SECURE WIRELESS SENSOR DATA TRANSMISSION AND STORAGE WITH NOVEL MODIFIED DH-ECC ALGORITHM

P. Lokesh Kumar Reddy[1], B. Rama Bhupal Reddy[2], S. Rama Krishna[3]
[1]Research Scholar, Dept of Computer Science, Rayalaseema University, Kurnool, AP, India,
[2]Dept of Mathematics, K.S.R.M. College of Engineering (Autonomous), Kadapa, AP, India,
[3]Dept of Computer Science, S.V. University, Tirupati, AP, India,

Abstract

Wireless Body Area Networks (WBANs) is an emergent technology has offered many contributions in healthcare applications such as therapeutic levels, monitoring, and the diagnosing. But, WBANs facades numerous problems while transmitting the patient health records such as security issues, less efficiency, high communication problems in encryption and decryption. To overcome these mentioned issues, proposed a Certificate-less Group Key Management scheme with Anonymization (CGKMA) system. In this paper, three different modes are performed to secure the patient health information. The patient health information is split into two forms such as personal information and sensor information. Primarily, the sensor data is secured with the help key pairing algorithm with the cryptographic algorithms like a Novel Modified Diffie Hellman with the Elliptic Curve Cryptography (NM-DHECC) algorithm. Then develop an efficient group key management scheme to validate the user with provide an authenticated access by utilizing the Advance Encryption Standard (AES) algorithm the Novel Shamir Secret Sharing (NSSS) technique. Secondarily, the patient personal information is preserved with the Novel Anonymization Algorithm (NAA) to generalize and suppress the data. This rule is produce the authenticate user can only access the information otherwise can't access the data. The proposed CGKMA system performance analysis is compared with the existing cryptographic techniques in terms of key agreement, security level, security strength, execution time, encryption/decryption time, and the outsourcing time. Hence, the proposed CGKMA system outperforms than other techniques.

Index Terms: Certificate-less, Group Key Management, Anonymization system, Key Pairing, Wireless Body Area Networks.

I. INTRODUCTION

The expanding utilization of wireless networks and the steady scaling down of electrical gadgets has enabled the advancement of Wireless Body Area Networks (WBANs)[1, 2]. In these systems, different sensors are connected on garments or on the body or even embedded under the skin. The remote idea of the system and the wide assortment of sensors which proposition of various new, down to earth and imaginative applications to enhance human health care and the Quality of Life. The sensors of a WBAN that estimate the following functions such as the body temperature, heartbeat, record a prolonged electrocardiogram. Utilizing a WBAN, the patient encounters a more prominent physical versatility and is never again constrained to remain in the doctor's facility. But it have produced issues such as coexistence issues, impacts of the radio channel, energy consumption issues[3]. In WBANs, the healthcare application produces a various security and privacy issues. In this survey discuss the WBAN communication architecture and its applications over security threats. The major requirements of the security and the privacy are the major drawbacks in this scenario. Fig.1 represents the WBAN architecture.

