EAI Endorsed Transactions
on Creative Technologies
Research Article EAI.EU

An Intelligent and Secured Privacy Preserving Framework For Wireless Body Area Networks (WBANs)

Muhammad Shoaib Akhtar, Tao Feng*

School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China

13.cs.194@gmail.com fengt@lut.cn

Abstract

In recent years, developments in information technology and emerging technologies have greatly benefited e-health. The adoption of Wireless Body Area Networks is a perfect example (WBAN). The WBAN is a popular device. Medical care can be delivered remotely to patients in their own homes via tele-homecare (also known as tele-diagnosis). Diabetes, dementia, falls, congestive heart failure, asthma, and infertility are among the conditions for which they are prescribed. An emergency response time could be sped up by using WBANs to monitor patients' health in real time. From a more traditional strategy to a more updated patient-centered one has been seen in recent years. Telemedicine and telemonitoring are two examples of current patient-centered practises that use technology to make it easier for patients to provide personal information. Telemonitoring has been discovered as a feasible research subject using the most up-to-date methods of turning raw data into meaningful information. WBAN stability is dependent on preventing node overheating and conserving energy. LB-EESAA routing mechanism for WBANs and the early warning system for attacks during Blockchain transactions are discussed in this study. Results show that LB-EESAA performs best in terms of both the number of live and dead nodes and the length of protocol stability. We were able to raise the level of security of the organisation after increasing the efficiency of WBANs. We examined the read throughput and basic transaction throughput of a blockchain-enabled system. After assuring and safeguarding the privacy of the system, we used the Logi-XGB prediction model machine learning to forecast assaults. Using the Logi-XGB model, 95.7 percent of the assault could be predicted in its early stages.

Keywords: WBANs, Blockchain, eHealth.

Received on 02 January 2022, accepted on 14 March 2022, published on 15 March 2022

doi: 10.4108/eai.15-3-2022.173609

* Corresponding author. Email: fengt@lut.cn

1. Introduction

E-health has benefited greatly from recent developments in new technologies and the information technology field. Wireless Body Area Networks (WBAN) adoption is a specific example of this. The WBAN is widely used in a variety of scenarios. A primary usage for these devices is in the field of tele-homecare (also known as tele-diagnosis), which is the practice of providing remote medical care to patients at home. Other medical situations where they are used include the treatment of diabetes and dementia, falls, congestive heart failure, asthma, and infertility. With WBAN, patients' health may be better tracked in real time, allowing for faster response in the event of an emergency.

In the context of mobile healthcare, wireless body area networks (WBANs) might be viewed as a key enabler. Sending sensor readings to a hospital or medical center's computers allows medical personnel to assess the data. As monitoring may be done in real-time and over a longer length of time even at home, these devices cut the large expenditures associated with ambulant patients in hospitals. A WBAN's sensors and Internet servers must be encrypted to preserve the patient's privacy when transmitting health-related data to and from each other. This data must also be

collected by medical professionals who are certain that it has not been tampered with and indeed belongs to the patient.

By integrating health-related things like sensors and remotely observed medical devices for the patient record, the internet of health things (IoHT) provides exceptional help in the field of healthcare, resulting in smarter and more efficient devices. In this study, we proposed an IoT with a cloud-based clinical decision support system for prediction and monitoring of illness severity levels using 5G services and block-chain technologies. [1]–[6]. Because of its transparency, a block-chain is a secure mechanism for storing and distributing information. In healthcare, block-chain has numerous uses. It has a number of useful functions, including secure patient medical data transmission, drug supply chain management, and genetic code unlocking assistance for healthcare researchers. Security, authentication, immutability, distributed ledger, and decentralized storage are just a few of the built-in properties of block chain. It has now moved from hype to reality by giving practical applications in industries such as healthcare. [7]–[9]. The security aspects of block chain, such as keeping a decentralized, incorruptible, and transparent log of all patient data, make it a particularly effective alternative for dealing with system security challenges. Furthermore, block chain maintains an individual's privacy using complicated and secure codes that give excellent protection for the sensitivity of medical data. Patients, healthcare providers, and doctors can communicate the same information remotely, swiftly, and securely thanks to the technology's decentralized structure. Blockchain technology has the potential to greatly improve the integration of currently dispersed healthcare data with a variety of service providers. A Blockchain-based solution can be useful for the integration of many intermediary channels in the medical care system because it is a distributed network. Interoperability between service providers and institutions is provided via Block Chain. Block-chain can be highly useful in achieving data integrity, decentralization, and precision medicine, as well as enhancing patient care and results and connecting medical records throughout the world. 5G is a fifth-generation technology that allows for extremely fast data transmission over cellular phones or other networks. For doctors, real-time patient information is vital so that they can make fast judgments in a variety of critical scenarios. Telemedicine, for example, necessitates an advanced network capable of enabling real-time connection with patients as well as high-quality video transmission without slowing down the network. Powerful capabilities such as real-time data transfer of photographs, documents, and real-time films for video-based medical consultations can be enabled with the integration of a 5G network into current infrastructure to improve health services. The data transfer rate is high and response time is reduced when 5G technology is used, resulting in an efficient healthcare system. [10], [11].

Fifth-generation (5G) aims at utilizing many promising communication technologies such as software-defined network and cloud computing technologies. Therefore, main challenge which should be addressed is the provision of security measures which makes all the speedy operations transparent and secure for system reliability. Protocols are required as the basis for 5G networks to address these security challenges [12].

5G is a fifth-generation technology that allows for extremely fast data transmission over cellular phones or other networks. For doctors, real-time patient information is vital so that they can make fast judgments in a variety of critical scenarios. Telemedicine, for example, necessitates an advanced network capable of enabling real-time connection with patients as well as high-quality video transmission without slowing down the network. Powerful capabilities such as real-time data transfer of photographs, documents, and real-time films for video-based medical consultations can be enabled with the integration of a 5G network into current infrastructure to improve health services. The data transfer rate is high and response time is reduced when 5G technology is used, resulting in an efficient healthcare system.

