International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/220734 Volume 10, Issue 2, March – April (2023)

RESEARCH ARTICLE

A Hybrid Cryptography and LogiXGBoost Model for Intelligent and Privacy Protection in Wireless Body Sensor Networks (WBSNS)

Mohammed Naif Alatawi
Department of Computer Information Technology, University of Tabuk, Tabuk, Saudi Arabia.
alatawimn@ut.edu.sa

Received: 15 December 2022 / Revised: 12 February 2023 / Accepted: 23 February 2023 / Published: 29 April 2023

Abstract – An increasing number of healthcare applications are making use of wireless body sensor networks (WBSNs). WBSN technology provides a framework that allows for remote physiological monitoring of patients without the use of wired connections in the house. Furthermore, these systems provide real-time data transfer for medical personnel, allowing them to make timely decisions regarding patient care. Despite this, worries remain about patient data being compromised. This research presents a strategy for protecting patient-provider communications by making use of WBSNs. To solve the problem of how to securely store sensitive information on blockchains, a hybrid cryptographic architecture is proposed. The strengths of both public key and symmetric key cryptography are leveraged in my approach. In order to achieve this goal, I have developed a new algorithm by fusing the AES, RSA, and Blowfish algorithms. My experiments have shown that the proposed solution can keep private data safe without affecting its scalability. Using Logi-XGB as a prediction model for attacks, the proposed approach can successfully thwart 99.7 percent of them.

Index Terms – WBSNs, IoT, Machine Learning, Logi-XGB, XGB, DL, Blockchain.

1. INTRODUCTION

E-health has benefited greatly from recent technological developments and advances in information technology. The use of WBSNs (Wireless Body Sensor Networks) in healthcare monitoring and diagnostics is on the rise [1]. The WBSN has been seen in a variety of settings within the healthcare sector in the past [2, 3]. They have been used for a variety of medical issues, including diabetes, Alzheimer's disease, congestive heart failure, and asthma [4]. WBSN enables real-time monitoring of patients during critical situations [5].

Using WBSNs (Wireless Body Sensor Networks) in a mobile healthcare setting has potential [6]. Sensor data can be analysed by computers at a healthcare facility [7]. Real-time monitoring at home allows patients to be kept under observation for longer periods of time, reducing the need for costly hospitalisation [8]. Sensing nodes and Internet servers in a WBSN should be encrypted [9] to prevent unauthorised parties from accessing patients' personal health information during transmission and reception. It is also important for doctors to get their hands on this data to verify that it is authentic and has not been tampered with [10]. Internet of Health Things (IoHT) [11] allows for the incorporation of sensors and remotely monitored medical devices with patient data. At today's hospitals, IoT-based Wireless Body Sensor Networks play a crucial role in patient care (WBSNs). Intelligent sensors can now be used to gather vital biological data from a patient in real time. The data collected can then be sent electronically to faraway medical professionals [12]. In recent years, many anonymous authentication solutions for WSNs have been presented [8]. Many of these methods, however, require higher computer power when utilised for anonymous authentication [13]. Existing procedures did not safeguard against tracking for either patients or clinicians [14–16], [17]. Based on the results of a thorough analysis [18], it is clear that the proposed system eliminates the security flaws of the aforementioned approaches, all while requiring very low computer resources for anonymous authentication [19–23].

Block-chains provide a more secure platform for storing and sharing data due to its open nature [24]. A number of healthcare organisations are exploring potential applications of blockchain technology [25]. Significant features of this system include [26] the safe transmission of patient medical records, the management of the drug supply chain, and the support of researchers working on the genetic code. The blockchain's inherent security stems from its immutable ledger and decentralised storage [27], [28]. People's sensitive health records are safe in the hands of blockchain's secure protocols [29]. Doctors and other medical professionals can now have more secure and productive conversations with their patients thanks to technological advancements [30].

Distributed and shared healthcare data is made possible by blockchain technology [31]. Since the Blockchain is a

RESEARCH ARTICLE

decentralised network, it can be used to consolidate many different parts of the healthcare system at once [32]. Exchanges of information between businesses and service providers are feasible via Block Chain [33]. Blockchain technology allows for decentralised storage and verification of data for greater accuracy [34]. High-speed data transfer between mobile and other networks is made possible by 5G telecommunications technology [35]. It's crucial that doctors have instantaneous access to patient records so they can make quick decisions even when time is of the essence. To interact with patients in real time across a telemedicine network, one needs a high-quality video communication system [36], [37].

The main goal of this study is to develop a quick reaction to a patient's aberrant condition. Figure 1 shows the overall system architecture. The patient's information is stored in a database. Blockchain technology ensures the security of database information. The patient's historical records can be used to check the integrity of the data stored in the cloud. 5G services are utilised by cloud storage facilities and medical specialists for the purpose of exchanging data. Treatment plans for patients are prescribed and carried out by medical experts. In order to ensure the quickest possible response time in terms of therapy, it is essential that all patient data is kept secure.

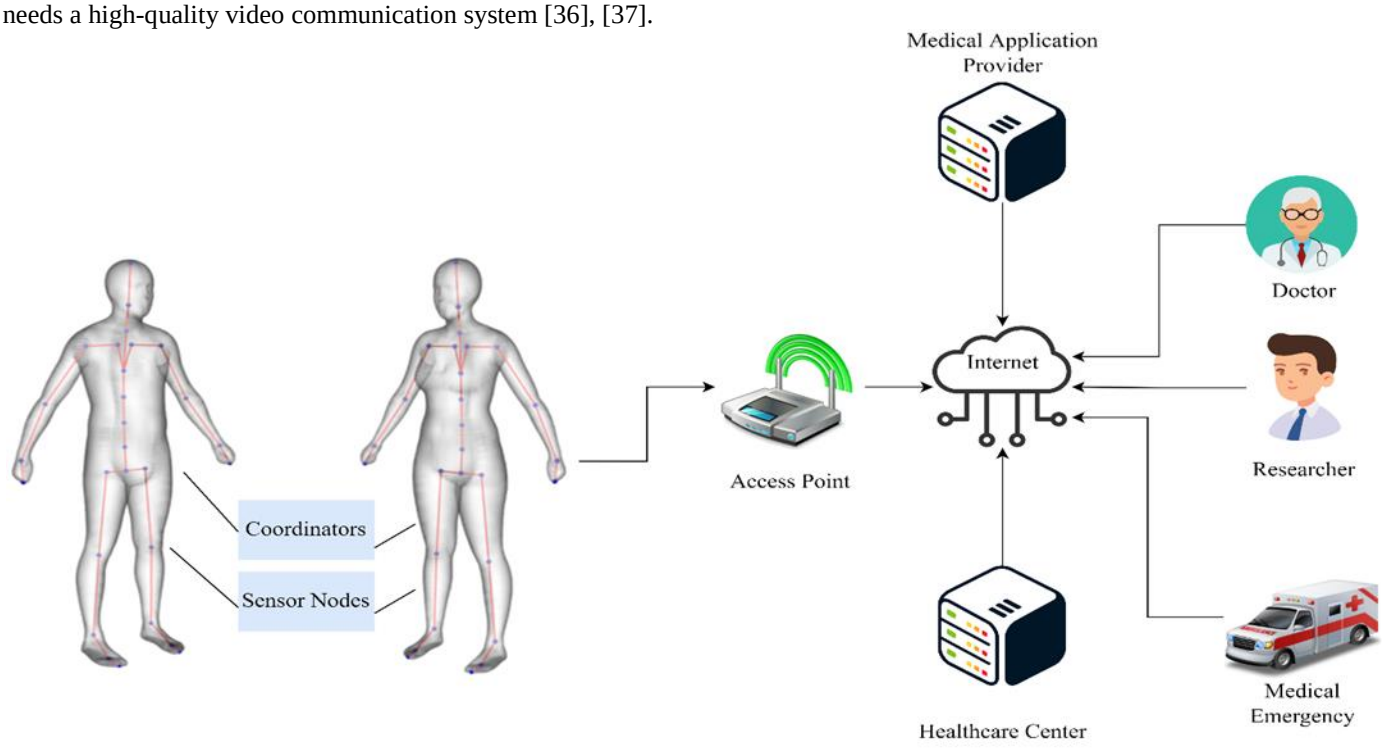

Figure 1 The Typical Scenario of WBSNs [38]

There has been an explosion of WBSN authentication options in recent years [39]. Using these methods, both the WBSN user and the application provider can verify one other's identities without jeopardising the security of their data [40], [41]. Experiments show that multiplying points on an elliptic curve takes significantly more time than pairing. This means that WBSNs should steer clear of these methods [42].

Nevertheless, multi-server authentication that does not rely on a remote server is easier to implement [43], [44]. An effective and secure authentication technique for WBSNs is proposed in this research, which makes use of Blockchain technology and a multi-server architecture. Concerns about security and energy efficiency in WBSNS have not been fully addressed [45]. The massive data sensing power of WBSNs poses a threat to the network's power efficiency, which in turn poses a threat to the network's security. Using IoT-based clinical decision support, cloud-based clinical decision support, 5G services [46], [47], and blockchain technology, I have developed a novel technique of Load Balancing Energy Efficient Sleep Awake Aware (LB-EESAA) protocol and an IoT-based clinical decision support system that can forecast and monitor sickness severity with security risks prediction.

