INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Integration of Blockchain Technology for Security and Privacy Enhancement in Wireless Body Area Network Systems

S Sanjith[1]*, P Ranjit Jeba Thangaiah[1], J Macklin Abraham Navamani[1], Attada Venkataramana[2]*

1 Department of Digital Sciences, Karunya Institute of Technology and Sciences, Karunya Nagar, Coimbatore, 641114, Tamilnadu, India
2 Department of Computer Science and Engineering, GMR Institute of Technology, Rajam, 532127, Andhra Pradesh, India

OPEN ACCESS

Received: 28-06-2023

Accepted: 24-09-2023

Published: 31-10-2023

Citation: Sanjith S, Thangaiah PRJ, Navamani JMA, Venkataramana A (2023) Integration of Blockchain Technology for Security and Privacy Enhancement in Wireless Body Area Network Systems . Indian Journal of Science and Technology 16(41): 3583-3590. https://doi.org/10.17485/IJST/v16i41.1610

* **Corresponding authors**.

drsanjith@gmail.com

venkataramana.a@gmrit.edu.in

Funding: None

Competing Interests: None

Copyright: © 2023 Sanjith et al. This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: Blockchain technology can improve the security and privacy of Wireless Body Area Network (WBAN) systems in healthcare. The primary goal of this research is to address the privacy and security concerns in technology-loaded devices and gadgets by proposing a novel approach that integrates blockchain and advanced cryptographic techniques with WBAN. **Methods:** Simulated physiological data collected from multiple body sensors in a WBAN environment, along with network traffic data, were gathered. A modified algorithm is developed for signature encryption in WBAN systems using a hyperelliptic curve secure channel. This approach incorporates blockchain technology to strengthen security and privacy measures for efficient and safe data transfer and storage. To achieve this, a hyperelliptic curve-based technique is used along with an authenticated certificate-less signature key encryption model, which helps overcome various attacks, such as man-in-the-middle attacks, basic impersonation attacks, and key offset attacks. **Findings:** The proposed methodology is compared to traditional approaches to assess its effectiveness. This methodology is evaluated using parameters such as Hardware Security Model (HSM) operations and time taken, which demonstrate its superiority. It is observed that the proposed methodology records 3 hsm operations within 2.03 ms with Signcryption and 3 hsm within 2.35 ms with Unsigncryption, proving to be better than other traditional approaches. **Novelty:** The integrity, security, and privacy features of blockchain, make it difficult for malicious actors to crack or hack the system. The security measures are further enhanced by using a hyperelliptic curve-based technique and an authenticated certificate-less signature key encryption model. This approach also addresses multiple attacks providing a comprehensive solution for secure data transmission.

Keywords: Blockchain; WBAN; Secured IoT; Attack mitigation; MultiFactor Authentication

1 Introduction

In recent years, there have been growing concerns about privacy and security issues in technology-based devices and systems, especially in the healthcare sector[1]. The protection of personal health information stored in databases requires high-security measures, which has led to the exploration of different encryption algorithms[2]. However, the selection of an algorithm depends on the specific application, environment, and operational requirements. The introduction of blockchain technology has greatly impacted data validation and integrity due to its inherent encryption capabilities[3]. As a result, blockchain has been widely adopted in sectors such as supply chain management, healthcare, and banking[4,5].

Wireless Body Area Networks (WBANs) are becoming increasingly popular in the healthcare sector due to their ability to monitor vital signs and transmit patient information in real-time, regardless of location[6]. However, they are vulnerable to attacks and privacy threats, such as denial-of-service, impersonation, and man-in-the-middle attacks[7]. Despite numerous algorithms and protocols proposed to secure WBAN networks, challenges related to resource constraints, data consistency, management, and quality persist[8–10].

The use of telemedicine has become a highly effective way to exchange electronic health records (EHR) and electronic medical records (EMR) securely and efficiently[11]. Many studies have suggested various methods to increase the security and privacy of healthcare systems, such as secure cloud-based systems, privacy-preserving decentralized data-sharing mechanisms, and blockchain-based methodologies[12]. However, the encryption methods used in WBANs have certain limitations, including concerns with privacy, verifiability, and efficiency[13].

