-Driven Intelligence in Wireless Networks: Concepts, Solutions, and Applications. 2023 Mar 27:107.

[78] Nyakomitta, P. S., Nyangaresi, V. O., & Ogara, S. O. (2021). Efficient authentication algorithm for secure remote access in wireless sensor networks. Journal of Computer Science Research, 3(4), 43-50.

[79] Jouini O, Sethom K. Physical layer security proposal for wireless body area networks. In2020 IEEE 5th Middle East and Africa Conference on Biomedical Engineering (MECBME) 2020 Oct 27 (pp. 1-5). IEEE.

[80] Mucchi L, Jayousi S, Martinelli A, Caputo S, Marcocci P. An overview of security threats, solutions and challenges in wbans for healthcare. In2019 13th International Symposium on Medical Information and Communication Technology (ISMICT) 2019 May 8 (pp. 1-6). IEEE.

[81] Berrahal S, Boudriga N. Toward secure and privacy-preserving WIBSN-based health monitoring applications. InWearable and Implantable Medical Devices 2020 Jan 1 (pp. 179-214). Academic Press.

[82] Papaioannou M, Karageorgou M, Mantas G, Sucasas V, Essop I, Rodriguez J, Lymberopoulos D. A survey on security threats and countermeasures in internet of medical things (IoMT). Transactions on Emerging Telecommunications Technologies. 2022 Jun;33(6):e4049.

[83] Nyangaresi, V. O., & Morsy, M. A. (2021, September). Towards privacy preservation in internet of drones. In 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) (pp. 306-311). IEEE.

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

[85] Arya KV, Gore R. Data security for WBAN in e-health IoT applications. InIntelligent data security solutions for e-health applications 2020 Jan 1 (pp. 205-218). Academic Press.

[86] 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.

[87] Guo R, Zhuang C, Shi H, Zhang Y, Zheng D. A lightweight verifiable outsourced decryption of attribute-based encryption scheme for blockchain-enabled wireless body area network in fog computing. International journal of distributed sensor networks. 2020 Feb;16(2):1550147720906796.

[88] Alsamhi, S. H., Shvetsov, A. V., Kumar, S., Shvetsova, S. V., Alhartomi, M. A., Hawbani, A., ... & Nyangaresi, V. O. (2022). UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones, 6(7), 154.

[89] Jahan M, Zohra FT, Parvez MK, Kabir U, Al Radi AM, Kabir S. An end-to-end authentication mechanism for wireless body area networks. Smart Health. 2023 May 27:100413.

[90] Jangir J, Tripathi K, Agarwal D, Jain A. Wireless Body Area Networks (WBANs)–Design Issues and Security Challenges. InImage Processing and Intelligent Computing Systems 2023 (pp. 235-244). CRC Press.

[91] Reshma G, Prasanna BT, Murthy HS, Murthy TS, Parthiban S, Sangeetha M. Privacy-aware access control (PAAC)-based biometric authentication protocol (Bap) for mobile edge computing environment. Soft Computing. 2023 Apr 28:1-20.

[92] Hasan MK, Habib AA, Shukur Z, Ibrahim F, Islam S, Razzaque MA. Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. Journal of Network and Computer Applications. 2023 Jan 1;209:103540.

[93] Nyangaresi, V. O., & Petrovic, N. (2021, July). Efficient PUF based authentication protocol for internet of drones. In 2021 International Telecommunications Conference (ITC-Egypt) (pp. 1-4). IEEE.

[94] Zulu N, Plessis DP, Mathonsi TE, Tshilongamulenzhe TM. A User-Based Authentication and DoS Mitigation Scheme for Wearable Wireless Body Sensor Networks. arXiv preprint arXiv:2303.14441. 2023 Mar 25.

[95] Verma P, Breslin JG, O'Shea D, Pateriya RK. A Stacked Ensemble Method with Adaptive Attribute Selection to Detect DDoS Attack in Cloud-Assisted WBAN. InMachine Learning, Image Processing, Network Security and Data

Sciences: 4th International Conference, MIND 2022, Virtual Event, January 19–20, 2023, Proceedings, Part II 2023 Jan 18 (pp. 329-344). Cham: Springer Nature Switzerland.

[96] Priyanka S, Vijay Bhanu S. A survey on variants of DoS attacks: Issues and defense mechanisms. Journal of applied research and technology. 2023;21(1):12-6.

[97] Yadav D, Raman R, Gangodkar D, Joshi SK, Sreedevi B, Prasad CR. An implementation of Wireless Mesh Routing Protocol system against Dos attacks in IoT-based Assistance system. In2023 International Conference on Artificial Intelligence and Smart Communication (AISC) 2023 Jan 27 (pp. 558-563). IEEE.

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

[99] Bai P, Kumar S, Dohare U. 8 Blockchain Solutions for Security and Privacy Issues in Smart. Computational Intelligence for Cybersecurity Management and Applications. 2023 Apr 28:147.

[100] Han W, Wang J, Hou S, Bai T, Jeon G, Rodrigues JJ. An PPG signal and body channel based encryption method for WBANs. Future Generation Computer Systems. 2023 Apr 1;141:704-12.