In this model, the patient is constantly monitored by a network of tiny, lightweight sensors. If you're developing a plan for healthcare, you must give serious consideration to issues of safety. In an online healthcare monitoring approach, sensors can be utilised to assess medical data and negotiate the patient's death. Blockchain technology is used in sensors and health monitoring equipment to secure the security of the data they acquire over the 5G network, enabling for more in-depth research into diseases.

RESEARCH ARTICLE

The prevalence of people in the general population who deal with ongoing medical issues has grown considerably in recent decades. Treatment for these disorders is often ongoing and requires close monitoring. So, many people would rather get therapy at home than at a hospital. Emerging technologies like Wireless Body Sensor Networks (WBSNs) are empowering individuals to take control of their health by providing them with remote access to their data. Many sensors, such as those attached to the heart, lungs, brain, skin, etc., and a gateway node that receives and transmits the acquired data to a remote server make up what is known as a wireless body sensor network (WBSN) [48], [49].

The patient's vital signs and other physiological data can be tracked using a WBSN. A WBSN may keep tabs on vitals including heart rate, breathing rate, temperature, and weight in addition to diagnostic tests like an ECG (ECG). A centralised database can receive these parameters and analyse them for use by doctors and nurses. As a result, WBSNs can aid in the diagnosis and treatment of patients. Nonetheless, there is still worry about patient data privacy and security. It is important for patients that their health information is protected while being sent to their doctor. Thus, it is important to create a safe system for safeguarding patient information.

When it comes to health care, the field of e-health is one of the most dynamic and expanding areas. The WBSN is one type of WSN. Examples of such popular technologies include WBSNs. In the healthcare industry, tele homecare, also known as remote monitoring and diagnosis, is a fast growing subsector. A patient's vital signs can be tracked in real-time over a wireless body area network, giving medical professionals more time to react in the event of an emergency. For the past few years, I've found myself caring more about patients than doctors. The focus of healthcare systems around the world is shifting to the patients who use them. Telemonitoring and telemedicine is one way to enhance the doctor-patient relationship. Telephone home care is becoming a more practical area of study as computing capabilities increase. I have researched the proposed technology extensively and provide an assessment based on typical data transfer rates and encryption/decryption timeframes. One of my primary discoveries is that sensitive information can be protected from prying eyes by using a privacy-preserving system that combines AES and RSA. There is a wide variety of metrics that may be used to gauge a blockchain's effectiveness. The typical rate of new blocks being generated, the throughput of individual transactions, and the total number Bitcoin transactions processed each second are all good illustrations. The outcomes show a blatant throughput-related trade-off between convenience and safety. An increase in latency is a cost of achieving a high throughput. Yet, with longer lags, it becomes trickier to spot accounting tampering. Also, a lightweight multi-party computation protocol is presented in the study that allows users to communicate encrypted messages without revealing their identities. The created framework has the potential to be used in peer-to-peer networks to ensure safe data exchange between nodes. Research methodology as depicted in Figure 2.

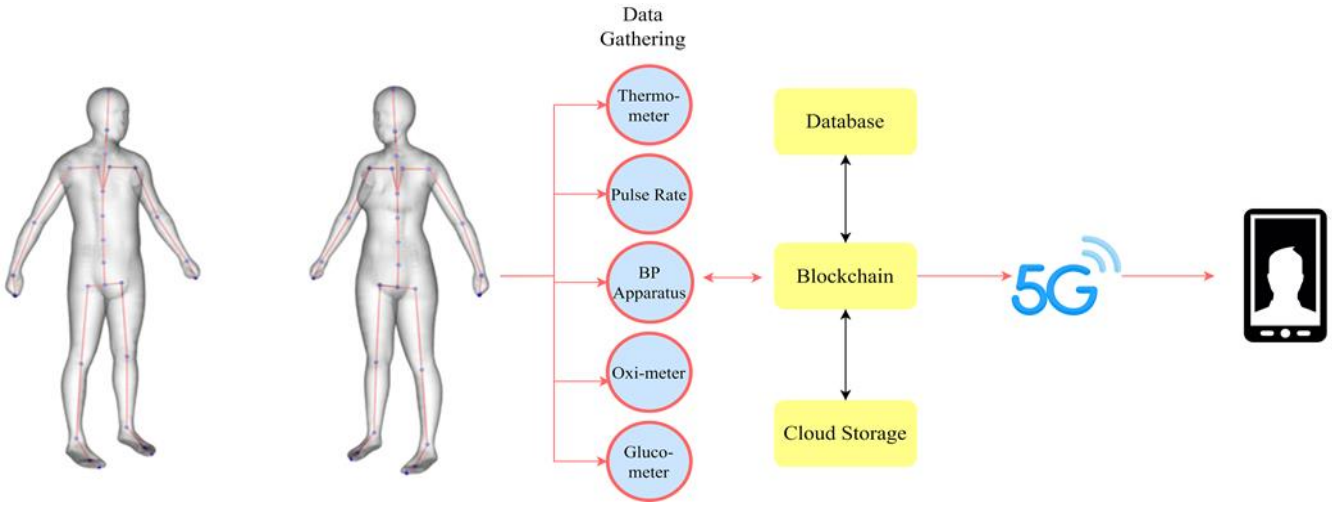

Figure 2 Proposed Workflow

2. RELATED WORK

The evolution and improvement of IT has helped bolster e-health in several ways. A growing number of healthcare diagnostic and monitoring systems employ Wireless Body Sensor Networks (WBSNs). Previous research has shown the WBSN's utility in a variety of settings, including healthcare providers and medical corporations. Tele-homecare, made possible by this gear, allows doctors to check on patients from afar. Common uses include treating diabetes, Alzheimer's,

RESEARCH ARTICLE

heart failure, and asthma. WBSN allows for continuous, real-time monitoring of patients even in the midst of a disaster. The field of wireless body sensor networks (WBSNs) has promise for enhancing the quality of mobile healthcare (WBSNs). Hospital or medical centre computers can process data collected by sensors. It's more cost-effective to monitor patients at home, and they can be monitored in real time for longer periods of time. Additionally, medical professionals will need access to this information to check for any signs of tampering and to confirm that it is, in fact, the patient's.

To cite Al-Janabi et al. [7] further research has to be done into the privacy and security concerns posed by WBSN's communication architecture. As an added bonus, this book delves into the topic of WBSN safety and the studies that have been conducted on the topic. In the end of the work, the author lays out potential avenues for future research and development.

Wireless body sensor networks are being implemented to provide a mobile healthcare system that is both secure for the elderly and linked to the internet (WBSNs). With its very efficient key generation procedure, the multi-biometric methodology developed by Ma et al. [50] ensures excellent levels of security.

The primary concerns regarding the safety and confidentiality of WBSN data are the subject of this study [28]. D-Sign, a data hybrid method available from us, is used to encrypt and decrypt digital signatures. Authentication strategies like the one presented by Saleem et al. [51], which do not reveal the identity of the patient or physician, can go a long way towards building confidence. Algorithms like DES and AES are used in cryptography.

The need for huge keys shared amongst many persons makes it harder for these systems to provide adequate data security. Using an affine cypher allows for a much smaller key size while yet providing adequate security. The proposed work has been shown to be secure enough in the face of a variety of destructive security threats, as demonstrated by the security analysis. The Performance Analysis contains price information for the suggested approach. According to the authors' calculations, this method reduces the computational complexity by 29 percent.

Since the development of biometrics, wearable sensors have grown increasingly popular. Due to the increased number of intermediate nodes where aggregated data is stored, it is more vulnerable to security and privacy breaches. Recently, academics' interest in security-assisted data aggregation has grown [38].

Based on their signature encryption method, Hussain et al. [52] design a means of controlling access to wireless body area networks (WBSNs). My method also has the added benefits of ensuring the privacy, authenticity, validity, and irrefutability of any cypher text produced. My controller uses significantly less computing and power than the top three widely-used signcryption-based access control methods. As a result of certificate-less encryption, my system no longer requires public keys or a central repository for all of my keys to operate properly.

In this age of widespread communication technology, unique applications for both patients and carers facilitate prompt action. Sensitive information is transmitted over Wireless Body Sensor Networks (WBSNs), which can be abused and lead to incorrect medical diagnosis and treatment (WBSNs). Security and privacy are difficult to implement in WBSN because of its limited resources and mission-critical applications. In terms of WBSN technology, there is a lot of attention paid to safety and confidentiality [53]. The paper concludes with a discussion of prospective future research topics and critical challenges.

Using a biometric-based security architecture that capitalises on the similarity between body sensors is one way to bolster WSN safety. The suggested authentication and selective encryption techniques need little in the way of computational power or other resources (such as battery life or network throughput) [1]. Proper implementation of the proposed strategy eliminates the need for widespread key distribution or precise timing.

3. METHODOLOGY

Figure 3 is a diagram displaying the proposed architecture for safe AI-based Block chain support in the healthcare sector. The expert system interacts with the user, wireless network, blockchain, trusted agent, and healthcare server. A user can be suffering from a wide variety of conditions, or they might have been cured of an illness.

The user has numerous sensors inserted and worn to track the health. Information from medical sensors can also be collected and stored on smartphones and other PDAs. An individual's health records can be encrypted and added to the blockchain on a regular basis if the user keeps a log using a personal digital assistant (PDA). This block references the information, time stamp, and data from the prior block.

