Sharing Information Securely in WBANs: A Novel Trusted Adaptive Dynamic Cryptosystem (ADC) Framework

P. Anitha
Ph.D. Research Scholar, Department of Computer Science,
Sree Narayana Guru College,
K.G.Chavadi, Coimbatore – 641105, Tamil Nadu, India.
Dr. R. Priya
Associate Professor and Head, Department of Computer Science,
Sree Narayana Guru College,
K.G.Chavadi, Coimbatore – 641105, Tamil Nadu, India.

ABSTRACT:
Increased necessitate for medical treatments and improved quality of care for people attributable to "Wireless Body Area Networks (WBANs)". The information obtained from the wearable sensors "Sensor Node (SN)" is generally stored in the server module. Challenges to the privacy of WBANs could originate from a multitude of sources due to the rapidly changing of the distributed system as well as the networking endpoints themselves. Mostly a set of biomedical parameters relevant to a patient's health are currently processed by the existing "Block Chain (BC)" technology. However, in BC, significant information will be lost in transmission and a lot of energy is used throughout the process of communication. Under this research, it provide a unique "Adaptive Dynamic Cryptosystem (ADC)" method centered on the "Data Encryption/Decryption Keys" paradigm to address privacy and security concerns. The proposed ADC method could support the management of clinical healthcare resources for patients from far areas by providing safe, privacy-protecting monitoring of patient activities. ADC is a flexible solution that can protect data of varying sizes. The patient's encrypted medical records are made available throughout the encryption procedure via the private key. For WBANs to be able to provide trustworthy remote patient monitoring services, the encrypting operation produce an encrypted message with a length of "n-bits". As a result, the suggested ADC method minimizes both the level of energy usage and the computation time. Utilizing health records as its foundation the proposed ADC provides a higher rate of data privacy and a higher security ratio. The suggested ADC method provides higher levels of security than the existing BC method in terms of "Security Ratio", "Energy Consumption Ratio", "Encryption Time" and "Decryption Time" as determined by the assessment methodologies used for both approaches.

Keywords: WBAN, Security, Block Chain, Adaptive Dynamic Cryptosystem

1. INTRODUCTION

"Wireless Sensor Networks (WSNs)" are networks of dispersed SNs which operate together to gather, process and relay information to the "Base Station (BS)" about environmental settings. The WSNs are being used for a wide range of tasks, notably healthcare observation and supervision [1].

The use of healthcare observation systems through WSN as a kind of management that facilitates constant feedback and interaction has risen in prominence in recent years. Healthcare deployments of WSNs are referred to as "WBANs" to distinguish them from other types of uses. Connecting patients and healthcare professionals such that serious clinical data may be shared in real-time has been the goal of a WBAN, a subset of a WSN [2].

Implantable and wearable channels with WBANs play a major role in medical diagnosis, tracking and device regulation by gathering information from several SNs placed across or within the human body. This allows for screening regardless of where a patient resides, seems to have no impact on their movement, can detect diseases quickly and avoid them and can provide assistance to patients remotely. This makes it perfect for round-the-clock tracking since it can provide doctors with accurate diagnoses and instantaneous responses [3].

WBANs have become an adaptation for the "Internet of Things (IoT)" which intends to raise the standard of patient care [4]. According to forecasts, the IoT industry will grow to over "$1.9 trillion (USD)" over the coming few years. An anticipated "100 billion IoT" gadgets are going to be used worldwide by 2025, including a complete financial value that exceeds "USD 11 trillion" [5].

WBAN has several potential uses in many fields, among them including healthcare provision, entertainment, sports and the military. Applications for the WBAN are classified as medical purposes or non-medical purposes [6]. Distant and continuous collection of biological data is made possible with the use of implanted and wearable sensors. Proactive death and anomaly detection can be identified by assessing cardiac and brain functions due to this new continuous monitoring. Automated medication distribution is made possible by actuators. Technology like cochlear implantation and hearing devices may help people lead better lives.

To make the public safer by reducing the likelihood of medical errors, WBAN applications use data from prior incidents to provide notifications to healthcare workers if anything similar occurs [7]. This means that WBAN should enhance the performance of the healthcare systems by improving the administration of diseases and the response to crises. The following categories pertain to WBAN healthcare applications. Figure 1 depicts how the WBAN for Healthcare applications is categorized for ease of reference. Medical and Non-Medical are further subdivided into applications.