[101] Rao PM, Deebak BD. A Comprehensive Survey on Authentication and Secure Key Management in Internet of Things: Challenges, Countermeasures, and Future Directions. Ad Hoc Networks. 2023 Mar 23:103159.

[102] Si-Ahmed A, Al-Garadi MA, Boustia N. Survey of Machine Learning based intrusion detection methods for Internet of Medical Things. Applied Soft Computing. 2023 Mar 22:110227.

[103] Nyangaresi, V. O. (2023, February). Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. In Proceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 (pp. 797-816). Singapore: Springer Nature Singapore.

[104] Asam M, Jamal T, Ajaz A, Haider Z, Butt SA. Security Issues in WBANs. arXiv preprint arXiv:1911.04330. 2019 Nov 7.

[105] Arogundade, O. R. (2023). Network Security Concepts, Dangers, and Defense Best Practical. Computer Engineering and Intelligent Systems, 14(2).\

[106] Devi, S. R., Kalyampudi, P. L., & Charitha, N. S. (2023). Cyber attacks, security data detection, and critical loads in the power systems. In Smart Energy and Electric Power Systems (pp. 169-184). Elsevier.

[107] Kioskli, K., Fotis, T., Nifakos, S., & Mouratidis, H. (2023). The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0. Applied Sciences, 13(6), 3410.

[108] Abduljabbar, Z. A., Abduljaleel, I. Q., Ma, J., Al Sibahee, M. A., Nyangaresi, V. O., Honi, D. G., ... & Jiao, X. (2022). Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access, 10, 26257-26270.

[109] Parvez, K., Zohra, F. T., & Jahan, M. (2019, December). A secure and lightweight user authentication mechanism for wireless body area network. In Proceedings of the 6th International Conference on Networking, Systems and Security (pp. 139-143).

[110] Shen, J., Gui, Z., Ji, S., Shen, J., Tan, H., & Tang, Y. (2018). Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. Journal of Network and Computer Applications, 106, 117-123.

[111] Wan T, Wang L, Liao W, Yue S. A lightweight continuous authentication scheme for medical wireless body area networks. Peer-to-Peer Networking and Applications. 2021 Nov;14(6):3473-87.

[112] Soni, M., & Singh, D. K. (2022). LAKA: lightweight authentication and key agreement protocol for internet of things based wireless body area network. Wireless Personal Communications, 127(2), 1067-1084.

[113] Al Sibahee, M. A., Abdulsada, A. I., Abduljabbar, Z. A., Ma, J., Nyangaresi, V. O., & Umran, S. M. (2021). Lightweight, Secure, Similar-Document Retrieval over Encrypted Data. Applied Sciences, 11(24), 12040.

[114] Nidhya, R., Shanthi, S., & Kumar, M. (2021). A novel encryption design for wireless body area network in remote healthcare system using enhanced RSA algorithm. In Intelligent System Design: Proceedings of Intelligent System Design: INDIA 2019 (pp. 255-263). Springer Singapore.

[115] Konan, M., & Wang, W. (2019). A secure mutual batch authentication scheme for patient data privacy preserving in WBAN. Sensors, 19(7), 1608.

[116] Iqbal, J., Adnan, M., Khan, Y., AlSalman, H., Hussain, S., Ullah, S. S., ... & Gumaei, A. (2022). Designing a healthcare-enabled software-defined wireless body area network architecture for secure medical data and efficient diagnosis. Journal of Healthcare Engineering, 2022, 1-19.

[117] Singla, R., Kaur, N., Koundal, D., & Bharadwaj, A. (2022). Challenges and developments in secure routing protocols for healthcare in WBAN: a comparative analysis. Wireless Personal Communications, 1-40.

[118] Nyangaresi, V. O. (2021). A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. In the 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612).

[119] Rastegari, P., Khalili, M., & Sakhaei, A. (2023). Security Analysis and Improvement of an Access Control Protocol for WBANs. International Journal of Network Security, 25(2), 285-296.

[120] Pawar, R. S., & Kalbande, D. R. (2023). Optimization of quality of service using ECEBA protocol in wireless body area network. International Journal of Information Technology, 1-16.

[121] Kumar, A., Rathore, P. S., Dubey, A. K., Agrawal, R., & Sharma, K. P. (2023). LTE-NBP with holistic UWB-WBAN approach for the energy efficient biomedical application. Multimedia Tools and Applications, 1-15.

[122] Ullah, F., Abdullah, A. H., Kaiwartya, O., Kumar, S., & Arshad, M. M. (2017). Medium access control (MAC) for wireless body area network (WBAN): superframe structure, multiple access technique, taxonomy, and challenges. Human-centric Computing and Information Sciences, 7, 1-39.

[123] Hussain, M. A., Hussien, Z. A., Abduljabbar, Z. A., Ma, J., Al Sibahee, M. A., Hussain, S. A., Nyangaresi V.O., & Jiao, X. (2022). Provably throttling SQLI using an enciphering query and secure matching. Egyptian Informatics Journal, 23(4), 145-162.

[124] Lokesh, B. S., & Kaulgud, N. (2023, February). A review on analysis of transport layer security in open quantum safe cryptographic algorithm. In 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC) (pp. 1-5). IEEE.