1.1 WBAN Security Challenges

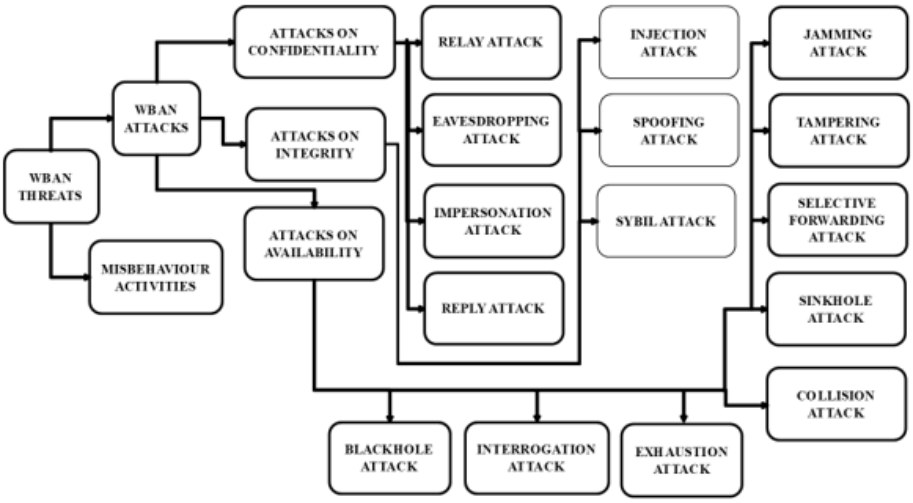

Fig 1. WBAN Threats

Using WBAN networks can present several challenges due to constraints like limited resources, physical size, communication bandwidth, storage capacity, energy, and power. As shown in Figure 1, WBAN networks face numerous threats. Some of the significant challenges include:

- **Sensor Validation:** Hardware limitations like energy and power efficiency, and communication issues can affect the accuracy of data obtained from the sensor nodes[9]. Therefore, it is necessary to validate the data obtained periodically.
- **Data Consistency:** The data collected from various locations across the nodes should contain all the essential information required to maintain the quality of the result.
- **Data Management:** Different types of sensors collect a large volume of data, resulting in a vast amount of data to manage and store, which can be a daunting task[10].
- **Data Quality:** The data collected from WBAN networks is crucial in interpreting healthcare. Any discrepancy in the data can lead to severe consequences, affecting subsequent processes and decision-making. Therefore, it is essential to collect high-quality data to enable optimal decision-making.

Internet technology has progressed dramatically in recent years, replacing several of the traditional models with advanced ones, and telemedicine is one among them. Legitimate users have access to and can exchange a large amount of Electronic Health Records (EHR) and Electronic Medical Records (EMR) generated [11]. However, the security and safety of the patient's privacy records, and other electronic medical information is a must, and there is much work carried out to ensure the security and privacy protection of these records. Telemedicine offers a secure, efficient, and novel model to exchange EHRs and EMRs, which will further enhance interoperability, privacy, and data security. In [12], Cao et al. have proposed a secure cloud-based assisted electronic health system that can be used to provide security from illegal modification in electronic health records. In [13], the authors introduced a privacy-preserving decentralized medical data-sharing mechanism using blockchain. An eHealthcare system with blockchain with Wireless Body Area Networks (WBAN) was introduced by Wang et al. [14].

Similarly, a patient-centric framework for exchanging health information was proposed by the authors in [15], while the authors in [16,17] recommended the use of blockchain based methodology to secure the system and establish privacy. An e-health system was introduced in [18] that used an electronic medical storage record that could save patients' information using a tree-based blockchain algorithm. A decentralized eHealth architecture that was used to explore the limitations of the medical system, such as the tools and framework, was analyzed by the authors in [19]. Authors in [20] introduced a novel blockchain-based methodology for several IoT healthcare applications [21] to ensure the safe sharing and storage of information.