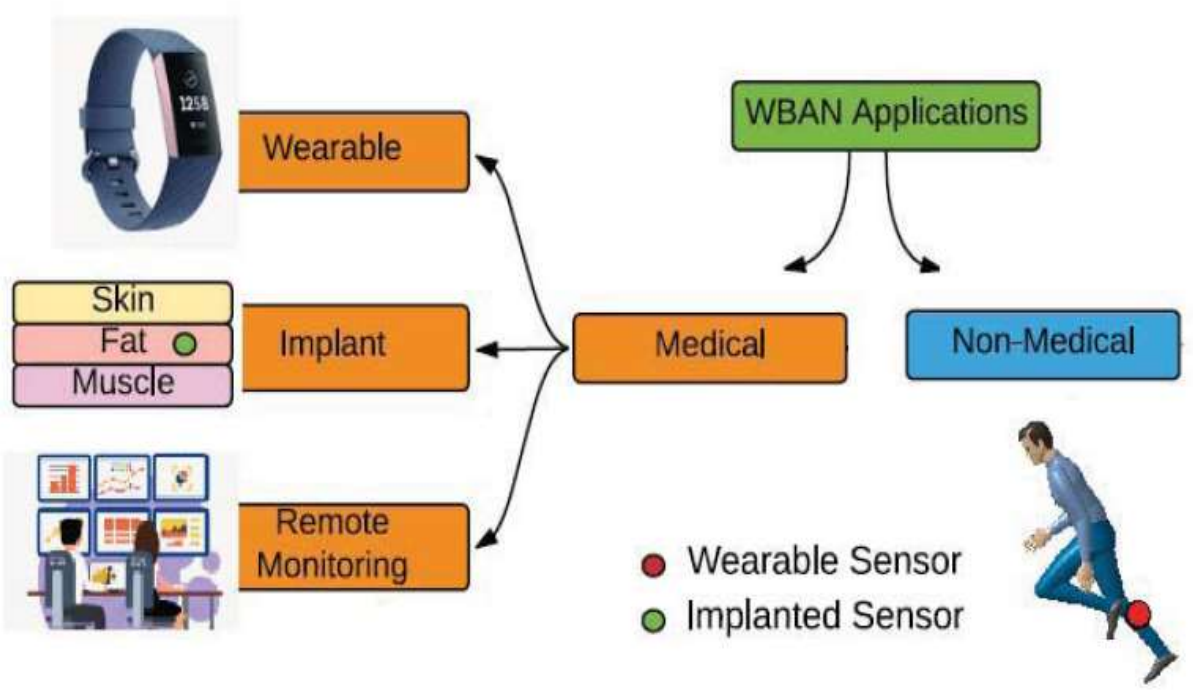


Figure 1: WBAN for Health care applications

(i) Applications concerning Medical:

The use of WBAN medical services allows for continuous observation of physiological indicators like as pulse rate, temperature and hypertension. The acquired data may be transferred to a faraway place, such as an ambulance service, using a smartphone, which serves as a gateway [8]. The usage of WBAN is useful in the early diagnosis and management of dangerous conditions including heart disease and diabetes. The following is a breakdown of medical WBAN applications based on the location of the medical sensors:

(a) Wearable technology:

Monitoring glucose levels, blood pressure, temperature, EEG, ECG, SpO2, EMG and medication administration are some of the medical wearable healthcare usages.

(b) Implant Monitoring:

These SNs have several monitoring applications once they have been implanted inside a body such as tracking diabetes, detecting heart problems and even detecting cancer.

(ii) Applications concerning Non-Medical:

The Non-Medical comprises two types of applications [9], namely:

(a) Detection of Motion:

Body movements and behaviors are detected, captured, recognized and identified by this program, which sends notifications to the application owner. Anxiety, for instance, causes a rise in heart rate and other sensations, such as shivering. As a result, it is possible to monitor one's emotional state.

(b) Secure authenticating:

Multi-modal biometrics and EEG may both benefit from this WBAN application. Anatomical and physiological biometric traits including fingerprints and face characteristics are used in this application.

Problem Statement: Regrettably, in this type of interconnected system, malicious people might easily access and misuse private health information due to the absence of proper data transmission safeguards. Consequently, patients are subjected to a serious violation of private information and personal documents. Wearing equipment or remote sensors placed on or within the body of the patient, for instance, could identify a cardiac arrest in advance. That's why a routing protocol must have a strong identity and information security so that a doctor can start treatment right away [10]. The safety of the WBANs network must be guaranteed using an efficient security mechanism. Several security issues have to be resolved with WBANs, particularly authenticating and data secrecy are notably demanding.

Paper Contribution: As an approach for addressing concerns about confidentiality and safety, the development of ADC based Data Encryption/Decryption model is being proposed. The proposed ADC could be employed for the administration of medical healthcare services for patients located in geographically dispersed areas by securing patient records using personal protection methods. The flexibility of the proposed model offers the data security of varied sizes in data. During the encryption process, the patient’s medical reports input with encryption are offered through the secret key. The encryption process output refers to ‘n’ bits of cipher text that get transmitted via a wireless network to achieve remote health monitoring services that are secure with WBANs. Therefore, the proposed model cuts down the rate of energy consumption and response time. Leveraging health records as its basis provides an improved privacy protection ratio as well as security ratio.

Paper Organization: Section 2 reviews some recent publications in WBAN for secure data transmissions, Section 3 elaborates the methodologies of the proposed ADC framework with crisp detail about the existing BC framework for WBAN security and Section 4 discusses the implementation results obtained by both the existing BC and the proposed ADC frameworks with its comparative analysis and the research paper is concluded in Section 5 with future suggestions for more investigation.

2. RELATED WORKS

The researchers in [11] propose a more effective method for network access within WBANs by combining the features of "Certificateless-Signcryption" and "Anonymous Mutual-Authentication" with a focus on minimizing operational expenses. With the help of the "XOR Operation" as well as the "One-Way Hash-Chain Function", a secured verification is accomplished using the "Chaos Baker Map" method. The results of the assessed methods show that the proposed method outperforms its predecessors across all of the categories examined such as "Delay", "Energy Consumption", "Packet Delivery Ratio", "Throughput" and "Coverage Time". Moreover, the idea of "Certificateless Cryptography" means that this method might be vulnerable to problems with "Partial Private-Key Distribution", greater processing power requirements and larger data usage. The absence of "Forwarding Secrecy", "Public Verifiability" and "Anti-Replay" attack may compromise the security of this method.

In [12], the researchers have described a search terms approach for WBANs that relies on "Heterogeneous-Signcryption", while the "Data Owner (DO)" uses "Certificateless Cryptography" whereas the "BS" and "Receiver" utilize "Public Key Infrastructure (PKI)" characteristics. The aforementioned strategy was created using the BP computational model. The researcher asserts that this method provides strong authentication including "Secrecy", "Unforgeability", "Non-Repudiation" and "Authenticity". However, BP could cause the network to suffer more overhead in terms of both communication and computation. Additionally, this could be limited due to the requirement for a secure channel for the DO propagation of "Partial Keys" and "PKI Certificate" management mostly on server and client ends. Other factors that might have an effect include an absence of "Forward Secrecy", "Mutual Authentication" and "Public Verifiability".

A novel approach for BSNs, centered on "Attribute-Cryptography" with "Blockchain (BC)", was suggested by the researchers in [13]. The safety and effectiveness of the proposed solution are dependent on BP. The researchers also note that their technique uses lower power, computing resources and network bandwidth than competing methods while maintaining adequate security like "Confidentiality", "Unforgeability", "Anti-Replay Attack" and resilience toward a "Man-in-the-Middle Attacks". Whereas "Certificateless Cryptography" and PKI might necessitate utilizing the wireless link for the transmission of "Partial Keys" and "Certificate Administration", BP could cause the approach to impose extra operational and transmission overhead. It may even be harmful when security requirements like "Mutual Authentication", "Public Verifiability" and "Forward Secrecy" are not met.

