Hindawi
Journal of Sensors
Volume 2023, Article ID 9865746, 1 page
https://doi.org/10.1155/2023/9865746

Retraction

Retracted: Efficient and Secure Key Management and Authentication Scheme for WBSNs Using CP-ABE and Consortium Blockchain

Journal of Sensors

Received 19 December 2023; Accepted 19 December 2023; Published 20 December 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

In addition, our investigation has also shown that one or more of the following human-subject reporting requirements has not been met in this article: ethical approval by an Institutional Review Board (IRB) committee or equivalent, patient/participant consent to participate, and/or agreement to publish patient/participant details (where relevant).

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] J. Iqbal, H. Bibi, N. U. Amin et al., "Efficient and Secure Key Management and Authentication Scheme for WBSNs Using CP-ABE and Consortium Blockchain," *Journal of Sensors*, vol. 2022, Article ID 2419992, 20 pages, 2022.

Hindawi
Journal of Sensors
Volume 2022, Article ID 2419992, 20 pages
https://doi.org/10.1155/2022/2419992

Research Article

Efficient and Secure Key Management and Authentication Scheme for WBSNs Using CP-ABE and Consortium Blockchain

Jawaid Iqbal,[1] **Hajira Bibi**,[2] **Noor Ul Amin**,[2] **Hussain AlSalman**,[3] **Syed Sajid Ullah**,[4] **Saddam Hussain**,[5] **and Naziha Al-Aidroos**[6]

[1]*Department of Computer Science Capital University of Science and Technology, Islamabad, Pakistan*
[2]*Department of Information Technology Hazara University Mansehra, Pakistan*
[3]*Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia*
[4]*Department of Information and Communication Technology, University of Agder (UiA), N-4898 Grimstad, Norway*
[5]*School of Digital Science, Universiti Brunei Darussalam, Jalan Tungku Link, Gadong BE1410, Brunei Darussalam*
[6]*Department of Computer Science, College of Computers and Information Technology, Hadhramout University, Hadhramout, Yemen*

Correspondence should be addressed to Syed Sajid Ullah; syed.s.ullah@uia.no and Naziha Al-Aidroos; naz.moh@hu.edu.ye

Received 16 February 2022; Accepted 1 September 2022; Published 22 September 2022

Academic Editor: Pradeep Kumar Singh

Wireless body sensor networks (WBSNs) pose significant security and privacy risks. The Medical Server (MS) will only allow legitimate stakeholders access to confidential patient medical records when successful mutual authentication between all registered users and the MS has been confirmed using preset secret attributes. This paper proposes a novel approach to overcome the security and privacy problems in WBSNs by using CP-ABE and a consortium blockchain for key management and authentication. In this paper, a fixed-size session key is computed by utilizing several attribute base rules and AND/OR logic gate combinations. IEEE 802.15.6 is also used to transmit the encoded patient data from the register and legitimately deployed biosensor nodes on a patient's body to the Base Station nearby (BS). This was done in part by leveraging consortium blockchains to construct partial blocks and then, transmit the encrypted partial blocks to MS via peer-to-peer networks, as well as aggregating critical physiological information. MS is now validating partial blocks with a hash function to ensure their integrity before converting them all into full blocks, which are subsequently mined and put on the blockchain effectively and ideally using a consensus mechanism. When sessions between MS and stakeholders are established, all legitimate consumers can view the secure medical records of a registered patient in a hospital using their predefined access structure.. The resource-constrained environment of WBSNs can benefit from enhanced data security and privacy by using CP-ABE in conjunction with the organization's consensus to encrypt the patient's critical features or attributes. Automated Validation of Internet Security Protocol and Applications (AVISPA) tool is used to verify the validity and correctness of the proposed authentication mechanism. The proposed scheme reduces transmission, processing and storage costs and energy usage by a significant margin when compared to current state-of-the-art alternatives. It is also worth noting that a multicriteria decision making (MCDM) approach known as Evaluation Based on Distance from Average Solution (EDAS) is employed to provide the ranking and determine which strategy is optimal across all of the domains involved.

1. Introduction

Wireless communications have significantly changed our way of life and the way health care services are delivered. To have a good impact on healthcare systems, there is a growing interest in illness prevention and early diagnosis, as well as optimal chronic disease management. The use of a Wireless Sensor Network (WSN) can aid in the development of a system that is capable of responding to crises and managing diseases. WBSNs are a subset of WSN in which various biosensor nodes are deployed on a human body to monitor real-time physiological signals such as pulse rate, ECG, EEG, BP, SPO2, and temperature in order to control the incidence of diseases, monitor vital signs on a regular basis, and treat patients to improve their quality of life. Aside from that, using the IEEE 802.15.6 standard, the Base Station (BS) or sink node directly collects the sensed physiological signals from deployed biosensor nodes, which are then forwarded to the Medical Server (MS) for further diagnosis based on their symptoms, and then, provides treatment to stop the progression of diseases in patients. Chronic patients, such as those with heart disease, Parkinson's disease, or epilepsy, are monitored by WBSNs in order to extend their lives. Furthermore, a patient's physiological data is exceedingly private, and maintaining its secrecy and privacy is vital. As a result, security and privacy are essential research domains in the modern period, particularly when a patient suffers from a humiliating illness.

Despite diseases are becoming more prevalent today, technology innovations are helping to address healthcare-related problems. The world's population is growing quickly as a result of numerous medical and health achievements. For instance, the number of individuals 65 age and older is predicted to double in in the US by 2040 [1], but the number of people 60 age and older is predicted to double in China by 2040 [2]. In a summary, estimations indicate that older adults with a range of diseases will probably face increased health issues and financial strains in the future. [3–5]. Since it is possible that patients' needs will not be met by the current healthcare system in the near future [4–6].

Through the fast development of sensors and wireless communication [7], WBSNs have developed for the improvement of existing healthcare-related problems.

After carefully examining WBSNs, we came to the conclusion that security and privacy are the two main issues. Although numerous studies have demonstrated the security and privacy of WBSNs, they still have vulnerabilities, including high processing and transmission costs, man-in-the-middle attacks, replay attacks, square root attacks, forgery attacks, and chosen ciphertext attacks. In order to strengthen the security and privacy of patient health records at a minimal cost, we developed an effective and secure key management and authentication mechanism for WBSNs. In this study, we combined CP-ABE and consortium blockchain into a hybrid approach. Additionally, CP-ABE is a useful and effective technology for enabling fine-grained access control, which allows only legitimate users to have access.

Where security and privacy preservation are essential considerations in the WBSNs, patient health data exchange can help to improve diagnosis accuracy. Due to its immutability, consortium blockchain has been touted as a viable option for achieving patient data sharing with security and privacy protection in recent decades. This paper presents CP-ABE along with a consortium blockchain based scheme to improve patient data security and privacy by the utilization of minimal resources. Moreover, the patient data records are transmitted and stored in authentic and secure way to the MS to protect it from adversaries' attacks in WBSNs. Besides, it achieves data security and access control, along with privacy preservation in a desirable way.

When it comes to outsourced encrypted data, attribute-based encryption (ABE) is a potential cryptographic solution that might be used for fine-grained access control [8–15]. In today's dynamic environment, traditional ABE systems [16–23] imply a fixed access policy, which is incompatible with today's dynamic environment. Although many ABE systems with dynamic access control policies have been described, these schemes do not address forward security, backward security, or integrity protection even if a policy changes [24–27]. In scheme [28], authors highlighted the security weakness in the previous authentication scheme and then, proposed a novel and efficient scheme to protect information from adversaries' attacks. Furthermore, the scheme demonstrated session key security by employing the ROR model. The authors of scheme [29] highlighted the shortcomings of ECC-based IoT communication, such as scalability and correctness, and proposed a novel scheme to address the aforementioned security flaws in an efficient and desirable manner. In scheme [30], authors highlighted the weakness of the Rajaram et al. scheme and proposed a novel and secure scheme for mutual authentication using smart cards. Moreover, in scheme [31], they reviewed the user authentication mechanisms using smart cards to avoid illegal access. In scheme [32], the authors proposed efficient and secure smart card-based authentication to protect information during transactions. In scheme [33], the authors proposed a lightweight, efficient, and anonymous scheme to satisfy the security properties of authentication and confidentiality in the resource limited environment of WBANs. In scheme [34], a novel and secure method called BBAAS was proposed that enhanced the security and privacy of VANET communication and permitted only authorized vehicles to join the network and access the sensitive information. Khalid et al. [35] elaborated about the potential of blockchain technologies, and how the private and consortium nature of the blockchain can be vital for the reforms in various use cases. Xu et al. discussed about the verifiable multikeyword search over encrypted data based on blockchain in detail [36]. Similarly, the use of the consortium blockchain has been discussed by Ehsan et al. [37].

We have created various security policies using CP-ABE to permit the use of patient data and to shield enemies from unauthorized access to patient data. Contrarily, a consortium blockchain is a type of blockchain that is controlled by a collection of working parties that conduct transactions on the blockchain in an effort to enhance governance, transparency, interoperability, traceability, and universal access. Furthermore, blockchain is a wholly decentralized network that does not require a central authority. The adoption of cryptographic algorithms also makes transactions secure and dependable [38–41]. The success of cryptocurrencies has made blockchain technology more well-known recently, but it has also migrated into a number of other fields. The use of blockchain in improving the accuracy of electronic medical patient records kept in MS is critical. The following are some of our important contributions.

(i) We design a novel and efficient key management and authentication protocol for resource constrained environment of WBSNs to enhance the patient data security and privacy by utilizing minimal resource.

(ii) First, we describe a method for building a CP-ABE with hidden attribute base access policies that is secure under the gap bilinear Diffie-Hellman assumptions.

(iii) In this study, access policies can be designed using AND/OR Boolean operators. Besides, each access policy attribute might have numerous values to design a complex structure.

(iv) Merkle Hash Tree can be used to express access policies along with verify the data structure by using hash function; the leaf nodes indicate the attribute present in the access policy/structure, while the interior nodes represent the AND/OR operators.

(v) Furthermore, we use the concept of consortium blockchain to enhance network interoperability, traceability, scalability, privacy, and universal access.

(vi) Our proposed scheme has been validated using the AVISPA tool and a well-known multicriteria decision making (MCDM) approach known as Evaluation Based on Distance from Average Solution (EDAS) is also used to demonstrate the ranking and to pick the best scheme among the entire domain.

(vii) The obtained numerical results along with security analysis demonstrate that our scheme is secure and efficient in terms of processing cost, communication overhead, storage cost, and energy consumption as compared to other state-of-the-art schemes.

The following parts of the article are structured as follows. Section 2 presents the interrelated works. In Section 3, the construction and network models are covered. Section 4 presents security analysis. Section 5 contains the analysis of cost-effectiveness. Section 6 concludes our research by bringing it to a conclusion.

2. Related Work

In this section, we discuss the related studies about WBSNs, CP-ABE, and consortium blockchain systems in detail, which are as follows:

Ren et al. [42] claim that WBANs devices cannot fulfil the requirements of users on the basis of security and privacy. In this paper, they contribute to adopt the blockchain technology to save data and upgrade the security as per user requirements. Furthermore, a storage model based on blockchain is designed to improve data security. To improve user privacy in WBANs environments, information is only seen by a designated person. Besides, the proposed new signature decreased the storage space of blockchain to efficiently manage the resources of the system.

Hong et al. [43] describe how different users access the patient's data in different scenarios. Access control of information is a significant problem here. They created a security mechanism that combines public-key cryptosystems and attribute-based encryption to address user access control in the constrained environment of WBANs. Furthermore, CP-ABE access policies are used to achieve data confidentiality and access control, while CP-ABS is used for real authentication, but this scheme still has a high computational cost in the key generation process.

Zhang et al. [44] propose a scheme for the security of physical health-related data in the cloud where patient detail history is stored in a secure manner. In this paper, after the verification process, the new block data is added to the blockchain for onward processing. Besides, it is a suitable approach for dynamic settings but still suffers due to impersonation attack and time-controlled revocation.

Bramm et al. [45] propose a novel and efficient scheme to improve security and privacy. In this scheme, the authors applied the Blockchain-based Distributed Attribute Based Encryption (BDABE) technique to store data on the cloud so it is easily available to the registered legal users from anywhere using an internet connection. Moreover, using this approach, the security and privacy are significantly improved, but the distribution of keys consumes more processing power, which is infeasible for the WBSN setting.

According to Al-Dahhan et al. [46], CP-ABE is a reliable method for implementing fine-grained access control in cloud storage. Additionally, this plan divides the access policies into two phases. Single authorities established policies for network registered users during the initial phase using the access structure. Using a single master secret key, a single attribute authority controls all system attributes. Additionally, an access structure is linked to each user's private decryption key in order to enhance system privacy in a practical and desirable way. Additionally, in the second step, multiple characteristics are divided into access structures and then, assigned to the registered stockholders for accessing private data from the cloud, according to the guidelines and rules of multiauthority attribute-based access control. This system can tolerate Type-I attacks but not Type-II attacks.

Zhang et al. [47] propose a novel scheme called multiattribute-based encryption. Authors provided different access control rights on stored data at the server in this scheme. Besides, only authorized users can be able to access the sensitive data stored on MS according to the valid and authentic attributes. Furthermore, for the management and security of IoT devices, blockchain technology is advised in this scheme to achieve transparency and interoperability in an efficient way.

Zhang et al. [48] proposes Cipher Text-Policy Attribute Based Signcryption (CP-ABSC) to reduce the computational cost and communication overhead of the resource constrained environment. Furthermore, the authors claimed that this scheme is protected against Type-I and Type-II adversary attacks, but according to our analysis, this scheme is still suffering due to Type-II adversary attacks and does not meet the required security features.