Website developers and application developers are used to monitor patient health problems in remote places, and are presented for people with a sensing model for the elderly and those with disabilities. The main focus of this model is to provide the quickest response in the event of a patient's abnormal condition. Figure 3 depicts the general design of the suggested system. In the first step, the patient's data is collected using sensors and medical devices, as well as patient history and the UCI repository. The patient's information is saved in a database. The block-chain technology is used to data saved in a database, after which the data is kept in blocks and remains secure, allowing for maximum privacy and transparency. This safe data is then kept in cloud storage, and data in cloud storage is also stored in protected storage for the future, assisting in the patient's therapy by checking their past data. Using 5G services, the data in cloud storage is also forwarded to healthcare providers. Healthcare providers are end-users who make treatment recommendations for patients. Furthermore, the main purpose of the system is to provide the best time response to the patient for treatment with privacy and secrecy of data. Figure below shows the typical scenario of WBANs.

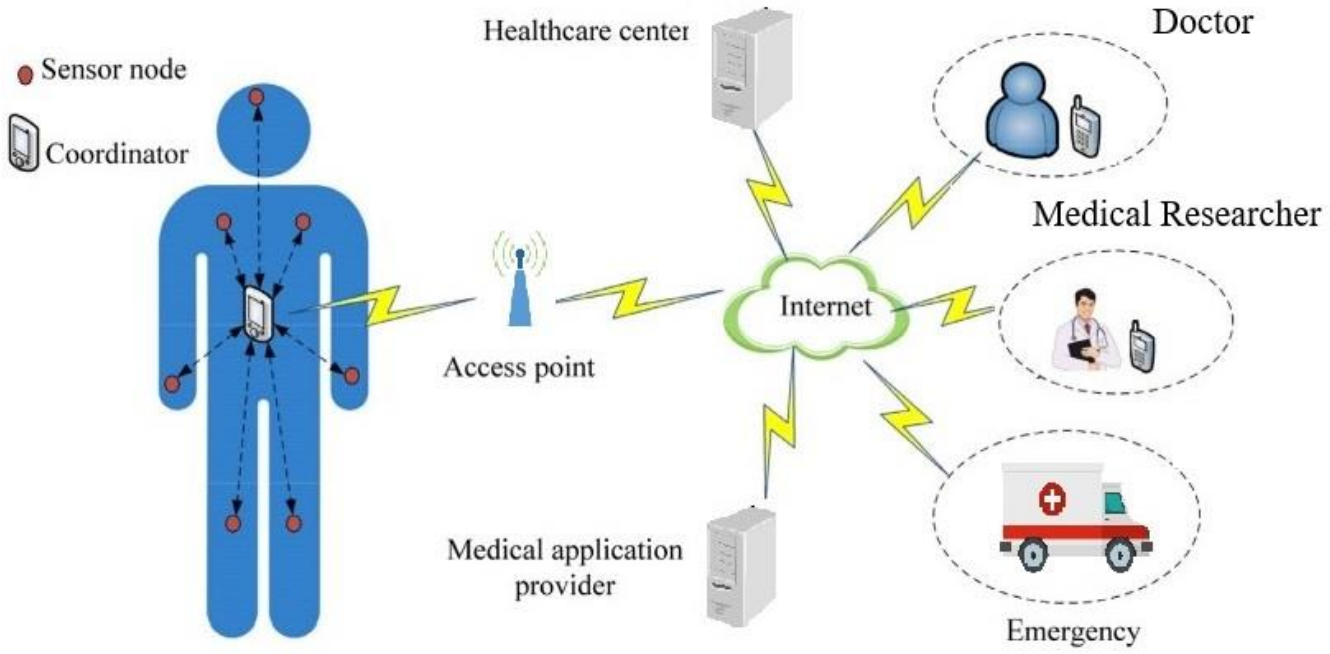

Figure 1. the typical scenario of WBANs [13]

In recent years, a number of WBAN authentication systems have evolved. Mutual authentication between the WBAN client and the application provider is possible with these technologies, while data privacy and integrity are protected. After careful consideration, some solutions employ time-consuming processes such as bilinear pairings and map to point hash operations. Experiments reveal that multiplication of elliptic curve points takes several times as long as pairing. As a result, these approaches are unsuited for WBANs. An ECC-based system provides the advantages of low arithmetic needs, small key size, and short operands. Most of these methods, including ECC-based authentication, have flaws that attackers can exploit, including tracking and impersonation attacks. Multi-server authentication without an online third party, on the other hand, is more practicable. WBANs clients can only receive medical services provided by application providers once enrolled. These application providers also do not need to store any user data for authentication. This research presents an efficient and secure authentication technique for WBANs using Blockchain technology in a multi-server architecture. The following are the two contributions we'd want to make:

a) We can protect WBAN users' data from manipulation with the use of blockchain.

b) Validating agents are recommended to use a sequential aggregate signature approach with a designated verification. Only administrators have access to users' private information, which can be compressed to match the capacity of the blockchain storage space, limiting unauthorized access.

c) Development of an AI-based machine learning system for assault detection.

Figure bellows shows the proposed workflow of research:

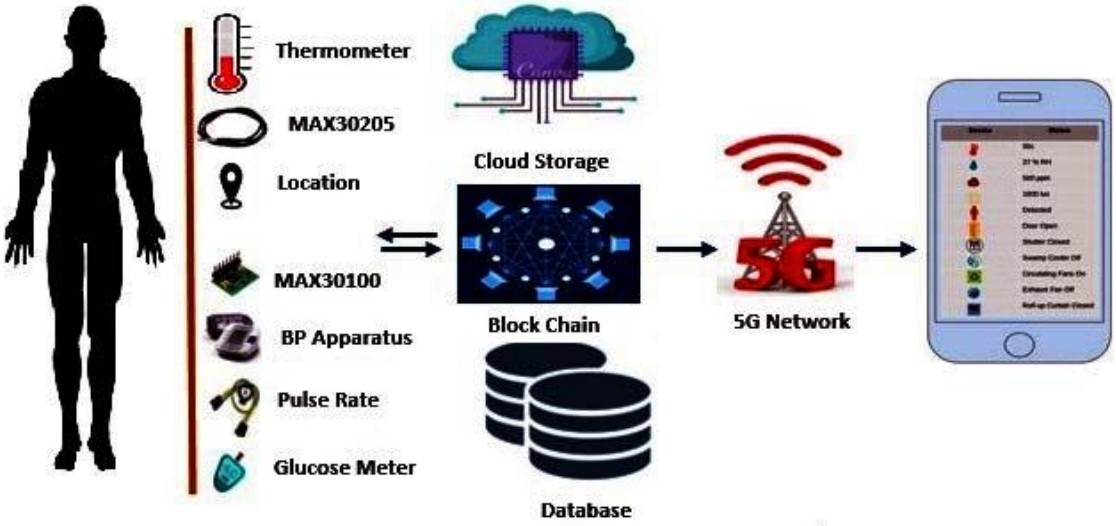

Figure 2. Proposed Workflow

2. Related Work

Al-Janabi et al [14] examine the most recent standards and publications on WBAN communication architecture, as well as the security and privacy needs and security concerns that have arisen. Security measures and studies conducted by the WBAN are also covered in this document. Author concludes by considering future research and development avenues that could be pursued.