There are two types of authorised agents, namely validators and recorders. The validity of all transactions is guaranteed by a network of nodes called validating agents. The diagnostic expert system's capacity for making decisions is comparable to that of a human specialist.

In the past, material that wasn't protected by a blockchain would be scanned for infections before it was encrypted. Lifesaving drugs can now be given to patients remotely thanks to sensors placed in the body. This diagram is a simplified representation of the paradigm that has been proposed.

RESEARCH ARTICLE

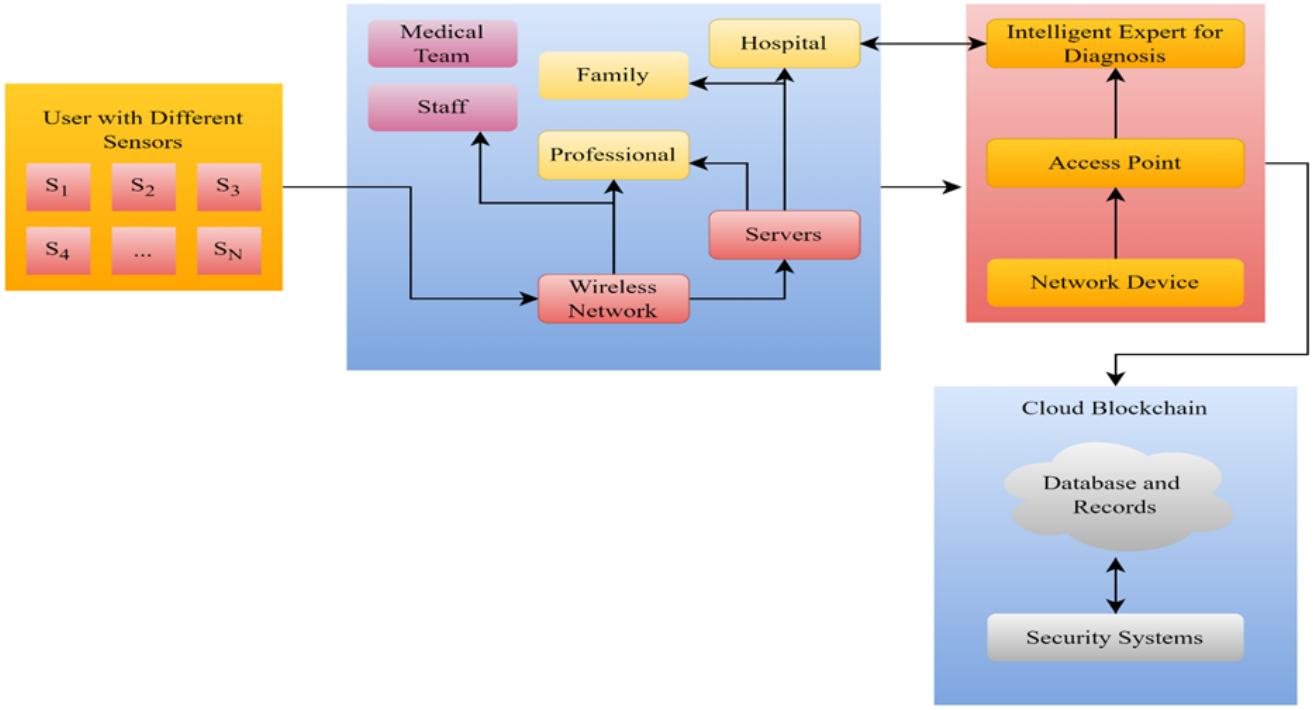

Figure 3 Proposed Architecture

3.1. Significance of System

There is a need for more healthcare facilities, including hospitals, medical facilities, and doctors. The inability to properly diagnose every sick patient in the country has resulted in many deaths. The proposed paradigm allows for the monitoring and diagnosing of large numbers of people simultaneously, which may help address such a widespread crisis.

This communication method will enable hospitals and their patients to share vital information. The patient's medical history is stored and managed on Blockchain, a distributed database. Using a public key cryptosystem allows information to be kept private and authentic yet easily verifiable. AI recommends a specialist, disease category, and medication based on the patient's medical history.

3.2. Identity-Based Crypto Secured and Privacy Preserving Approach

The suggested method safeguards medical records by employing an elliptic curve cryptosystem-based identity-based cryptosystem. In this case, the IBC is not responsible for validating the recipient's public key. Compared to modular exponentiation, ECC arithmetic is roughly 20 times faster and RSA claims that a 1024-bit RSA key is as secure as an ECC 128-bit key. There are several ways in which IoT applications can make use of the unique qualities of IBC and ECC.

3.3. Proposed Wireless Body Sensor Network Model for E-Healthcare

WBSN interaction can be divided into in vivo and in vitro forms based on the environment in which the radio signal is received. A new in-vivo communication strategy called body-coupled communication is used to determine people's identities in the body domain network. In this context, I am referring to low-power, short-range communication because the person wears most WBSN devices. As an illustration of "external communication," consider the following.

3.4. Blockchain Model

P2P networks are responsible for facilitating unlimited communication between blockchain nodes since nodes can be located anywhere in the world and still have equal access to the application. Every participant in a P2P system acts as both a customer and a seller. Connecting to and communicating with other nodes, broadcasting and validating transactions, and syncing data blocks are all routing aspects.

In a network, each node is just one piece of the puzzle (both transactions and blocks are data structures of the blockchain, as described below). This is typical of the distributed nature and flat design of P2P networks. Many blockchain apps have input/output interfaces (application programming interfaces), and users can skip the underlying infrastructure of the service and interact directly with the APIs. Figure 4 shows the proposed WBSNs Sensors.

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/220734 Volume 10, Issue 2, March – April (2023)

RESEARCH ARTICLE

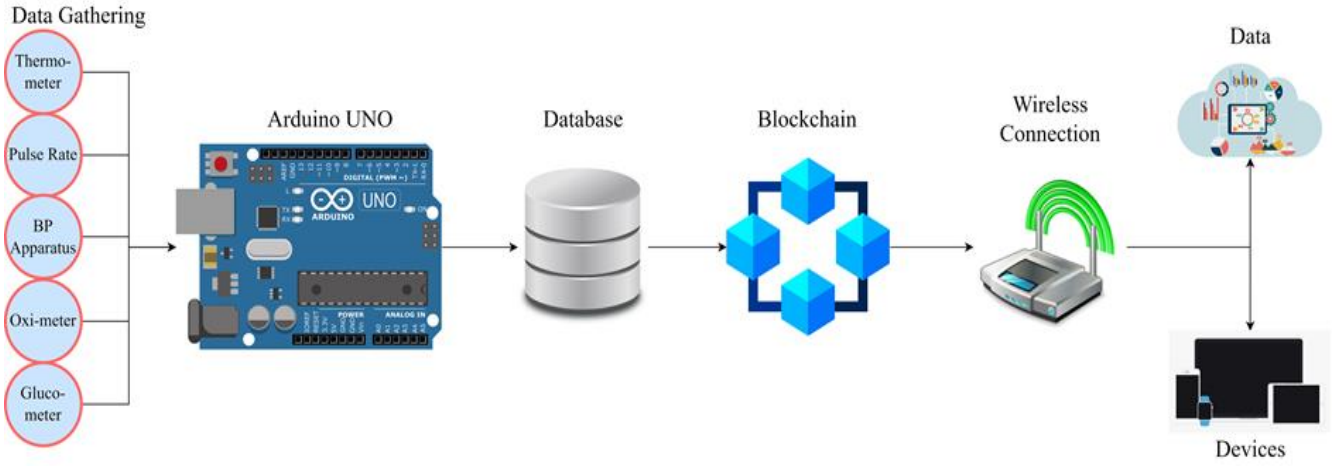

Figure 4 Proposed WBSNs Sensors

3.5. Public Blockchain Technology

The advantage of the fact that anyone can join a public blockchain network anytime. Everybody is welcome to join in. As a result, the ledger is accessible to anyone, and everyone can have a voice in establishing the agreement. It's easy to think of Ethereum as an example of a public blockchain platform. Since public blockchains are accessible to the general public, no single entity can exert absolute control over their evolution. The fact that new users can join a blockchain at any time is what makes it public. A public blockchain could allow anybody to create new data blocks and provide everyone access to the existing data blocks. The majority of cryptocurrency transactions and mining have taken place on public blockchains. The Public Blockchain concept will aid in resolving data tempering issues in cloud-based data storage by centralizing data storage in a blockchain.

3.6. Cloud-Based Blockchain

A large number of businesses now use centralized databases for fear-free information storage. However, there has been an increase in the coverage of cybercriminals. One standard method for hackers to obtain vast amounts of data is through a script assault on a central database. However, the introduction of distributed ledger technologies like blockchain increases complexity. In blockchain applications, the original cryptocurrency is frequently used. Users can make money from data collected by third parties to protect themselves from identity theft and other consequences of the recent massive data breaches. Digital signatures are used to ensure the authenticity of a transaction on the blockchain. Smaller data sets are more suitable for storage with a blockchain cloud solution. After that, a second safeguard is sent across the system. This is made feasible with the help of a hash algorithm, public/private key encryption, and transaction logs. Blockchain storage has the potential to outperform cloud storage in terms of price, security, and reliability. Cloud storage providers create multiple backups to safeguard their customers' information and store them in different locations. Previous research had found cloud storage to be problematic because of the ease with which data might be tampered with, but in this study, I used centralized cloud storage to solve this problem. Cloud storage providers guarantee data safety by making numerous copies and keeping them in different locations.