Lai et al. [49] propose a secure technique which is a combination of CP-ABE and CP-ABSC to achieve confidentiality, integrity, authentication, and surveillance. Furthermore, using this scheme, well-known attacks are protected, such as replay and impersonation attacks. Moreover, message verification is performed to check the integrity of the received data on the server side. This scheme is still suffering due to the high cost of the de-signcryption phase.

For effective and secure fine-grained access control, Hu et al. [50] propose a system based on File Hierarchy Cipher text-Policy Attribute Based Encryption (FH-CP-ABE). Additionally, this approach incorporated a number of attributes to construct an access configuration for a hierarchically encrypted file. According to authors, it performs better than other cutting-edge approaches that have been published in the literature. Additionally, it provided confidentiality, authentication, and integrity as security attributes but lacked nonrepudiation. The network performance has drastically declined, which prevents the designed access policies in this system from being more flexible [51–53].

Möser et al. [54] propose a scheme which is discovered on blockchain storage space in which authors used the concept of digital signature for guarantee confidentiality and security of data gathered in from biosensor nodes on WBANs environment. Furthermore, at the end, data is transfer toward the cloud for online accessing and to improve the security of the sensitive medical information.

Pal et al. [55] propose a scheme to resolve the access control problem and policy management in IoT. The proposed architecture highlighted the significance of access control in the public network where adversaries attack on the server to access personal and confidential information. In this scheme authors design a novel and efficient privacy protection mechanism using secret key cryptosystem to achieve fine grained access control along with protection of data from unauthorized users. Moreover, decentralized authentication system for IoT allows healthcare system to deliver reasonable replay in low time power-driven devices. Besides, using innovative microcontroller used in this architecture can overcome the computational burden on the client side for improving the performance of the networks.

Ding et al. [56] design a trustable attribute-based access control in IoT devices to enhance the reliability, accuracy, and security of the transmitted data using open wireless channel. In this scheme, blockchain technology used to record sharing of attributes, ignore collapse on a point, and protect data tempering using encrypted hash. Other properties which are fulfill by this scheme are high productivity and light computation. This scheme helps to prevent multiple attacks on cloud data and adequately appliance on IoT systems.

Gao et al. [57] propose a scheme which helps to enhance the security of physical health information in WBANs and fully controlled accessibility using Certificateless Signcryption (CLSC). Proposed scheme is an appropriate because it is demonstrating by mathematical rules and equations. This scheme also provides privacy and unforgeability for indiscriminate model of Computational Diffie-Hellman (CDH) and Discrete Logarithms (DL) problems. This scheme also provides better security in terms of less computational cost and utilized less energy as compared with other access control schemes.

Gupta et al. [58] propose a scheme based on blockchain technology to improve the data security and privacy on server side and protect adversaries from illegal attacks. The proposed algorithm ensured to protect DDoS attack and arrangement for hash value. This additive factor implements the algorithm to use physical healthcare related data for better management on cloud. Moreover, the proposed scheme ensured data privacy, access control, and secured search function. Obtained results of the proposed scheme are also providing low latency at 400 req/sec (less than750ms).

Gupta [19] suggests a new Attribute Based Keyword Search (ABKS) technique with consistent-size secret keys and cypher texts, to improve the security of m-Health system. Moreover, it is built a cipher text-policy design framework to stored data on cloud using secure access structure. In addition, the suggested CP-ABKS system can be shown to be secure in the selected security model using augmented multisequence of exponents decisional logic. Additionally, it does fulfill the security properties of mutual authentication and forward and backward secrecy. Besides, adversaries can easily perform square root attack to expose the confidential information.

For blockchain-enabled, WBANs in fog computing, Guo et al. [20] introduce a lightweight verifiability cypher text-policy attribute-based encryption protocol with outsourced decryption. However, this scheme is still suffered due to forgery and chosen ciphertext attacks.

Using 0-1 coding technology, Li et al. [21] offer a novel access policy expression approach for IoHT. The scheme accepts not only weighted attributes but also any type of weighted attribute comparison. The authors employ offline/online encryption and outsourced decryption technologies. Therefore, it consumed high resources in terms of communication cost and energy consumption due to overhearing and does not suitable for resource constrained environment. Furthermore, this study is insecure against replay, square root, along with chosen ciphertext attacks.

For secure data access in the cloud, Sivasangari et al. [22] develop attribute-based encryption for accessing medical data. The propose method is assessed based on its false acceptance rate (FAR), false rejection rate (FRR), and half total error rate (HTER). The system is tested at different levels of tolerance. Moreover, the results of the simulation suggest that the propose work is efficient in term of performance than the other previous methods but consume more energy during key exchange process. Besides, this study is insecure in their define security model and does not provide protection against forgery attack, and still needs improvement in terms of data security and privacy.

Wang et al. [23] present a unique multiserver edge computing architecture and handover authentication mechanism for ITS that allows the authenticated server to help users in afterwards authenticating with another server. Finally, blockchain technology and a robust anonymity mechanism are incorporated to ensure that users' privacy is protected to the fullest extent possible. The suggested approach, according to the authors, is the first in the literature to provide efficient authentication, stringent anonymity, and computational load transfer all at the same time. According to the authors the scheme improves the cost complexities but still needs improvements in terms of performance.

Jiang et al. [59] propose a scheme for health data transmission using blockchain. Furthermore, in this scheme, authors have proposed two loosely coupled methods based on blockchain to control and manage various types of healthcare data. Later, combined the off-chain storage and on chain verification to fulfill the security properties of authentication and privacy.

FAIR-PACK, the first fairness-based transaction packing technique for permissioned blockchain-enabled IIoT systems, is proposed by Jiang et al. [60]. First, we observe from theoretical studies that fairness is strongly correlated with the total waiting times for the chosen transactions. Based on this concept, we transform the fairness problem into the subset sum problem, which asks us to choose a valid subset from a given set with the highest subset sum possible. An exponentially large number of subsets exist for each set, making it difficult to solve the issue using a brute-force strategy. We provide a heuristic and a min-heap-based optimum technique for different parameter selections to improve performance.

Jiang et al. [61] propose a bloom filter-enabled multikeyword search protocol with improved efficiency and privacy preservation. When executing a multikeyword search, the protocol will employ a low frequency term selected by a bloom filter to filter the database.

Fine-grained access control is a technique where actual users can authenticate the data, except malicious users. In a dynamic environment, traditional schemes are used, which are not suitable due to fixed access policies. On the other hand, some ABE schemes have been introduced, but they have not addressed the forward secrecy, backward secrecy, and integrity achieved with policy updating. Therefore, an efficient and secure key management and authentication scheme are needed to enhance data security and privacy using CP-ABE and consortium blockchain. A CP-ABE is a type of policy in which the system administrator assigns different access policies to different users for data encryption and decryption. Moreover, consortium blockchain provides decentralization and a public ledger to improve the privacy of the networks.

3. Proposed Scheme

In our propose CP-ABE we have assume a set of attributes ($\mathscr{A}$), session key ($\mathscr{S}_{\mathscr{K}}$), and cipher text ($\mathscr{C}_{\text{i}}$) and access structure ($\mathbb{A}$). The relationship of ($\mathscr{A}$) is depend on ($\mathscr{S}_{\mathscr{K}}$) and ($\mathscr{C}_{\text{i}}$). Moreover, ($\mathbb{A}$) is derived from set of attributes using AND/OR logic gates. Data consumers only access the ($\mathscr{C}_{\text{i}}$), if it has attributes matched with predefined access tree. Our designed CP-ABE scheme comprises of four phases, which are the setup phase, key agreement and authentication phase, the encoding phase, and the last one is the decoding phase:

Setup phase: in this phase, the system administrator takes initial security parameters and a description of valid attributes, public key, and master secret key. Moreover, the system administrator is responsible for protecting all these initial security parameters from adversaries' attacks

Key agreement and authentication phase: in this phase, mutual authentication and key agreement are performed to securely generate and distribute secret session keys for onward secure communication among biosensor nodes, BS, and MS. However, secret key updates are also performed on each session to maintain the key exposer problem by using forward and backward secrecy. Moreover, we use algorithms 1 and 2 for key agreement and authentication among biosensor nodes, MS, and stakeholders

Encoding phase: patient vital signs were encoded using the public key of the concerned data consumer and a set of attributes, policies, and generated cipher text. Furthermore, the access structure ($\mathbb{A}$) of the MS is used to store the patient data in a secure and efficient manner. Besides, we use algorithm 3 for patient data encoding

Decoding phase: in this phase, data consumers such as nurses, doctors, family members, researchers, and security agencies take cipher text and some other system parameters as an encrypted input. Furthermore, only these users can decode the patient's sensitive data, which attribute matched with the assigned attribute's structure. Additionally, we applied algorithm (4) for the decoding process to obtain the patient's information for decision making

3.1. Proposed Network Architecture. In this section, we design efficient network architecture for WBSNs communication using CP-ABE with consortium blockchain to improve patient data security and privacy and protect patient data from adversaries' attacks. The following Figure 1 shows the network model for data communication in the resource constrained environment of WBSNs.

In our proposed scheme, only authorized users can access the patient's secure information stored on MS after verification of attributes-based access policies which are defined by the system administrator at the deployment time of the biosensor nodes on a patient's body. As shown in Figure 1, there are multiple numbers of entities involved in the communication architecture, which are as follows:

(1) System administrator

(2) Medical service provider

(3) Data owner

(4) Consortium blockchain

(5) Medical data server

(6) Validation server

(7) Data consumers

3.1.1. System Administrator. The system administrator is working as a manager of the WBSNs and handles all the attribute-based policies that are designed to enhance patient data privacy in an efficient and desirable way. Besides, all the

```
Input→data get $(\mathcal{M}_{\mathcal{S}\mathcal{K}}, \mathcal{I}\mathcal{D}_{\mathcal{S}i}, S_i, M_i, \mathcal{E}_{\mathcal{K}r1}, \mathcal{T}_{\mathcal{S}}, \mathcal{N}_{\mathcal{Y}}, \mathcal{E}_{\mathcal{S}_{\mathcal{K}}})$
System administration deployed $\mathcal{M}_{\mathcal{S}\mathcal{K}}$ on Sink nodes/BS, along with Medical Server (MS)
Preloaded $\mathcal{I}\mathcal{D}_{\mathcal{S}i}$ of all deployed registered sensor nodes on to the sink node
Biosensor node $(S_i)$ continuously sense real time vital signs $(M_i)$
If vital sign $(M_i)$ value < predefined threshold value
Then Discard $(M_i)$
Else
Transmitted $(M_i)$ toward the $\mathcal{B}\mathcal{S}$
Computes $\mathcal{Q} = \mathcal{K}\mathcal{H}_{\mathcal{K}1}(M_i \| \mathcal{T}_{\mathcal{S}})$
Computes $\mathcal{C}_i = \mathcal{E}_{\mathcal{K}r1}(M_i \| \mathcal{Q} \| \mathcal{N}_{\mathcal{Y}} \| \mathcal{I}\mathcal{D}_{\mathcal{S}i})$
Transmitted $\mathcal{C}_{\mathrm{i}}$ toward the sink nodes/BS
BS computes $(M_i \| \mathcal{Q} \| \mathcal{N}_{\mathcal{Y}} \| \mathcal{I}\mathcal{D}_{\mathcal{S}i}) = \mathcal{D}_{\mathcal{P}r}(\mathcal{C}_i)$
Compared $\mathcal{I}\mathcal{D}_{\mathcal{S}i}$= pre-stored $\mathcal{I}\mathcal{D}_{\mathcal{S}i}$
If $\mathcal{I}\mathcal{D}_{\mathcal{S}i} = \mathcal{I}\mathcal{D}_{\mathcal{S}i}{}'$ then authentication granted
Else
Request disallowed and blacklisted from network
Computes $\mathcal{S}_{\mathcal{K}} = \mathcal{X}/\mathscr{r} + \mathcal{X}_{\mathscr{a}}\mathscr{m}\mathcal{O}\mathscr{d}\mathscr{q}$
Computes $\mathcal{T} = \mathcal{E}_{\mathcal{M}_{\mathcal{S}\mathcal{K}}}(\mathcal{S}_{\mathcal{K}})$
Transmitted $(\mathcal{T})$ towords the MS
MS computes $\mathcal{S}_{\mathcal{K}} = \mathcal{D}_{\mathcal{M}_{\mathcal{S}\mathcal{K}}}(\mathcal{T})$
$\mathcal{G} = \mathcal{K}\mathcal{H}_{\mathcal{K}2}(\mathcal{S}_{\mathcal{P}} \| \mathcal{T}_{\mathcal{S}})$
$\mathcal{C}_i = \mathcal{E}_{\mathcal{S}_{\mathcal{K}}}(\mathcal{S}_{\mathcal{P}} \| \mathcal{G} \| \mathcal{T}_{\mathcal{S}})$
```