Wireless body area networks (WBANs) are employed to provide a safe cloud-based mobile healthcare system for the elderly (WBANs). Starting with the inter-sensor communication security, the multi-biometric based key generation approach in WBANs is being used to protect patient privacy by securely storing electronic medical records (EMRs) on a hospital cloud. Because of its very efficient key generation method, [15] proposed a multi-biometric-based mechanism provides significant security protections.

Throughout this study, [16] explore the most significant obstacles and concerns in the field of WBAN data security and confidentiality. D-Sign, a data hybrid technique, is used for digital signature-based encryption and decryption, and is available from us. The present state-of-the-art security and privacy safeguards for WBANs are also compared to our proposed approach in this section.

An anonymous authentication approach, such as the one provided here by [17], can aid in the establishment of confidence by not disclosing the name of the patient or the identity of the doctor. AES and DES are just two examples of cryptographic encryption techniques that can help safeguard data. However, the size of the key and the sharing of the key are the two most significant challenges to establishing a high level of data security using these systems. Because of the use of a new, more efficient affine cypher, the key size required to offer the same level of confidentiality as earlier encryption methods can be decreased significantly. The ability of the proposed work to survive a wide range of destructive security attacks is demonstrated in the security analysis portion of the proposal. The storage, communication, and compute costs associated with the suggested approach may be observed in great detail in the performance analysis portion of this document as well. This results in a reduction of around 29% in the computational complexity of the suggested approach, according to the authors.

Significant technological developments have had a significant impact on the proliferation of wearable sensors in recent years, particularly in the field of biometrics. Data is exposed to numerous intermediate nodes when it is aggregated, making it more vulnerable to security and privacy risks, as a result. The scientific community has paid a significant lot of attention to the topic of security-assisted data aggregation in recent years. As part of this chapter, [18] explore an architectural framework referred as the Adaptable SDA, which is meant to give critical security characteristics to end network nodes that are linked together in a specific data aggregation architecture.

Li et al [19] provide an efficient certificate less signcryption technique, and then author develop an access control mechanism for wireless body area networks (WBANs) that makes use of the signcryption strategy author have developed. In addition to its confidentiality, integrity, authentication, non-repudiation, public verifiability, and validity of the cipher text, our technique has several other advantages. For example, if the computational cost and energy consumption of the controller for our system are compared to those of the other three known signcryption-based access control methods, our scheme is the most efficient. Because it is based on certificate less cryptography, our system does not require either key escrow or public key certificates in order to function properly, which is a significant advantage.

Wireless healthcare networks provide novel applications to improve the quality of patients' lives, provide caregivers with helpful monitoring tools, and allow for rapid intervention in the era of communication technology. Insecure data compromises patient privacy and may lead to

incorrect medical diagnosis and/or treatment because of the sensitive information contained in Wireless Body Area Networks (WBANs). Due to WBAN's resource constraints and important applications, achieving a high level of security and privacy is a difficulty. WBAN technology is examined in detail by [20], with an emphasis on security and privacy challenges and possible solutions. Finally, future research paths and outstanding topics are discussed.

Wang et al [21] proposes an integrated biometric-based security framework for wireless body area networks that leverages biometric features shared by body sensors deployed at various body locations. The suggested authentication and selective encryption techniques need modest processing power and resources (e.g., battery and bandwidth). Specifically, a wavelet-domain Hidden Markov Model (HMM) classification algorithm is used for accurate authentication of ECG signals. The system also uses biometric data like ECG signals as a biometric key for encryption. Our results show that the proposed approach can accomplish accurate authentication without additional key distribution or time synchronization requirements.

In order to address the issue of data privacy in WBANs, [22] suggests an innovative method of dealing with the problem. author improved the Kalman filter in order to reduce noise and acquire correct data; and, in order to provide a new secure privacy-preserving model based on homomorphic characteristics and chaotic cryptosystems, our main contribution is twofold: first, author developed a new secure privacy-preserving model that uses homomorphic characteristics and chaotic cryptosystems; and, second, author developed a new secure privacy-preserving model that uses homomorphic characteristics and chaotic cryptosystems .This new paradigm in healthcare monitoring safeguards real-time analytics while simultaneously protecting patient privacy and the integrity of their personal health information.

Author begin by examining the current authentication techniques' security flaws. When session ephemeral secrets are revealed to an adversary, most systems fail to provide privacy for user credentials. For wireless body area networks, [23] offer a privacy-preserving device authentication strategy to solve the shortcomings of the current schemes. Even if adversaries have access to transient secrets, the suggested system still guarantees strong security. Another benefit of using the suggested method is that it reduces the need for the client device to manage a large number of public-keys for application providers. author ran simulations with the Java Pairing-Based Cryptography Library (JPBC) to show that our proposed technique reduces computational overhead for both the client device and the application provider.

The most significant issue in cloud-assisted Wireless Body Area Networks is data secrecy, which is why author recommend that you use the Multi-valued and Ambiguous Scheme to protect your data. Using existing encryption algorithms in conjunction with the new system, it is possible to install applications. Following the findings of [24], it appears that it is possible to establish secure data exchanges between the cloud and Wireless Body Area Networks.

When patients move between blocks outside, cloud-assisted WBANs are more vulnerable to sophisticated threats like node compromise. [25] Proposes a safe and privacy-preserving key management system that is impervious to mobile assaults based on time and location. Using blindness and Blom's symmetric key approach with modified proactive secret sharing; it protects patients' identities, sensor deployments, and sensor locations. Delegating the computationally demanding but privacy-preserving key material update to the cloud server saves significant computing power for energy-constrained WBANs. Moreover, our system outperforms earlier schemes in terms of mobile assault resistance, storage, compute, and communication overhead.