3.7. Privacy Preserving Strategy

Based on the findings, it is suggested that a hybrid algorithm that combines the strengths of the three most popular cryptographic algorithms (Advanced Encryption Standard, Blowfish, and RSA) to protect users' personal information. Information transmitted over WBSNs is encrypted using several different algorithms. However, advanced new technologies are rendering these older methods useless. The time needed to crack a cryptographic system has been drastically cut down thanks to technological advancements, and a wide range of attacks has compromised the current defenses.

These systems are particularly susceptible to being broken by cryptographers due to crypto-analysis and specialized mathematical attacks. Modern systems also have the issue of key security to deal with. The inability of current systems to reliably store and transmit secret keys is a serious flaw. Maintaining peak performance is also crucial when it comes to protecting sensitive information. While longer key lengths make for a more secure encryption technique, they arrive at the expense of overall system efficiency.

In some cases, the benefits of using a solo crypto-system with only one layer can outweigh the risks, resulting in compromised data or key security. There are risks to data security in a solitary system, and sometimes the speed and

RESEARCH ARTICLE

efficiency are compromised by the many problems inherent in stand-alone systems. Therefore, it is becoming increasingly important to have a system that can compensate for the performance-security trade-offs inherent in employing unique cryptographic algorithms.

The need for a combined strategy to solve these problems is more significant than ever. The suggested system combines three of the most influential and widely used algorithms for data security—the blend of the symmetric AES and Blowfish algorithms with the asymmetric RSA algorithm. Over the Internet, particularly at the Transport Layer Security (TLS) level, RSA is one of the most used asymmetric encryption algorithms for various purposes besides data encryption.

However, Blowfish and AES are called Symmetric Ciphers because they employ the same key for encryption and decryption. AES is the safest and most efficient encryption technique, whereas Blowfish is the fastest. They can overcome problems that would otherwise be difficult to solve using either method alone.

The suggested system in this study uses a layered encryption architecture, which encrypts data three times with three separate algorithms. The keys are encrypted and stored in an image using steganography to guarantee key security. The password hash is used as the AES key to encrypt the keys, and the user's password is hashed using the SHA-1 algorithm. Based on experimental results, the proposed system written in Python is a feasible cryptosystem for safeguarding data.

The plaintext, or data, is passed into the hybrid system, where it is encrypted three times with the Blowfish mentioned above, RSA, and AES algorithms. Keys are generated by hashing a user-supplied password with the SHA1 hash function before being placed in an AES-encrypted list. To break down the system into its parts:

The System consists of three Encryption Layers, a Key Generator, and a List of Keys. The Key Generator generates the random n-bits Key depending on the Encryption Algorithm, while the List of Keys stores the Key Generated in each layer. The plaintext P is first encrypted using the Blowfish Algorithm with a 32 Bit / 64 Bit / 128 Bit Key, KBlowfish. The Key KBlowfish is generated by the Key Generator and is used for Blowfish Encryption. It is then appended to the List of Keys, L. The Plaintext, P, is encrypted to generate Cipher Output C1 as shown in Equation (1) and (2).

$$c_1 = Blowfish(P\,laintext = P;\ Key = K_{Blowfish}) \ldots (1)$$

$$L = [\,]\,KBlowfish \ldots (2)$$

The Cipher Output, C1 is then encrypted using RSA Encryption with the 1024/2048 Bit Public Key, K RSA Public generated by the Key Generator. A Private Key, KRSAPrivate, is also generated for Decryption. While the Public Key is used in Encryption, it is not stored in the List of Keys, L. The Private Key generated is appended to the List of Keys. C1 is encrypted to generate Cipher Output C2 as shown in equation (3) and (4).

$$c_2 = RSA(plaintext = c_1;\ Key = K_{RSA\ Public}) \ldots (3)$$

$$L = [\,KBlowfish\,]\,KRSA\ \ P\,rivate \ldots (4)$$

The Cipher Output, C2 is then encrypted using AES-128 Encryption with the 128 Bit, KAES generated by the Key Generator. The Key, KAES generated is appended to the List of Keys, L. This Step gives the final encrypted Cipher Output C as shown in equation (5) and (6).

$$Ciphertext;\ C = AES(Plaintext = c_2;\ Key = K_{AES}) \ldots (5)$$

$$L = [\,KBlowfish\,;\ KRSA\ \ P\,rivate\,]KAES \ldots (6)$$

The output of the system is the Cipher Output, C, and the list of keys L with all the keys as shown in equation (7).

$$List\ of\ Keys;\ L = [\,KBlowfish\,;\ KRSA\ \ P\,rivate\,;\ KAES\,] \ldots (7)$$

3.8. Key Encryption

Using the proposed system, the Keys used for encryption at the various layers can be securely stored. The List of keys, L stores all the keys generated throughout the Data Encryption Process. Whenever the key for a particular Encryption Layer is generated, it is appended to the List of Keys, L.

In the system, the encryption layers are Blowfish, RSA, and AES, respectively, so the Keys used, are stored in the same order as shown in equation (8):

$$List\ of\ Keys;\ L = [\,KBlowfish\,;\ KRSA\ \ P\,rivate\,;\ KAES\,] \ldots (8)$$

This List, L is then passed into a function that converts the list into a single string of keys separated by separators (x ,$*$,/) as shown in equation (9)

$$LS = Stringif\,y(\,L;\ separator = 0{,}0\,) \ldots (9)$$

The String, LS is then encrypted using the AES Encryption Algorithm with a Key generated from user-input password. The user inputs a password, PW which is hashed using SHA1, & the first 16 Bits of the Hash is used as the key KPassword. The Key, KPassword is used for the Encryption, generating the encrypted string LS Encrypted as shown in equation (10) and (11).

$$HashedPassword;\ H_p = SHA(P_W\,) \ldots (10)$$

$$Key;\ K_{Password} = H_P\,[0:16]LS\ \ Encrypted = AES(LS;\ KP\ assword) \ldots (11)$$

RESEARCH ARTICLE

This Encrypted string is then embedded into a Cover Image using Least Significant Bit Steganography, giving the embedded Stego-Key as shown in equation (12).

$$Stego\ Key = LSBSteganography\left(L_{S\,,Encrypted}\ ;\ CoverImage\right) \ldots (12)$$

The Stego-Key is transferred to the Receiver along with the Encrypted Data.

Figure 5 illustrated the Proposed Data Encryption Scheme and Figure 6 shows the Proposed Key Encryption Scheme.