Algorithm 1: Mutual authentication and key agreement.

```
Computes $(\mathcal{S}_{\mathcal{P}} \| \mathcal{G} \| \mathcal{T}_{\mathcal{S}}) = \mathcal{D}_{\mathcal{S}_{\mathcal{K}}}(\mathcal{C}_i)$
Only legitimate users can access data from server using access structure
Computes $\mathcal{G}' = (\mathcal{S}_{\mathcal{P}} \| \mathcal{T}_{\mathcal{S}})$
Compared if $(\mathcal{G}' = \mathcal{G})$
Satisfied data accuracy
Else
Data modified
Decision = reject
Bs computes $\mathcal{Z} = \mathcal{E}_{\mathcal{S}_{\mathcal{K}}}(\mathcal{N}_{\mathcal{Y}}+1)$
Send $(\mathcal{N}_{\mathcal{Y}}+1)$ to bio sensor nodes
Biosensor computes $\mathcal{D}_{\mathcal{S}_{\mathcal{K}}}(\mathcal{Z}) = (\mathcal{N}_{\mathcal{Y}}+1)$
Now using $(\mathcal{S}_{\mathcal{K}})$ communication will be started
```

Algorithm 2: Input → *Stakeholders* $(\mathcal{D}_{\mathcal{S}_{\mathcal{K}}}, \mathcal{C}_i, \mathcal{T}_{\mathcal{S}}, \mathcal{S}_{\mathcal{P}}, \mathcal{G}\,\mathcal{I}\mathcal{D}_{\mathcal{S}i})$.

```
Input → Encoding $(\mathcal{E}_{\mathcal{K}r1}, S_i, \mathcal{P}_i, M_i, TH, \mathcal{T}_{\mathcal{S}}, \mathcal{N}_{\mathcal{Y}}, \mathcal{I}\mathcal{D}_{\mathcal{S}i})$
Sensor node $(S_i) \in \mathcal{P}_i$ continuously sense physiological signal $(M_i)$
If $(M_i$ < predefined threshold value $(TH))$
Then discard $(M_i)$
Else
Encrypt data $(M_i)$ using predefine access structure
Transmitted $(M_i)$ toward the $\mathcal{B}\mathcal{S}$
Computes $\mathcal{Q} = \mathcal{K}\mathcal{H}_{\mathcal{K}1}(M_i \| \mathcal{T}_{\mathcal{S}})$
Computes $\mathcal{C}_i = \mathcal{E}_{\mathcal{K}r1}(M_i \| \mathcal{Q} \| \mathcal{N}_{\mathcal{Y}} \| \mathcal{I}\mathcal{D}_{\mathcal{S}i})$
Transmitted $\mathcal{C}_i$ toward the MS via sink node
```

Algorithm 3: Encoding Phase.

data owners and external users are registered by the system administration upon joining the networks. It manages and distributes all the designed CP-ABE policies among different users to protect the adversary's attacks and access data according to their needs. Thus, mutual authentication and key agreement between data producers (patients) and data

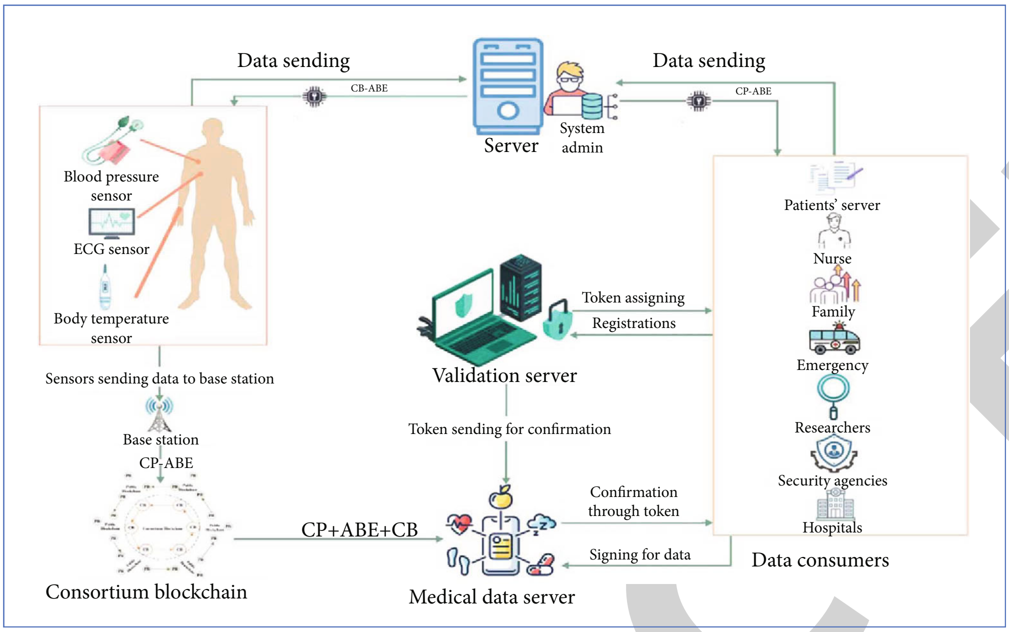


Figure 1: Proposed network architecture for communication in WBSNs.

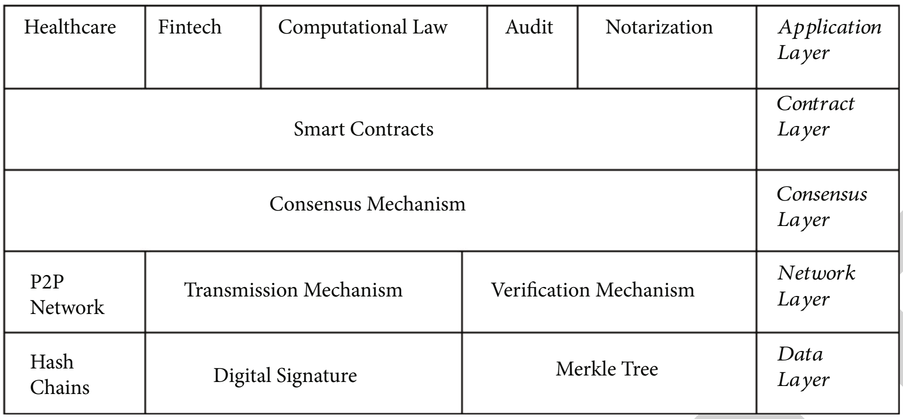
consumers (doctors) are performed to avoid unauthorized users from accessing the networks and to securely manage the session key for further patient data transmission. Initially, all deployed sensors/nodes on a patient's body continuously monitor vital signs such as pulse rate, ECG, EEG, BP, SPO2, and temperature and then, further communicate these vital signs to BS in a secure manner by using different standard protocols like IEEE 802.15.6 or Zigbee etc.

3.1.2. Medical Service Provider. Medical service provider (MSP) delivers medical services to the patients when any emergency happened. In our scheme, doctors and nurses are the medical service providers, but pharmacies, hospitals, labs, clinics, and a variety of other institutions are also included. A healthcare provider is a company or individual which provides medical care in efficient way. Each client is operated by a specific doctor for diagnosis and gives response to their patient according to their medical history. The server is responsible for the registration of the user's/patient and secures record keeping in a table for future references. Server should verify the new blocks of consortium blockchain and also authenticate the doctor before accessing the patient private data stored on a chain of blocks in the consortium blockchain. Moreover, consensus mechanisms are applied on the data stored on a block and then, transmit patient data from consensus layer to network layer. Besides, network layer used the transmission and verification mechanisms to communicate the patient sensitive information in a secure and authentic way towards the MS. Therefore, data layer of the consortium blockchain uses the concept of hash function, digital signature, and Merkle tree to ensure the authenticity and integrity, transparency, and privacy of the patient information an efficient way. The following Figure 2 shows the blockchain architecture in WBSNs environment.

3.1.3. Data Owner. In our case data owner is a registered patient who designs the attribute base policies according to their desire and privacy. Moreover, different logic gates such as (AND/OR) is used to design access structure policies for fine-grained access control to protect adversaries' attacks form illegal accessing of patient information from MS. Furthermore, data owner sends their authorized letter to access the dataset of the consortium blockchain for access the data sharing policies.

3.1.4. Consortium Blockchain. In consortium blockchain, we have offered decentralization using multiple authorities on networks for decision making of patient attributes to improve the transaction speed with lower cost, scalability, low energy, along with minimizing criminal activities to protect WBSN from adversaries' attacks. We have applied one-way hash function such as Hash-512 to computes the hash value of data and store into the block of the blockchain in decentralized manner for integrity purposes. Furthermore, no risk of 51% attack and improve the regulation of transactions with cheaper cost. Thus, using multiparty consensus, it consumes low energy for dissemination of patient information inside the blockchain. While multiple authority of the concerned hospital ward can read/write the patient data store in the server using their predefine attributes. The following Figure 2 shows the structure of blockchain.

3.1.5. Medical Data Server. In medical data server (MDS), we used the predesigned access structure of CP-ABE to store medical information of the registered patients of a hospital ward along with authorized access letter in to the consensus nodes of the blockchain in efficient and secure way. Besides, data consumers access the data pool of the blockchain for any decision making on patient information using their authorized attributes.



Healthcare	Fintech	Computational Law	Audit	Notarization	*Application Layer*
Smart Contracts					*Contract Layer*
Consensus Mechanism					*Consensus Layer*
P2P Network	Transmission Mechanism		Verification Mechanism		*Network Layer*
Hash Chains	Digital Signature		Merkle Tree		*Data Layer*

Figure 2: Blockchain architecture in WBSNs.

3.1.6. Validation Server. A data consumer uses their valid credentials such as ID, email address, location, and timestamp for registration with validation server (VS). Besides, after authentication process, the VS assign a unique token to each registered participant for further communication with MDS. Moreover, the generated token is also transferred in a secure way towards the MDS for onward verifications of data consumers when he/she put request for data accessing. Furthermore, after confirmation of token at MDS, data consumers can permit to access the patient data stored in a MDS according to access policies and their assign attributes.

3.1.7. Data Consumers. Data consumers such as nurse, doctor, family member, researchers, and security agencies first login in to MDS to access patient information. Using login phase, MDS verified the identity of data consumers by using predefines stored token in his database. In case, token matched with predefine stored token so permission is granted otherwise the request is rejected and blocked for onward communication.

3.2. Proposed CP-ABE Based Storage Architecture. In our proposed scheme using this architecture, we have securely shared the patient information among data owner, storage server, and doctor. Furthermore, in this data sharing system, we have design an efficient architecture which based on CP-ABE. Entities which are involved are as follows:

(1) Key generation center

(2) Data storage server

(3) Data owner

(4) Merkle Hash Tree

(5) Access structure

3.2.1. Key Generation Center. Key generation center produces two parameters i.e., private and public parameters for CP-ABE. It is responsible for generating, removing, and modifying attribute-based access keys for the users. However, using attribute tree sets every user authenticate by their own different access right based on their assigned attributes. The public attributes are known to all users in the networks while the private attribute is only access by the authorized users according to the access tree structure. In this phase, efficient session key is computed for secure transmission of patient medical vital sign towards the MS.

3.2.2. Data Storage Server. In data storage server, we have securely stored the patient medical sensitive information. However, in the time of data storage, server is responsible to authenticate the origin of the data and the information itself to avoid malicious activities of the attackers. Data storage server also computes private key by using KGC and some other system parameters such as partial master secret key and set of attributes tree. Moreover, if the key matched with access structure, so only those authentic users can join the networks and access the sensitive data from data storage server. The pervious history of the registered patients is also stored in the server for future reference and efficient feedback from the concerned doctor.

3.2.3. Data Owner. Data owner is an individual who preserves patient data and move the encrypted data toward the data storage server for efficient data security and privacy. Besides, data owner describes attribute-based access policy and accomplish it on its own data by encrypting data under the policy before assigning it to the data storage server. Only the authorized users can access the data of the patient stored in the server using CP-ABE policies. Using these policies, we have achieved fine-grain access control over the patient sensitive medical records stored in secure and efficient fashion inside the server.

3.2.4. Merkle Hash Tree. In our proposed scheme, we have applied the concept of Merkle Hash Tree (MHT) that can authenticate the accuracy of the data that are stored in the MS. Moreover, it is full binary tree that verify the data structure by using hash function. In MHT, we have added the hash value of each individual data in the particular node of the tree. However, the root node value is computed by performing hash function on all the child nodes and the obtained hash values of all child nodes are combined to calculate the value of root node. Let assume there is a set of data $\{d_1, d_{2,}d_3, d_4 \cdots ..d_n\}$; $\{h_1, h_2, h_3, h_4 \cdots \cdots .h_n\}$ are the computed hash values of the

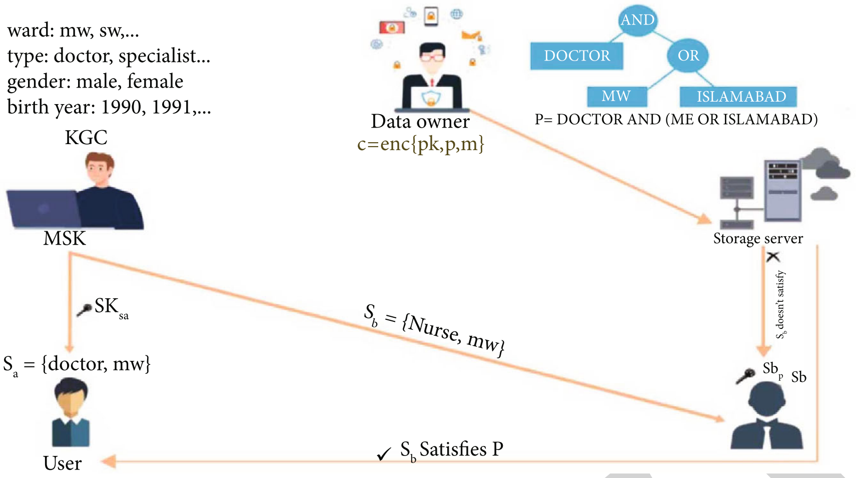


Figure 3: Proposed storage architecture of CP-ABE.

data set $\{d_1, d_{2,}d_3, d_4 \cdots ..d_n\}$, correspondingly. The value of the root node is computed from the child nodes until the final value of root node is obtained: $\text{Root}_{h1} = \text{Hash}(h_1 \| h_2)$, $\text{Root}_{h2} = \text{Hash}(h_3 \| h_4)$, $\text{Root}_{final} = \text{Hash}(\text{Root}_{h1} \| \text{Root}_{h2})$. Thus, to check the correctness of data such as $\{d_1, d_{2,}d_3, d_4 \cdots ..d_n\}$,the identifier can apply the rules of MHT and computes the value of parent/root node in efficient way.