[125] Ullah, I., Khan, M. A., Abdullah, A. M., Noor, F., Innab, N., & Chen, C. M. (2023). Enabling Secure Communication in Wireless Body Area Networks with Heterogeneous Authentication Scheme. Sensors, 23(3), 1121.

[126] Sakthivel, K., & Ganesan, R. (2023). ESTEEM–Enhanced stability and throughput for energy efficient multihop routing based on Markov Chain Model in wireless body area networks. Sustainable Energy Technologies and Assessments, 56, 103100.

[127] Hai, T., Zhou, J., Masdari, M., & Marhoon, H. A. (2023). A hybrid marine predator algorithm for thermal-aware routing scheme in wireless body area networks. Journal of Bionic Engineering, 20(1), 81-104.

[128] Nyangaresi, V. O., & Alsamhi, S. H. (2021, October). Towards secure traffic signaling in smart grids. In 2021 3rd Global Power, Energy and Communication Conference (GPECOM) (pp. 196-201). IEEE.

[129] Abdulrahman, S. A., Ahmed, E. Q., Jaaz, Z. A., & Ali, A. A. R. (2023). Intrusion Detection in Wireless Body Area Network using Attentive with Graphical Bidirectional Long-Short Term Memory. International Journal of Online & Biomedical Engineering, 19(6).

[130] Bengag, A., Bengag, A., Moussaoui, O., & Mohamed, B. (2023, April). A Fuzzy Logic-Based Intrusion Detection System for WBAN Against Jamming Attacks. In Proceedings of the 3rd International Conference on Electronic Engineering and Renewable Energy Systems: ICEERE 2022, 20-22 May 2022, Saidia, Morocco (pp. 3-11). Singapore: Springer Nature Singapore.

[131] Gautami, A., Shanthini, J., & Karthik, S. (2023). A Quasi-Newton Neural Network Based Efficient Intrusion Detection System for Wireless Sensor Network. Computer Systems Science & Engineering, 45(1).

[132] Soula, M., Mbarek, B., Meddeb, A., & Pitner, T. (2023, March). A Survey of Intrusion Detection-Based Trust Management Approaches in IoT Networks. In Advanced Information Networking and Applications: Proceedings of the 37th International Conference on Advanced Information Networking and Applications (AINA-2023), Volume 3 (pp. 504-517). Cham: Springer International Publishing.

[133] Omollo VN, Musyoki S. Blue bugging Java Enabled Phones via Bluetooth Protocol Stack Flaws. International Journal of Computer and Communication System Engineering. 2015 Jun 9, 2 (4):608-613.

[134] Gite, P., Chouhan, K., Krishna, K. M., Nayak, C. K., Soni, M., & Shrivastava, A. (2023). ML Based Intrusion Detection Scheme for various types of attacks in a WSN using C4. 5 and CART classifiers. Materials Today: Proceedings, 80, 3769-3776.

[135] Nasir, M. H., Arshad, J., & Khan, M. M. (2023). Collaborative device-level botnet detection for internet of things. Computers & Security, 129, 103172.

[136] Lopez, T., Sharp, H., Bandara, A., Tun, T., Levine, M., & Nuseibeh, B. (2023). Security responses in software development. ACM Transactions on Software Engineering and Methodology, 32(3), 1-29.

[137] Lende, D., Monkhouse, A., Ligatti, J., & Ou, X. (2023). Co-Creation in Secure Software Development: Applied Ethnography and the Interface of Software and Development. Human Organization, 82(1), 13-24.

[138] Nyangaresi, V. O. (2022). Terminal independent security token derivation scheme for ultra-dense IoT networks. Array, 15, 100210.

[139] Alhirabi, N., Beaumont, S., Llanos, J. T., Meedeniya, D., Rana, O., & Perera, C. (2023). PARROT: Interactive privacy-aware internet of things application design tool. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 7(1), 1-37.

[140] Bakkiam Deebak, D., & AL-Turjman, F. (2023). Lightweight privacy-aware secure authentication scheme for cyber-physical systems in the edge intelligence era. Concurrency and Computation: Practice and Experience, 35(13), e6510.

[141] Alnashwan, R., Gope, P., & Dowling, B. (2023). Privacy-aware secure region-based handover for small cell networks in 5G-enabled mobile communication. IEEE Transactions on Information Forensics and Security, 18, 1898-1913.

[142] He, Y., He, X., Jin, R., & Dai, H. (2023). Location Privacy-Aware and Energy-Efficient Offloading for Distributed Edge Computing. IEEE Transactions on Wireless Communications.

[143] Mutlaq, K. A. A., Nyangaresi, V. O., Omar, M. A., & Abduljabbar, Z. A. (2022, October). Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. In Applied Cryptography in Computer and Communications: Second EAI International Conference, AC3 2022, Virtual Event, May 14-15, 2022, Proceedings (pp. 46-64). Cham: Springer Nature Switzerland.

[144] Kang, J., & Adibi, S. (2015). A review of security protocols in mHealth wireless body area networks (WBAN). In Future Network Systems and Security: First International Conference, FNSS 2015, Paris, France, June 11-13, 2015, Proceedings 1 (pp. 61-83). Springer International Publishing.