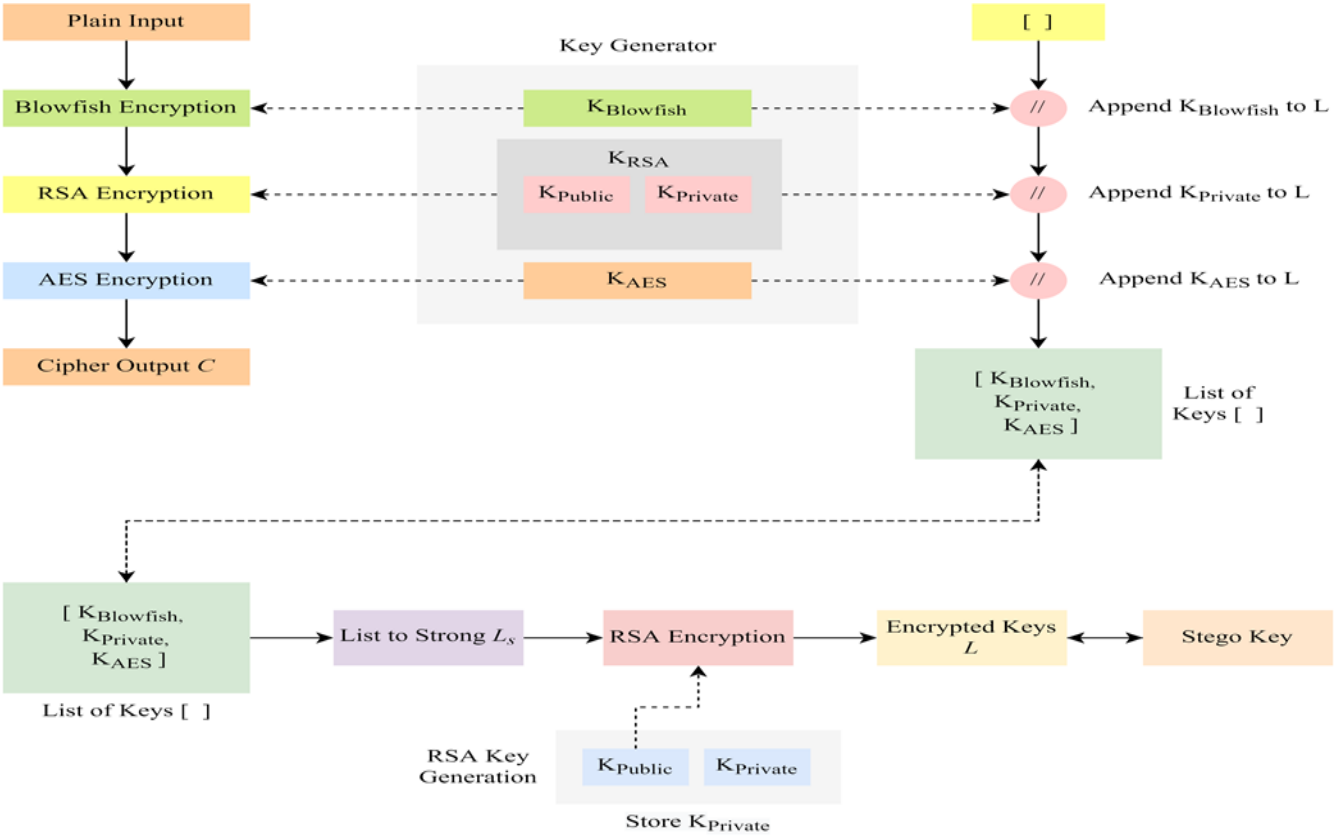

Figure 5 Proposed Data Encryption Scheme

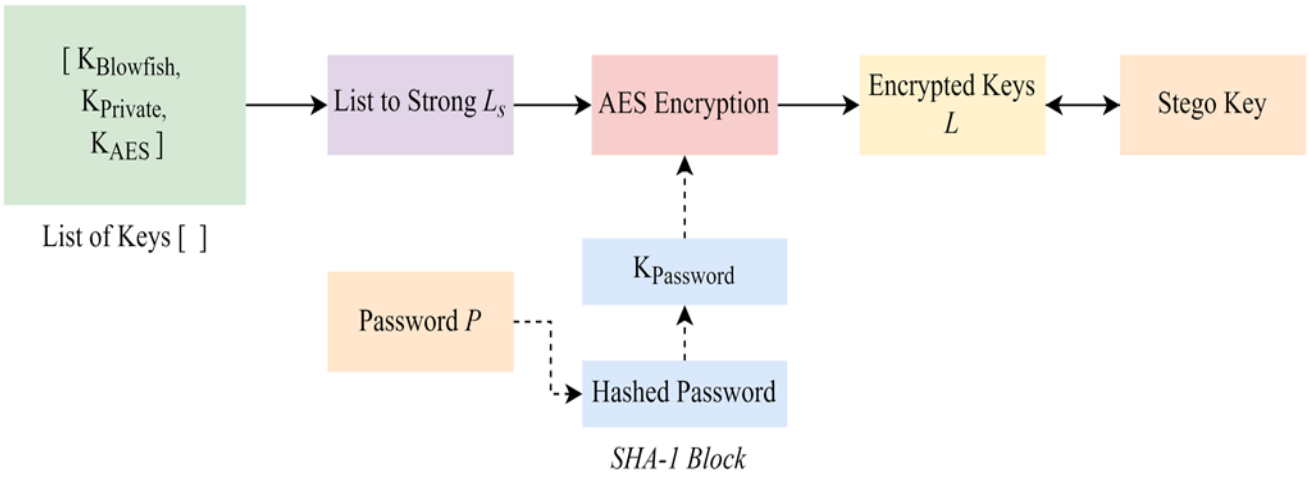

Figure 6 Proposed Key Encryption Scheme

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/220734 Volume 10, Issue 2, March – April (2023)

RESEARCH ARTICLE

4. RESULTS AND DISCUSSIONS

While employing Blockchains to encrypt patient data, it was concerned about the substantial energy consumption involved in transmitting and communicating messages in Wireless Body Sensor Networks. Given the need for early detection, the author relied on machine learning techniques to provide a foolproof system.

4.1. Communication vs. Security Level in WBSNs

The amount of network overhead rises dramatically when sign encryption is used, and the size of the signed message primarily determines the transmission overhead. When using a WBSN, it is common for only two bits to be required of each user. Figure 7 displays the communication cost and the precautions taken to ensure security. Enhanced safety measures need more consistent.

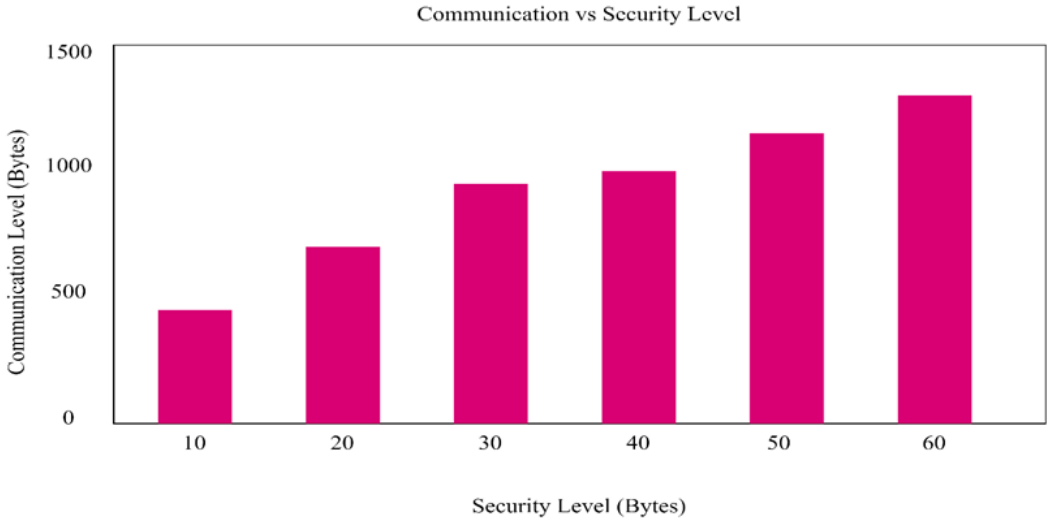

Figure 7 Performance of Proposed Protocol

4.2. Blockchain Performance

The proposed blockchain-enabled WBSN platform was put to the test in this subsection by having its block size, read throughput, transaction throughput, read latency, and transaction latency measured. Four peer nodes were used in experiments with one ordered node to test the performance of the blockchain network. The TPS transmit rate was varied to determine the throughput of the proposed blockchain-enabled WBSN network. For instance, throughput can be broken down into transactional and read throughput. The transaction throughput was decided upon as being the total number of blockchain transactions carried out during a given time frame. A read-through was utilized to tally the number of blockchain network readings that took place during the specified length of time. Several settings for TPS transmit and random machine utilization were used to calculate variations in transaction read throughput. Figure 9 shows the identical operation in reverse, whereas Figure 8 shows the Read throughout the entire Transaction process. The total number of blocks committed during concurrent transactions is rather large, as shown in Figure 10. Figure 11 displays the average throughput per parallel transaction for the proposed blockchain.