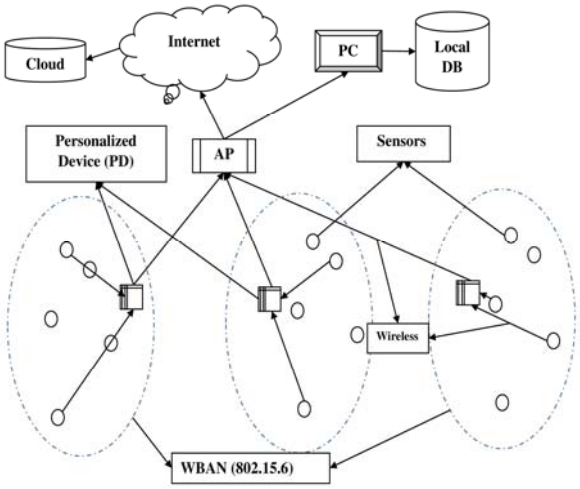

Fig. 1 WBAN Architecture

Hence, effective key management system [4] is needed for securing the transmission in the WSN. The CL-EKM protocol is needed to secure the communication process. They utilized four different categories of secrets such as certificate less public/private, pair wise, individual node, and the cluster key are supported with the CL-EKM. The Contiki OS are mainly secondhand to implement the CL-EKM approach and evaluate the overhead issue of communication, energy consumption, and the computation by a TI exp5438 emulator. In that grid, the Random Walk Mobility and the Manhattan Mobility Model is employed to simulate the node movement. The major problems in key management are the fraudulent certificates and the certificate revocations. Therefore, used the Twin Peaks infrastructure [5]for provided that the public secrets to the entire entitled individuals. If any changes occur in the public information then spontaneously change the public key itself. The main objective of this work is to remove the impersonation attack and can change/comprised the public and the public key data. And also develop the DNS-like hierarchical structure of public key servers to removes the CA hierarchy in the Twin Peaks.

A. Objectives

- To design an effective key pairing algorithm with provable security of the patient sensor data by using the Novel Modified Diffie Hellman with ECC (NM-DHECC) algorithm.
- To develop an efficient group key management scheme with authenticated access for the registered user by utilizing the AES with Shamir Secret Sharing technique.
- To apply a privacy preserving procedure in a patient personal information for securing the personal data with the help of Novel Anonymization Algorithm (NAA).

B. Organization of Paper

The remaining section of this paper is prearranged as monitors: the brief description about the existing methods and the security weakness are explained in Section II. The implementation details of the proposed certificate-less group key management with Anonymization system is discussed in Section III. The overall performance results and the various tests of the proposed system is showed in Section IV. Finally, concludes the proposed work in Section V.

II. LITERATURE SURVEY

This literature survey part discusses the various existing techniques and their limitations. The assessment of secure storage and transmission of patient's medical data, which demands to demonstrate some problems were surveyed in the following sections. Surveyed the concept of WBANs and its issues. The main objective of this survey is to monitor the patient health records and transmission over data with security. They discussed the different technologies position that related to the WBAN communication and considered some scenarios: existing MAC, network protocols, physical layer, quality of service, and the cross layer. Finally, explained the WBANs research issues and the challenges. Utilized the attribute based encryption (ABE) to securely share and scalable of personal health records in the cloud computing. They called a novel framework as ABE based PHR sharing with minimal key management overhead. Then, established a multi-authority ABE (MA-ABE) technique in the public domain for avoiding key escrow problem and improving the security predictions. In the personal domain, the enriched MA-ABE with on-demand user/attribute annulment scheme was employed to provide the packed privacy control completed their PHRs.

But, the security protection issue was to be improved in furthermore process. *Ramli, et al.* [8] Recommended the biometric based security

system framework for authenticating the data in the WBAN. The computational complexity and the power efficiency were reduced and secured the data communication was the major requirement scenarios in the biometric characteristics. Thus, the recommended framework explored the human body unique features to authenticate the identity. *Belsis and Pantziou* [9]Presented the k-anonymity based privacy-preserving technique for preserving the patient information. The effective data aggregation and the network management was produced the user's privacy by utilized the clustering based anonymity scheme. Thus, the security was the necessary thing to improve in further more process. *Tirthani and Ganesan* [10] suggested a Diffie Hellman and Elliptical Curve Cryptography (ECC) techniques for providing security to the cloud architecture. The main intention of this work was to ensure the secure movement of data at both client and server side.