The usage of elliptic curve cryptography has been employed in the development of a fast and secure authentication mechanism for WBANs (ECC). The use of identity-based encryption rather than certificate less authentication in multi-server systems makes this solution appropriate for online third-party involvement because it is designed to work with multiple servers according to [26]. The suggested privacy-preserving authentication technique has been shown to provide the necessary security properties while also reducing computation costs when compared to five comparable authentication systems, as evidenced by the security analysis and comparison.

[27] combines compressed sensing and wireless physical layer security to provide a lightweight encryption architecture.

As a result of using the measurement matrix as an encryption key, compressed sensing can be augmented to include security at the moment of sampling an analogue signal. The suggested approach saves sensor-node resources by eliminating the necessity for a separate encryption algorithm and the pre-deployment of a key. For testing, a wireless ECG setup with a sensor-node, access point, and an eavesdropper executing a proximity attack is used along with analysis, simulation, and experimentation. If the eavesdropper is placed at a suitable distance from the sensor-node and the access point, the results show that lawful communication is secure and reliable.

Wang et al[28] analyses how this conduit can be employed in the security mechanism to safeguard inter-BASN communications with the goal of protecting inter-BASN communications. This biometrics strategy takes use of an intrinsic trait of a person's body to validate their identity or to secure the distribution of a cypher key in order to protect sensitive information. 99 patients had their ECG and photoplethysmogram recorded at the same time, resulting in 838 simultaneous recordings. When signals were sampled at 1000 Hz and encoded into 128-bit binary sequences, an IPI-based biometric feature was shown to have a minimal half-total error rate of 2.58 percent when the interpulse interval was less than 1 millisecond (IPI). The result poses a number of crucial concerns for future research, such as how to correct for the asynchrony of numerous channels and coding schemes, which are discussed below.

For WBANs, [29] developed a mutual authentication system that is both secure and anonymous, which author have discussed previously (SAMAKA). The conclusion is that SAMAKA provides protection against a broad spectrum of security dangers posed by an attacker. SAMAKA's formal security is demonstrated through the use of BAN Logic and AVISPA. In addition, it has been shown to be safe in the RoR simulation model. Furthermore, a detailed informal security examination demonstrates that SAMAKA is capable of withstanding well-known security risks. Finally, a performance comparison reveals that SAMAKA outperforms the competition and produces promising results while also providing more extensive security and privacy protections than the competition.

Recent years have seen a significant rise in the development of wireless sensor networks (WSN) that have evolved to body area networks (BAN). In the event of a medical emergency, BANs enable for remote patient monitoring. The low-power sensor nodes can be implanted into the human body or worn outside as a monitor. Electronic health record (EHCR) systems have been used to store a colossal amount of patient health data generated during treatment. EHCRs could be shared with a wide range of people in order to improve healthcare services. The usage of this procedure in daily life raises serious concerns about privacy and security. There is a lot of work being done to come up with standards and solutions to the difficulties listed above, but so far the results are disappointing. Security and privacy in EHCR systems are systematically reviewed by [30].

Before addressing security and privacy requirements and attacks at various network tiers in a WBAN, author will present a quick overview of WBANs and how they might be utilized in healthcare monitoring and surveillance applications. Finally, [31] explore several cryptographic algorithms and laws that can be used to provide a solution to the problems of security and privacy in wireless body area networks.

The Elliptic Curve Digital Signature Algorithm (ECDSA) has been described by [32] as a possible use for cross layer protocol design architecture. Unlike WBAN (IEEE 802.15.6), WMAN (IEEE 802.16) and 3G, WLAN (IEEE 802.11) or wired networks, it replaces the protocol architecture of WBAN. The ECDA-based proxy signature algorithm is used by the lightweight secure system to provide secure data transport and access control features. The simulation models generated with NS-2 are used to implement the system's efficiency, and the results reveal an optimal solution in terms of latency, PDR, throughput, jitter, packet transmission time, dropping ratio, and packet delivery. The simulation models used to achieve this efficiency. The response demonstrates the practicality of the proposed methodology.

The concept of Wireless Body Area Networks is explored by [33]. For the time being, author will focus on a few patient-monitoring applications. After that, author will talk about how a WBAN communicates and where it fits in the IT landscape. The physical layer, existing MACs, and contemporary network protocols are described in detail. Cross-layer and service quality are also discussed. Due to WBANs' location on the human body, security must be taken in to account. Present and historical projects are discussed. These concerns and obstacles are then outlined.

An authentication mechanism based on zero-knowledge proofs, TinyZKP, is presented and implemented on TinyOS-based sensor nodes by [34]. TinyZKP performs 1.9 and 1.4 times quicker, respectively, and consumes 48 percent less energy than TinyECC and WM-ECC, two ECDSA-based authentication methods, according to our experiments. TinyECC and WM-ECC also perform 1.9 and 1.4 times faster, respectively.

Ma et al [35] describe a technique for securely transferring patient data to medical authorities while utilizing the least amount of electricity possible. To improve the system's reliability, the RelAODV protocol, a modified adhoc on-demand distance vector (AODV) protocol, is being proposed (Reliable AODV). The proposed methodology has been shown to be energy efficient and to improve the overall quality of the overall system.

Raja et al [36] compare the computational costs of two recent WBAN anonymous authentication systems. Authentication is anonymous and data is protected by encryption with these two methods. A new lightweight authentication strategy for wearable devices has recently been proposed that enables anonymity and privacy combined with security at a very low computational cost. Author then examine this new authentication scheme. Authentication and anonymity are achieved by the use of hash functions in this method, which does not use encryption. However, it is possible to apply this method to the WBAN environment with the necessary modifications. The most recent authentication strategy in the WBAN environment has a lower calculation cost when compared to the other options. In the WBAN environment, author propose a novel authentication strategy based on the light-weight authentication scheme proposed for wearable devices an in-depth evaluation reveals that our proposed technique minimizes computation costs while maintaining privacy and security, in addition to anonymous identification.