3.2.5. Access Structure. It is an attributes base access structure which authorize patient data by using set of attributes. If a particular user acquires a set of attributes who satisfying the policy of encrypted data, so it is permitted to join the storage server and access the required encrypted patient information. Otherwise, the request is denied and the data packet is discarded. The following Figure 3 shows the proposed storage architecture using CP-ABE.

The following table 1 shows the notation guide used in the proposed scheme.

Table 1: Notation guide.

Notation	Description
S_i	Sensor node
M_i	Critical vital sign
$\mathscr{KH}$	Keyed hash function
$\mathscr{C}_i$	Cipher text
$\mathscr{N}_{\mathscr{Y}}$	Nonce
$\mathscr{ID}_{\mathscr{S}i}$	Identification number of sensor
$\mathscr{E}_{\mathscr{X}}/\mathscr{D}_{\mathscr{X}}$	Encryption and decryption with key
$\mathscr{S}_{\mathscr{K}}$	Session key
$\mathscr{N}_{\mathscr{Y}}+1$	Acknowledgement
$\mathscr{K}_{r}$	Public key
$\mathscr{P}_{r}$	Private key
$\mathscr{S}$	Secret credentials
$\mathscr{T}_{\mathscr{S}}$	Time stamp
$\mathscr{M}_{\mathscr{SK}}$	Master secret key
$\mathscr{BS}$	Base Station/sink node
$\mathscr{MS}$	Medical server
$\mathscr{S}_{\mathscr{P}}$	Structure policies
AND/OR	Logic gates
VS	Validation server
MDS	Medical data server
MSP	Medical service provider

3.3. Radio Model. Here, we used a radio model for the assessment of the energy consumption by communicating patient data in WBSNs. The basic constraints of the model are G_t for energy communication, r packet measurement and s transmission distance. Equation (1) for data communication

$$\mathrm{G_t}(r, s) = \begin{cases} r\mathrm{E_{elec}} + r\,\mathrm{e_{ij}}\,f^2, f < f_{0,} \\ r\mathrm{E_{elec}} + r\,\mathrm{e_{st}}\,f^4, f \geq f_{0,} \end{cases} \tag{1}$$

where $\mathrm{G_t}(r, s)$ is the percentage of expended by a sensor in communication, energy consumption is directly related to the packet measurement r and s distance.

Energy consumption depends upon the transmission distance, long distance more energy consumption, and short distance less energy consumption.

$$\mathrm{H_r}(r) = r\mathrm{E_{elec}}. \tag{2}$$

Equation (2) is used to measure the consumed energy on patient data receiving where $\mathrm{H_r}(r)$. The energy required for receiving data by a sensor node r is packet length and $\mathrm{E_{elec}}$ Energy consumption per bit as:

$$\frac{E_{\mathrm{elec=}}50\mathrm{mo}}{\mathrm{bit}}, \quad f_0 = \text{One hundred meter}. \tag{3}$$

In our projected scheme, we used the idea of the free space model $\mathrm{e} = \mathrm{e_{ij}} = 10\ \mathrm{Lo/bit}/m^2$ because the distance $f < f_0$. Moreover, $\mathrm{e_{ij}}$ is the power of the amplifier via in this model.

```
$Input \rightarrow \text{Decoding}(\mathscr{C}_i, \mathscr{T}_{\mathscr{S}}, \mathscr{X}, \mathscr{M}_{\mathscr{S}\mathscr{K}}, \mathscr{S}_{\mathscr{P}}, \mathscr{G}, \mathscr{N}_{\mathscr{Y}})$
Computes $(M_i \| \mathscr{Q} \| \mathscr{N}_{\mathscr{Y}} \| \mathscr{I}\mathscr{D}_{\mathscr{S}i}) = \mathscr{D}_{\mathscr{P}r}(\mathscr{C}_i)$
Computes $\mathscr{S}_{\mathscr{K}} = (\mathscr{X}/r + \mathscr{X}_{a}) m\mathscr{O}d q$
Computes $\mathscr{T} = \mathscr{E}_{\mathscr{M}_{\mathscr{S}\mathscr{K}}}(\mathscr{S}_{\mathscr{K}})$
Transmitted $(\mathscr{T})$ towards the MS via BS
If access structure match, then
Computes $\mathscr{S}_{\mathscr{K}} = \mathscr{D}_{\mathscr{M}_{\mathscr{S}\mathscr{K}}}(\mathscr{T})$
$\mathscr{G} = \mathscr{K}\mathscr{H}_{\mathscr{K}2}(\mathscr{S}_{\mathscr{P}} \| \mathscr{T}_{\mathscr{S}})$
$\mathscr{C}_i = \mathscr{E}_{\mathscr{S}_{\mathscr{K}}}(\mathscr{S}_{\mathscr{P}} \| \mathscr{G} \| \mathscr{T}_{\mathscr{S}})$
Transmitted $(\mathscr{C}_i)$ towards the stakeholders
Computes $(\mathscr{S}_{\mathscr{P}} \| \mathscr{G} \| \mathscr{T}_{\mathscr{S}}) = \mathscr{D}_{\mathscr{S}_{\mathscr{K}}}(\mathscr{C}_i)$
Computes $\mathscr{G}' = (\mathscr{S}_{\mathscr{P}} \| \mathscr{T}_{\mathscr{S}})$
Compared if $(\mathscr{G}' = \mathscr{G})$
Accepted
*Else*
Rejected
Computes $\mathscr{Z} = \mathscr{E}_{\mathscr{S}_{\mathscr{K}}}(\mathscr{N}_{\mathscr{Y}}+1)$
Send $(\mathscr{N}_{\mathscr{Y}}+1)$ to bio sensor nodes
Biosensor computes $\mathscr{D}_{\mathscr{S}_{\mathscr{K}}}(\mathscr{Z}) = (\mathscr{N}_{\mathscr{Y}}+1)$
Now using $(\mathscr{S}_{\mathscr{K}})$ communication will be started
```

Algorithm 4: Decoding Phase.

Table 2: Comparative analysis of security properties.

Schemes	$\mathscr{p}_1$	$\mathscr{p}_2$	$\mathscr{p}_3$	$\mathscr{p}_4$	$\mathscr{p}_5$	$\mathscr{p}_6$	$\mathscr{p}_7$
Gupta et al. [19]	No	Yes	Yes	No	Yes	Yes	No
Guo et al. [20]	Yes	Yes	Yes	Yes	No	No	Yes
Li et al. [21]	Yes	Yes	No	No	Yes	No	No
Sivasangari et al. [22]	No	Yes	Yes	Yes	No	Yes	Yes
Wang et al. [23]	Yes	Yes	Yes	No	Yes	Yes	No
Proposed	Yes	Yes	Yes	Yes	Yes	Yes	Yes

$\mathscr{p}_1$: mutual authentication, $\mathscr{p}_2$: Resist Man in the middle attack, $\mathscr{p}_3$: protection of replay attack, $\mathscr{p}_4$: protected square-root attack, $\mathscr{p}_5$: protected forgery attack, $\mathscr{p}_6$: protected chosen ciphertext attack, $\mathscr{p}_7$: forward and backward secrecy.

4. Security Analysis

The basic security properties of our proposed technique based on CP-ABE and the Consortium Blockchain have been demonstrated through security analysis. In addition, we have enhanced the security of critical medical data when transmitting it over public networks by employing minimal resources to prevent unauthorized access and modification. We offer a lightweight solution that reduces the deployed sensor node's energy consumption and so extends the lifespan of WBSNs while also cutting costs. Only the registered user can access the medical database in ti-er-4 and use their valid predefined attributes for further decision making. The following Table 2 compares the proposed scheme's security level to those of various current state-of-the-art techniques [19–23].

4.1. Mutual Authentication. WBSN authentication is a significant area for the identification of participating nodes in the resource constrained environment of WBSN for onward data flow between illegal users. ABE and consortium blockchain concepts have been used to verify nodes in the networks and to secure communication with the MS, respectively. Only sensors that have been authenticated by the medical server are allowed to store medical data in the database for further data processing and decision making. Only valid tier-4 users will be able to access the data with their predefined qualities in our smart and secure cryptosystem, which will block and isolate illegal users throughout the authentication process if they are found.

$$\begin{aligned} \mathscr{D}_{\mathscr{P}r}(\mathscr{C}_i) &= \left(M_i \| \mathscr{Q} \| \mathscr{N}_{\mathscr{Y}} \| \mathscr{I}\mathscr{D}_{\mathscr{S}i}\right), \\ \mathscr{I}\mathscr{D}_{\mathscr{S}i} &= \mathscr{I}\mathscr{D}_{\mathscr{S}i}{}'. \end{aligned} \tag{4}$$

If $(\mathscr{I}\mathscr{D}_{\mathscr{S}i} = \mathscr{I}\mathscr{D}_{\mathscr{S}i}{}')$, then, mutual authentication granted; otherwise, request disallowed and blacklisted from network.

4.2. Resist Man in the Middle Attack. To protect the patient medical information from adversaries' attacks such as man in the middle attack we have established a secure access policies using logic gates such as OR/AND, other secret parameters to avoid data modification during data communication. Besides the hidden access structure allow only legitimate users to access the prestored patient medical records using authentic attributes assigned from system administrator. Additionally, intruder is unable to decrypt the patient sensitive information in the middle way during transmission.

$$\begin{aligned} \mathscr{Q} &= \mathscr{K}\mathscr{H}_{\mathscr{K}1}(M_i \| \mathscr{T}_{\mathscr{S}}), \\ \mathscr{C}_i &= \mathscr{E}_{\mathscr{K}r1}\left(M_i \| \mathscr{Q} \| \mathscr{N}_{\mathscr{Y}} \| \mathscr{I}\mathscr{D}_{\mathscr{S}i}\right), \\ \mathscr{C}_i{}' &= \mathscr{E}_{\mathscr{K}r2}(\mathscr{C}_i \| \mathscr{P}\mathscr{K}, \mathscr{P}, \mathscr{M}). \end{aligned} \tag{5}$$

4.3. Protection of Replay Attack. In this study, we have used the concept of nonce and timestamp to protect the replay attack in the WBSNs in efficient and desirable way. Furthermore, the hidden access structure can improve the privacy of the patient confidential information during communication and storage on a particular server. Intruders are unable to compute accurate timestamp and nonce for cryptanalytic reply attack. Only legitimate users can able to access the sensitive medical records of the particular patients if he/she attribute are matched; otherwise, the request is discard and isolated from the WBSNs. The secret session key is applied for encryption when connection established among biosensor nodes and MS.

$$\begin{aligned} T &= \mathscr{E}_{\mathscr{S}_{\mathscr{K}}}\left(\mathrm{M_i} \| \mathscr{T}_{\mathscr{S}} \| \mathscr{N}_{\mathscr{Y}}\right), \\ \mathscr{S}_{\mathscr{A}} &= \text{Satisfies } \mathscr{P}, \\ \mathscr{S}_{\mathscr{B}} &= \text{does not Satisfies } \mathscr{P}. \end{aligned} \tag{6}$$

4.4. Protected Square Root Attack. In this study, we have applied efficient and complex hidden access policies along with consortium blockchain to protect the WBSNs from adversaries' attack during transmission on public channel. Moreover, Merkle Hash Tree can authenticate the accuracy of the data that are stored in the MS. Besides, it is full binary tree that verify the data structure by using hash function. In MHT, we have added the hash value of each individual data in the particular node of the tree. However, the root node value is computed by performing hash function on all the child nodes and the obtained hash values of all child nodes are combined to calculate the value of root node. Thus, we have protected adversaries to performed square root attack on the WBSNs.

$$\begin{aligned} \mathscr{MSK} &= \mathscr{S}_{\mathscr{A}}(\text{Doctor}, \mathscr{MW}), \\ \mathscr{P} &= \text{Doctor AND } (\mathscr{MW} \text{ OR Islamabad}). \end{aligned} \tag{7}$$

4.5. Protected Forgery Attack. In this study, the computed session key is mutually authenticated among source and destination nodes to enhanced the privacy of the medical records. Furthermore, the master secret key along with other secret credentials are securely communicated among biosensor nodes, BS, and MS to avoid the forgery attack. However, the external users can only access the particular patient records if their attributes matched with prestored attribute of the concerned ward medical server. Additionally, we have used CP-ABE along with consortium blockchain to improve the scalability, privacy, and transaction speed in optimal way.

$$\begin{aligned} \mathscr{S}_{\mathscr{K}} &= \frac{\mathscr{X}}{\mathscr{r} + \mathscr{X}_{\mathscr{a}}} \mathscr{m}\mathscr{O}\mathscr{d}\ \mathscr{q}, \\ \mathscr{T} &= \mathscr{E}_{\mathscr{MSK}}(\mathscr{S}_{\mathscr{K}}). \end{aligned} \tag{8}$$