Moreover, this work includes the following stages: construction establishment, account formation, authentication, and data exchange. It was observed that the speed of data access was affected due to the complexity of the algorithm. However, this paper failed to prove the effectiveness of the suggested technique by comparing it with other architectures. Suggested a Chinese Remainder Theorem (CRT) and hash function based cryptographic techniques for providing privacy preservation to the cloud data. The main focus of this research work was to reduce the storage overhead, communication, and computational complexity. This work includes three phases that include: data sending, request sending, key sharing, and auditing. In this framework, the data owner has performed the data auditing process. From this, it was analyzed that the CRT provided a secure privacy preservation with an efficient calculation.*Zhou, et al.* [12] provided the privacy-preserving key management pattern and the protected m-healthcare social networks based on the cloud-assisted WBANs. This scheme was integrated the similar social group with the collaboration of the mobile patients between the distributed and the hierarchical location. In that scenario, the resistant among the location and the time-based mobile assaults were surveyed. From the human body's symmetric construction and the blinding technique were implanted to proclaim the procedure of Blom's symmetric key with modified pre-emptive secret distribution that mainly used to protect the privacy of sensor deployment, patient's identity, and the location. Afterwards, the energy-constrained WBANs resources was saved and updated the cloud server privacy-preserving key material.

Furthermore, the medical data integrity was the most important issues. *He, et al.* [13] recommended the efficient certificateless public auditing (CLPA) scheme for checking the stored data integrity in the cloud-assisted WBANs. In this work, the key escrow problems and the key management issues were mainly concentrated. This scheme reviewed the double challenges categories are as follows:

- Substituted the users' public secrets in the type-I challenge
- Accessed the master key in the type-II adversary

Further, privacy was majorly rigorous term to be concentrate. *Li, et al.* [14] presented the certificateless public auditing scheme with multi-user data sharing and privacy preserving for the cloud based WBAN. It also supported the function of multi-user sharing cloud stored data and the third party's public verification. They dynamically join and leave the group. Henceforth, protected the forward security and cancelled the illegal users. Offered the new anonymous authentication (AA) method for WBANsto improve the security. In this method, three main analyses has been performed as: the new AA schemes was employed to avoid various attacks nevertheless it couldn't suitable for the impersonation attack, reduced computation burden, and performed the in-depth security analysis. In this case, the security was the major drawbacks.

III. PROBLEM IDENTIFICATION

Security is a standout amongst the most vital issues in numerous basic dynamic WSN applications. Dynamic WSNs consequently want to report key security necessities, for example, hub confirmation, information classification and trustworthiness, at whatever point and wherever the hubs move. In a traditional framework strategies utilized the symmetric key encryption and asymmetric key based methodologies have been projected for the dynamic WSNs. Asymmetric key based methodologies found the security shortcomings of an existing ECC-based

methods that these methodologies are powerless against message fraud, key bargain and the known-key assaults. Likewise, they investigated the basic security imperfections of that the static private key is presented to the next when the two hubs set up the session key. Also, these ECC-based methods with certificates when straightforwardly connected to the dynamic WSNs, that experiences the endorsement administration overhead of all the sensor hubs as are not a commonsense application for vast scale WSNs. The matching operation based ID-PKC [16]method are a wasteful because of the computational overhead to pair operations.

A. Issues

- Symmetric key encryption experiences high correspondence overhead and requires extensive memory space to store shared pair wise keys. Additionally, it was not adaptable and versatile against bargains, and unfit to help hub portability. Thus, the symmetric key encryption wasn't reasonable for dynamic WSNs.
- Asymmetric key based methodologies that experiences ill effects of the authentication administration overhead of the whole sensor data as that never used in the practical application for vast scale WSNs.
- Sensor gadgets are helpless against malignant assaults, for example, pantomime, and block attempt, catch or physical demolition because of their unattended agent conditions and passes of network in remote correspondence.

IV. PROPOSED WORK

This section discusses the implementation process of the proposed Certificate-less Group Key Management with Anonymization (CGKMA) system for securing the patients personal health records while transmitting the data. Fig. 2 represents the overall workflow of the proposed system.