At the physical, medium access control (MAC), network, and transport layers, [37] firstly discuss the critical security requirements and Denial of Service (DoS) attacks that can occur in the WBAN environment. Then author explore the IEEE 802.15.4 security architecture and highlight the security weaknesses and key threats in the context of Wireless Body Area Network. It is examined and discussed several assaults on the super frame superframe's Contention Access Period (CAP) and Contention Free Period (CFP). It's been found that a clever attacker can corrupt an increasing number of GTS slots during the CFP period, which has the potential to significantly impact WBAN's Quality of Service (since most of the data is carried in CFP period). Increases in the number of malicious nodes corrupting GTS slots restrict the legitimate nodes from making optimum use of the bandwidth. This means that for some WBAN applications, the direct adaptation of the IEEE 802.15.4 security framework is not completely secure. In order to implement high-level security in WBAN, new solutions are needed.

Presented a public-key cryptography-based [38] authentication method for MSNs, which aids in identifying the most serious security flaws in current authentication procedures for remote patient monitoring. Sensors and

actuators are organized into nodes in medical sensor networks (MSNs). Sensors collect information about the human body, while actuators respond to medical commands. If these orders are changed in any manner, the system could be jeopardized. The recommended protocol can be employed with time-sensitive MSN applications since the Rabin authentication technique is improved in this research to improve the signature signing procedure. With the help of Tmote Sky motes and an FPGA, author implemented the Rabin algorithm in a variety of hardware configurations and evaluated its design and performance. It is also tested using the MIRACL (Multiprecision Integer and Rational Arithmetic C/C++) library, which implements the proposed protocol. MSN nodes are capable of receiving commands from medical staff in a secure, immediate, authorized manner.

3. Methodology

Figure 3 depicts the proposed architecture for the health care systems secure AI-based Block chain-assistance. There are six components: a user, a wireless network, a block chain, a trusted agent, a medical server, and an expert system. Users can be infected with different diseases or have already recovered from one. In order to acquire medical data, he implants or wears a collection of sensors. Wireless system i.e. Personal digital assistant (PDA) such as a smartphone also captures and retains medical data from each sensor for the user. The user is able to keep track of his or her health information on a PDA, which he or she can then encrypt and regularly upload to the blockchain as a block. The data, timestamp, and information of the previous block are included in each communication here.

Validating and recording agents are two types of permissioned agents. The transaction is validated by a group of nodes known as validating agents, as you can see (VA). Only transactions that have been verified by the majority of validating agents can be stored on the blockchain. Recording agents save data in the form of a block and only those in the network with authorization can access it after it has been validated.

Each component of the network, including the medical staff, hospital, and diagnosing expert system, has their own ledger, which they control. A diagnosis expert system is similar to a human expert when it comes to making decisions. Before being processed to determine disease types, encrypted blockchain data is decoded using DES. It can also remotely instruct the sensors on the patient's body to deliver the recommended medication if the patient is in a serious condition. In this approach, the brief of our proposed model has been summarized.

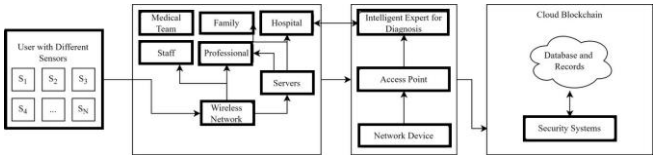

Figure 3. Proposed Architecture

3.1 Significance of System

There aren't enough hospitals, medical devices, and doctors to go around. Inability to diagnose every infected patient within their country has resulted in the deaths of a large number of people. Many patients can be monitored and diagnosed simultaneously in the suggested paradigm, which can help resolve a crisis of this magnitude. It is the job of this technology to collect data between hospitals and their patients. The patient's medical record is managed through Blockchain, which creates a distributed database. The integrity, secrecy, and validity of data are all ensured by the public key cryptosystem. Based on the patient's medical history, AI recommends a type of physician, a disease type, and a prescribed medication.

3.2 Secured and Privacy Preserving

To protect patient information, the suggested model makes use of a lightweight public-key cryptosystem, namely an identity-based cryptosystem based on the elliptic curve cryptosystem. The public key of the recipient is not required to be verified by the IBC. In terms of processing overhead, ECC-based arithmetic is roughly 20 times faster than modular exponentiation. In addition, the 128-bit ECC key is as secure as a 1024-bit RSA key in terms of bit length. IoT applications can benefit from the unique properties of IBC and ECC.

3.3 Proposed Wireless Body Area Network

Depending on the location of the radio signal, WBAN communication can be divided into two types: in vivo and in vitro. An entirely new technique of in-vivo communication, called body-coupled communication, is being used to identify individuals in the body domain network. We are talking about short-range, low-power communication in WBAN because most devices are worn on the body. This is what we mean by "external communication".

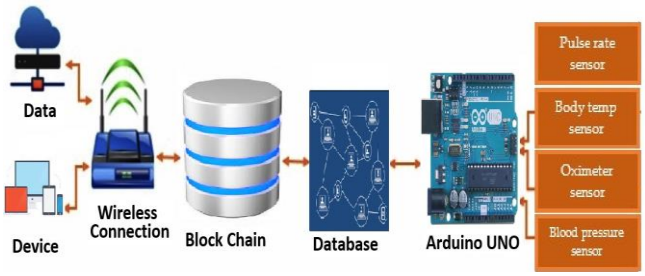

Figure 4. Proposed WBANs Sensors

3.4 Proposed Blockchain Model

Since blockchain nodes might be located all over the world but have equal access to the application, it is up to P2P

networks to make sure that communication between nodes is unrestricted. The P2P network does not have a central server, and each node is both an informed user and a provider of information. Every node is involved in the network's routing process, which includes establishing and networks. Blockchain apps provide APIs (application programming interfaces) in a number of situations. Users can interface directly with these APIs without having to worry about the underlying technology concerns.

3.5 Cloud Based Blockchain

Central databases are heavily used to store data safely. However, hackers are more focused. A script attack on a central database is one of the most popular ways hackers get access to large volumes of data. However, blockchain and distributed ledger technology make cracking much more difficult. Many blockchain projects aim to increase data storage security. This might be a game changer for users. While the blockchain initiative may lead to more secure data storage methods, it also gives people unfettered access to their data. Several blockchain projects use the original cryptocurrency as a markup. Apart from preventing identity theft and other issues raised by recent large-scale data breaches, this also allows users to monetize third-party data. Digital signatures ensure the message's integrity and non-repudiation in blockchain transactions.