1.2 Issues with WBAN Encryption Schemes

Based on the level of difficulty, the WBAN signcryption techniques can be further categorized into hyperelliptic curves in cryptography, fuzzy-based encryption, elliptic curve cryptography, and bilinear pairing-based cryptography. Several authors have used identity-based cryptography (IBC) for controlling access in WBANs. The elliptic curve cryptography (ECC) is used to determine widespread uses due to its relatively cheap cost of usage. When used in an app, this technique requires the use of partial keys along with controller key escrow. However, these keys do not provide the necessary privacy as they are publicly verifiable. Authentication of the networks is established with the help of the Internet of Things, wherein it is possible to access the network using certificates. Bilinear pairing is used by several authors to enhance efficiency and security as it conserves cost and energy.

2 Methodology

A modified WBAN signature encryption algorithm is presented in the paper that uses a hyperelliptic curve secure channel of the certificate. This helps in overcoming several challenges of the existing systems discussed in the previous sections. Man-in-the-middle attacks (MMA), basic impersonation attacks (BIA), and key offset attacks (KOA) of the malicious key generation centre (KGC) administrators are overcome using this technique. The research utilizes simulated physiological data collected from multiple body sensors in a WBAN environment, along with network traffic data.

The algorithm is first trained using a standard wearable security dataset called ICU of size 15.46 MB with 56609 samples collected from nine patient monitoring sensors. This dataset includes network-related features and a binary label of either 0 for non-attack or 1 for attack [22]. The data is split for training and testing in a 70:30 ratio. Testing and evaluation of the methodology are performed using parameters such as HSM operations and time taken.

2.1 WBAN Signcryption Schemes

The WBA signcryption techniques are classified using theoretical and Asymmetric crypto system considerations. A public key infrastructure based cryptography is used in several processes of attribute based signcryption. In several methodologies certificateless and heterogeneous signcryption is used.

2.2 Proposed Work

The proposed encryption system for WBAN signatures involves modifying the sender's message and having an adversary transmit it to the receiver using KOA. This causes a disparity in the final session keys estimated by both parties. For example, the adversary multiplies the sender's ephemeral public key with a random value and sends it to the receiver. Most authenticated key agreement protocols do not verify the final session key, making it vulnerable to attacks. This technique does not use communication security information compared to MMA. KOAR can mitigate such attack scenarios. BIR prevents attackers from impersonating legitimate communication participants without a static private key. MMAR mitigates an attacker's ability to impersonate themselves between two participants and share the key with the other participant in MMA [23]. WBANs are gaining popularity among researchers and manufacturers as they can monitor a user's heart rate and transmit data to a physician

wirelessly. The proposed system does not require certificate revocation or renewal as there is no central authority. Public verifiability is overseen in this work.

Physiological data can be captured by WBAN sensors implanted in the body. To protect resource-constrained devices and sensors, signature encryption can be used efficiently. WBAN encryption schemes use elliptic and hyperelliptic curves along with bilinear pairing. A sign encryption query is utilized to verify the sender, and, upon confirmation, the data is decrypted by the application provider and sent to the controller. Symmetric encryption requires a single key. The physiological data captured by WBAN from the implanted sensors is analyzed further. If an attacker is detected, the encryption and decryption keys are changed to protect the user's identity and nullify the sender's private key. These keys can be stored in key escrow for future use, increasing the possibility of recovering lost data. However, key escrows require meticulous administration and organization compared to money reserves. Certificate-less signature encryption and an authenticated key encryption model utilizing hyperelliptic curve-based techniques are employed for this purpose.

Cluster head selection and session key generation can be done in a single step with conventional algorithms, but their genuineness and integrity are questionable. These systems also consume significant amounts of power and data. To ensure effective encryption, the total number of bits in the key can be analyzed. However, decoding encrypted data can take longer with multiple computers involved, and it's impossible to know the amount of encryption used until a transaction is complete. This can lead to issues with renewing certifications, lack of nonrepudiation, and forward secrecy.