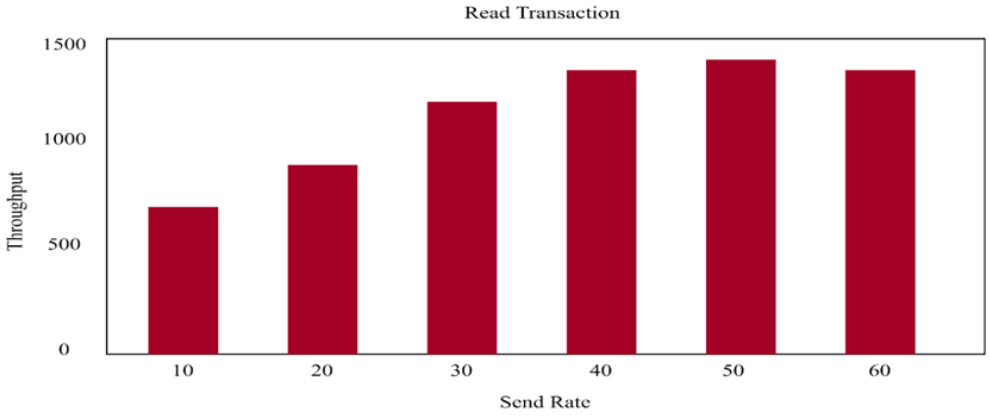

Figure 8 Read Transaction Throughout

RESEARCH ARTICLE

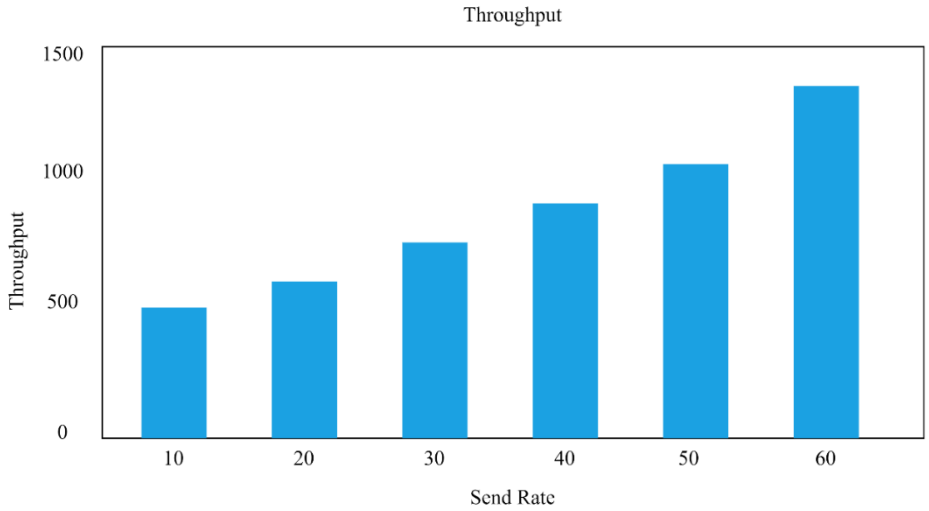

Figure 9 Transaction Throughout

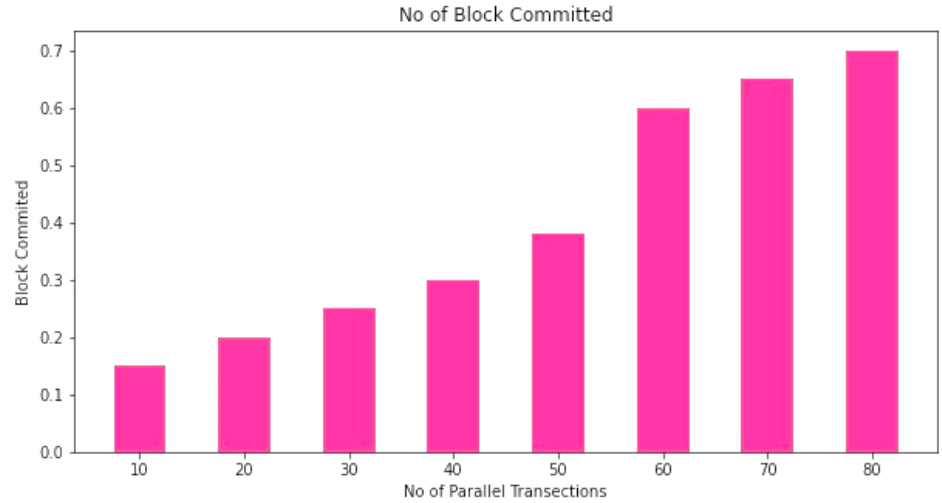

Figure 10 Number of Blocks Committed

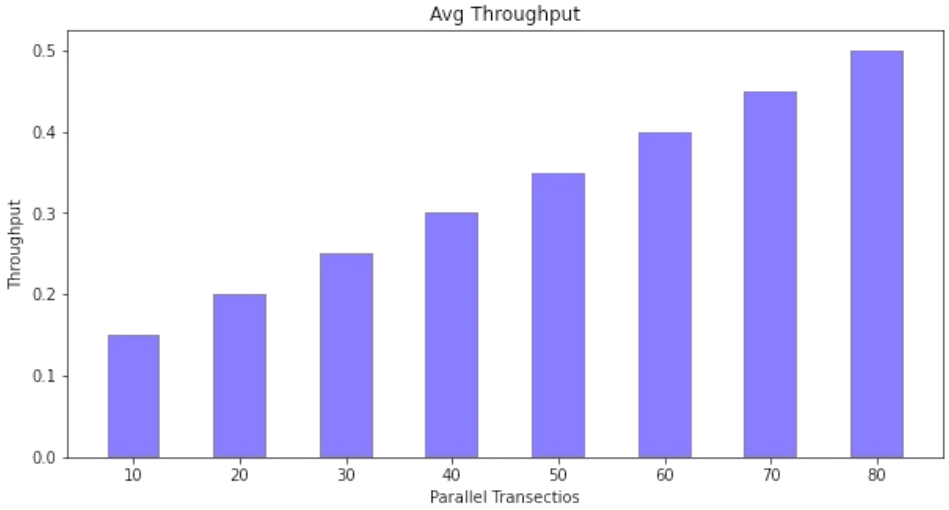

Figure 11 Average Throughput per Parallel Transaction

RESEARCH ARTICLE

4.3. Privacy Preserving

Based on the findings, it is suggested that a hybrid algorithm that combines the strengths of the three most popular cryptographic algorithms (Advanced Encryption Standard, Blowfish, and RSA) to protect users' personal information. Information transmitted over WBSNs is encrypted using many different algorithms. However, advanced new technologies are rendering these older methods useless. The time needed to crack a cryptographic system has been drastically cut down thanks to technological advancements, and a wide range of attacks has compromised the current defenses. The evaluation and results of the Privacy Preserving Strategy are depicted in Figure 12.

The following results were obtained from comparison tests between the Proposed Cryptosystem and two current systems: a Hybrid (AES-RSA) and a Standalone (Blowfish). Summary comparison test results are shown in Table 1.

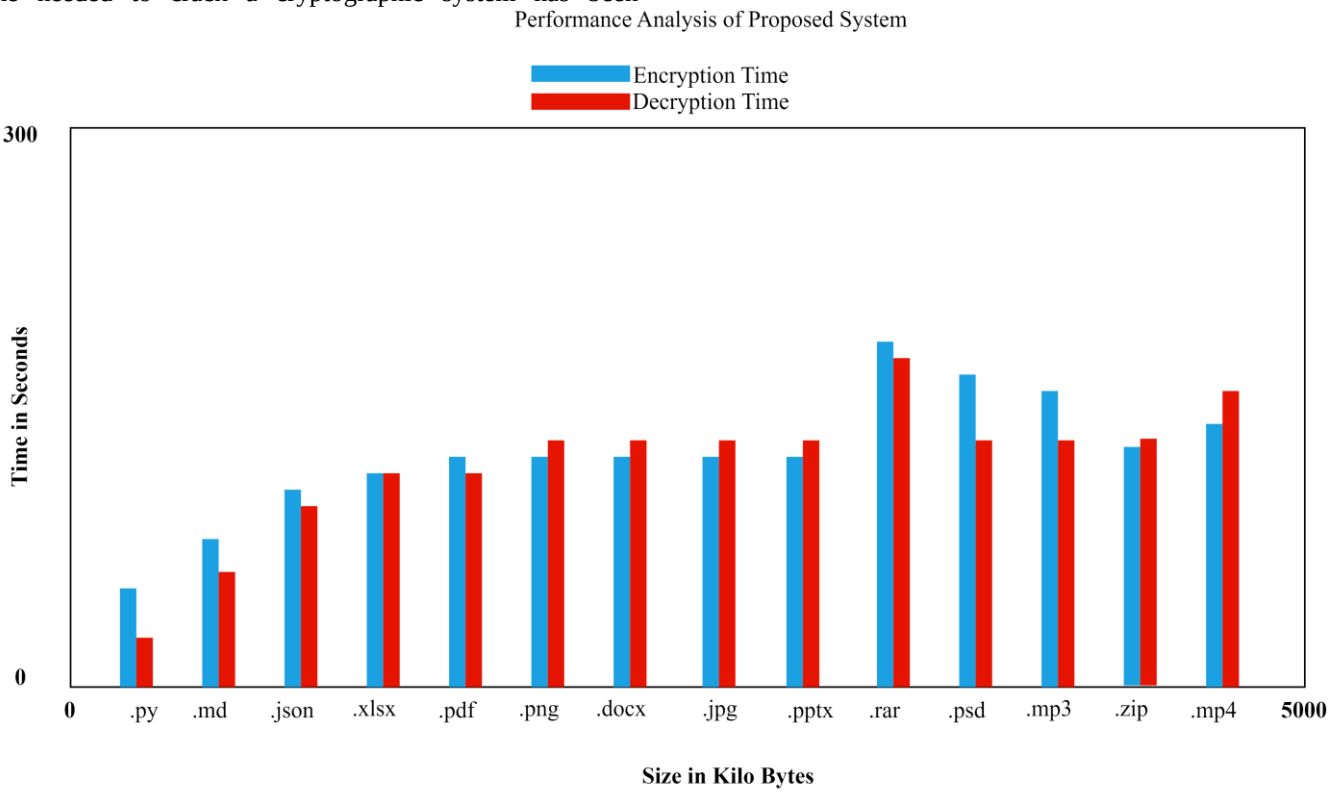

Figure 12 Performance Analysis of Privacy Preserving Strategy

Table 1 Performance Comparison – Summary

Systems	Average Encryption Time	Average Decryption Time	Average Encryption Rate	Average Decryption Rate
Crypto-system (Blowfish-RSA-AES)	140.53 sec	508.8 sec	50.206	15.6
Crypto-system (Blowfish)	122.6 sec	231.2 sec	53.74450004	34.0260998
Crypto-system (RSA-AES)	121.4 sec	367 sec	55.10561916	23.45880341

4.4. Security Prediction

To detect assaults on the WBSNs-based blockchain privacy-protecting system for healthcare, the author has gathered a sizable amount of transaction data and trained a machine learning model.

4.4.1. Logi-XGB

Combining the XGBoost Classifier with the logistic regression model led to higher precision. The mathematical model behind the Logi-XGB Classification system is as follows in Equation (13)-(16):

RESEARCH ARTICLE

$$y = \sum_{k=1}^{n} f(x) \dots (13)$$

$$\ln \frac{P}{1-P} = a + by \dots (14)$$

$$\frac{P}{1-P} = e^{a+by} \dots (15)$$

$$P = \frac{e^{a+by}}{1+e^{a+by}} \dots (16)$$

In this example, Y is the result of the XGBoost classification model, and P is the Logistic Regression probability function. This study provides empirical evidence for the efficacy of the boosting function of the XGB Classifier. When XGB collects information on y, a logistic regression model determines the likelihood of an assault. This diagram shows a sample Logi-XGB Classification Model hybrid.