4. Results & Discussions

We were particularly concerned about the amount of power used in message calculation and transmission in Wireless Body area networks with the security preservation of patients data using secured transactions of Block chains. To ensure security and early detection of attacks we have used machine learning models.

4.1 Energy Consumption

We have used different models for energy efficiency of Wireless Body Area network to ensure efficiency in energy consumption for security purposes. We have proposed load balancing based EESAA protocol called LB-ESSA. In order to evaluate the novel LB-EESAA protocol's performance, five additional protocols are simulated and compared to it. Using MATLAB, we are able to simulate a real-world system in order to better understand how it works. The following metrics are used to compare the LB-EESAA protocol to the HLEACH, PEGASIS, MAMC, LEACH and SEP protocols.

Evaluation Parameters

Stability period: This will measure the duration of network operation from the beginning until the death of the first node.

Network lifetime with 1st, 1st 10 and half nodes dead numbers: is between the beginning and end of the last node.

Instability period: duration of network operation from the first node to the death of the node

maintaining connections with other nodes, propagating and validating transactions, and synchronizing data blocks. Each node (both transactions and blocks are data structures of the blockchain, as described below). This exemplifies decentralization and the flat topology of peer-to-peer

When it comes to optimizing resources, load balancing is all about maximizing efficiency. There are a variety of ways to make the most of sensor node energy. With the clustering approach, network energy costs are significantly reduced. For example, clustering reduces redundant data packets and energy usage, while also saving communication bandwidth and extending the useful life of networks.

The nodes in active mode choose themselves as CH in the first round based on the likelihood of picking CH using a distributed algorithm when all nodes have the same beginning energy E_o. A random integer between 0 and 1 is chosen by each node, and the comparison is made with a threshold T_h determined for load balancing as follows:

$$\begin{cases} \dfrac{Pd}{1-Pd} & first\ round\ [1]\ if\ n \in A \\ 0 & otherwise \end{cases}$$

For the sake of performance evaluation, we have compared the proposed model with previous state of art models. Figure 5 shows the stability period of LB-EESAA, H-LEACH, LEACH and MAMC respectively. Highest stability period was attained by LB-EESAA protocol as 2300 seconds.

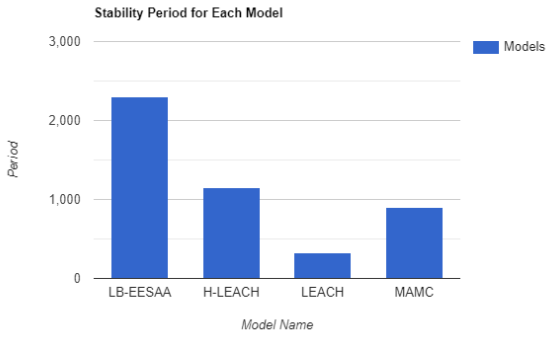

Figure 5. Stability Period

Figure 6 shows the maximum rounds for all dead nodes of each protocol. LB-ESSA has shown the highest number of rounds with alive nodes.

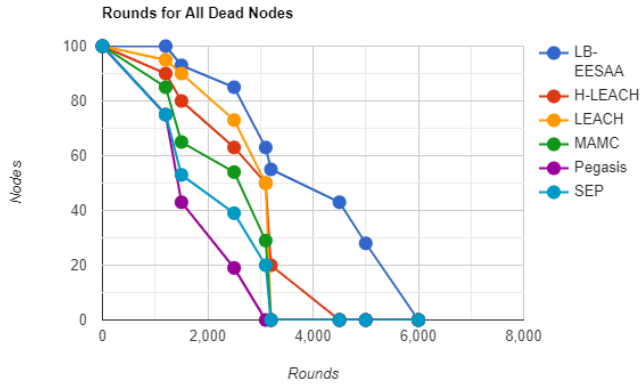

Figure 6. Rounds for All Dead Nodes

Comparison graph has been shown in Figure 7, showing the performance of LB-EESAA, H-LEACH, MAMC, LEACH, SEP and Pegasis protocol.

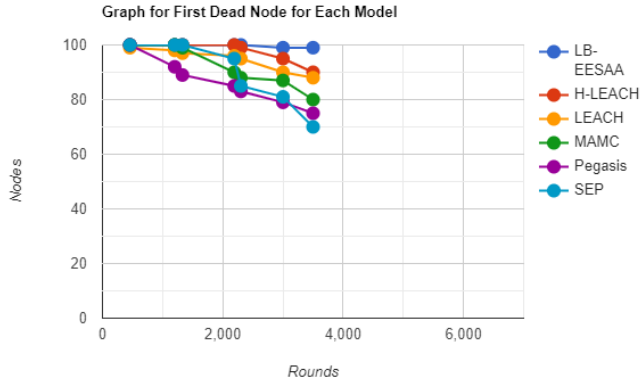

Figure 7. Graph for First Dead Node for Each Model

Figure 8 shows the graph of first 10 dead nodes. LB-EESAA has shown the highest number of rounds which shows that LB-EESAA is best protocol amongst others in terms of Number of Dead Nodes, Number of Alive Nodes, Stability Period and Energy Efficiency which is a key feature for security and preserving the privacy of patient in WBANs.

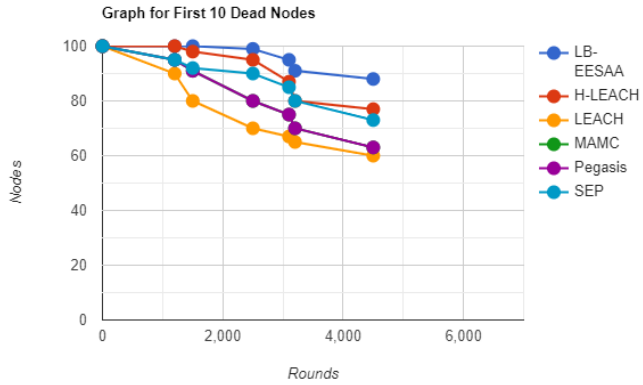

Figure 8. First 10 Dead Nodes

4.2 Communication vs Security Level in WBANs

Signcryption adds a significant amount of overhead to communications. The size of the signed message is the primary factor in determining the transmission overhead. Each user only needs two bytes in a conventional WBAN. On the other hand, communication overhead and security levels are shown in Figure 9. There is an increase in communication overhead as security levels rise.