Bilinear pairing security provides computational Diffie-Hellman assumption and guarantees nonrepudiation and secrecy. The private key of the user and controller is produced, but this system consumes a considerable amount of bandwidth and energy while avoiding public verification and antireplay. The proposed WBAN system, which uses ant colony optimization and fuzzy ontology techniques, is more efficient and practical than existing elliptical curve-based models. It ensures forward secrecy and confidentiality but doesn't address challenges in inter-user private key exchange and key escrow due to large traffic and energy requirements for binding and insufficient private key distribution. The proposed WBAN system is computationally efficient, authentic, and easily verifiable.

2.3 Preliminaries

Consider a predetermined set given by S_t with a hyperelliptic curve of genus hεc and presume δ, of the order $\delta \geq 2$,

$$h\varepsilon c \;=\; \omega^2 + (v)\;\omega \;=\; f(v) \tag{1}$$

Here, deg (h(v))$\leq\delta$ and f(v) and (v), f(v) ε S_t[v] is a monic polynomial with the deg f(v)=2δ+1. When compared to the elliptic curve, the hεc points are different. The order of the Jacobian group J_{hec} is as follows:

$$\left(\sqrt{t-1}\right)^{2\delta} \leq J_{h\varepsilon c}(S_t) \leq \left(\sqrt{t+1}\right)^{2\delta} \tag{2}$$

The discrete logarithm problem (dlP) provides the divisor d of the network with L, a randomly picked private number from S_t.

2.4 Architecture

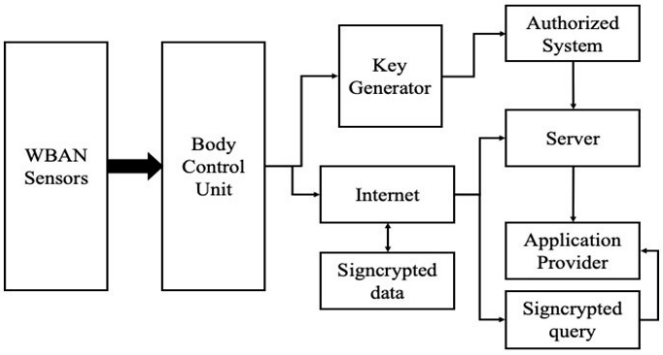

Fig 2. Block diagram of the proposed model

Figure 2 represents the block diagram of the proposed model. Low communication overhead and computational cost is crucial in WBAN signature encryption. Hyperelliptic and elliptic curves and bilinear paring techniques are used for encryption.

An optimum scheme is chosen and the pairing time is estimated. Hyperelliptic curve is an optimal choice in this case as it does not require additional transmission cost. Application developers, reputable authorities, controllers, sensors and other resource constrained devices are safeguarded using WBAN signature encryption model. The certificates and keys must be provided by a trusted third-party authority to use the public key cryptography. A signature encryption query is used for verifying the sender. The query is decrypted and transmitted to the controller by the application provider on confirming the data. A single key pair is used for encryption of the access control query that is transmitted to the controller by the application provider. The identity of the sender is verified to perform this action. Data is transmitted and received by the application provider using a secret key and encryption. This secret key is known only to the application provider and the controller. The use of symmetric encryption increases the speed of processing as the same key can be used for data encryption and description. However, the key exchange must be performed in a reliable manner. Data encryption can limit what users can read and write while using access control encryption (ACE)[24]. The resource constrained sensor data can be efficiently safeguarded using the signature encryption technique.

Secure channels are established with the use of key escrow and certificate management. However, these systems lack certain security features and require high computational costs for communication. Even though the concept of using keys in escrow look simple, it is possible to recoup cash even if the keying material or cryptographic keys are misplaced. In order to store the keys to be used when required, the key escrow is used. The key escrows need meticulous administration and organization when compared to money reserves. Certificateless signature encryption using WBAN dubbed secured channel architecture can overcome the issues of conventional key escrows. This technique overcomes the need for a secure route to distribute partial private keys among participants. KGCs, application providers, controllers and smart sensor nodes are used in this system.