4.6. Protected Chosen Ciphertext Attack. In our suggested approach, the master secret key is used to generate the other session keys for secure data transmissions. MS can verify the identity of each external user by looking up the encrypted attributes that have been prestored in the database. Additionally, the nonce are generated and provided to third parties for verification. The authorization permissions granted to each and every registered network user in an efficient and secure manner for further data access, and diagnostics are also successful following the successful verification utilizing attribute-based policies. Additionally, our proposed scheme used the concept of distributed ledger and distributed consensus of consortium blockchain to protect the chosen ciphertext attack. Thus, intruder is unable to capture secret information from cipher text.

$$\begin{aligned} \mathscr{T} &= \mathscr{E}_{\mathscr{MSK}}(\mathscr{S}_{\mathscr{K}}), \\ \mathscr{S}_{\mathscr{K}} &= \mathscr{D}_{\mathscr{MSK}}(\mathscr{T}), \\ \mathscr{G} &= \mathscr{KH}_{\mathscr{K}2}(\mathscr{S}_{\mathscr{P}} \| \mathscr{T}_{\mathscr{S}}), \\ \mathscr{C}_i &= \mathscr{E}_{\mathscr{S}_{\mathscr{K}}}(\mathscr{S}_{\mathscr{P}} \| \mathscr{G} \| \mathscr{T}_{\mathscr{S}}). \end{aligned} \tag{9}$$

4.7. Interoperability. In this study, we have achieved confidentiality using CP-ABE. Later, we integrated the CP-ABE with blockchain to enhance the security and privacy of the whole medical system along with transparency to provide user friendly platform to all registered participants. Now, in blockchain services are called the transactions that stored the sensitive medical history of the registered patient in the form of connected blocks. We used the Merkle tree to maintain the data security, the transaction on the bottom (child nodes) are combined and make the root hash that is included in the block. If we have the odd number of transaction (patient records) than we have applied Merkle tree which duplicates the last transactions to maintain it as a binary tree. On every step, we compute the hash. So, this way we can enhanced the data security. While intruder cannot interpret it easily, as they need 51% control along high computational power for patient data modification stored in medical server. When any transaction is performed, they go through this mechanism. Along with this, we implemented consortium blockchain, so we required the consensus of only the involved parties/organizations. As we know, that public blockchain is immutable. Here we required to update the data of the patients by the mutual consensus of hospitals so we are using consortium blockchain. Moreover, if we use private blockchain then, single authority can update the records of patient that is not sure as compared to the updating by mutual consensus of involved parties. Using consensus mechanisms we have control the trust problem of the collaboration among multiple participants.

4.8. Scalability. In this study, scalability refers to a platform's ability to handle a rising volume of transactions while also expanding the network's nodes. Maximum assignment throughput and latency may be achieved by integrating our CP-ABE with consortium scheme.

4.9. Forward and Backward Secrecy. After termination of existing session, the session keys in our proposed scheme are updated. A secret session key has also been produced for new sessions between biosensor nodes, BS, and MS. The confidentiality of the entire session can be compromised if we employ a single session key for long-distance connections. Furthermore, we have achieved data security and privacy aspects including forward and backward secrecy in our suggested approach employing a key updating mechanism after a specific time interval. The old session key can no longer be guessed by adversaries and used to access critical patient data.

4.10. Ensuring Privacy. Blockchain are entirely open-source software that means anybody can sight the code and also gives inspects the aptitude to analyze the security. As a result, there is no governing authority. Thus, the vast majority of people on the network are in agreement that the new code will affect existing code. As new blocks are confirmed and added, each node has its own copy of the chain. Modification of any block on the blockchain is nearly impossible. Medical records for WBSN patients can be regulated on the blockchain by the WBSN providers. As a result, only one or a few people can access the user's private record on the blockchain ensuring privacy. Using a consortium blockchain, our suggested solution provides a high level of security.

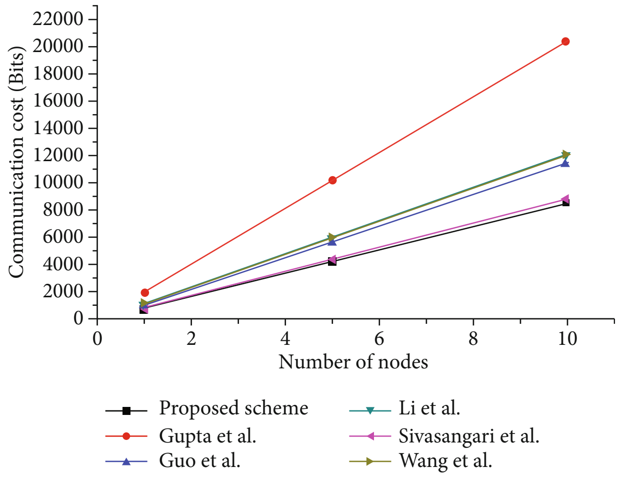


Figure 4: Comparison of transmission overhead.

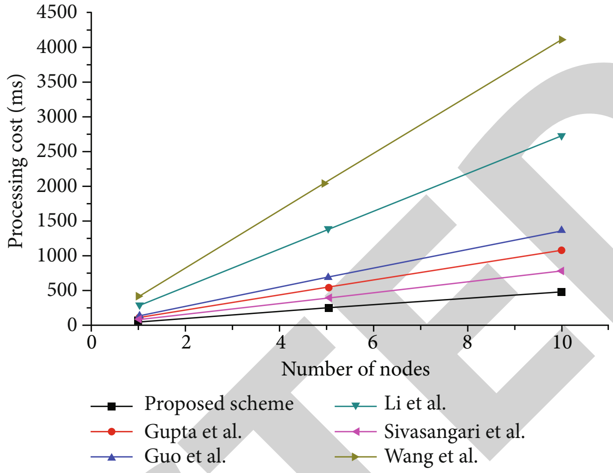


Figure 5: Comparison of processing cost at sensor side.

5. Performance Analysis

In the following sections, we have analyzed the performance comparison of our proposed scheme and other state of the art schemes [19–23] in terms of transmission cost, processing cost, storage cost, and energy consumption.

5.1. Transmission Cost. In this study, we have designed an efficient and secure key management and authentication scheme to resolve the key-exposer problem and protect WBSNs from unauthorized patient data accessing and modification during communication on public networks. For this purpose, we have applied the concept of CP-ABE along with consortium blockchain to enhance the patient data security and privacy in optimal way. In our proposed scheme, we have deployed various biosensor nodes in the registered patient body to continuously monitor the vital signs such BP, EEG, and ECG. Furthermore, the deployed biosensor nodes transmitted the sensed patient vital signs towards the BS. Now, the collected patient data is aggregated on BS level and only the encrypted critical information are further communicated with the MS using internet technology for diagnoses and treatment. We have applied free space model for data transmission to reduce the energy consumption of biosensor nodes in WBSNs. Additionally, in our proposed scheme, we have analyzed and transmitted only the critical information which enhanced the overall network life time of WBSNs. We have compared the transmission cost of our proposed scheme with other state of the arts schemes [19–23] which are shows in the following Figure 4. The result in Figure 4 shows that our proposed scheme in efficient in term of transmission cost as compared to other state of the art schemes [19–23].

5.2. Processing Cost. In our proposed scheme, we have designed secure and efficient access control structure using logical AND/OR gates along with other secret parameters to maintain the tradeoff between processing cost and security in the recourse constrained environment of WBSNs. In this study, we have applied the concept of CP-ABE along with consortium blockchain to improve the security level of WBSNs with minimal resource utilization. As compared to other state of the arts scheme, [19–23] our scheme reduces the processing cost and provides sufficient security in all the tiers of WBSNs. The following Figure 5 indicates that our proposed scheme is efficient in term of processing cost.

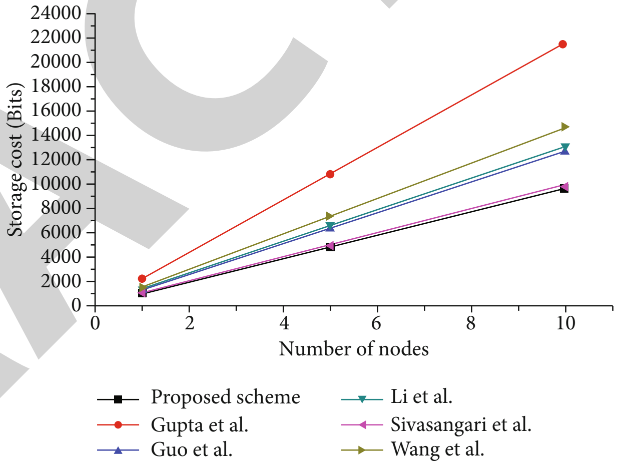


Figure 6: Comparison of keys storage cost.

5.3. Storage Cost. In this study, we have applied smart security algorithms based on CP-ABE and consortium blockchain to efficiently utilized the sensor memory and reduce the storage cost in the resource constrained environment of WBSNs. In our proposed scheme, we have applied the hidden access structure and some other security parameters such as session key and master secret key to improve the data security and privacy by utilizing minimal system resources. The following Figure 6 shows the storage cost comparison of our proposed scheme and other state of the art schemes [19–23]. Moreover, Figure 6 indicates that our scheme consumes less memory and suitable for resource constrained devices such as WBSNs, satellite communication, and IoT environments.

5.4. Energy Consumption. In our proposed scheme, we have deployed tiny biosensor nodes in the patient body to

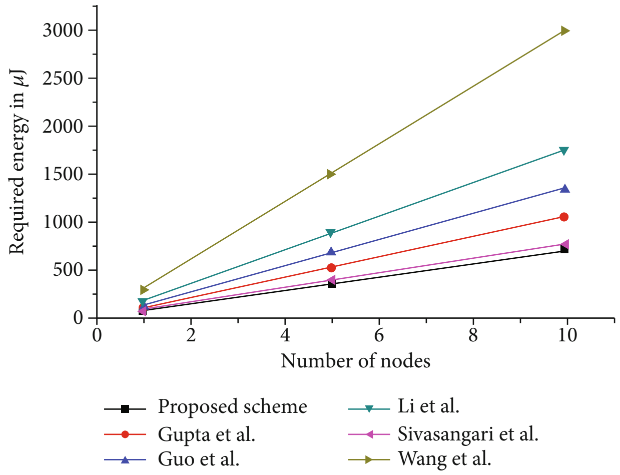


Figure 7: Comparison of energy consumption at sensor side.

continuously monitor physiological signals such as BP, ECG, and EMG. Furthermore, BS collected sensed patient data from deployed sensor nodes using IEEE 802.15.6 standard. Now, BS transmitted only encrypted critical patient information towards the MS using public networks for further diagnoses and treatment and the normal patient data are discard at tier -1 to preserve the energy of the sensor nodes and enhanced the life time of the WBSNs. Furthermore, in our proposed scheme, we have applied efficient and secure algorithms for mutual authentication along with key agreement, encoding, and decoding to protect the patient data from adversaries' attacks and avoid needless transmission to enhance the performance of the networks by utilizing minimum energy. The following Figure 7 shows that our proposed scheme consumes less energy as compared to other state of the art schemes [19–23].

5.5. Ranking Based on Performance Evaluation Using EDAS. The EDAS is a method for evaluating alternatives that is used as a middle-of-the-road solution. Ghorabaee et al. [62] were the first to present the method. EDAS measures two activities for evaluation purposes, which are defined as positive distance from average solution and negative distance from average solution, respectively. The MCDM method calculates the distance between each alternative solution and the average solution, and then, uses that specific information to select the best alternative [63, 64].

Additionally, the existing schemes utilizing the MCDM approach has been analyzed and compared by employing the EDAS technique to a cryptographic scheme for the first time, in order to evaluate the previously suggested schemes, as well as the previously proposed solution proposed in the domain. It is a useful method to compare the performance of different schemes, as demonstrated by the excellent results [65, 66]. Communication cost, processing cost, storage cost, energy, consumption, and security are the performance metrics that have been selected, as shown in Table 3.

Fuzzy logic is used in this case. In this survey, the method of evaluating performance based on EDAS is used for the ranking-based performance evaluation [67–69]. The performance matrices that have been identified in Table 3 are compared in this section. Additionally, the cross-EDAS method is used in this appraisal to select the most effective values of the six different approaches on the basis of the parameters that have been chosen for evaluation. The assessment scores, on the other hand, are used to calculate the ranking of the various techniques that are currently available. Besides, the cross-efficient values and comparative analysis results of the $(WS_{\mathscr{P}_d})_a$ are shows in Tables 4 and 5, respectively.

Step 1. The solution of the average value (π) of the selected matrices is calculated as

$$(\phi) = [\pi_b]_{1\times\beta}, \tag{10}$$

$$\text{while} = \frac{\sum_{i=1}^{y} X_{ab}}{y}. \tag{11}$$

In the aforementioned procedure, the effectiveness of the chosen matrices is cited as the criteria for the suggested solutions. It is also possible to obtain π for each computed value on each chosen matrix by summing the results of Equations (10) and (11), as shown in Table 5.

Step 2. In step two of the EDAS-based on Positive Distance from Average (P_{dav}), Equations (12)–(14) are as follows:

$$P_{\text{dav}} = \left[(P_{\text{dav}})_{ab}\right]_{\beta\times\beta}. \tag{12}$$

If the state b^{th} is favorable, than

$$(P_{\text{dav}})_{ab} = \frac{\mathscr{MAX}(0, (\text{Ave}_b - X_{ab}))}{\text{Ave}_b} \tag{13}$$

And for less favorable, it becomes

$$(P_{\text{dav}})_{\text{ab}} = \frac{\mathscr{MAX}(0, (X_{ab} - Ave_b))}{\text{Ave}_b}, \tag{14}$$

where P_{dav} represents the Negative Distance of b^{th} rated algorithm from the given average value on the a^{th} rating performance matrices.