Initially, load the patient personal details with the corresponding sensor information in the cloud storage based on the cryptographic technique. If can access the stored database from the cloud by using the Novel Modified Diffie Hellman (NMDH) algorithm to generate the secret key and shares that key from patient to the base station. After that, the patient personal information have loaded with the help of Novel Anonymization Algorithm (NAA) to hide the personal information for securing the health records. Then, the results of anonymized data are stored in the cloud service provider (CSP). Generate the sensor information from the WBAN and then split into three forms such as sen1, sen2, and the sen3. These categorized sensor details is stored in the base station by using one of the cryptographic technique as Novel Modified Elliptic Curve Cryptography (NMECC) technique. After decrypt the encrypted data with the NMECC technique to store the data in the Medical Information System (MIS). If the requestor send request to MIS, the required system to validate the authentication and then accept the request. If not means, then skip the process automatically.

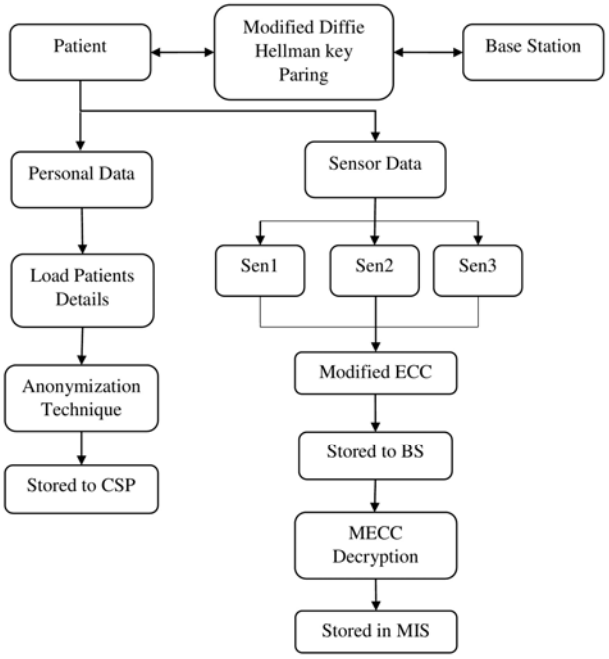

Fig. 2 Workflow of the proposed work

Table I presents the different symbols used in the proposed algorithm.

TABLE I
SYMBOLS AND DESCRIPTIONS

List of Symbols	Description
N	Size of the alphabetic attributes
In_{str}	Input String
Ch_{inp}	Set of characters
x	Public key
s	Secret key

A. Generation of Sensor Information

In the proposed system, the basic idea is given as follows. After registering the user to the network server, he/she will allowed to access the collected personal health details or otherwise reject the file access. If verifying his/her registration information, the network server assigns an individual patient identity details. The patient sensor details collects from the input dataset and create a secret generation for accessing the files securely. The patient chooses to give an authority to a specific user to access his/her medical records on the cloud at any time. This process is done by pairing the secret keys of both into the key access management scheme. This is expected to be done at the time registration of patient details. A Novel Modified Diffie Hellman (NMDH) algorithm is employed to generate a secret key and pair them between the patient and the base station. The proposed NMDH algorithm, assigns the two different random value (i.e., $p\ and\ g$) for estimating the secret value of both the patient and the base station (BS). Fig. 3 represents the proposed NMDH algorithm key pairing.

Initially, setting an individual secret key value (i.e., $a\ and\ b$) for both patient and the BS. Then, to find the public key value of x as,

$$x = (int)g^a \quad (1)$$

If $int = x_1$

Thus,

$$x_1 = x\ mod\ p; \quad (2)$$

Therefore, the predicted integer value ofx_1 asthe required secret value of the patient. Secondarily, the same procedure is followed as to calculate the BS value as,

$$y = (int)g^b \quad (3)$$

If $int = y_1$

Thus, the equation be

$$y_1 = y\ mod\ p; \quad (4)$$

Therefore, the BS secret key value is obtained from $Y_1$and then pairing the secret value to one another. In the patient side, the secret key value are received from the BS as y_1. Then, estimate the individual secret a_1 as,

$$a_1 = (int)d^{y_1} \quad (5)$$

And predict the common secret value of patient as,

$$s_1 = a_1\ mod\ p \quad (6)$$

In the BS section, receive the secret key $x_1$from the Patient side andderive the individual secret of b_1 as,