3 Results and Discussion

Several tiny sensors are used for gathering the health information. A controller is required to process the data relayed by these sensors. Observant management, personal computers, laptops, PDAs and smartphones can receive the data from the sensors. The app developers can control this data. On obtaining a signed inquiry, the next line of inquiry is provided by the controller. The data checks, decryption and validation are performed here. An encrypted message is initially sent by the controller. The KGC is accessed by the partial private key. Two pieces of data can be combined together to create a private key by the user. The partial private keys (PPKs) are generated using master secret key generation machines (KGCs) while the user generates secret values. The master secret and its identity are hidden from the user. The public key of the user is the only data necessary for decoding the encrypted message by the third party. The identity of the user and public key is already available with the third party. The public keys can be exchanged by the opponents with the users. The private key can be used to validate the public keys of the user and does not include any certificates. The PPK must be available to the controller as it gathers the data and is used for creating the key pair.

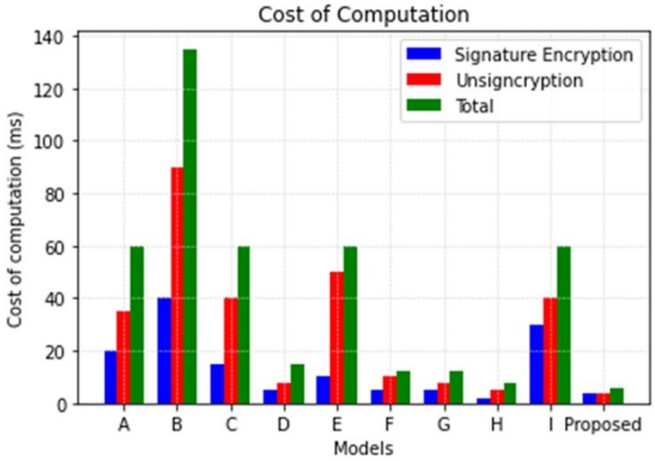

Fig 3. Computational cost in time

The developers have regained access to the private session and obtained a decryption key to decrypt the data. This technology ensures security and patient privacy through data encryption, as the controller decrypts and encrypts the signed access control.

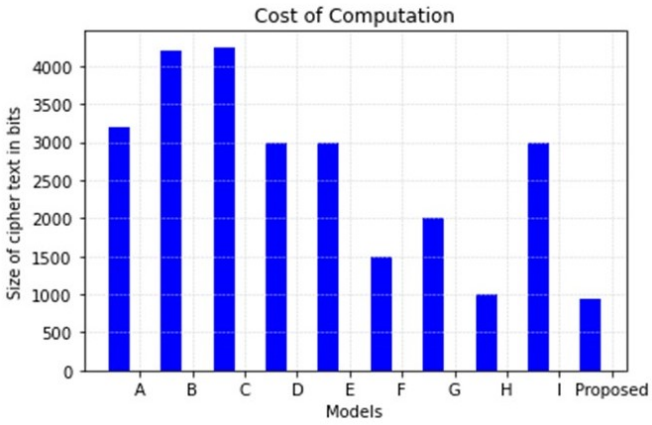

Fig 4. Computational cost in size

To create a fake signature, the controller requires a secret key. Even though the private or application provider controller key is available, disclosure is prevented. A comparison between the proposed and conventional techniques is provided regarding unsigncryption and signcryption, with the proposed model outperforming conventional techniques. The application vendors and controller identities remain concealed, and their IDs are not communicated in plain text. Conflicts between controllers and application providers are resolved using a new strategy and public verifiability security. Encryption and transfer of this data achieve replay-attack resistance. Figures 3 and 4represent the computational cost of the existing and proposed models in terms of time and size.