Step 3. The Negative Distance from Average (N_{dav}) is calculated in this step using Equations (15)–(17).

$$(N_{\text{dav}}) = \left[(N_{\text{dav}})_{ab}\right]_{\beta\times\beta}. \tag{15}$$

If the b^{th} criterion is more favorable than

$$(N_{\text{dav}})_{ab} = \frac{\mathscr{MAX}(0, (\text{Ave}_b - X_{ab}))}{\text{Ave}_b}, \tag{16}$$

and less desirable, then, the given above equations become

$$(N_{\text{dav}})_{ab} = \frac{\mathscr{MAX}(0, (X_{ab} - \text{Ave}_b))}{\text{Ave}_b}, \tag{17}$$

Table 3: Performance metrics of suggested schemes.

Criteria	Nonbeneficial				Beneficial
Probability	0.2	0.2	0.2	0.2	0.2
Schemes | parameters	Communication cost	Processing cost	Storage cost	Energy consumption	Security
Proposed scheme	864	45.29	964	70.56	1
Gupta et al. [19]	2056	105.2	2156	105.2	0.5
Guo et al. [20]	1152	134.44	1264	134.44	0.5
Li et al. [21]	1216	270.83	1316	174.33	0.5
Sivasangari et al. [22]	896	75.96	986	75.96	0.5
Wang et al. [23]	1234	410.3	14640	297.9	0

Table 4: Cross-Efficient Values.

Criteria	Nonbeneficial				Beneficial
Probability	0.2	0.2	0.2	0.2	0.2
Schemes | parameters	Communication cost	Processing cost	Storage cost	Energy consumption	Security
Proposed scheme	864	45.29	964	70.56	1
Gupta et al. [19]	2056	105.2	2156	105.2	0.5
Guo et al. [20]	1152	134.44	1264	134.44	0.5
Li et al. [21]	1216	270.83	1316	174.33	0.5
Sivasangari et al. [22]	896	75.96	986	75.96	0.5
Wang et al. [23]	1234	410.3	14640	297.9	0
Average	1236.333333	173.67	3554.333333	143.065	0.5

Table 5: Comparative analysis results of the $(\mathrm{WS}_{\mathscr{P}_d})_a$.

Criteria	Nonbeneficial				Beneficial	
Probability	0.2	0.2	0.2	0.2	0.2	
Schemes | parameters	Communication cost	Processing cost	Storage cost	Energy consumption	Security	$(WS_{\mathscr{P}_d})_a$
Proposed scheme	0.06023187	0.14784361	0.14575635	0.10135952	0.2	0.65519136
Gupta et al. [19]	0	0.07885069	0.0786833	0.05293398	0	0.21046797
Guo et al. [20]	0.01364249	0.04517764	0.12887555	0.01205746	0	0.19975313
Li et al. [21]	0.0032893	0	0.12594955	0	0	0.12923884
Sivasangari et al. [22]	0.05505527	0.11252375	0.14451843	0.09381051	0	0.40590796
Wang et al. [23]	0.00037746	0	0	0	0	0.00037746

where $(N_{\mathrm{dav}})_{ab}$ represents the Negative Distance of b^{th} rated algorithm from the given average value of the a^{th} rating performance matrices.

Step 4. The weighted sum of the Positive Distance ($\mathscr{P}_d$) for the rated algorithm is calculated at this stage as

$$\left(\mathrm{WS}_{\mathscr{P}_d}\right)_a = \sum_{b=1}^{y} \lambda_b (\mathscr{P}_d)_{ab}. \tag{18}$$

Step 5. The weighted sum of the Negative Distance ($\mathscr{N}_d$) for the rated algorithms is calculated in this stage.

$$\left(\mathrm{WS}_{\mathscr{N}_d}\right)_a = \sum_{b=1}^{y} \lambda_b (\mathscr{N}_d)_{ab}. \tag{19}$$

Step 6. The calculated scores based on the $(\mathrm{WS}_{\mathscr{P}_d})_a$& $(\mathrm{WS}_{\mathscr{N}_d})_a$, which are based on the rated technique, are, respectively, given in the subsequent Equations (20) and (21).

$$\mathscr{N}\left(\mathrm{WS}_{\mathscr{P}_d}\right)_a = \frac{\left(\mathrm{WS}_{\mathscr{P}_d}\right)_a}{\mathscr{MAX}_a\left(\left(\mathrm{WS}_{\mathscr{P}_d}\right)_a\right)}, \tag{20}$$

$$\mathscr{N}\left(\mathrm{WS}_{\mathscr{N}_d}\right)_a = 1 - \frac{\left(\mathrm{WS}_{\mathscr{N}_d}\right)_a}{\mathscr{MAX}_a\left(\left(\mathrm{WS}_{\mathscr{N}_d}\right)_a\right)}. \tag{21}$$

Step 7. The score values based on $(\mathrm{WS}_{\mathscr{P}_d})_a$&$\mathscr{N}(\mathrm{WS}_{\mathscr{N}_d})_a$, which are based on the evaluation scores (ψ) for the rated

Table 6: Analysis results of the aggregate $(\mathrm{WS}_{\mathcal{N}_d})_a$.

Criteria	Nonbeneficial				Beneficial	
Probability	0.2	0.2	0.2	0.2	0.2	
Schemes | parameters	Communication cost	Processing cost	Storage cost	Energy consumption	Security	$(\mathrm{WS}_{\mathcal{N}_d})_a$
Proposed scheme	0	0	0	0	0	0
Gupta et al. [19]	0.13259639	0	0	0	0	0.13259639
Rui Guo et al. [20]	0	0	0	0	0	0
Li et al. [21]	0	0.11189037	0	0.04370741	0	0.15559777
Sivasangari et al. [22]	0	0	0	0	0	0
Wang et al. [23]	0	0.27250533	0.62378318	0.21645406	0.2	1.31274256

Table 7: Performance analysis of the suggested schemes.

Schemes	$(WS_{\mathcal{P}_d})_a$	$(WS_{\mathcal{N}_d})_a$	$\mathcal{N}(WS_{\mathcal{P}_d})_a$	$\mathcal{N}(WS_{\mathcal{N}_d})_a$	Δ	RANK
Proposed scheme	0.655191355	0	1.000000001	1	1	1
Gupta et al. [19]	0.210467972	0.132596387	0.321231302	0.898992848	0.610112075	4
Guo et al. [20]	0.199753134	0	0.304877549	1	0.652438774	3
Li et al. [21]	0.129238841	0.155597773	0.197253582	0.881471221	0.539362401	5
Sivasangari et al. [22]	0.405907957	0	0.619525813	1	0.809762906	2

schemes mentioned in Equation (22), are evaluated as

$$\Delta = \frac{1}{2}\left(\mathcal{N}\left(WS_{\mathcal{P}_d}\right)_a - \mathcal{N}\left(WS_{\mathcal{N}_d}\right)_a\right), \text{where } 0 \le \Delta \ge 1. \quad (22)$$

The final output of Δ is determined using the aggregate values of both $\mathcal{N}\mathrm{WS}_{\mathcal{P}_d}\&\mathcal{N}\mathrm{WS}_{\mathcal{N}_d}$. Besides In following Table 6 shows analysis results of the aggregate $(\mathrm{WS}_{\mathcal{N}_d})_a$

Step 8. According to the preceding activities, the extent of a given scheme is considered, and the ranking of different schemes is generated. Results show that the best solution has received higher evaluation scores than the other solutions, which is confirmed by the obtained results. As a result, the proposed scheme has received the highest evaluation score, as shown in Table 7.

The final result of the EDAS ranking indicates that the solution proposed scheme outperforms the remaining schemes that have been proposed in the domain, according to the final output. Furthermore, the output table contains a list of schemes that have been suggested based on the matrices that have been selected. The fuzzy logic-based comparative analysis revealed that the proposed scheme is the most effective based on the selected matrices, with the schemes developed by Sivasangari et al. [22], Guo et al. [20] ranking second and third, respectively.

5.6. Simulation Using AVISPA Tool. Security protocols and applications written in HLPSL are examined by AVISPA. As a result of this, HLPSL is made up of generic roles and character combinations that can be portrayed by many different individuals. The roles are not interdependent, collecting preliminary data through parameters and others. Communicating characteristic using [70] AVISPA backend parameters like CL-ATSE [71] have also been used to verify the authenticity of the communication method. Figure 8 depicts a flow diagram of AVISPA. For data dissemination through public networks, AVISPA is a one-button solution that mutually authenticates communication protocols. During transmission, it provides a role-oriented and complete validation mechanism. In addition, each network participant has a distinct role to play in verifying and authenticating critical patient information during the protocol's execution [71].

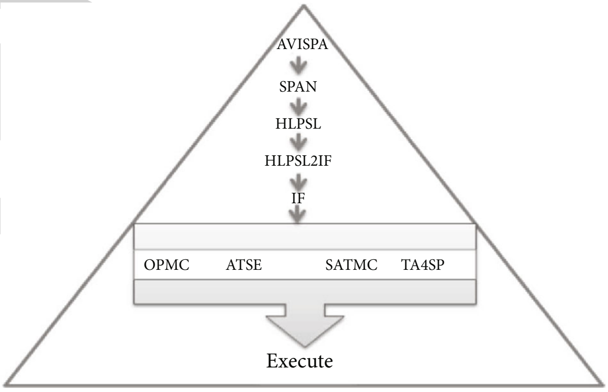
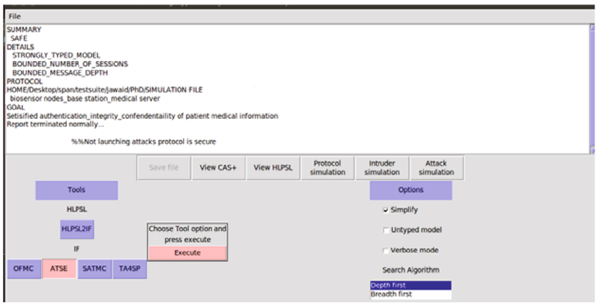


Figure 8: General architecture of AVISPA [71].

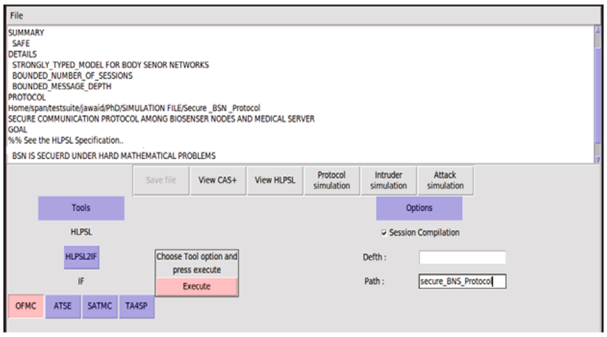
5.7. Proposed Scheme Validation Using AVISPA. In this section, we have validated the security correctness of our proposed authentication and key management scheme using HLPSL codes along with AVISPA tool. Furthermore, our scheme applied the concept of CP-ABE and consortium blockchain to enhance the security and privacy of patient information along with efficient resource utilization in the resource constrained environment of WBSNs.



```
SUMMARY
 SAFE
DETAILS
  STRONGLY_TYPED_MODEL
  BOUNDED_NUMBER_OF_SESSIONS
  BOUNDED_MESSAGE_DEPTH
PROTOCOL
HOME/Desktop/span/testsuite/jawaid/PhD/SIMULATION FILE
 biosensor nodes_base station_medical server
GOAL
Setisified authentication_integrity_confendentaility of patient medical information
Report terminated normally...

                %%Not launching attacks protocol is secure
```

Options
☑ Simplify
□ Untyped model
□ Verbose mode
Search Algorithm: Depth first

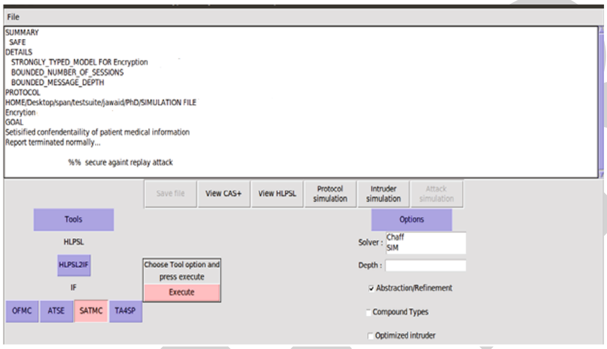
Figure 9: Secure against adversaries' attack (CL-ATSE).



```
SUMMARY
 SAFE
DETAILS
 STRONGLY_TYPED_MODEL FOR BODY SENOR NETWORKS
 BOUNDED_NUMBER_OF_SESSIONS
 BOUNDED_MESSAGE_DEPTH
PROTOCOL
Home/span/testsuite/jawaid/PhD/SIMULATION FILE/Secure _BSN _Protocol
SECURE COMMUNICATION PROTOCOL AMONG BIOSENSER NODES AND MEDICAL SERVER
GOAL
%% See the HLPSL Specification..
 BSN IS SECUERD UNDER HARD MATHEMATICAL PROBLEMS
```

Options
☑ Session Compilation
Defth :
Path : secure_BNS_Protocol

Figure 10: Secure session key communication (OFMC)



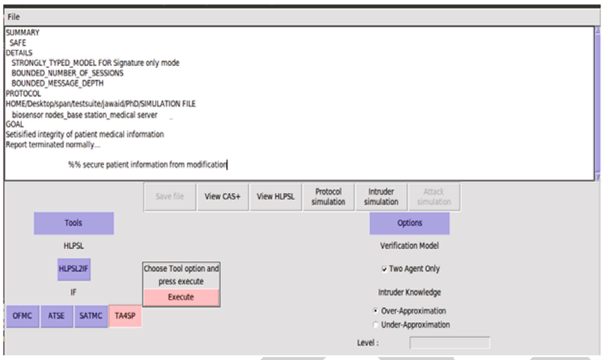
```
SUMMARY
 SAFE
DETAILS
  STRONGLY_TYPED_MODEL FOR Encryption
  BOUNDED_NUMBER_OF_SESSIONS
  BOUNDED_MESSAGE_DEPTH
PROTOCOL
HOME/Desktop/span/testsuite/jawaid/PhD/SIMULATION FILE
Encrytion
GOAL
Setisified confendentaility of patient medical information
Report terminated normally...

            %%  secure againt replay attack
```

Options
Solver : Chaff SIM
Depth :
☑ Abstraction/Refinement
□ Compound Types
□ Optimized intruder

Figure 11: Attribute's role for encryption in session creation (SATMC).