For the transition from "Identity" to PKI, the researchers of [14] proposed a heterogeneity approach for WBAN centered on an equivalence criterion. Sensing devices use "Identity-based Cryptography" for encrypting personal data before sending it to the server, where it's safeguarded mostly by the administration hub's "Public Key" within PKI. Moreover, the suggested technique uses BP to improve the privacy complexity, which constitutes a very time-consuming and complex computing task.

In [15], the researchers introduced a novel architecture for WBANs that makes use of the "Hyperelliptic Curve" method. Contrarily, the researchers offered no evidence, official or informally, to back up any of their claimed assurance criteria.

3. METHODOLOGIES

According to the ADC framework model, its sensors are useful for human physiological values measurement connected with bodies to sense "Temperature", "ElectroCardioGram (ECG)" and "ElectroEncephaloGram (EEG)" values. Each patient of the ADC framework has a "Personal Computer/Laptop/Mobile" for data collection from the sensors on the body of the patient and the collected data is transmitted through personal servers and to the hospital community server.

This proposed ADC allows for patient accounting to take place outside of the confines of the hospital and also the server. All patients are linked with "Remote BS (RBS)". Patients' RBSs send their health records' information to a hospital's communal server. A patient's host, or WBAN, is responsible for creating the interbody connection which delivers the information of the patients to the RBS whenever the patient has been located outside of the RBS's coverage area.

The sensors may be worn mostly on the body and are programmed to access the individual's health data. Sensing devices check here on the patient's condition in real-time from various vantage points. Patients' data within WBANs may be sensed more ease owing to the extensible nature of the networking infrastructure based on SNs. Those SNs have been linked to a network that usually focuses on data from several patients. The PC may access the server where clinical records are kept through a network connection. WBANs employing remote monitoring of health services benefit from the increased security afforded by the encrypted data transmission among doctors and patients.

3.1 Block-Chain (BC) Framework for WBAN (Existing Framework)

This BC is part of a larger shared network of databases. Collectively, several SNs inside the network keeps track of an interlinked listing of interconnected blocks and strong cryptography is implemented to both update the listing and ensure the BC's ongoing integrity. Whenever a hacker tampers with the contents of a BC block, the block's "Hash Value (HV)" would modify, causing it to no longer be able to link to the block after it. This signifies that information inside a shared database created utilizing BC architecture is more secure against manipulation. To ensure the integrity of the BC and produce fresh blocks, all participating SNs rely on a central consensus mechanism.

A "Double-Hop" shared infrastructure of WBANs is created using BC systems [16]. The "Perception Layer (PL)", "Cloud Server Layer (CSL)" and "Beyond-WBAN (BWBAN)" are the 3 stages that make up the architecture. The PL, which consists of an SN with a "Super Node (SuN)", is always in charge of gathering and transmitting the patient's essential values to the CSL. Due to power constraints, the SN implanted inside the patient's body is unable to transmit information straight to the "Hub Node (HuN)" inside the CSL. Instead, the SuN's robust communication capabilities are required to relay the SN's results. The SuN associated with the intermediate nodes doesn't undertake any further processing or storage arrays on the relayed information, but it may interact with a nearby HuN and also other HuNs across zones to facilitate this cross-regional connectivity for SNs. The majority of HuNs use BC architecture to generate WBAN CSLs.

Every HuN is responsible for overseeing the SNs as well as SuNs within its administrative region. The HuN is capable of completing cooperative authorization and key negotiating with its SN owing to its dependable computational resources, transmission efficiency and memory space. The information sent by the SN would be received by the HuN and after that, it would be preserved as a personal BC inside the databases. Both SN registration information and patient physical information are included. To ensure only authorized physicians, caregivers and patients have access to sensitive individual clinical information, the HuN and also the SN utilize the user information from the SN to authenticate and negotiate on a shared set of keys for sharing the data. By connecting to any HuN, they may have accessibility to the patient's morphological parameters.

Disadvantages:

- The hacker may change, collect and repeat information sent over the open channel during the key and authentication negotiation phase.
- The BC's information is kept inside the HuN's databases, whereby the hacker could retrieve.
- Data exchanged across HuNs during the networking SN agreement process is impenetrable to hackers.

3.2 ADC Framework for WBAN (Proposed Framework)

In an attempt to protect the confidentiality of a patient's healthcare records stored inside a WBAN, a reliable distant healthcare observation system architecture is required. The WBAN privacy problem was addressed with the development of the ADC architecture. The use of distant medical service observation technology is being encouraged as a means to better safeguard the confidentiality of patients within WBANs.

As shown in Figure 2, the "Adaptive Dynamic Key (ADK)" is used for encrypting the patient data before sending it over the wireless connection to the physician or medical management station. The encrypted patient records are transmitted to the receiving end, where the ADK is used to decode the data in accordance to determine the patient's condition. The ADK has been exchanged between both the transmitter and the recipient inside an ADC architecture. Patients' clinical records could become accessible only to those who have been given this key, while anybody else would be denied permission. As a result, ADC architecture improves the confidentiality and safety of patient data.