The XGBoost Classifier was employed to combine these two models. XGB will use the information from y as input for the logistic regression probability function. Similar results were discovered in a subsequent Logistic Regression investigation, demonstrating that a hybrid classifier significantly increased accuracy to 99.7 percent. The results of a hybrid version of the Logi-XGB Classification Model are presented in Figure 13.

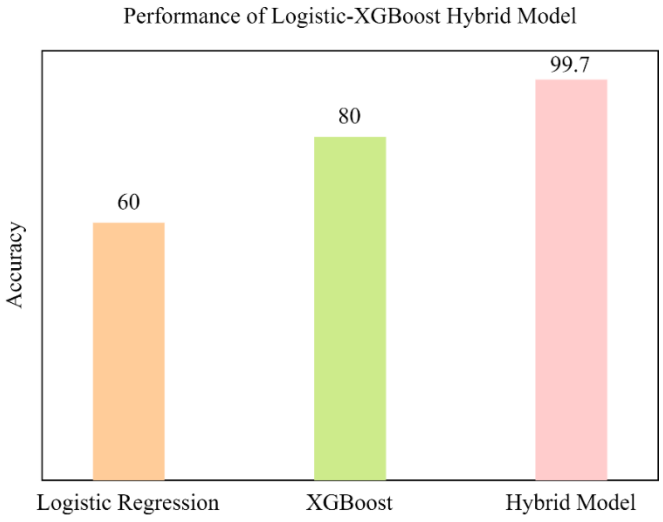

Figure 13 Logi-XGB Classification Model Performance

5. CONCLUSION

Increases in data storage and processing speed are only two examples of how recent technological advances have benefited the e-health industry. WBSNs are one such example (Wireless Body Sensor Networks). The WBSN is a well-known example of such a tool. Tele-homecare, also known as tele-diagnosis and tele-healthcare, refers to providing medical care to patients in their homes by remote means. The usage of wireless body sensor networks in medical settings has increased in recent years (WBSNs). WBSN technology provides a framework that allows wireless monitoring of patients' vitals without wired connections. Furthermore, these technologies provide medical personnel with real-time data transfer, allowing quicker treatment decisions. However, keeping patients' personal information private and secure is still needed. This paper describes how to use WBSNs to protect patients' and doctors' interactions from prying ears. To encrypt sensitive information in blockchains, a hybrid cryptographic system that combines the best features of existing solutions is proposed. The approach makes the most of both public key and symmetric key cryptography. AES, RSA, and Blowfish, formerly different algorithms, have been integrated into a single approach to achieving this goal. Experiments show that the suggested system can keep its secrets safe without sacrificing scalability. Using Logi-XGB as an attack prediction model, the proposed technique can prevent 99.7 percent of attacks. While this research does not yet account for the possibility of real-time attacks, it is aimed to address this shortcoming by developing a real-time system implementation that prioritizes privacy and security detection.

REFERENCES

[1] W. Xu, Wu, Daneshmand, Liu, "A data privacy protective mechanism for WBAN," *Wirel. Commun. Mob. Comput.*, no. February 2015, pp. 421–430, 2015, doi: 10.1002/wcm.

[2] V. Odelu, S. Saha, R. Prasath, L. Sadineni, M. Conti, and M. Jo, "Efficient privacy preserving device authentication in WBANs for industrial e-health applications," *Comput. Secur.*, vol. 83, pp. 300–312, 2019, doi: 10.1016/j.cose.2019.03.002.

[3] A. Bengag, O. Moussaoui, and M. Moussaoui, "A new IDS for detecting jamming attacks in WBAN," *2019 3rd Int. Conf. Intell. Comput. Data Sci. ICDS 2019*, pp. 1–5, 2019, doi: 10.1109/ICDS47004.2019.8942268.

[4] H. Wang, H. Fang, L. Xing, and M. Chen, "An integrated biometric-based security framework using wavelet-domain HMM in wireless body area networks (WBAN)," *IEEE Int. Conf. Commun.*, 2011, doi: 10.1109/icc.2011.5962757.

[5] Z. Ullah *et al.*, "Energy-efficient harvested-aware clustering and cooperative routing protocol for WBAN (E-HARP)," *IEEE Access*, vol. 7, pp. 100036–100050, 2019, doi: 10.1109/ACCESS.2019.2930652.

[6] F. A. Khan, A. Ali, H. Abbas, and N. A. H. Haldar, "A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks," *Procedia Comput. Sci.*, vol. 34, pp. 511–517, 2014, doi: 10.1016/j.procs.2014.07.058.

[7] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," *Egypt. Informatics J.*, vol. 18, no. 2, pp. 113–122, 2017, doi: 10.1016/j.eij.2016.11.001.

[8] P. S. Brar, B. Shah, J. Singh, F. Ali, and D. Kwak, "Using Modified Technology Acceptance Model to Evaluate the Adoption of a Proposed IoT-Based Indoor Disaster Management Software Tool by Rescue Workers," *Sensors*, vol. 22, no. 5, 2022, doi: 10.3390/s22051866.

[9] F. Li and J. Hong, "Efficient Certificateless Access Control for Wireless Body Area Networks," *IEEE Sens. J.*, vol. 16, no. 13, pp. 5389–5396, 2016, doi: 10.1109/JSEN.2016.2554625.

[10] M. S. Hajar, M. O. Al-Kadri, and H. K. Kalutarage, "A survey on wireless body area networks: architecture, security challenges and research opportunities," *Comput. Secur.*, vol. 104, 2021, doi:

RESEARCH ARTICLE

10.1016/j.cose.2021.102211.

[11] Z. Zhengl, X. Zheng, J. Tian, and M. Shu, "A Transmission Power Control Algorithm for Wireless Body Area Networks," *Proc. 2018 IEEE 22nd Int. Conf. Comput. Support. Coop. Work Des. CSCWD 2018*, vol. 3, pp. 98–103, 2018, doi: 10.1109/CSCWD.2018.8465245.

[12] S. Jegadeesan, M. Azees, N. Ramesh Babu, U. Subramaniam, and J. D. Almakhles, "EPAW: Efficient Privacy Preserving Anonymous Mutual Authentication Scheme for Wireless Body Area Networks (WBANs)," *IEEE Access*, vol. 8, pp. 48576–48586, 2020, doi: 10.1109/ACCESS.2020.2977968.

[13] M. Babar, M. S. Khan, U. Habib, B. Shah, F. Ali, and D. Song, "Scalable Edge Computing for IoT and Multimedia Applications Using Machine Learning," *Human-centric Comput. Inf. Sci.*, vol. 11, 2021, doi: 10.22967/HCIS.2021.11.041.

[14] D. Thakur, Y. Kumar, A. Kumar, and P. K. Singh, *Applicability of Wireless Sensor Networks in Precision Agriculture: A Review*, no. 0123456789. Springer US, 2019. doi: 10.1007/s11277-019-06285-2.

[15] Bangotra, Deep Kumar, et al. "An intelligent opportunistic routing algorithm for wireless sensor networks and its application towards e-healthcare." Sensors 20.14 (2020): 3887.

[16] I. Kaushik and N. Sharma, *Black Hole Attack and Its Security Measure in Wireless Sensors Networks*, vol. 1132. 2020. doi: 10.1007/978-3-030-40305-8_20.

[17] P. Gangwani, A. Perez-Pons, T. Bhardwaj, H. Upadhyay, S. Joshi, and L. Lagos, "Securing environmental IoT data using masked authentication messaging protocol in a DAG-based blockchain: IOTA tangle," *Futur. Internet*, vol. 13, no. 12, 2021, doi: 10.3390/fi13120312.

[18] P. Vijayakumar, M. S. Obaidat, M. Azees, S. H. Islam, and N. Kumar, "Efficient and Secure Anonymous Authentication with Location Privacy for IoT-Based WBANs," *IEEE Trans. Ind. Informatics*, vol. 16, no. 4, pp. 2603–2611, 2020, doi: 10.1109/TII.2019.2925071.

[19] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, "IoMT Malware Detection Approaches: Analysis and Research Challenges," *IEEE Access*, vol. 7, pp. 182459–182476, 2019, doi: 10.1109/ACCESS.2019.2960412.

[20] A. M. Joshi, P. Jain, S. P. Mohanty, and N. Agrawal, "IGLU 2.0: A New Wearable for Accurate Non-Invasive Continuous Serum Glucose Measurement in IoMT Framework," *IEEE Trans. Consum. Electron.*, vol. 66, no. 4, pp. 327–335, 2020, doi: 10.1109/TCE.2020.3011966.

[21] S. Manimurugan *et al.*, "Two-Stage Classification Model for the Prediction of Heart Disease Using IoMT and Artificial Intelligence," *Sensors*, vol. 22, no. 2, 2022, doi: 10.3390/s22020476.

[22] Shilan S. Hameed *et al.,* "A Hybrid Lightweight System for Early Attack Detection in the IoMT Fog," *Sensors* 2021, *21*(24), 8289; https://doi.org/10.3390/s21248289

[23] S. Razdan and S. Sharma, "Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies," *IETE Tech. Rev. (Institution Electron. Telecommun. Eng. India)*, 2021, doi: 10.1080/02564602.2021.1927863.