Additionally, in figure 9 we have shown the validation process of secure communication among MS and biosensor nodes. Each time, a biosensor node requests to communicate with the BS, it transmits a cryptographic parameter such as (Ny) along with the request. Moreover, BS's session key and the patient's public key (Kr) are used to scramble the parameter (Ny) before it is sent across the channel (R). The channel's status changes from 0 to 1 while it is in use. An indication that it belongs to the "Dolev-Yao" threat model may be seen by looking at the channel's name (dy). For the purpose of defining attributes, the variable "S" is employed. It is hoped that the same nonce number and R's qualifications will be returned. Besides, the following Figure 10 shows the result of OFMC in safe mode.

Figure 11 depicts the role of the data requester (R) or stockholder in HLPSL. The patient's information was initially decoded using secret key generated from attribute-based access hidden policies. Thus, using hidden attribute-based policies we have improved the patient data security and privacy, and we have securely monitored and disseminate medical records among legitimate and registered users. Moreover, we have also sent the patient's credentials along with medical history to the cloud for future references and decision making in efficient and desirable way. The following Figure 9 indicates that our scheme is safe and provides protection against adversary's attack.



```
SUMMARY
 SAFE
DETAILS
  STRONGLY_TYPED_MODEL FOR Signature only mode
  BOUNDED_NUMBER_OF_SESSIONS
  BOUNDED_MESSAGE_DEPTH
PROTOCOL
HOME/Desktop/span/testsuite/jawaid/PhD/SIMULATION FILE
  biosensor nodes_base station_medical server
GOAL
Setisified integrity of patient medical information
Report terminated normally...

            %% secure patient information from modification
```

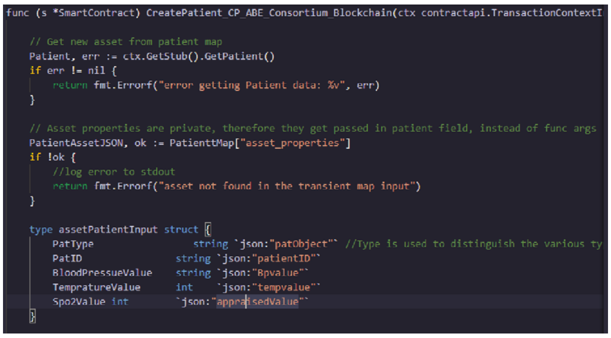
Options
Verification Model
☑ Two Agent Only
Intruder Knowledge
● Over-Approximation
○ Under-Approximation
Level :

Figure 12: Accuracy of the blockchain transactions verified using (TA4SP).

Figure 11 depicts the importance of a secret session key and an environment attribute in developing secret policies for securely transmitting patient data to the cloud and to the MS. Patients' medical records can only be accessed by registered doctors for a short period of time using their given registration attributes. Furthermore, using CP-ABE along with consortium blockchain we have encrypted the patient information during a specific session to protect key exposer problem. Furthermore, our proposed security procedures satisfy the stated authentication and secrecy criteria. The master secret key and session key are only known to the sink node/BS and MS. When it comes to the biosensor nodes, BS can validate their data using legitimate attributes and allocate them utilizing policy constructs.

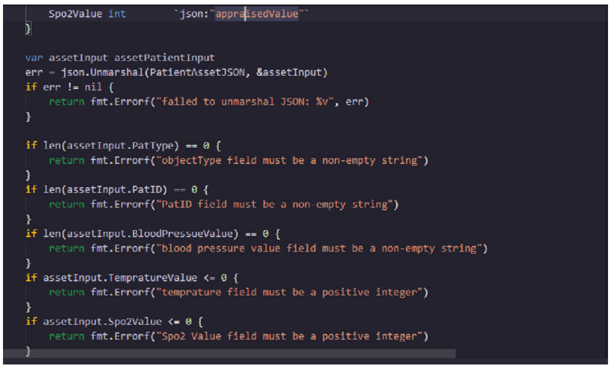
The integrity of the sensitive patient information is authenticated using hash function of the consortium blockchain. Furthermore, the correctness and accuracy of the blockchain transactions is verified using TA4SP setup shows in the following Figure 12. Besides, our proposed scheme can also verify the legitimate and illegal users during joining the WBSNs, and then, distribute the confidential privileges for a particular session among each register nodes. Thus, when session expires, the secret parameters and hidden access policies are rollback to satisfy the backward and forward secrecy in efficient manner. System administrator set new policies and parameters for new session when the request of the stakeholder is verified.

We have applied AVISPA tool to validate the security and privacy of our proposed scheme in efficient way. Moreover, the EDAS method is used to ranking the proposed scheme as compared to other state of the arts schemes [19–21]. The obtained results shows that our scheme securely and efficiently distributed the session key along with other system parameters among biosensor nodes, BS, and



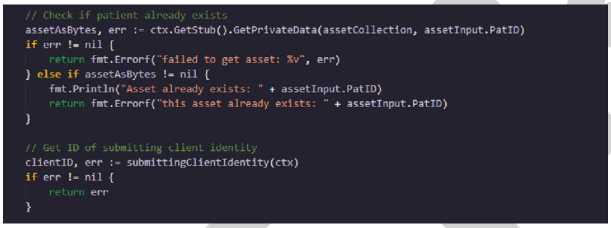
```
func (s *SmartContract) CreatePatient_CP_ABE_Consortium_Blockchain(ctx contractapi.TransactionContextI

    // Get new asset from patient map
    Patient, err := ctx.GetStub().GetPatient()
    if err != nil {
        return fmt.Errorf("error getting Patient data: %v", err)
    }

    // Asset properties are private, therefore they get passed in patient field, instead of func args
    PatientAssetJSON, ok := PatienttMap["asset_properties"]
    if !ok {
        //log error to stdout
        return fmt.Errorf("asset not found in the transient map input")
    }

    type assetPatientInput struct {
        PatType               string `json:"patObject"` //Type is used to distinguish the various ty
        PatID               string `json:"patientID"`
        BloodPressueValue   string `json:"Bpvalue"`
        TempratureValue     int    `json:"tempvalue"`
        Spo2Value int       `json:"appraisedValue"`
    }
```

Figure 13: Code part 1.



```
        Spo2Value int       `json:"appraisedValue"`
    }

    var assetInput assetPatientInput
    err = json.Unmarshal(PatientAssetJSON, &assetInput)
    if err != nil {
        return fmt.Errorf("failed to unmarshal JSON: %v", err)
    }

    if len(assetInput.PatType) == 0 {
        return fmt.Errorf("objectType field must be a non-empty string")
    }
    if len(assetInput.PatID) == 0 {
        return fmt.Errorf("PatID field must be a non-empty string")
    }
    if len(assetInput.BloodPressueValue) == 0 {
        return fmt.Errorf("blood pressure value field must be a non-empty string")
    }
    if assetInput.TempratureValue <= 0 {
        return fmt.Errorf("temprature field must be a positive integer")
    }
    if assetInput.Spo2Value <= 0 {
        return fmt.Errorf("Spo2 Value field must be a positive integer")
    }
```

Figure 14: Code part 2.



```
    // Check if patient already exists
    assetAsBytes, err := ctx.GetStub().GetPrivateData(assetCollection, assetInput.PatID)
    if err != nil {
        return fmt.Errorf("failed to get asset: %v", err)
    } else if assetAsBytes != nil {
        fmt.Println("Asset already exists: " + assetInput.PatID)
        return fmt.Errorf("this asset already exists: " + assetInput.PatID)
    }

    // Get ID of submitting client identity
    clientID, err := submittingClientIdentity(ctx)
    if err != nil {
        return err
    }
```

Figure 15: Code part 3.

MS for onward confidential patient data transmission to protect the data during transmitting using public open channel from adversaries' attacks. Moreover, in terms of cost comparison, graphs shows that our scheme consumed less processing, communication, storage, and energy as compared to other schemes [19–23]. The final result of the EDAS ranking indicates that our proposed scheme outperforms as compared to remaining schemes [19–21].

We are using the consortium blockchain to store the patient data as shown in our code. In order to make the data secure, we integrated the CP-ABE cryptographic mechanism to store the data, so an unauthorized user cannot read the patient data. In this way, we maintain the secrecy of the data. As shown in Figure 13, we are storing the patient records such as the PatID, BP, and Temp attributes in our smart contract for testing of our proposed approach. In Figure 14, we placed the checks to ensure the data integrity and data completeness. In the case of a wrong value error, it will be shown to the patient, such as in the case where an identification number is not assigned to the patient. Our code shows the error, "The PatID field must be a non-empty field." We are using the consortium blockchain. In the consortium blockchain, we give access to the authorized organizations for this we write the "GetPrivateData" function and apply the conditions accordingly as shown in Figure 15.

6. Conclusion

In this paper, we have designed an efficient and secure key management and authentication technique for WBSNs with minimal computational and communicational costs to overcome the problems of data security and privacy in a desirable way. In this scheme, we have combined the ideas of CP-ABE and consortium blockchain to improve security and privacy by utilizing minimal system resources. Furthermore, we have used constant-size secret keys along with complex access structures and other system parameters to protect against adversaries' attacks. Besides, the deployed biosensor nodes transmitted encrypted patient information using standard WBSNs protocols along with CP-ABE to their nearby Base Station (BS). Now BS transmitted the partial blocks of the patient data to the Peer-to-Peer (P2P) network server to complete the full block for further secure transactions using consensus algorithms. While using the Merkle Hash Tree, the full blocks are verified and mined, and then, added to the blockchain for further verification using the hash function. Moreover, the integration of CP-ABE and the consortium blockchain can encrypt the patient's critical attributes using complex access structures and other secret parameters to enhance the system's security, privacy, transparency, and scalability. Furthermore, we have used the AVISPA tool to verify the validity and correctness of the proposed key management and authentication approach. Additionally, the ranking criteria of the proposed scheme along with other state of the arts schemes are demonstrated using a well-known MCDM approach known as EDAS. Furthermore, the obtained numerical results along with security analysis demonstrate that our scheme is secure and efficient in terms of processing cost, communication overhead, storage cost, and energy consumption as compared to other state-of-the-art schemes.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by the Researchers Supporting Project number (RSP2021/244), King Saud University, Riyadh, Saudi Arabia.

References

[1] K. Kevin and H. Wan, *Unprecedented Global Aging Examined in New Census Bureau Report Commissioned by the National Institute on Aging*, National Institutes of Health, Bethesda, MD, USA, 2009.

[2] W. Chen and J. J. Liu, *Future Population Trends in China: 2005-2050; Centre of Policy Studies (CoPS)*, Victoria University, Melbourne, Australia, 2009.

[3] T. Bodenheimer, E. Chen, and H. D. Bennett, *Burden of Chronic Disease*, 2009.

[4] G. Anderson and J. Horvath, "The growing burden of chronic disease in America," *Public health reports*, vol. 119, no. 3, pp. 263–270, 2004.

[5] T. Lehnert, D. Heider, H. Leicht et al., "Review: health care utilization and costs of elderly persons with multiple chronic conditions," *Medical Care Research and Review*, vol. 68, no. 4, pp. 387–420, 2011.

[6] D. Yach, C. Hawkes, C. L. Gould, and K. J. Hofman, "The global burden of chronic diseases overcoming impediments to prevention and control," *Jama*, vol. 290, 2015.

[7] S. Movassaghi, S. Member, M. Abolhasan, and S. Member, "Wireless body area networks: a survey," *IEEE Communications surveys & tutorials*, vol. 16, no. 3, pp. 1658–1686, 2014.

[8] H. Wang and Y. Song, "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain," *Journal of medical systems*, vol. 42, no. 8, p. 152, 2018.

[9] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, 2017.

[10] C. Hu, S. Member, H. Li, and X. Cheng, "Secure and efficient data communication protocol for wireless body area networks," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 2, no. 2, pp. 94–107, 2016.

[11] H. Mukhtar, S. Rubaiee, M. Krichen, and R. Alroobaea, "An IoT framework for screening of COVID-19 using real-time data from wearable sensors," *International journal of environmental research and public health*, vol. 18, no. 8, p. 4022, 2021.

[12] Y. Tian, Y. Peng, G. Gao, and X. Peng, "Role-based access control for body area networks using attribute-based encryption in cloud storage," *International Journal of Network Security*, vol. 19, no. 5, pp. 720–726, 2017.