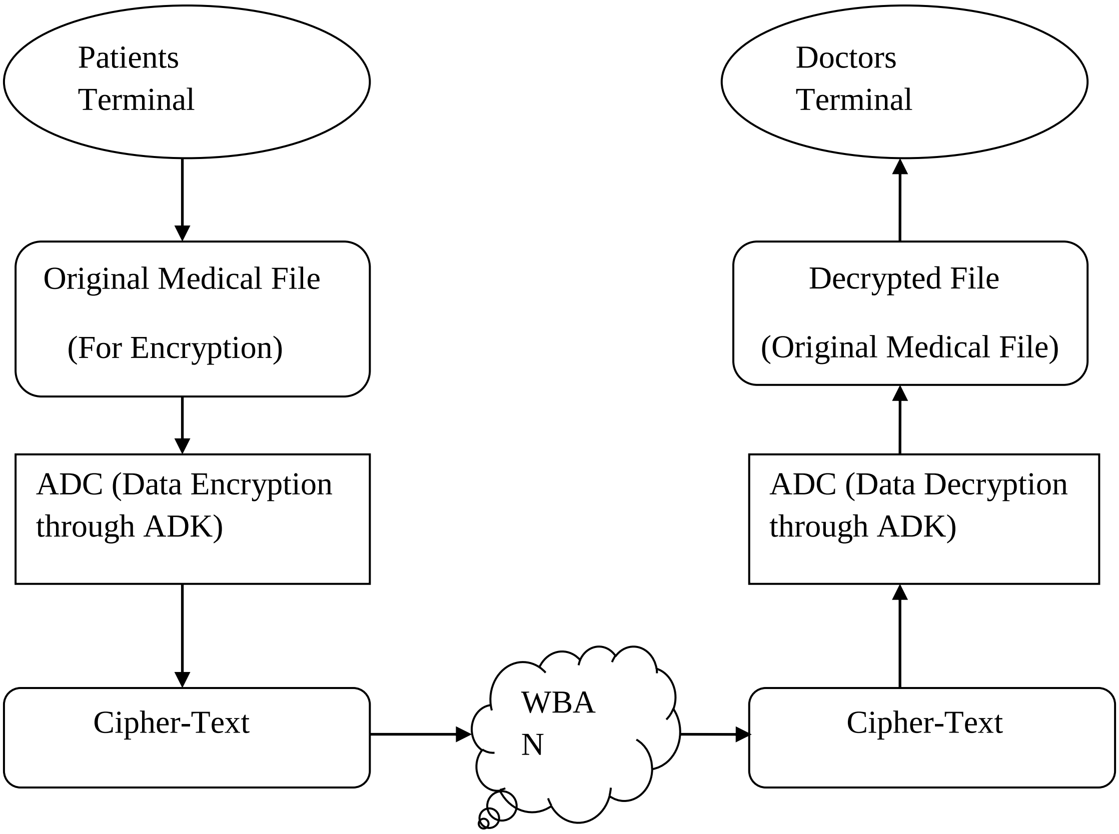


Figure 2: Proposed ADC Framework Overall Architecture

In the existing BC framework for WBAN, the sensor handles data access through the structure of planning access. In the data offered through cipher text format in the data sink, the trust is lowered owing to the failure of the data sink with the decrypt stored cipher-text key. However, in this proposed ADC framework for WBAN, the ADK handled such issues through adaptive data encryption.

3.2.1 ADC Encryption Process

This ADC algorithm makes use of ADK for data encryption of patients. The proposed ADC did not boost the format of input and length of the patient data based on encryption but instead changed the input order of the patient data. It is flexible to offer data security having varied information sizes. The Data Encryption processes based on ADK are given below in Figure 3.

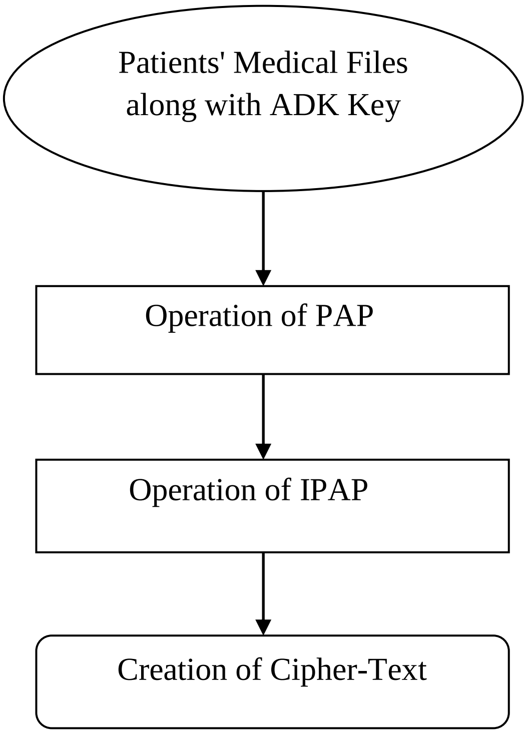


Figure 3: ADC based ADK Data Encryption process

The ADC framework handles the patient's medical files as input along with ADK then performs "Pair-Wise Autonomous Permutation (PAP)" and "Inverse Pair-Wise Autonomous Permutation (IPAP)" to create cipher text. Several secret keys were utilized for the ADC algorithm like matrixes "A, B" and "Tweak (T)". The ADK is the secret key with a "128-bit" length. ADK is useful for "Pseudo-Random Function (PRF)". At ADC algorithm, generation of ADK with "Key Derivative Function" or "Best Entropy Source" with the password that is user supplied. The supply of the string by the user is referred to as "Tweak (T)" which has an encoding of fixed-length "Binary String" using a "Cryptographic Hash Function". The ADC algorithm uses two matrices, "A, B" that have "A" as the "invertible binary matrix" with "N*N" size and "B" refers to a "binary vector" with "1 × N" size while "N" stands for the "input bits" value (or the patient data). The uniform distribution of A and B and random generation is given as following Equations (1) and (2):

$$A_{n,n} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix}$$

Eq→1

whereas,

$$a_{i,j} \in \{0,1\} \forall_{i,j} \in \{1, \dots, n\}$$

$$B_{1,n} = (b_{1,1} \quad b_{1,2} \quad \cdots \quad b_{1,n})$$

Eq→2

whereas,

$$b_{1,j} \in \{0,1\} \forall_{j} \in \{1, \dots, n\}$$

The PAP in the ADC framework is performed to achieve uniform distribution of permutation for the input that is known. The autonomous permutation that is pair-wise has two distinct inputs "x, y" plus their properties and "x_1, y_1", as the two distinct outputs having "x1 = PwAP (x)" as the probability and uniformity of "y1 = PAP (y)" i.e. "1/((2^n)*(2^n-1)) with independent variables like "x, y, x_1, y_1". Here "X" input acts as the "Binary Vector" having "n bits" size also held "1*N" matrices, with the formulation of "$PAP_{A,\ B}$(X)".