[145] Hajar, M. S., Kalutarage, H. K., & Al-Kadri, M. O. (2023). Security Challenges in Wireless Body Area Networks for Smart Healthcare. In Artificial Intelligence for Disease Diagnosis and Prognosis in Smart Healthcare (pp. 255-286). CRC Press.

[146] Jabeen, T., Jabeen, I., Ashraf, H., Ullah, A., Jhanjhi, N. Z., Ghoniem, R. M., & Ray, S. K. (2023). Smart Wireless Sensor Technology for Healthcare Monitoring System using Cognitive Radio Networks.

[147] Bhushan, B., Kumar, A., Agarwal, A. K., Kumar, A., Bhattacharya, P., & Kumar, A. (2023). Towards a Secure and Sustainable Internet of Medical Things (IoMT): Requirements, Design Challenges, Security Techniques, and Future Trends. Sustainability, 15(7), 6177.

[148] Nyangaresi, V. O. (2022). A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science, 3(5), 364.

[149] López Martínez, A., Gil Pérez, M., & Ruiz-Martínez, A. (2023). A Comprehensive Review of the State-of-the-Art on Security and Privacy Issues in Healthcare. ACM Computing Surveys, 55(12), 1-38.

[150] Al-Dalati, I. (2023). Digital twins and cybersecurity in healthcare systems. In Digital Twin for Healthcare (pp. 195-221). Academic Press.

[151] Cleveland, S. M., & Haddara, M. (2023). Internet of Things for Diabetics: Identifying Adoption Issues. Internet of Things, 100798.

[152] Ahad, A., Ali, Z., Mateen, A., Tahir, M., Hannan, A., Garcia, N. M., & Pires, I. M. (2023). A Comprehensive review on 5G-based Smart Healthcare Network Security: Taxonomy, Issues, Solutions and Future research directions. Array, 100290.

[153] Abood, E. W., Hussien, Z. A., Kawi, H. A., Abduljabbar, Z. A., Nyangaresi, V. O., Ma, J., ... & Ahmad, S. (2023). Provably secure and efficient audio compression based on compressive sensing. International Journal of Electrical & Computer Engineering (2088-8708), 13(1).

[154] Cornet, B., Fang, H., Ngo, H., Boyer, E. W., & Wang, H. (2022). An overview of wireless body area networks for mobile health applications. IEEE Network, 36(1), 76-82.

[155] Zou, S., Xu, Y., Wang, H., Li, Z., Chen, S., & Hu, B. (2017). A survey on secure wireless body area networks. Security and communication networks, 2017.

[156] Gherairi, S. (2022). Healthcare: a priority-based energy harvesting scheme for managing sensor nodes in WBANs. Ad Hoc Networks, 133, 102876.

[157] Hodgkiss, J., & Djahel, S. (2022, January). MARS-Towards Mobile Assisted RSSI Secret Key Extraction Strategy in WBANs. In 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC) (pp. 703-706). IEEE.

[158] Nyangaresi, V. O. (2021). Hardware assisted protocol for attacks prevention in ad hoc networks. In Emerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 (pp. 3-20). Springer International Publishing.

[159] Roy, M., Chowdhury, C., & Aslam, N. (2020). Security and privacy issues in wireless sensor and body area networks. Handbook of Computer Networks and Cyber Security: Principles and Paradigms, 173-200.

[160] Sharmila, A. H., & Jaisankar, N. (2021). Edge intelligent agent assisted hybrid hierarchical blockchain for continuous healthcare monitoring & recommendation system in 5G WBAN-IoT. Computer Networks, 200, 108508.

[161] Ananthi, J. V., & Jose, P. S. H. (2021). A perspective review of security challenges in body area networks for healthcare applications. International Journal of Wireless Information Networks, 1-16.

[162] Hussain, S. J., Irfan, M., Jhanjhi, N. Z., Hussain, K., & Humayun, M. (2021). Performance enhancement in wireless body area networks with secure communication. Wireless Personal Communications, 116, 1-22.

[163] Abood, E. W., Abdullah, A. M., Al Sibahe, M. A., Abduljabbar, Z. A., Nyangaresi, V. O., Kalafy, S. A. A., & Ghrabta, M. J. J. (2022). Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics, 11(1), 185-194.

[164] Kettani, H., & Wainwright, P. (2019, March). On the top threats to cyber systems. In 2019 IEEE 2nd international conference on information and computer technologies (ICICT) (pp. 175-179). IEEE.

[165] Bharadiya, J. (2023). Machine Learning in Cybersecurity: Techniques and Challenges. European Journal of Technology, 7(2), 1-14.

[166] Brass, I., & Sowell, J. H. (2021). Adaptive governance for the Internet of Things: Coping with emerging security risks. Regulation & Governance, 15(4), 1092-1110.

[167] Mughal, A. A. (2022). Well-Architected Wireless Network Security. Journal of Humanities and Applied Science Research, 5(1), 32-42.