$$b_1 = (int)e^{x_1} \quad (7)$$

Afterwards derive the common secret key as,

$$s_2 = b_1\ mod\ p \quad (8)$$

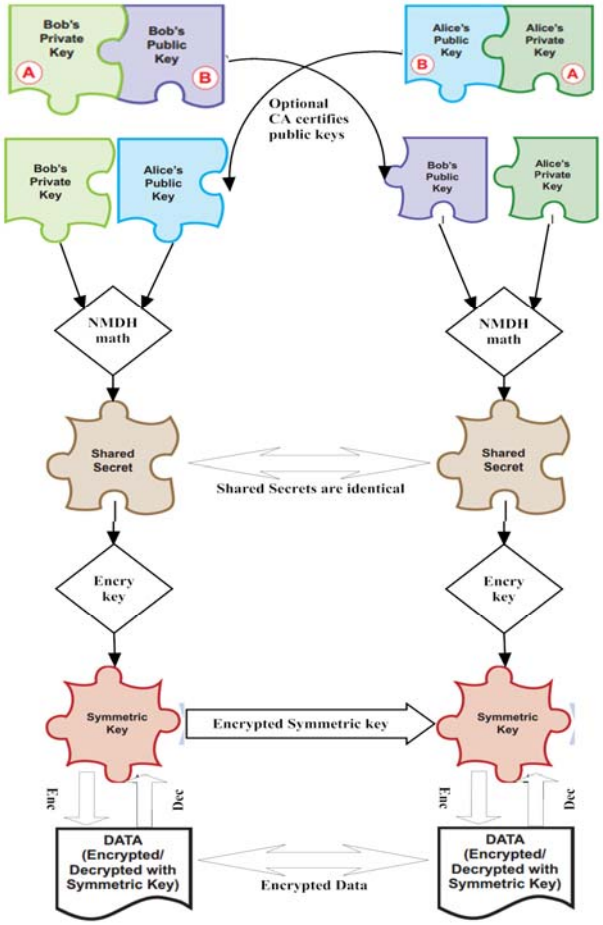

Fig. 3 NMDH Key Pairing

By running the scientific operation against your own private key and the opposite side's public key, to create an esteem. The proposed NMDH convention produces a "common secret"– an indistinguishable cryptographic key shared by each side of the correspondence. The proposed NMDH algorithm is as follows:

NovelModified Diffie Hellman Algorithm
Input *: p=23; &g=9;* ***Output :*** *Secret Key for Patient and Base Station;*
Step 1*: find the patient secret key* ***Step 2****: Assign a=4;* ***Step 3****: find x using the equation (1);* *using if condition;* *Estimate the x_1 using equation (2);* ***Step 4****: Compute the secret key;* ***Step 5****: Secret Key for Patient;* *Secret key =x_1;* *x_1=6;* ***Step 6****: Find Base station key value;* ***Step 7****: Assign b=3;*

***Step 8**: Find public key y using the equation (3);*
***Step 9**: using if condition;*
Compute y_1 using equation (4);
***Step 10**: Estimate the secret value;*
Base Station Secret key = y_1;
y_1=16;
***Step 11**: Perform Key Pairing process*
From patient side;
Computea_1 using equation (5)
Find the common keys$_1$ using equation (6);
s_1=9;
***Step 12**: From the Base Station side;*
Find$b_1$using the equation (7);
Find the common secret key using the equation (8);
s_2=9;