$$X_{1,n} = (x_{1,1} \quad x_{1,2} \quad \cdots \quad x_{1,n})$$

Eq→3

whereas,

$$x_{1,i} \in \{0,1\} \forall_{i} \in \{1, \dots, n\}$$

$$PAP_{A,B}(X) = (X \times A) \oplus B$$

Eq→4

The definition of "A, B" is provided in Equations (1) and (2). The formula of IPAP is given in the following Equation (5):

$$PAP_{A,B}^{-1}(Y) = ((Y \oplus B) \times A^{-1})$$

Eq→5

The "Feistel Network (FN)" and ADC algorithm have a symmetric structure for planning the cipher's block. In its simplest form, FN would be a "2n bit permutation (δ)" using the "Round Function (n-bit)" as provided by Equation (6):

$$\delta_f(L, R) = (R, L \otimes f(R)) \text{ Where } |L| = |R| = n$$

Eq→6

Using the FN having "r" one designed with FN structures while varying with "r" n-bit functions "f_1, f_2,...f_r" as "2n-bit permutation" is obtained as per Equation (7):

$$\delta_{f_1,f_2,\dots f_r}(L, R) = \delta(f_1) \circ \delta(f_2) \circ \dots \delta(f_r)$$

Eq→7

In the proposed ADC framework, security is achieved through the FN scheme constructed based on PRF security. The security guarantee is offered by security assurance with several round functions for each round. The employment of ADC algorithm in "Electronic Code Book (ECB)" mode like the round functions. The guarantee of security of the output is achieved in several ways for every round. The process that occurs through mixing round constantly with each PRF input can be formulated as per Equation (8):

$$round\_const_r = \{0x00, 0x03, 0x0c, 0x0f, 0x30, 0x33, 0x3c\}$$ Eq→8

whereas,

$$r \in \{1,7\}$$

So, the encryption by ADC algorithm with patient data having ADK for generation of the cipher-text has the following mathematical formulation provided in Equation (9):

$$C = Encryption\ (D, ADK, T, A, B)$$ Eq→9

Equation (9) helps to obtain the cipher-text. Inside the doctor's office or distant patient observation service, the "Cipher-Text (C)" has been sent.

Through WBAN a patient's information is transmitted with increased security over the wireless network using cipher text. Cipher Text is the final output of the inverse pairwise autonomous permutation which uses the FN's output. The FN's "Rounds (r=7)" have been executed. To obtain a uniform distributed permutation, the PAP uses the input patient data. The input to the specified ADC algorithm is a "Patient Medical report (D)" encrypted with "Secret Key (ADK)", "Matrices (A, B)" and a "Tweak (T)". The resultant output of this algorithm is "Cipher Text (C)" of "n bits".

3.2.2 ADC Decryption Process

In an attempt to retrieve a patient's health information from a transmitted message, the ADC methodology must be executed at the receiving end. Both "Cipher Text (C)" and "Secret Key (ADK)" are compelled as inputs for the ADC framework.

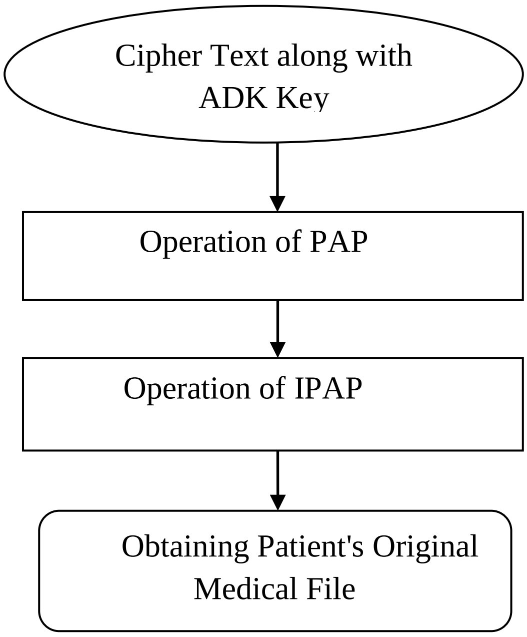

Cipher Text along with ADK Key
Operation of PAP
Operation of IPAP
Obtaining Patient's Original Medical File

Figure 4: ADC based Data Decryption process

After that, it uses PAP as well as IPAP to acquire details about patients so that the present health state of those individuals may be evaluated. The ADC based Data Decryption process is described in Figure 4.

The logical formulation of the ADC process for decrypting the encrypted text to retrieve the authentic patients' health record is given by Equation (10):

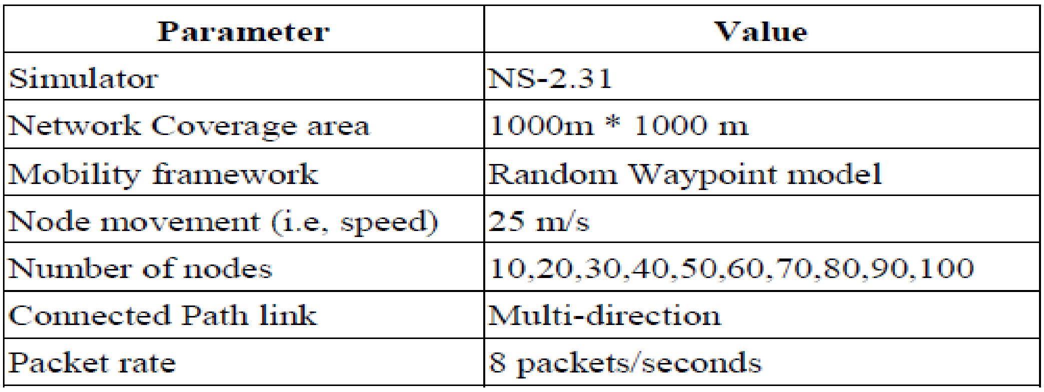
$$D = Decryption\ (C, ADK, T, A, B) \qquad \text{Eq}\rightarrow 10$$

The patient's "D" Original health record can be derived using Equation (10). Once the PAP and IPAP have been executed, the encrypted patient's health record may be decrypted and retrieved. ADK guarantees that only authorized users may retrieve provided patient records. The ADC concept effectively increases the safety of distant health observation systems.