[168] Nyangaresi, V. O., & Mohammad, Z. (2021, July). Privacy preservation protocol for smart grid networks. In 2021 International Telecommunications Conference (ITC-Egypt) (pp. 1-4). IEEE.

[169] Shahbazi, Z., & Byun, Y. C. (2020). Towards a secure thermal-energy aware routing protocol in wireless body area network based on blockchain technology. Sensors, 20(12), 3604.

[170] Khernane, N., Potop-Butucaru, M., & Chaudet, C. (2016, October). BANZKP: A secure authentication scheme using zero knowledge proof for WBANs. In 2016 IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems (MASS) (pp. 307-315). IEEE.

[171] Tahir, S., Bakhsh, S. T., Abulkhair, M., & Alassafi, M. O. (2019). An energy-efficient fog-to-cloud Internet of Medical Things architecture. International Journal of Distributed Sensor Networks, 15(5), 1550147719851977.

[172] Sammoud, A., Chalouf, M. A., Hamdi, O., Montavont, N., & Bouallegue, A. (2020). A new biometrics-based key establishment protocol in WBAN: Energy efficiency and security robustness analysis. Computers & Security, 96, 101838.

[173] Nyakomitta, S. P., & Omollo, V. (2014). Biometric-Based Authentication Model for E-Card Payment Technology. IOSR Journal of Computer Engineering (IOSRJCE), 16(5), 137-44.

[174] Bhatti, D. S., Saleem, S., Imran, A., Iqbal, Z., Alzahrani, A., Kim, H., & Kim, K. I. (2022). A Survey on Wireless Wearable Body Area Networks: A Perspective of Technology and Economy. Sensors, 22(20), 7722.

[175] Awad, M., Sallabi, F., Shuaib, K., & Naeem, F. (2022). Artificial intelligence-based fault prediction framework for WBAN. Journal of King Saud University-Computer and Information Sciences, 34(9), 7126-7137.

[176] Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data protection and privacy of the internet of healthcare things (IoHTs). Applied Sciences, 12(4), 1927.

[177] Davies, J. N., Verovko, M., Verovko, O., & Solomakha, I. (2022, February). Usage of WBAN Systems and IoT Solutions in a Medical Environment. In Mathematical Modeling and Simulation of Systems: Selected Papers of 16th International Scientific-practical Conference, MODS, 2021 June 28–July 01, Chernihiv, Ukraine (pp. 297-311). Cham: Springer International Publishing.

[178] Nyangaresi, V. O. (2021, September). Lightweight key agreement and authentication protocol for smart homes. In 2021 IEEE AFRICON (pp. 1-6). IEEE.

[179] Ahmed, S., Javaid, N., Yousaf, S., Ahmad, A., Sandhu, M. M., Imran, M., ... & Alrajeh, N. (2015). Co-LAEEBA: Cooperative link aware and energy efficient protocol for wireless body area networks. Computers in Human Behavior, 51, 1205-1215.

[180] Silic, M., & Lowry, P. B. (2020). Using design-science based gamification to improve organizational security training and compliance. Journal of management information systems, 37(1), 129-161.

[181] Lee, I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. Future Internet, 12(9), 157.

[182] Upadhyay, D., & Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. Computers & Security, 89, 101666.

[183] Omollo VN, Musyoki S. Global Positioning System Based Routing Algorithm for Adaptive Delay Tolerant Mobile Adhoc Networks. International Journal of Computer and Communication System Engineering. 2015 May 11, 2(3): 399-406.

[184] Amudha, S., & Murali, M. (2021). Deep learning based energy efficient novel scheduling algorithms for body-fog-cloud in smart hospital. Journal of Ambient Intelligence and Humanized Computing, 12, 7441-7460.

[185] Chunka, C., & Banerjee, S. (2021). An efficient mutual authentication and symmetric key agreement scheme for wireless body area network. Arabian Journal for Science and Engineering, 46(9), 8457-8473.

[186] Olatinwo, D. D., Abu-Mahfouz, A. M., & Hancke, G. P. (2021). Towards achieving efficient MAC protocols for WBAN-enabled IoT technology: a review. EURASIP Journal on Wireless Communications and Networking, 2021(1), 1-47.

[187] Wang, X., Zheng, G., Ma, H., Bai, W., Wu, H., & Ji, B. (2021). Fuzzy control-based energy-aware routing protocol for wireless body area networks. Journal of Sensors, 2021, 1-13.

[188] Nyangaresi, V. O., Ahmad, M., Alkhayyat, A., & Feng, W. (2022). Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems, 39(10), e13126.

[189] Saif, S., Gupta, R., & Biswas, S. (2021). A complete secure cloud-based WBAN framework for health data transmission by implementing authenticity, confidentiality and integrity. International Journal of Advanced Intelligence Paradigms, 20(1-2), 171-189.

[190] Xu, G., Wu, Q., Daneshmand, M., Liu, Y., & Wang, M. (2016). A data privacy protective mechanism for wireless body area networks. wireless communications and mobile computing, 16(13), 1746-1758.

[191] Krishnamoorthy, S., Dua, A., & Gupta, S. (2023). Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: A survey, current challenges and future directions. Journal of Ambient Intelligence and Humanized Computing, 14(1), 361-407.