Table 1. Comparison of existing and proposed models in terms of computational cost

Code	Model	Signcryption		Unsigncryption		Total	
		Operations	Time (ms)	Operations	Time (ms)	Operations	Time (ms)
A	Omala et al.[17]	3 esm	2.91	4 esm	2.91	7 esm	5.82
B	Arul et al.[18]	3 esm	36.63	4 esm	92.84	7 esm	148.68
C	Ullah et al.[19]	4 esm	2.03	4 esm	2.03	8 esm	4.06
D	Gao et al.[20]	3 esm	2.91	2 esm	3.88	5 esm	6.77
E	Kiran et al.[21]	4 esm	4.05	4 esm	6.02	8 esm	10.07
F	Braken et al.[22]	5 esm	3.88	5 esm	4.85	10 esm	8.73
G	Saeed et al.[23]	3 esm	3.02	3 esm	3.04	6 esm	6.06
H	Bouani et al.[24]	3 esm	3.02	2 esm	4.99	5 esm	8.01
I	Li et al.[25]	4 esm + 1 mxp	5.13	2 esm +1 mxp + 2 bp	31.81	6 esm + 2 mxp + 2 bp	36.94
Proposed		3 hsm	2.03	3 hsm	2.35	6 hsm	4.38

When designing a cryptographic algorithm, it involves expensive mathematical operations that add to the computational cost. These operations include hyper-elliptic curve divisor scalar multiplication (HSM), elliptic curve scalar multiplication (ESM), modular exponential (MXP), and bilinear pairing (BP). Table 1 compares the computational cost and time of existing and proposed models based on mathematical operations. In the proposed model, the Certificateless Online/Offline Signcryption (COOSC) technique addresses the issues faced by conventional methods that aren't suitable for devices with limited resources. Figure 5 shows the private key sizes of three schemes at different security levels.

The security performance is measured in terms of formal verification, random oracle mode, public verifiability, forward secrecy, anti-replay attack, integrity, authentication, unforgeability, and confidentiality. Table 2 provides the comparison of the average of selected parameters of the proposed model with respect to the existing models.

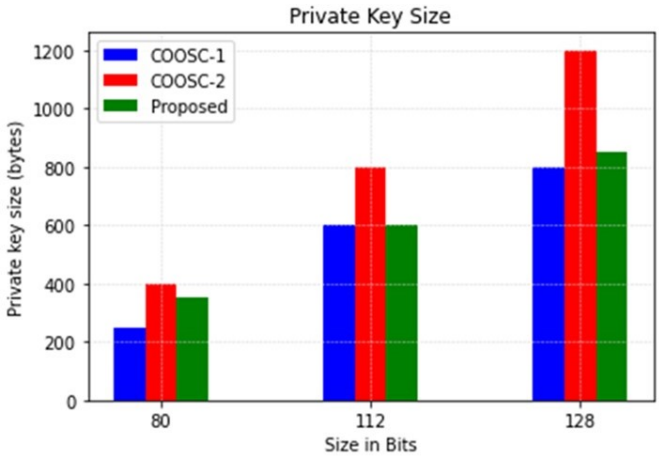

Fig 5. Comparison of private key size

Table 2. Average of selected parameters

Code	Model	Parameters		
		Security requirements	Security hardness	Security strength
A	Omala et al. [17]	0	0.5	1
B	Arul et al. [18]	0	0	0.5
C	Ullah et al. [19]	0	1	0
D	Gao et al. [20]	1	0	0
E	Kiran et al. [21]	1	0	1
F	Braken et al. [22]	1	1	1
G	Saeed et al. [23]	1	0.5	1
H	Bouani et al. [24]	0	0.5	0
I	Li et al. [25]	1	1	1
Proposed		0.55	0.25	0.65

4 Conclusion

The proposed algorithm involves an encryption model that utilizes an authenticated certificate-less signature key and a strategy based on hyperelliptic curves. This approach safeguards against harmful attacks like MMA, BIA, and KOA, and provides strong resistance against unauthorized access. It overcomes issues related to key escrow and certificate management and offers a secure connection with low-cost data processing and transmission. The system eliminates the need for certificate revocation or renewal by removing the requirement for a central authority. Instead, it utilizes certificate-less signature encryption and an authenticated key encryption model to ensure forward secrecy and confidentiality. This approach overcomes the challenges of inter-user private key exchange and key escrow, which have large traffic and energy requirements for binding and insufficient private key distribution. The effectiveness of this methodology is evaluated using parameters such as HSM operations and time taken, which show its superiority when compared to traditional approaches. In fact, the proposed methodology records only 3 HSM operations within 2.03 ms with Signcryption and 3 HSM operations within 2.35 ms with Unsigncryption, demonstrating its superiority over other traditional approaches. Future work aims to protect against other types of malicious attacks and include multi-factor authentication in cloud-assisted networks.