4. RESULTS AND DISCUSSIONS

Using "NS-2 Simulator", with a size of the network "1000m * 1000m", both the proposed ADC as well as the existing BC framework can operate. The WBAN's SN has been positioned to observe the patient's activity and uncover the health records using highly secured standards. The sampling rate while carrying out the individual operation is "25 milliseconds". In the "Random Way Point (RWM)" paradigm, any SN moves individually within every route inside the shared network. When setting up a network, RWM typically employs an average SN count. Using the aforementioned counts and proportions, user can specify a location to go to at a random pace.

Table 1: Simulation parameters



Parameter	Value
Simulator	NS-2.31
Network Coverage area	1000m * 1000 m
Mobility framework	Random Waypoint model
Node movement (i.e, speed)	25 m/s
Number of nodes	10,20,30,40,50,60,70,80,90,100
Connected Path link	Multi-direction
Packet rate	8 packets/seconds

In Table 1, it provide the simulation settings used to carry out the experiments. The modeling outcomes are achieved by utilizing numerous setups with repeated runs. Analyses of both the existing BC as well as the proposed ADC framework's effectiveness are conducted. The correct measurements are used to assess the effectiveness comparison with help of tables and graphs.

(i) Security Ratio (SR):

A patient's SR has been calculated as the percentage of their data that was transmitted securely relative to the overall amount of data. The SR calculated from a patient's medical records is most often expressed as a "Percentage (%)" and has been statistically constructed according to Equation (11):

$$\text{Security Ratio (SR)} = \frac{\text{number of patient data that are securely transferred to the destination}}{\text{total number of patient data}}$$

Eq→11

If a patient's health data has a greater SR, the approach is considered to work effectively.

Table 2: Security Ratio

Average Patient's Data	BC	ADC
100	90	95
200	84	92
300	76	89
400	66	86
500	54	83

Table 2 shows the SR measure for different patients' information for the proposed ADC framework in comparison with the existing BC framework. The number of patient data in WBAN is varied from 100 to 500 in WBAN. Table 2 and Figure 5 demonstrate that the ADC framework improves the SR of patient records over the existing BC framework. The SR varies between 54% and 95% according to its patient's records. When comparing the SR of the existing BC to the SR of the proposed ADC considering 500 patient records, it is discovered that the SR of the existing BC is 54% as well as the SR of the proposed ADC is 83%. Hence, employing the proposed ADC framework increases the SR of the patient's health records over the existing BC framework.

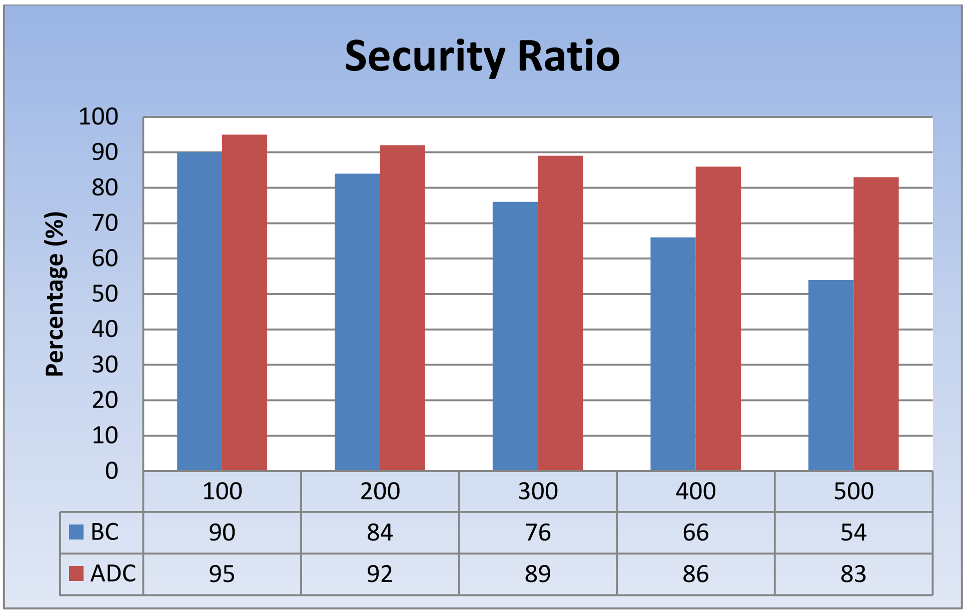


Figure 5: Security Ratio

(ii) Energy-Consumption Ratio (ECR):

When comparing the consumption of energy for a particular SN to the entire number of SNs inside a WBAN, the ADC framework provides a measurement of the ECR for transferring patient records from one SN to another. The ECR is expressed in terms of "Joules (J)" using the following Equation (12):

$$Energy\ Consumption\ Ratio\ (ECR) = Energy_{SN} * Total_{SN}$$

Eq→12

Energy per single SN "Energy$_{SN}$" multiplied by the number of SNs inside the WBAN networks "Total$_{SN}$" provides the ECR for reliable distant health observation operations as per Equation (12). Whenever the ECR remains minimal, the methodology is considered to work better.

Table 3: Energy Consumption Ratio

Total SNs	BC	ADC
20	1180	780
40	2360	1560
60	3540	2340
80	4720	3120
100	5900	3900

Table 3 shows the ECR for different patients' information for the proposed ADC approach in comparison with the existing BC approach. The number of SNs in WBAN is varied from 20 to 100. Table 3 and Figure 6 indicate that the ADC framework results in a lower ECR for SN than the existing BC framework. The ECR of the frameworks varies from 780 joules to 5900 joules. Whereas SN has several 100, the proposed ADC framework results in the consumption of 3900 J of energy for secure monitoring the patient data whereas the existing BC framework results in the consumption of 5900 J. Hence, it is evident that the proposed ADC framework results in a shorter ECR than the already existing BC frameworks. Figure 6 shows a visualization of the data from Table 3 in graphical form.