At the point when the inaccessible end runs a similar operation against your public key and its own particular private key, that end likewise produces an esteem. The essential point is that the two esteems created are indistinguishable. They are the "shared secret" that can encode the data between frameworks in view of the NMECC cryptographic procedures. The common secret at that point encodes the symmetric key for secure transmittal. The sensor information of the patient and the secret key are the required source of NMECC technique. In this system, the original sensor information is converted into cipher information based on NMECC encryption and then converts into original text based on NMECC decryption model. Initially, derive the public key as,

$$Pub_{(key)} = Pvt_{(key)} * \mathrm{p} \quad (9)$$

Then, estimate the cipher text of the patient sensor information as,

$$Cipher_{(f)} = SecKey_{(k)} * \mathrm{p} \quad (10)$$

After that, establish the ASCII code for the converted cipher text by using the equation as,

$$ASCII = (length)\ of\ Ch_{(f)} \quad (11)$$

And also predict the cipher text of the key value is calculated as,

$$Cipher_{(f)} = SecKey_{(k)} * Pub_{(key)} \quad (12)$$

Here after, decrypt the cipher text into original sensor information by using corresponding secret key for authenticating the user based on the following equation as,

$$Str_{(d)} = (\mathrm{int})Ch_{(f)} \quad (13)$$

The total number of integer and the characters of the sensor information file is the input to derive the string of the decryption characters. Then, estimate the corresponding ASCII code of the integer value as,

$$Ascii_j = Str_{(d)} - (Pvt_{(key)} * Cipher_{(f)}); \quad (14)$$

After that, estimate the characters of ASCII code and finally establish the original sensor data details. The proposed NMECC algorithm is shows below,

Novel Modified ECC Algorithm

***Input** : keys, file*
***Output :** Cypher text*

***Step 1**: Consider patient sensor information f;*
***Step 2**: read Chfrom the file f;*
$Ch_{(f)}$
***Step 3**:* Initialize$Pvt_{(key)}, Pub_{(key)}$;
***Step 4**:* Initialize the value $int\ (p)$ and$SecKey_{(k)}$;
***Step 5**: Compute public key using the equation* (9);
***Step 6:** find the $Cipher_{(f)}$ using equation* (10);
***Step 7**:* find ASCII of$Cipher_{(f)}$ using equation (11);
***Step 8**: Compute the cipher text secret key using the equation* (12);
***Step 9**:* Consider a string which is be in decryption using equation (13);
***Step 10**:* Find the ASCII code of integer value using the equation (14);
***Step 11**:* find the $Ch_{(ascii)}$;
***Step 9**:* end Ch_f;
***Step 10**: Cipher text*

B. Group key Management

The certificate less effective key management technique is evolved in this proposed work based on the AES algorithm with the Novel Shamir Secret Sharing algorithm. The proposed AES Encryption, patient who needs to register his file in the cloud would prefer to keep his file secured; it is done by using the AES Encryption method. The file to be uploaded must be selected for which a key is generated in an affine matrix and the concerned file is generated as our codes to be encrypted. Our file is then generated and encrypted using Random S -box. The modified S-box tends to provide higher security to the encrypted file. The encrypted file with a secured key is uploaded in the cloud again. Then, the secret key is secured with the help of NSSS algorithm. If the user needs a specific patient records then he/she request to a Medical Information System (MIS). Then, the requestor gets 2 secret key from MIS and single secret key

value from the patient. When the secret to being reconstructed, the requested user gets the corresponding file from the MIS, which can combine the shares and retrieves the secret. Fig. 4 represents the GKM process flow.

In the group, the data owners request to upload the data in the cloud have needed the secret key to encrypt the data and then upload it. Then, the corresponding group users can receive the permission to access the encrypted file. If the new user joins the group will be given as a share for the authentication purpose which will be constructed by using the NSSS technique. While registering the user into the group, a share is generated for each user by the NSSS generator and given to the corresponding user. Then, the data owners will encrypt the data with the secret key and data owner will send the authorities who will validate the user for the data access.