References

1) Pawar RS, Kalbande DR. Optimization of quality of service using ECEBA protocol in wireless body area network. *International Journal of Information Technology*. 2023;15(2):595–610. Available from: https://doi.org/10.1007/s41870-022-01152-z.
2) Shahbazi Z, Byun YC. Towards a Secure Thermal-Energy Aware Routing Protocol in Wireless Body Area Network Based on Blockchain Technology. *Sensors*. 2020;20(12):1–26. Available from: https://doi.org/10.3390/s20123604.

3) Jegadeesan S, Azees M, Babu NR, Subramaniam U, Almakhles JD. EPAW: Efficient Privacy Preserving Anonymous Mutual Authentication Scheme for Wireless Body Area Networks (WBANs). *IEEE Access*. 2020;8:48576–48586. Available from: https://ieeexplore.ieee.org/document/9022923.
4) Jabeen T, Ashraf H, Ullah A. A survey on healthcare data security in wireless body area networks. *Journal of Ambient Intelligence and Humanized Computing*. 2021;12(5):9841–9854. Available from: https://doi.org/10.1007/s12652-020-02728-y.
5) Liu H, Chen Y, Tian H, Wang T. A Secure and Efficient Data Aggregation Scheme for Cloud-Assisted Wireless Body Area Network. *International Journal of Network Security*. 2019;21(2):243–249. Available from: https://doi.org/10.6633/IJNS.201903_21(2).08.
6) Liu S, Chen L, Wang H, Fu S, Shi L. O^3HSC: Outsourced Online/Offline Hybrid Signcryption for Wireless Body Area Networks. *IEEE Transactions on Network and Service Management*. 2022;19(3):2421–2433. Available from: https://ieeexplore.ieee.org/document/9718545.
7) Vijayakumar P, Obaidat MS, Azees M, Islam SH, Kumar N. Efficient and Secure Anonymous Authentication With Location Privacy for IoT-Based WBANs. *IEEE Transactions on Industrial Informatics*. 2020;16(4):2603–2611. Available from: https://ieeexplore.ieee.org/document/8746610.
8) Zhang J, Zhang Q, Li Z, Lu X, Gan Y. A Lightweight and Secure Anonymous User Authentication Protocol for Wireless Body Area Networks. *Security and Communication Networks*. 2021;2021:1–11. Available from: https://doi.org/10.1155/2021/4939589.
9) Awotunde JB, Chakraborty C, Folorunso SO. A Secured Smart Healthcare Monitoring Systems Using Blockchain Technology. In: Ghosh U, Chakraborty C, Garg L, Srivastava G, Srivastava, G, editors. Intelligent Internet of Things for Healthcare and Industry . Internet of Things book series;Springer, Cham. 2022;p. 127–143. Available from: https://doi.org/10.1007/978-3-030-81473-1_6.
10) Wang Y, Zhang A, Zhang P, Wang H. Cloud-Assisted EHR Sharing With Security and Privacy Preservation via Consortium Blockchain. *IEEE Access*. 2019;7:136704–136719. Available from: https://ieeexplore.ieee.org/document/8846684.
11) Tang J, Nie J, Yang W, Lim B, Zhang Y, Xiong Z, et al. Intelligent Edge-Aided Network Slicing for 5G and Beyond Networks. In: ICC 2022 - IEEE International Conference on Communications, 16-20 May 2022, Seoul, Korea, Republic of. IEEE. 2022;p. 1–6. Available from: https://ieeexplore.ieee.org/document/9882270.
12) Wang J, Han K, Alexandridis A, Chen Z, Zilic Z, Pang Y, et al. A blockchain-based eHealthcare system interoperating with WBANs. *Future Generation Computer Systems*. 2020;110:675–685. Available from: https://doi.org/10.1016/j.future.2019.09.049.
13) Omala AA, Ali I, Li F. Heterogeneous signcryption with keyword search for wireless body area network. *Security and Privacy*. 2018;1(5). Available from: https://doi.org/10.1002/spy2.25.