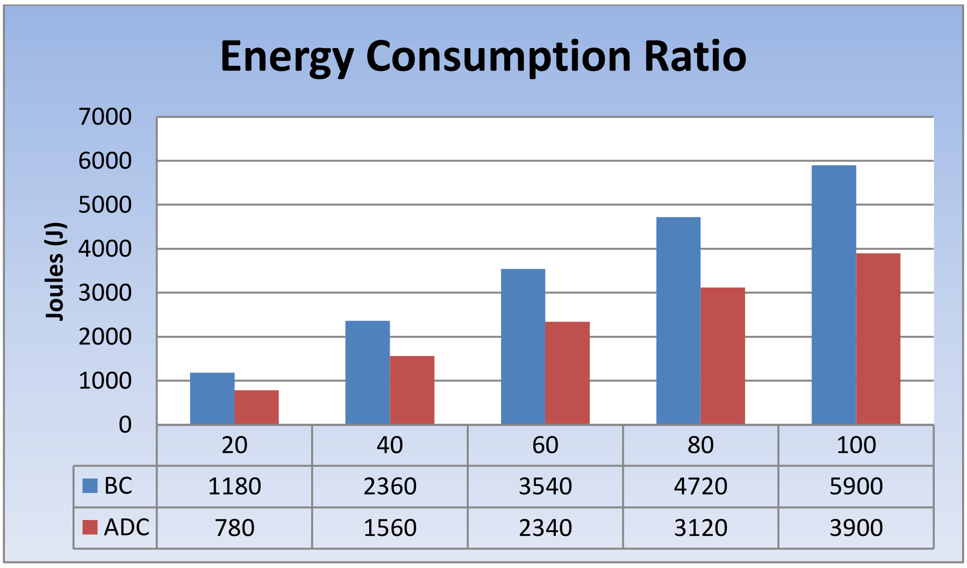


Figure 6: Energy Consumption Ratio

(iii) Encryption Time:

The ET is measured in seconds, or the amount of time it takes for a given technique for encrypting a file using a given secret-key. This does not consider the time spent processing "Input/Output (IO)" files.

Table 4: Encryption Time

Average Patient's Data	BC	ADC
100	9.2	7.2
200	18.4	14.4
300	27.6	21.6
400	36.8	28.8
500	46	36

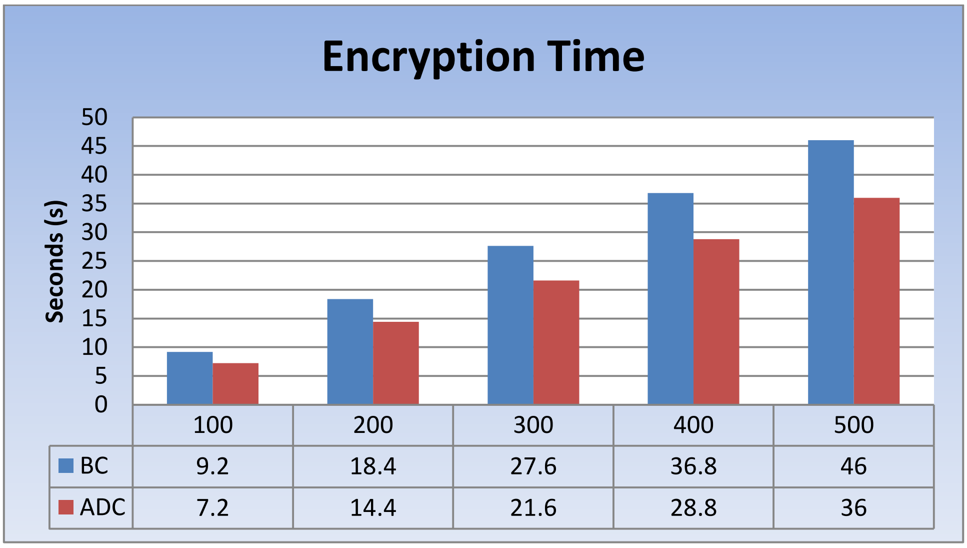


Figure 7: Encryption Time

As shown in Table 4 and Figure 7, the proposed ADC framework, with the existing BC framework, was compared for ET calculations. Overall Patient's Data attribute variability inside the ET has been examined. Patients' data contributions would vary between 100 and 500. It shows that the proposed ADC framework has an initial ET of 7.2 seconds for 100 Patient's data, whereas the existing BC framework has ETs of 9.2 seconds. For 500 Patient's data, ADC's ET is 36 seconds, whereas the ETs for HSCS is 46 seconds. The ET is typically quantified in terms of "seconds". When more attributes are added, the ET rises. When compared to the existing BC framework, the ET of the proposed ADC framework is more advantageous.

(iv) Decryption Time:

The DT is measured in seconds, or the amount of time it takes for a given technique for decrypting a file using a given secret-key. This does not consider the time spent processing "Input/Output (IO)" files.