[13] N. Sharma and R. Bhatt, "Privacy preservation in WSN for healthcare application," *Procedia computer science*, vol. 132, pp. 1243–1252, 2018.

[14] Y. Zhao, P. Fan, H. Cai, Z. Qin, and H. Xiong, "Attribute-based encryption with non monotonic access structures supporting fine-grained attribute revocation in Mhealthcare," *International Journal of Network Security*, vol. 19, no. 6, pp. 1044–1052, 2017.

[15] A. Wu, Y. Zhang, X. Zheng, R. Guo, Q. Zhao, and D. Zheng, "Efficient and privacy-preserving traceable attribute-based encryption in blockchain," *Annals of Telecommunications*, vol. 74, no. 7-8, pp. 401–411, 2019.

[16] J. Iqbal, A. Waheed, M. Zareei et al., "A lightweight and secure attribute-based multi receiver generalized signcryption scheme for body sensor networks," *IEEE Access*, vol. 8, pp. 200283–200304, 2020.

[17] J. Iqbal, A. I. Umar, N. Amin, and A. Waheed, "Efficient and secure attribute-based heterogeneous online/offline signcryption for body sensor networks based on blockchain," *International Journal of Distributed Sensor Networks*, vol. 15, no. 9, 2019.

[18] F. Saleem, M. N. Majeed, J. Iqbal et al., "Ant lion optimizer based clustering algorithm for wireless body area networks in livestock industry," *IEEE Access*, vol. 9, pp. 114495–114513, 2021.

[19] B. Gupta, "An attribute-based keyword search for m-health networks," *Journal of Computer Virology and Hacking Techniques*, vol. 17, no. 1, pp. 21–36, 2021.

[20] R. Guo, C. Zhuang, H. Shi, Y. Zhang, and D. Zheng, "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*, vol. 16, no. 2, 2020.

[21] H. Li, K. Yu, B. Liu, C. Feng, Z. Qin, and G. Srivastava, "An efficient ciphertext-policy weighted attribute-based encryption for the Internet of health things," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 5, pp. 1949–1960, 2022.

[22] A. Sivasangari, A. Ananthi, D. Deepa, G. Rajesh, and X. M. Raajini, "Security and privacy in wireless body sensor networks using lightweight cryptography scheme," in *Security and Privacy Issues in IoT Devices and Sensor Networks*, pp. 43–59, Academic press, 2021.

[23] W. Wang, H. Huang, L. Xue, Q. Li, R. Malekian, and Y. Zhang, "Blockchain-assisted handover authentication for intelligent telehealth in multi-server edge computing environment," *Journal of Systems Architecture*, vol. 115, p. 102024, 2021.

[24] Q. Han, Y. Zhang, and H. Li, "Efficient and robust attribute-based encryption supporting access policy hiding in Internet of Things," *Future Generation Computer Systems*, vol. 83, pp. 269–277, 2018.

[25] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, and F. M. Almansour, "Blockchain-assisted secured data management framework for health information analysis based on internet of medical things," *Personal and ubiquitous computing*, pp. 1–14, 2021.

[26] H. U. A. Ma, Y. Xie, J. Wang, G. Tian, and Z. Liu, "Revocable attribute-based encryption scheme with efficient deduplication for ehealth systems," *IEEE Access*, vol. 7, pp. 89205–89217, 2019.

[27] A. Arfaoui, A. Kribèche, O. R. Boudia, A. B. Letaifa, S. M. Senouci, and M. Hamdi, "Context-aware authorization and anonymous authentication in wireless body area networks," in *2018 IEEE International Conference on Communications (ICC)*, Kansas City, MO, USA, 2018.

[28] M. Karuppiah, A. K. Das, X. Li et al., "Secure remote user mutual authentication scheme with key agreement for cloud environment," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 1046–1062, 2019.

[29] M. Naeem, S. A. Chaudhry, K. Mahmood, M. Karuppiah, and S. Kumari, "A scalable and secure RFID mutual authentication protocol using ECC for Internet of Things," *International Journal of Communication Systems*, vol. 33, no. 13, 2020.

[30] M. Karuppiah and R. Saravanan, "Cryptanalysis and an improvement of new remote mutual authentication scheme using smart cards," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 18, no. 5, pp. 623–649, 2015.

[31] M. Karuppiah, "Remote user authentication scheme using smart card: a review," *International Journal of Internet Protocol Technology*, vol. 9, no. 2/3, pp. 107–120, 2016.

[32] A. Pradhan, M. Karuppiah, R. Niranchana, M. A. Jerlin, and S. Rajkumar, "Design and analysis of smart card-based

authentication scheme for secure transactions," *International Journal of Internet Technology and Secured Transactions*, vol. 8, no. 4, p. 494, 2018.

[33] M. Azees, P. Vijayakumar, M. Karuppiah, and A. Nayyar, "An efficient anonymous authentication and confidentiality preservation schemes for secure communications in wireless body area networks," *Wireless Networks*, vol. 27, no. 3, pp. 2119–2130, 2021.

[34] A. Maria, V. Pandi, J. D. Lazarus, M. Karuppiah, and M. S. Christo, "BBAAS: blockchain-based anonymous authentication scheme for providing secure communication in VANETs," *Security and Communication Networks*, vol. 2021, Article ID 6679882, 11 pages, 2021.

[35] M. I. Khalid, J. Iqbal, A. Alturki, S. Hussain, A. Alabrah, and S. S. Ullah, "Blockchain-based land registration system: a conceptual framework," *Applied Bionics and Biomechanics*, vol. 2022, Article ID 3859629, 21 pages, 2022.

[36] W. Xu, J. Zhang, Y. Yuan, X. Wang, Y. Liu, and M. I. Khalid, "Towards efficient verifiable multi-keyword search over encrypted data based on blockchain," *Peer J Computer Science*, vol. 8, article e930, 2022.

[37] I. Ehsan, M. Irfan Khalid, L. Ricci et al., "Conceptual model for blockchain-based agriculture food supply chain system," *Scientific Programming*, vol. 2022, Article ID 7358354, 15 pages, 2022.

[38] S. Hussain, S. S. Ullah, A. Gumaei, M. Al-Rakhami, I. Ahmad, and S. M. Arif, "A novel efficient certificateless signature scheme for the prevention of content poisoning attack in named data networking-based Internet of Things," *IEEE Access*, vol. 9, pp. 40198–40215, 2021.

[39] M. Rehman, H. Khattak, A. S. Alzahrani et al., "A lightweight nature heterogeneous generalized signcryption (HGSC) scheme for named data networking-enabled Internet of Things," *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 8857272, 20 pages, 2020.

[40] S. Hussain, S. S. Ullah, M. Uddin, J. Iqbal, and C. L. Chen, "A comprehensive survey on signcryption security mechanisms in wireless body area networks," *Sensors*, vol. 22, no. 3, 2022.

[41] S. Hussain, S. S. Ullah, I. Ali, J. Xie, and V. N. Inukollu, "Certificateless signature schemes in industrial Internet of Things: a comparative survey," *Computer Communications*, vol. 181, pp. 116–131, 2022.

[42] Y. Ren, Y. Leng, F. Zhu, J. Wang, and H. J. Kim, "Data storage mechanism based on blockchain with privacy protection in wireless body area network," *Sensors*, vol. 19, no. 10, pp. 1–16, 2019.

[43] J. Hong, B. Liu, Q. Sun, and F. Li, "A combined public-key scheme in the case of attribute-based for wireless body area networks," *Wireless Networks*, vol. 25, no. 2, pp. 845–859, 2019.

[44] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health dystems via consortium blockchain," *Journal of medical systems*, vol. 42, no. 8, p. 140, 2018.

[45] G. Bramm, M. Gall, and J. Schütte, "BDABE-blockchain-based distributed attribute based encryption," in *Proceedings of the 15th International Joint Conference on e-Business and Telecommunications*, Porto, Portugal, July 2018.

[46] R. R. Al-Dahhan, Q. Shi, G. M. Lee, and K. Kifayat, "Survey on revocation in ciphertext-policy attribute-based encryption," *Sensors (Switzerland)*, vol. 19, no. 7, pp. 1–22, 2019.

[47] Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: efficient policy-hiding attribute-based access control," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2130–2145, 2018.

[48] Y. Zhang, X. Chen, J. Li, D. S. Wong, H. Li, and I. You, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing," *Information Sciences*, vol. 379, pp. 42–61, 2017.

[49] J. Lai, R. H. Deng, Y. Yang, and J. Weng, "Adaptable ciphertext-policy attribute-based encryption," in *International Conference on Pairing-Based Cryptography*, pp. 199–214, Cham, 2014.

[50] C. Hu, X. Cheng, Z. Tian, J. Yu, K. Akkaya, and L. Sun, "An attribute-based signcryption scheme to secure attribute-defined multicast communications," in *International Conference on Security and Privacy in Communication Systems*, vol. 164, pp. 418–437, Cham, 2015.

[51] B. Chandrasekaran, R. Balakrishnan, and Y. Nogami, "Secure data communication using file hierarchy attribute based encryption in wireless body area networks," *Journal of Communications Software and Systems*, vol. 14, no. 1, 2018.

[52] J. Wang, J. Cao, R. S. Sherratt, and J. H. Park, "An improved ant colony optimization-based approach with mobile sink for wireless sensor networks," *The Journal of Supercomputing*, vol. 74, no. 12, pp. 6633–6645, 2018.

[53] S. Kornmesser, "Theoretizität im logischen empirismus und im strukturalismus - erläutert am fallbeispiel des neurobiologischen konstruktivismus," *Journal for General Philosophy of Science*, vol. 39, no. 1, pp. 53–67, 2008.

[54] M. Möser, K. Soska, E. Heilman et al., "An empirical analysis of traceability in the Monero blockchain," *Proceedings on Privacy Enhancing Technologies*, vol. 2018, no. 3, pp. 143–163, 2018.

[55] S. Pal, M. Hitchens, V. Varadharajan, and T. Rabehaja, "Policy-based access control for constrained healthcare resources in the context of the Internet of Things," *Journal of Network and Computer Applications*, vol. 139, pp. 57–74, 2019.

[56] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, no. 8, pp. 38431–38441, 2019.

[57] Y. Gao, X. Dong, and Y. Tian, "A New signcryption scheme without certificate and linear pairing," in *Proceedings of the 2nd International Conference on Computer Science and Application Engineering*, Hohhot, China, October 2018.

[58] J. Hathaliya, P. Sharma, S. Tanwar, and R. Gupta, "Blockchain-based remote patient monitoring in healthcare 4.0," in *IEEE 9th international conference on advanced computing (IACC)*, pp. 87–89, Tiruchirappalli, India, December 2019.

[59] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, "Blochie: a blockchain-based platform for healthcare information exchange," in *2018 IEEE international conference on smart computing (smartcomp)*, pp. 49–56, Taormina, Italy, 2018, June.

[60] S. Jiang, J. Cao, H. Wu, and Y. Yang, "Fairness-based packing of industrial IoT data in permissioned blockchains," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7639–7649, 2021.

[61] S. Jiang, J. Cao, J. A. McCann et al., "Privacy-preserving and efficient multi-keyword search over encrypted data on blockchain," in *2019 IEEE international conference on Blockchain (Blockchain)*, pp. 405–410, Atlanta, GA, USA, 2019, July.

[62] M. Keshavarz Ghorabaee, E. K. Zavadskas, L. Olfat, and Z. Turskis, "Multi-criteria inventory classification using a

new method of Evaluation Based on Distance from Average Solution (EDAS)," *Informatica*, vol. 26, no. 3, pp. 435–451, 2015.

[63] K. Keshavarz Ghorabaee, E. K. Zavadskas, M. Amiri, and Z. Turskis, "Extended EDAS method for fuzzy multi-criteria decision-making: an application to supplier selection," *International Journal of Computers Communications & Control*, vol. 11, no. 3, pp. 358–371, 2016.

[64] L. A. Zadeh, "Fuzzy logic," *Computer*, vol. 21, no. 4, pp. 83–93, 1988.

[65] K. Tanaka, *An Introduction to Fuzzy Logic for Practical Applications*, Springer, Tokyo, 1997.

[66] N. A. Malik and M. Rai, "Enhanced secure and efficient key management algorithm and fuzzy with trust management for MANETs," in *in Proc. Int. Conf. Innov. Comput. Commun. (ICICC)*, New Delhi, India, February 2020.

[67] G. Mehmood, M. Z. Khan, A. Waheed, M. Zareei, and E. M. Mohamed, "A trust-based energy-efficient and reliable communication scheme (trust-based ERCS) for remote patient monitoring in wireless body area networks," *IEEE Access*, vol. 8, pp. 131397–131413, 2020.

[68] D. Zindani, S. R. Maity, and S. Bhowmik, "Fuzzy-EDAS (Evaluation Based on Distance from Average Solution) for material selection problems," in *Advances in Computational Methods in Manufacturing*, pp. 755–771, Springer, Singapore, 2019.

[69] M. Yazdani, A. E. Torkayesh, E. D. Santibanez-Gonzalez, and S. K. Otaghsara, "Evaluation of renewable energy resources using integrated Shannon Entropy– EDAS model," *Sustainable Operations and Computers*, vol. 1, pp. 35–42, 2020.

[70] Avispa Team, *Automated validation of internet security protocols and applications*, 2015, http://www.avispa-project.org/.

[71] Avispa Team, *AVISPA web tool*http://www.avispa-project.org/webinterface/expert.php/.