14) Prabadevi B, Deepa N, Pham QV, Nguyen DC, Reddy MPK, Reddy GT, et al. Toward Blockchain for Edge-of-Things: A New Paradigm, Opportunities, and Future Directions. *IEEE Internet of Things Magazine*. 2021;4(2):102–108. Available from: https://ieeexplore.ieee.org/document/9409843/authors#authors.
15) Noor F, Kordy TA, Alkhodre AB, Benrhouma O, Nadeem A, Alzahrani A. Securing Wireless Body Area Network with Efficient Secure Channel Free and Anonymous Certificateless Signcryption. *Wireless Communications and Mobile Computing*. 2021;2021:1–14. Available from: https://doi.org/10.1155/2021/5986469.
16) Hussain S, Ullah I, Khattak H, Adnan M, Kumari S, Ullah SS, et al. A Lightweight and Formally Secure Certificate Based Signcryption With Proxy Re-Encryption (CBSRE) for Internet of Things Enabled Smart Grid. *IEEE Access*. 2020;8:93230–93248. Available from: https://ieeexplore.ieee.org/document/9094323.
17) Kasyoka P, Kimwele M, Angolo SM. Towards an Efficient Certificateless Access Control Scheme for Wireless Body Area Networks. *Wireless Personal Communications*. 2020;115(2):1257–1275. Available from: https://doi.org/10.1007/s11277-020-07621-7.
18) Kiran GM, Nalini N. Enhanced security-aware technique and ontology data access control in cloud computing. *International Journal of Communication Systems*. 2020;33(15). Available from: https://doi.org/10.1002/dac.4554.
19) Shabisha P, Braeken A, Touhafi A, Steenhaut K. Elliptic Curve Qu-Vanstone Based Signcryption Schemes with Proxy Re-encryption for Secure Cloud Data Storage. In: International Conference of Cloud Computing Technologies and Applications: CloudTech 2017: Cloud Computing and Big Data: Technologies, Applications and Security;vol. 49 of Lecture Notes in Networks and Systems. Springer International Publishing. 2018;p. 1–18. Available from: https://link.springer.com/chapter/10.1007/978-3-319-97719-5_1.
20) Shan S. Cryptanalysis of a Certificateless Hybrid Signcryption Scheme and a Certificateless Encryption Scheme for Internet of Things. *Security and Communication Networks*. 2022;2022:1–6. Available from: https://doi.org/10.1155/2022/6174031.
21) Elkhalil A, Zhang J, Elhabob R, Eltayieb N. An efficient signcryption of heterogeneous systems for Internet of Vehicles. *Journal of Systems Architecture*. 2021;113:101885. Available from: https://doi.org/10.1016/j.sysarc.2020.101885.
22) Liu X, Wang Z, Ye Y, Li F. An efficient and practical certificateless signcryption scheme for wireless body area networks. *Computer Communications*. 2020;162:169–178. Available from: https://doi.org/10.1016/j.comcom.2020.08.014.
23) Anbarasan HS, Natarajan J. Blockchain Based Delay and Energy Harvest Aware Healthcare Monitoring System in WBAN Environment. *Sensors*. 2022;22(15):1–29. Available from: https://doi.org/10.3390/s22155763.
24) Wang J, Han K, Alexandridis A, Chen Z, Zilic Z, Pang Y, et al. A blockchain-based eHealthcare system interoperating with WBANs. *Future Generation Computer Systems*. 2020;110:675–685. Available from: https://doi.org/10.1016/j.future.2019.09.049.
25) Hu Y, Hu A, Li C, Li P, Zhang C. Towards a privacy protection-capable noise fingerprinting for numerically aggregated data. *Computers & Security*. 2022;119:102755. Available from: https://doi.org/10.1016/j.cose.2022.102755.