Table 5: Decryption Time

Average Patient's Data	BC	ADC
100	10.2	8.2
200	20.4	16.4
300	30.6	24.6

400	40.8	32.8
500	51	42

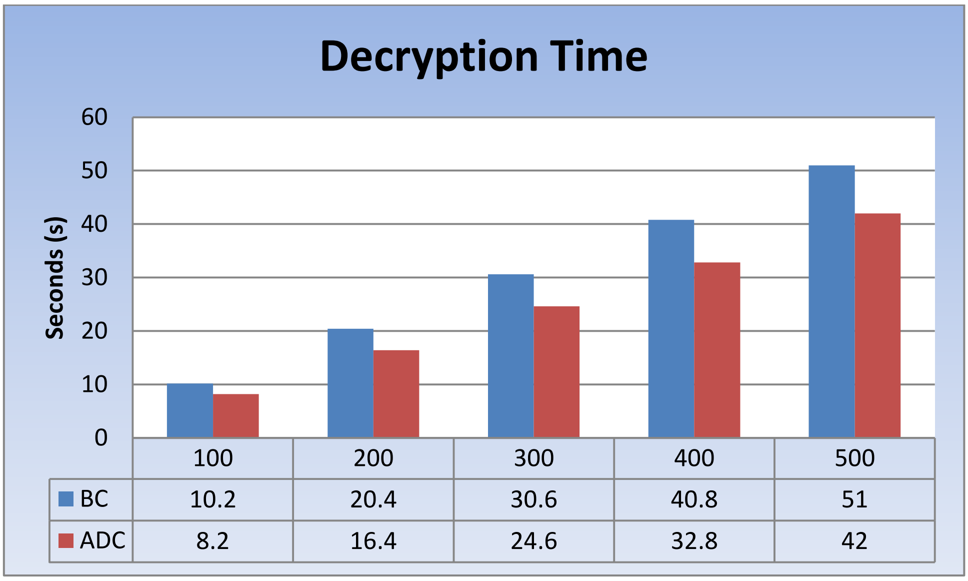


Figure 8: Decryption Time

As shown in Table 5 and Figure 8, the proposed ADC framework, together with the existing BC framework, was compared for DT calculations. Overall Patient's Data attribute variability inside the DT has been examined. Patient's Data contributions would vary between 100 and 500. It shows that the proposed ADC framework has an initial DT of 8.2 seconds for 100 Patient's Data, whereas the existing BC framework has DTs of 10.2 seconds. For 500 Patient's Data, ADC's DT is 42 seconds, whereas the DTs for BC is 51 seconds. The DT is typically quantified in terms of "seconds". When more Patient Data are added, the DT rises. When compared to the existing BC framework, the DT of the proposed ADC framework is more advantageous.

5. CONCLUSION

WBANs are considered for both medical and non-medical applications. But, implanted WBANs are mostly employed for medical and healthcare applications due to the constraints in security, ultra-low power consumption, long battery lifetime and high bandwidth. Reduced reaction time for evaluating patients' health records with reduced consumption of energy and improved security when accessing the system on WBANs has been a primary goal of the proposed ADC framework. An effective ADC framework methodology has been developed to provide highly protected distant monitoring of health operations in WBANs. An ADC framework has been developed using an encryption/decryption technique to achieve safe smart health observation solutions. By using an ADK cryptographic key, sensitive patient information within WBANs, such as the patient's medical record, could be handled privately and protected. The decryption at the recipient side is done using the same ADK key for extracting the data that is being encrypted. It has been shown that the proposed framework, which incorporates an ADC with PAP and IPAP, significantly reduces the consumption of energy by WBANs during communication. The performance comparison based on the

"Security Ratio", "Energy Consumption Ratio", "Encryption Time" and "Decryption Time" is done for both the existing BC and proposed ADC frameworks. From this, it is inferred that the ADC framework exhibits higher security with more accuracy when compared to the BC framework. In the future, it can be enhanced for the advanced algorithm to increase the security ratio with lesser encryption/decryption time.

REFERENCES

[1] Abidi, B.; Jilbab, A.; El Haziti, M. Optimization of energy consumption with the gateway nodes in wireless sensor networks. Int. J. Sens. Wirel. Commun. Control 2017, 7, 152–160.

[2] Arif, A.; Zubair, M.; Ali, M.; Khan, M.U.; Mehmood, M.Q. A compact, low-profle fractal antenna for wearable on-body WBAN applications. IEEE Antennas Wirel. Propag. Lett. 2019, 18, 981–985.

[3] Ullah, F.; Khan, M.Z.; Mehmood, G.; Qureshi, M.S.; Fayaz, M. Energy Efficiency and Reliability Considerations in Wireless Body Area Networks: A Survey. Comput. Math. Methods Med. 2022, 2022, 1090131.

[4] Sobin, C.C. A survey on architecture, protocols and challenges in IoT. Wirel. Pers. Commun. 2020, 112, 1383–1429.

[5] Jindal, F.; Jamar, R.; Churi, P. Future and challenges of internet of things. Int. J. Comput. Sci. Inf. Technol. 2018, 10, 13–25.

[6] Punj, R.; Kumar, R. Technological aspects of WBANs for health monitoring: A comprehensive review. Wireless Netw. 2019, 25, 1125–1157.

[7] Sharma, A.; Kumar, R. A constrained framework for context–aware remote E–healthcare (CARE) services. Trans. Emerg.Telecommun. Technol. 2019, e3649.

[8] Fotouhi, M.; Bayat, M.; Das, A.K.; Far, H.A.; Pournaghi, S.M.; Doostari, M.A. A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. Comput. Netw. 2020, 177, 107333.

[9] Chen, K.; Lu, X.; Chen, R.; Liu, J. Wireless wearable biosensor smart physiological monitoring system for risk avoidance and rescue. Math. Biosci. Eng. 2022, 19, 1496–1514.

[10] P. Anitha., & Dr. R. Priya. (2022). A Technical Aspect of WBAN Security Protocols and Their Challenges: Brief Survey. Neuroquantology, 20(8), 9029–9040. Retrieved July 2022, from https://www.neuroquantology.com/.

[11] Prameela, P. Enhanced Certificateless Security Improved Anonymous Access Control with Obfuscated QualityAware Confidential Data Discovery and Dissemination Protocol in WBAN. Int. J. Pure Appl. Math. 2018, 118, 2627–2635.

[12] Omala, A.A.; Ali, I.; Li, F. Heterogeneous signcryption with keyword search for wireless body area network. Secur. Priv. 2018, 1, e25.

[13] Iqbal, J.; Umar, A.I.; Amin, N.; Waheed, A. Efficient and secure attribute-based heterogeneous online/offline signcryption for body sensor networks based on blockchain. Int. J. Distrib. Sens. Netw. 2019, 15, 1550147719875654.

[14] Xiong, H.; Hou, Y.; Huang, X.; Zhao, Y.; Chen, C.M. Heterogeneous Signcryption Scheme from IBC to PKI With Equality Test for WBANs. IEEE Syst. J. 2021, 1–10.

[15] Noor, F.; Kordy, T.A.; Alkhodre, A.B.; Benrhouma, O.; Nadeem, A.; Alzahrani, A. SecuringWireless Body Area Network with Efficient Secure Channel Free and Anonymous Certificateless Signcryption. Wirel. Commun. Mob. Comput. 2021, 2021, 5986469.

[16] L. Xiao, D. Han, X. Meng, W. Liang and K. -C. Li, "A Secure Framework for Data Sharing in Private Blockchain-Based WBANs," in IEEE Access, vol. 8, pp. 153956-153968, 2020, DOI: 10.1109/ACCESS.2020.3018119.