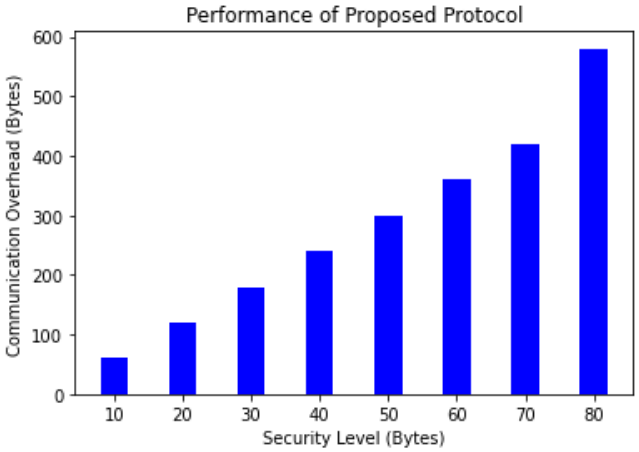

Figure 9. Performance of Proposed Protocol

4.3 Blockchain Performance

To validate its performance, the proposed blockchain-enabled WBAN platform was tested in this section in terms of block size, read throughput, transaction throughput, read latency, and transaction latency. For the blockchain network's performance evaluation, one ordered node and four peer nodes were chosen as experimental parameters. By changing the TPS send rate in the proposed blockchain-enabled WBAN network, we were able to compute throughput. Transactional throughput and read throughput are two examples of how throughput can be divided. The transaction throughput was defined as the number of transactions initiated on the blockchain network during the permitted time window. During the specified time window, read-through was employed to measure the reads operation on the blockchain network. Transaction read throughput was measured using variations in TPS transmit and random machine utilization setup.

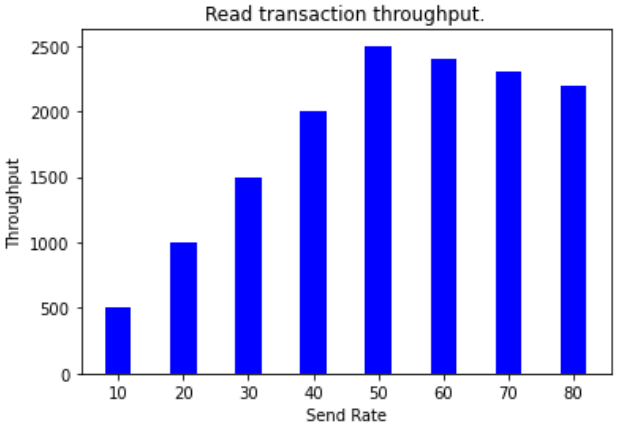

Figure 10. Read Transaction Throughout

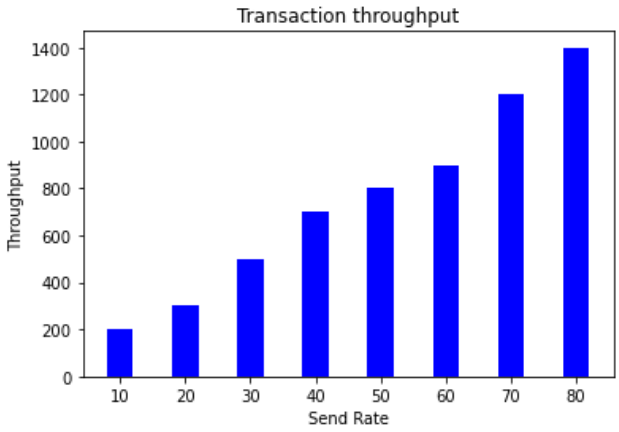

Figure 11. Transaction Throughout

4.4 Early Security Prediction

For the early prediction of attacks, we have collected the data of transactions and trained on machine learning model and evaluated to predict the attack on the WBANs based blockchain privacy preserving system for healthcare.

Logi-XGB

This model has been developed by ensembling the logistic regression model into XGBoost Classifier to improve both models' accuracy. Mathematical model of Logi-XGB Classification model is as follows:

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

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

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

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

Here P is the probability function of Logistic Regression and Y is the output of XGBoost classification model. $\sum_{k=1}^{n} f(x)$ Shows the boosting function of XGB Classifier. When XGB takes the output of y it will be sent to probability function of logistic regression for classification of any attack. Figure below shows the hybrid model of Logi-XGB Classification Model:

These two models have been combined in order to simultaneously increase their accuracy by using the XGBoost Classifier. Logistic regression's probability function will be fed the data received from y by XGB. An independent Logistic Regression study found that 69.2 percent of the time, the hybrid classifier raised this accuracy to 95.7 percent. Figure 12 shows a hybrid model of Logi-XGB Classification Model Performance.

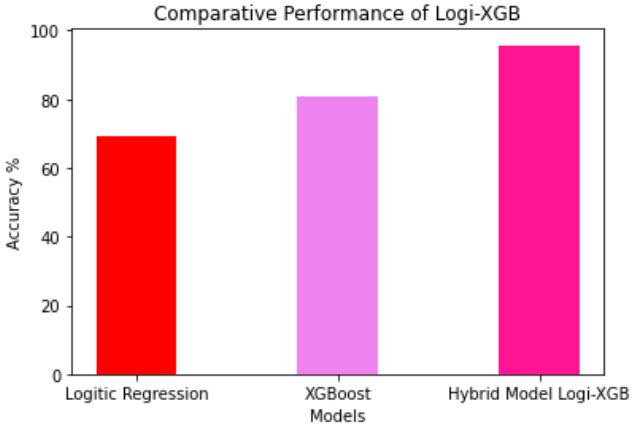

Figure 12. Logi-XGB Classification Model Performance

5. Conclusions

Humanity's most pressing need is access to quality healthcare, and the WHO has underlined this right as a fundamental human right. In recent years, the healthcare system has shifted from a traditional to a modernized patient-centered approach. In a modernized patient-oriented approach, tele monitoring and telemedicine systems are implemented to facilitate the sharing of personal data of patients. Tele monitoring has been acknowledged as a potential study subject by applying the latest methods to transform raw data into valuable data. WBAN stability requires minimizing node overheating and conserving energy. This paper presents a blockchain-enabled routing system LB-EESAA for the WBANs and implemented the early prediction system of attacks during Blockchain transactions. LB-EESAA has shown the best performance in terms of alive, dead nodes and highest stability period of the protocol. After increasing the efficiency of WBANs, we have secured the security level in terms of security level. For blockchain enabled system we have evaluated the system on read throughput and simple throughput transaction. After securing and making the system privacy preserved, we have used Logi-XGB prediction model machine learning for attacks prediction. Logi-XGB model has shown the accuracy of 95.7% in predicting the attack on early stages.