[192] Mahajan, H. B., Rashid, A. S., Junnarkar, A. A., Uke, N., Deshpande, S. D., Futane, P. R., ... & Alhayani, B. (2023). Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems. Applied Nanoscience, 13(3), 2329-2342.

[193] Honi, D. G., Ali, A. H., Abduljabbar, Z. A., Ma, J., Nyangaresi, V. O., Mutlaq, K. A. A., & Umran, S. M. (2022, December). Towards Fast Edge Detection Approach for Industrial Products. In 2022 IEEE 21st International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS) (pp. 239-244). IEEE.

[194] Gao, Q., Agarwal, S., Greiner, A., & Zhang, T. (2023). Electrospun Fiber-Based Flexible Electronics: Fiber Fabrication, Device Platform, Functionality Integration and Applications. Progress in Materials Science, 101139.

[195] Heredia-Rivera, U., Kasi, V., Krishnakumar, A., Kadian, S., Barui, A. K., He, Z., ... & Rahimi, R. (2023). Cold Atmospheric Plasma-Assisted Direct Deposition of Polypyrrole-Ag Nanocomposites for Flexible Electronic Sensors. ACS Applied Materials & Interfaces, 15(13), 17078-17090.

[196] Nawaz, A., Merces, L., Ferro, L. M., Sonar, P., & Bufon, C. C. (2023). Impact of Planar and Vertical Organic Field-Effect Transistors on Flexible Electronics. Advanced Materials, 35(11), 2204804.

[197] Eid M.M., Arunachalam R., Sorathiya V., Lavadiya S., Patel S.K., Parmar J., Delwar T.S., Ryu J.Y., Nyangaresi V.O., Zaki Rashed A.N. (2022). QAM receiver based on light amplifiers measured with effective role of optical coherent duobinary transmitter. Journal of Optical Communications, (0).

[198] Wu, D., Yang, Z., Zhang, P., Wang, R., Yang, B., & Ma, X. (2023). Virtual-Reality Inter-Promotion Technology for Metaverse: A Survey. IEEE Internet of Things Journal.

[199] Rajendran, S., Pan, W., Sabuncu, M. R., Zhou, J., & Wang, F. (2023). Patchwork Learning: A Paradigm Towards Integrative Analysis across Diverse Biomedical Data Sources. arXiv preprint arXiv:2305.06217.

[200] Rodríguez-Rodríguez, I., Rodríguez, J. V., & Campo-Valera, M. (2023). Applications of the internet of medical things to type 1 diabetes mellitus. Electronics, 12(3), 756.

[201] Heidari, A., Jafari Navimipour, N., Unal, M., & Zhang, G. (2023). Machine learning applications in internet-of-drones: systematic review, recent deployments, and open issues. ACM Computing Surveys, 55(12), 1-45.

[202] Nyangaresi VO, Abduljabbar ZA, Al Sibahee MA, Ibrahim A, Yahya AN, Abduljaleel IQ, Abood EW. Optimized Hysteresis Region Authenticated Handover for 5G HetNets. InArtificial Intelligence and Sustainable Computing: Proceedings of ICSISCET 2021 2022 Nov 16 (pp. 91-111). Singapore: Springer Nature Singapore.

[203] Shukla, S., Hassan, M. F., Jung, L. T., & Awang, A. (2019). Architecture for latency reduction in healthcare internet-of-things using reinforcement learning and fuzzy based fog computing. In Recent Trends in Data Science and Soft Computing: Proceedings of the 3rd International Conference of Reliable Information and Communication Technology (IRICT 2018) (pp. 372-383). Springer International Publishing.

[204] Shukla, S., Hassan, M. F., Khan, M. K., Jung, L. T., & Awang, A. (2019). An analytical model to minimize the latency in healthcare internet-of-things in fog computing environment. PloS one, 14(11), e0224934.

[205] Whig, P., Kouser, S., Velu, A., & Nadikattu, R. R. (2022). Fog-IoT-Assisted-Based Smart Agriculture Application. In Demystifying Federated Learning for Blockchain and Industrial Internet of Things (pp. 74-93). IGI Global.

[206] Garg, S., Singh, A., Batra, S., Kumar, N., & Yang, L. T. (2018). UAV-empowered edge computing environment for cyber-threat detection in smart vehicles. IEEE network, 32(3), 42-51.

[207] Rashed A.N., Ahammad S.H., Daher M.G., Sorathiya V., Siddique A., Asaduzzaman S., Rehana H., Dutta N., Patel S.K., Nyangaresi V.O., Jibon R.H. (2022). Spatial single mode laser source interaction with measured pulse based parabolic index multimode fiber. Journal of Optical Communications.

[208] Huang, J., Zhou, Y., Ning, Z., & Gharavi, H. (2019). Wireless power transfer and energy harvesting: Current status and future prospects. IEEE wireless communications, 26(4), 163-169.

[209] Shinohara, N. (2020). Trends in wireless power transfer: WPT technology for energy harvesting, mllimeter-wave/THz rectennas, MIMO-WPT, and advances in near-field WPT applications. IEEE microwave magazine, 22(1), 46-59.