[24] J. Zhou, Z. Cao, X. Dong, N. Xiong, and A. V. Vasilakos, "4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks," *Inf. Sci. (Ny).*, vol. 314, no. September, pp. 255–276, 2015, doi: 10.1016/j.ins.2014.09.003.

[25] A. H. Abdullah, R. A. Butt, M. W. Ashraf, K. N. Qureshi, and F. Ullah, "Securing Data Communication in Wireless Body Area Networks Using Digital Signatures," *Tech. J.*, vol. 23, no. 02, pp. 50–55, 2018.

[26] M. Shuai, B. Liu, N. Yu, L. Xiong, and C. Wang, "Efficient and privacy-preserving authentication scheme for wireless body area networks," *J. Inf. Secur. Appl.*, vol. 52, p. 102499, 2020, doi: 10.1016/j.jisa.2020.102499.

[27] K. S. Raja and U. Kiruthika, "An Energy Efficient Method for Secure and Reliable Data Transmission in Wireless Body Area Networks Using RelAODV," *Wirel. Pers. Commun.*, vol. 83, no. 4, pp. 2975–2997, 2015, doi: 10.1007/s11277-015-2577-x.

[28] A. H. Sodhro, Y. Li, and M. A. Shah, "Energy-efficient adaptive transmission power control for wireless body area networks," *IET Commun.*, vol. 10, no. 1, pp. 81–90, 2016, doi: 10.1049/iet-com.2015.0368.

[29] Y. Vineetha, Y. Misra, and K. Krishna Kishore, "A real time IoT based patient health monitoring system using machine learning algorithms," *Eur. J. Mol. Clin. Med.*, vol. 7, no. 4, pp. 2912–2925, 2020.

[30] R. Kadel, N. Islam, K. Ahmed, and S. J. Halder, "Opportunities and Challenges for Error Correction Scheme for Wireless Body Area Network—A Survey," *J. Sens. Actuator Networks*, vol. 8, no. 1, p. 1, 2018, doi: 10.3390/jsan8010001.

[31] G. Marquez, H. Astudillo, and C. Taramasco, "Exploring security issues in telehealth systems," *Proc. - 2019 IEEE/ACM 1st Int. Work. Softw. Eng. Heal. SEH 2019*, no. March, pp. 65–72, 2019, doi: 10.1109/SEH.2019.00019.

[32] R. Latha and P. Vetrivelan, "Decision making patient assistive strategies in wireless body area networks for remote healthcare system," *Int. J. Recent Technol. Eng.*, vol. 8, no. 1, pp. 2199–2203, 2019.

[33] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wirel. Networks*, vol. 17, no. 1, pp. 1–18, 2011, doi: 10.1007/s11276-010-0252-4.

[34] H. Ur Rahman, G. Wang, M. Z. A. Bhuiyan, and J. Chen, "In-network generalized trustworthy data collection for event detection in cyber-physical systems," *PeerJ Comput. Sci.*, vol. 7, no. May, pp. 1–25, 2021, doi: 10.7717/PEERJ-CS.504.

[35] M. Anand Kumar and C. Vidya Raj, "On designing lightweight QoS routing protocol for delay-sensitive wireless body area networks," *2017 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2017*, vol. 2017-Janua, pp. 740–744, 2017, doi: 10.1109/ICACCI.2017.8125930.

[36] M. Ghamari, B. Janko, R. S. Sherratt, W. Harwin, R. Piechockic, and C. Soltanpur, "A survey on wireless body area networks for ehealthcare systems in residential environments," *Sensors (Switzerland)*, vol. 16, no. 6, pp. 1–33, 2016, doi: 10.3390/s16060831.

[37] R. Negra, I. Jemili, and A. Belghith, "Wireless Body Area Networks: Applications and Technologies," *Procedia Comput. Sci.*, vol. 83, pp. 1274–1281, 2016, doi: 10.1016/j.procs.2016.04.266.

[38] M. Shuai, B. Liu, N. Yu, L. Xiong, and C. Wang, "Efficient and privacy-preserving authentication scheme for wireless body area networks," *J. Inf. Secur. Appl.*, vol. 52, p. 102499, 2020, doi: 10.1016/j.jisa.2020.102499.

[39] A. Muthulakshmi and K. Shyamala, "Efficient Patient Care Through Wireless Body Area Networks—Enhanced Technique for Handling Emergency Situations with Better Quality of Service," *Wirel. Pers. Commun.*, vol. 95, no. 4, pp. 3755–3769, 2017, doi: 10.1007/s11277-017-4024-7.

[40] M. S. Arshad Malik, M. Ahmed, T. Abdullah, N. Kousar, M. N. Shumaila, and M. Awais, "Wireless body area network security and privacy issue in E-healthcare," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 4, pp. 209–215, 2018, doi: 10.14569/IJACSA.2018.090433.

[41] 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," *Wirel. Networks*, vol. 27, no. 3, pp. 2119–2130, 2021, doi: 10.1007/s11276-021-02560-y.

[42] F. Akhtar and M. H. Rehmani, "Energy Harvesting for Self-Sustainable Wireless Body Area Networks," *IT Prof.*, vol. 19, no. 2, pp. 32–40, 2017, doi: 10.1109/MITP.2017.34.

[43] J. Zhu, G. Zhang, Z. Zhu, and K. Yang, "Joint Time Switching and Transmission Scheduling for Wireless-Powered Body Area Networks," *Mob. Inf. Syst.*, vol. 2019, 2019, doi: 10.1155/2019/9620153.

[44] N. Mekki, M. Hamdi, T. Aguili, and T. H. Kim, "A Privacy-Preserving Scheme Using Chaos Theory for Wireless Body Area Network," *2018 14th Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2018*, pp. 774–779, 2018, doi: 10.1109/IWCMC.2018.8450293.

[45] B. Narwal and A. K. Mohapatra, "SAMAKA: Secure and Anonymous Mutual Authentication and Key Agreement Scheme for Wireless Body Area Networks," *Arab. J. Sci. Eng.*, vol. 46, no. 9, pp. 9197–9219, 2021, doi: 10.1007/s13369-021-05707-3.

[46] F. ; Khan *et al.*, "Development of a Model for Spoofing Attacks in

RESEARCH ARTICLE

Internet of Things," *Math. 2022, Vol. 10, Page 3686*, vol. 10, no. 19, p. 3686, Oct. 2022, doi: 10.3390/MATH10193686.

[47] A. A. Al-Atawi, F. Khan, and C. G. Kim, "Application and Challenges of IoT Healthcare System in COVID-19," *Sensors 2022, Vol. 22, Page 7304*, vol. 22, no. 19, p. 7304, Sep. 2022, doi: 10.3390/S22197304.

[48] M. H. da Fonseca, F. Kovaleski, C. T. Picinin, B. Pedroso, and P. Rubbo, "E-Health Practices and Technologies: A Systematic Review from 2014 to 2019," *Healthc. (Basel, Switzerland)*, vol. 9, no. 9, Sep. 2021, doi: 10.3390/HEALTHCARE9091192.

[49] X. Wu, J. Xu, W. Liang, and W. Jian, "Research on Authentication and Key Agreement Protocol of Smart Medical Systems Based on Blockchain Technology," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 13156 LNCS, pp. 439–452, 2022, doi: 10.1007/978-3-030-95388-1_29.

[50] L. Ma, Y. Ge, and Y. Zhu, "TinyZKP: A lightweight authentication scheme based on zero-knowledge proof for wireless body area networks," *Wirel. Pers. Commun.*, vol. 77, no. 2, pp. 1077–1090, 2014, doi: 10.1007/s11277-013-1555-4.

[51] S. Saleem, S. Ullah, and K. S. Kwak, "A study of IEEE 802.15.4 security framework for wireless body area networks," *Sensors*, vol. 11, no. 2, pp. 1383–1395, 2011, doi: 10.3390/s110201383.

[52] S. J. Hussain, M. Irfan, N. Z. Jhanjhi, K. Hussain, and M. Humayun, "Performance Enhancement in Wireless Body Area Networks with Secure Communication," *Wirel. Pers. Commun.*, vol. 116, no. 1, pp. 1–22, 2021, doi: 10.1007/s11277-020-07702-7.

[53] P. T. Sharavanan, D. Sridharan, and R. Kumar, "A Privacy Preservation Secure Cross Layer Protocol Design for IoT Based Wireless Body Area Networks Using ECDSA Framework," *J. Med. Syst.*, vol. 42, no. 10, 2018, doi: 10.1007/s10916-018-1050-2.

Author

Mohammed Naif Alatawi is currently working as an Assistant Professor in University of Tabuk, Saudi Arabia. He has completed his Ph.D. in Computer Information Systems from Nova Southeastern University USA in 2019 and Masters from Florida Institute of Technology USA in 2015. His research interests includes Computer Security, Software Engineering, Databases, and IoT.

How to cite this article:

Mohammed Naif Alatawi, "A Hybrid Cryptography and LogiXGBoost Model for Intelligent and Privacy Protection in Wireless Body Sensor Networks (WBSNS)", International Journal of Computer Networks and Applications (IJCNA), 10(2), PP: 166-179, 2023, DOI: 10.22247/ijcna/2023/220734.