References

[1] F. A. Awin, Y. M. Alginahi, E. Abdel-Raheem, and K. Tepe, "Technical Issues on Cognitive Radio-Based Internet of Things Systems: A Survey," IEEE Access, vol. 7, pp. 97887–97908, 2019, doi: 10.1109/ACCESS.2019.2929915.

[2] I. Z. Memon, S. Talpur, S. Narejo, A. Z. Junejo, and F. Hassan, "Short-term prediction model for multi-currency exchange using artificial neural network," Proc. - 3rd Int. Conf. Inf. Comput. Technol. ICICT 2020, no. August, pp. 102–106, 2020, doi: 10.1109/ICICT50521.2020.00024.

[3] A. Scarlett and M. Zeilinger, "Rethinking Affordance," pp. 1–48, 2019.

[4] W. Akram, "Scenario Analysis and Proposed Plan for Pakistani Universities – COVID – 19 : Application of Design Thinking Model," Cambridge Open Engag., no. April, 2020, doi: 10.13140/RG.2.2.27794.61127.

[5] K. Hameed, I. S. Bajwa, S. Ramzan, W. Anwar, and A. Khan, "An Intelligent IoT Based Healthcare System Using Fuzzy Neural Networks," Sci. Program., vol. 2020, 2020, doi: 10.1155/2020/8836927.

[6] Muhammad Shoaib Akhtar Tao Feng Year: 2022 IOTA Based Anomaly Detection Machine learning in Mobile Sensing CT EAI DOI: 10.4108/eai.11-1-2022.172814.

[7] R. M. Parizi, A. Dehghantanha, K. K. R. Choo, and A. Singh, "Empirical vulnerability analysis of automated smart contracts security testing on blockchains," arXiv, 2018, doi: 10.5555/3291291.3291303.

[8] A. K. Shrestha and J. Vassileva, "User acceptance of usable blockchain-based research data sharing system: An extended TAM-based study," Proc. - 1st IEEE Int. Conf. Trust. Priv. Secur. Intell. Syst. Appl. TPS-ISA 2019, pp. 203–208, 2019, doi: 10.1109/TPS-ISA48467.2019.00033.

[9] D. Mao, F. Wang, Y. Wang, and Z. Hao, "Visual and User-Defined Smart Contract Designing System Based on Automatic Coding," IEEE Access, vol. 7, pp. 73131–73143, 2019, doi: 10.1109/ACCESS.2019.2920776.

[10] S. Zhao, Y. Feng, and G. Yu, "D2D communication channel allocation and resource optimization in 5G network based on game theory," Comput. Commun., vol. 169, pp. 26–32, Mar. 2021, doi: 10.1016/j.comcom.2021.01.016.

[11] J. Gante, G. Falcão, and L. Sousa, "Deep Learning Architectures for Accurate Millimeter Wave Positioning in 5G," Neural Process. Lett., vol. 51, no. 1, pp. 487–514, 2020, doi: 10.1007/s11063-019-10073-1.

[12] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT Scenarios," IEEE Access, vol. 8, pp. 23022–23040, 2020, doi: 10.1109/ACCESS.2020.2970118.

[13] Muhammad Shoaib Akhtar Tao Feng Year: 2021 An overview of the applications of Artificial Intelligence in Cybersecurity CT EAI DOI: 10.4108/eai.23-11-2021.172218

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] V. J. Jariwala and D. C. Jinwala, AdaptableSDA: secure data aggregation framework in wireless body area networks. Elsevier Inc., 2020.

[19] Muhammad Shoaib Akhtar Tao Feng Year: 2022 Comparison of Classification Model for the Detection of Cyber-attack using Ensemble Learning Models SIS EAI DOI: 10.4108/eai.1-2-2022.173293

[20] 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: 10.1016/j.cose.2021.102211.

[21] 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.

[22] 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.

[23] 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.

[24] N. D. Han, L. Han, D. M. Tuan, H. P. In, and M. Jo, "A scheme for data confidentiality in Cloud-assisted Wireless Body Area Networks," Inf. Sci. (Ny)., vol. 284, pp. 157–166, 2014, doi: 10.1016/j.ins.2014.03.126.

[25] 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.

[26] 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.

[27] 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.

[28] R. Wang and G. R. Tsouri, "Securing while sampling in wireless body area networks with application to electrocardiography," IEEE J. Biomed. Heal. Informatics, vol. 20, no. 1, pp. 135–142, 2016, doi: 10.1109/JBHI.2014.2366125.

[29] C. C. Y. Poon, Y. T. Zhang, and S. Di Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and M-health," IEEE Commun. Mag., vol. 44, no. 4, pp. 73–81, 2006, doi: 10.1109/MCOM.2006.1632652.

[30] 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.

[31] R. Nidhya and S. Karthik, "Security and privacy issues in remote healthcare systems using wireless body area networks," EAI/Springer Innov. Commun. Comput., pp. 37–53, 2019, doi: 10.1007/978-3-030-00865-9_3.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] Feng Tao Muhammad Shoaib Akhtar Zhang Jiayuan Year: 2021 The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey CT EAI DOI: 10.4108/eai.7-7-2021.170285

[38] T. Hayajneh, B. J. Mohd, M. Imran, G. Almashaqbeh, and A. V. Vasilakos, "Secure authentication for remote patient monitoring withwireless medical sensor networks," Sensors (Switzerland), vol. 16, no. 4, pp. 1–25, 2016, doi: 10.3390/s16040424.

[39] Muhammad Shoaib Akhtar, Tao Feng, "Deep Learning-Based Framework for the Detection of Cyberattack Using Feature Engineering", Security and Communication Networks, vol. 2021, Article ID 6129210, 12 pages, 2021. https://doi.org/10.1155/2021/6129210