[210] Ijemaru, G. K., Ang, K. L. M., & Seng, J. K. (2022). Wireless power transfer and energy harvesting in distributed sensor networks: Survey, opportunities, and challenges. International journal of distributed sensor networks, 18(3), 15501477211067740.

[211] Meile, L., Ulrich, A., & Magno, M. (2019, June). Wireless power transmission powering miniaturized low power iot devices: A revie. In 2019 IEEE 8th International Workshop on Advances in Sensors and Interfaces (IWASI) (pp. 312-317). IEEE.

[212] Zaki Rashed A.N., Ahammad S.H., Daher M.G., Sorathiya V., Siddique A., Asaduzzaman S., Rehana H., Dutta N., Patel S.K., Nyangaresi V.O., Jibon R.H. (2022). Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications, (0).

[213] Sridhar, M., Priya, N., & Muniyappan, A. (2020). Wireless body area networks: requirements, characteristics, design consideration, and challenges. In Incorporating the Internet of Things in Healthcare Applications and Wearable Devices (pp. 67-85). IGI Global.

[214] Khatoon, N., Roy, S., & Pranav, P. (2020). A survey on Applications of Internet of Things in Healthcare. Internet of Things and Big Data Applications: Recent Advances and Challenges, 89-106.

[215] Saeed, J. N., & Ameen, S. Y. (2021). Smart Healthcare for ECG Telemonitoring System. Journal of Soft Computing and Data Mining, 2(2), 75-85.

[216] Khan, M. D., Ullah, Z., Ahmad, A., Hayat, B., Almogren, A., Kim, K. H., ... & Ali, M. (2020). Energy harvested and cooperative enabled efficient routing protocol (EHCRP) for IoT-WBAN. Sensors, 20(21), 6267.

[217] Nyangaresi, V. O. (2022, July). Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In 2022 International Conference on Inventive Computation Technologies (ICICT) (pp. 1-6). IEEE.

[218] Das, A. K., Wazid, M., Kumar, N., Khan, M. K., Choo, K. K. R., & Park, Y. (2017). Design of secure and lightweight authentication protocol for wearable devices environment. IEEE journal of biomedical and health informatics, 22(4), 1310-1322.

[219] Oh, J., Yu, S., Lee, J., Son, S., Kim, M., & Park, Y. (2021). A secure and lightweight authentication protocol for IoT-based smart homes. Sensors, 21(4), 1488.

[220] Almulhim, M., & Zaman, N. (2018, February). Proposing secure and lightweight authentication scheme for IoT based E-health applications. In 2018 20th International Conference on advanced communication technology (ICACT) (pp. 481-487). IEEE.

[221] Rana, M., Shafiq, A., Altaf, I., Alazab, M., Mahmood, K., Chaudhry, S. A., & Zikria, Y. B. (2021). A secure and lightweight authentication scheme for next generation IoT infrastructure. Computer Communications, 165, 85-96.

[222] Garg, S., Kaur, K., Kaddoum, G., Rodrigues, J. J., & Guizani, M. (2019). Secure and lightweight authentication scheme for smart metering infrastructure in smart grid. IEEE Transactions on Industrial Informatics, 16(5), 3548-3557.

[223] Nyangaresi, V. O. (2022). Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture, 133, 102763.

[224] Jegadeesan, S., Azees, M., Babu, N. R., Subramaniam, U., & Almakhles, J. D. (2020). EPAW: Efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs). IEEE Access, 8, 48576-48586.

[225] Ara, A., Al-Rodhaan, M., Tian, Y., & Al-Dhelaan, A. (2017). A secure privacy-preserving data aggregation scheme based on bilinear ElGamal cryptosystem for remote health monitoring systems. IEEE Access, 5, 12601-12617.

[226] Shuai, M., Liu, B., Yu, N., Xiong, L., & Wang, C. (2020). Efficient and privacy-preserving authentication scheme for wireless body area networks. Journal of Information Security and Applications, 52, 102499.

[227] Zhao, K., Sun, D., Ren, G., & Zhang, Y. (2020). Public auditing scheme with identity privacy preserving based on certificateless ring signature for wireless body area networks. IEEE Access, 8, 41975-41984.

[228] Abduljaleel IQ, Abduljabbar ZA, Al Sibahee MA, Ghrabat MJ, Ma J, Nyangaresi VO. A Lightweight Hybrid Scheme for Hiding Text Messages in Colour Images Using LSB, Lah Transform and Chaotic Techniques. Journal of Sensor and Actuator Networks. 2022 Dec;11(4):66.

[229] Mehdy, H. S., Qasim, N. J., Habeeb, F. A., Jabbar, Z. S., Tawfeq, J. F., & Radhi, A. D. (2023). A Deep learning approach for trust-untrust nodes classification problem in WBAN. Periodicals of Engineering and Natural Sciences, 11(3), 87-96.

[230] Ayed, S., Chaari, L., & Fares, A. (2020). A survey on trust management for WBAN: Investigations and future directions. Sensors, 20(21), 6041.

[231] Khater, H. M., Sallabi, F., Serhani, M. A., Turaev, S., & Barka, E. (2023). Efficient Hybrid Fault-Management Clustering Algorithm (HFMCA) in WBANs Based on Weighted Bipartite Graph. IEEE Access.

[232] Hu, J., Xu, G., Hu, L., & Li, S. (2023). A Cooperative Transmission Scheme in Radio Frequency Energy-Harvesting WBANs. Sustainability, 15(10), 8367.

[233] Nyangaresi, V. O. (2021, November). Provably secure protocol for 5G HetNets. In 2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) (pp. 17-22). IEEE.

[234] Fareed, M., & Yassin, A. A. (2023). A lightweight and secure multilayer authentication scheme for wireless body area networks in healthcare system. International Journal of Electrical and Computer Engineering, 13(2), 1782.

[235] Hammi, B., Zeadally, S., & Nebhen, J. (2023). Security threats, countermeasures, and challenges of digital supply chains. ACM Computing Surveys.

[236] Dawod, A. Y., Hakim, B. A., Radhi, A. D., Jabbar, Z. S., Tawfeq, J. F., & JosephNg, P. S. (2023). A novel nomadic people optimizer-based energy-efficient routing for WBAN. Periodicals of Engineering and Natural Sciences, 11(3), 97-108.

[237] Preethichandra, D. M. G., Piyathilaka, L., Izhar, U., Samarasinghe, R., & De Silva, L. C. (2023). Wireless Body Area Networks and Their Applications–A Review. IEEE Access.

[238] Hu, X., Guo, K., Wang, C., Chen, Y., Qian, Y., & Zhang, J. (2023). Maximizing Throughput for Coexisting Wireless Body Area Networks (WBANs) Based on Optimal Clustering. IEEE Internet of Things Journal.

[239] Nyangaresi, V. O., & Mohammad, Z. (2022, June). Session Key Agreement Protocol for Secure D2D Communication. In The Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 (pp. 81-99). Cham: Springer International Publishing.

[240] Singh, S., & Kumar, D. (2023). Energy-efficient secure data fusion scheme for IoT based healthcare system. Future Generation Computer Systems.

[241] Pahuja, M., & Kumar, D. (2023, February). Several Energy-Efficient Routing Protocols, Design-based Routing Problems and Challenges in IoT-Based WSN: A Review. In 2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS) (pp. 694-699). IEEE.

[242] Jariwala, V. J., & Jinwala, D. C. (2020). AdaptableSDA: secure data aggregation framework in wireless body area networks. In Wearable and Implantable Medical Devices (pp. 79-114). Academic Press.

[243] Qiu Z, Ma J, Zhang H, Al Sibahee MA, Abduljabbar ZA, Nyangaresi VO. Concurrent pipeline rendering scheme based on GPU multi-queue and partitioning images. InInternational Conference on Optics and Machine Vision (ICOMV 2023) 2023 Apr 14 (Vol. 12634, pp. 143-149). SPIE.

[244] Mihovska, A., & Sarkar, M. (2018). Smart connectivity for internet of things (IoT) applications. New advances in the internet of things, 105-118.

[245] Fayoumi, A., Sobati-Moghadam, S., Rajaiyan, A., Oxley, C., Montero, P. F., & Safarian, A. (2023, January). Home Care Automation: Market Research, Industry Analysis, and Security Assessment. In 2023 International Conference On Cyber Management And Engineering (CyMaEn) (pp. 418-423). IEEE.

[246] Taherdoost, H. (2023). Blockchain-Based Internet of Medical Things. Applied Sciences, 13(3), 1287.

[247] Lee, A., Mhatre, J., Das, R. K., & Hong, M. (2023). Hybrid Mobile Cloud Computing Architecture with Load Balancing for Healthcare Systems. Computers, Materials & Continua, 74(1).

[248] Al Sibahee MA, Ma J, Nyangaresi VO, Abduljabbar ZA. Efficient Extreme Gradient Boosting Based Algorithm for QoS Optimization in Inter-Radio Access Technology Handoffs. In2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 2022 Jun 9 (pp. 1-6). IEEE.

[249] Li, C. T., Lee, C. C., & Weng, C. Y. (2016). A secure cloud-assisted wireless body area network in mobile emergency medical care system. Journal of medical systems, 40, 1-15.

[250] Gupta, S. H., & Devarajan, N. (2020). Performance exploration of on-body WBAN using CM3A-IEEE 802.15. 6 channel model. Journal of Ambient Intelligence and Humanized Computing, 1-12.

[251] Sharavanan, P. T., Sridharan, D., & Kumar, R. (2018). A privacy preservation secure cross layer protocol design for IoT based wireless body area networks using ECDSA framework. Journal of Medical Systems, 42, 1-11.

[252] Roy, S., Khatua, S., Chattopadhyay, S., & Chowdhury, C. (2023). A Multi-criteria Prioritization-Based Data Transmission Scheme for Inter-WBAN Communications. Journal of The Institution of Engineers (India): Series B, 104(1), 1-7.

[253] Bilandi, N., Verma, H. K., & Dhir, R. (2019). PSOBAN: a novel particle swarm optimization based protocol for wireless body area networks. SN Applied Sciences, 1, 1-14.