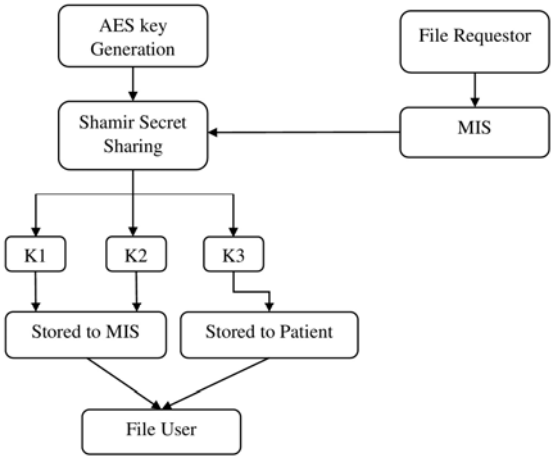

Fig. 4 Group Key Management process flow

First of all, generate the total number of secret shares based on the key length as,

$s = " ******* ";$ (15)

Here after, the secret keys are splitted into n no of sub parts. Thus, the secret value is assigned with the random integer and also the prime integer. The mathematical form of assumption is to follows:

$$Int_j = \sum_{k=0}^{n} \binom{n}{k} s^k a^{n-k} \quad (16)$$

After predicting the random integer then split the secret value into three shares. The first share and second secret as follows,

$Skey_1 = \sum_{k=0}^{1}(s1)Ran_n;$ (17)

$Skey_2 = \sum_{k=0}^{1}(s2)Ran_n$ (18)

This secret share 1 & 2 is generated by the MIS of the hospital and again generate the third secret as,

$Skey_3 = \sum_{k=0}^{1}(s3)Ran_n$ (19)

Hence, the secret share 3 is generated by the patient. Then, the summation of the three predicted shares as,

$s = Skey_1 + Skey_2 + Skey_3$ (20)

Thus,

$s = \sum_{k=0}^{1}(s1)Ran_n + \sum_{k=0}^{1}(s2)Ran_n + \sum_{k=0}^{1}(s3)Ran_n$ (21)

After getting the overall secret key value and then decrypt the Patient original sensor data's.

The proposed NSSS algorithm is shown below.

Novel Shamir Secret Sharing
Input : *Patient sensor details, secret key, consider certainty = " ";* ***Output :*** s1, s2, s3;
Step 1*: Generate secret key shares using the equation* (15)*;* ***Step 2****: Assign n=3;* ***Step 3****: Generate the secret value of random integer as* Ran_n; ***Step 4:*** Find the larger integer Int_a ; ***Step 5****: Compute the prime integer using the equation* (16); ***Step 6****:* Spit the Secret share into three shares; ***Step 7:*** Find the first share $Skey_1$ using the equation (17); ***Step 8****:* Find share $Skey_2$ using the equation (18); ***Step 9****:*Find share $Skey_3$ using the equation (19); ***Step10****:* Get Secret Keys from the three shares using equation (20); ***Step 11****: Compute the overall shares using equation* (21); ***Step 12****:* Established the overall shares of *s*;

C. Pricy Preservation Rule

The privacy preservation rule is used to preserve the patient personal information. It is protected with the help of NA algorithm. The NA algorithm can be performed by two processes such as generalization and suppression. Primarily, generalization is the process of altering the inducement to a low specific common series. For ex, "Male" and "Female" can be generalized to "Any". At the accompanying levels generalization procedures can be connected. It is performed under attribute and cell based generalization. Secondarily,

suppression is performed that contains avoidance elusive data through leaving process. It can be associate with the whole tuple or entire segment, level of single cell, and certificates weakening the measure of speculation to be forced to accomplish k-anonymity.

Initializing the patient personal information that consists of alphabetic, and the numeric values. The list of attributes which are represent in terms of alphabetic like name, address, mail Id and the list of attributes which are represent in terms of numeric such as phone no, age, date of birth. Primarily, consider the alphabetic values and initialize the string. Then, convert the input string into a set of characters as,

$$Ch_{inp} = \text{char}\ (In_{Str}) \quad (22)$$

After, estimating the set of characters and verify all the characters in the personal data then changed into ASII code format. The ASII code conversion equation as,

$$Ascii_j = \text{Ascii}(Ch_j)\ + 10 \quad (23)$$

Then, establish the ASII code for the secret key value and the characters as,

$$Ascii_k = \text{int}(Ascii_k) \quad (24)$$

$$Ascii_k = (\text{int})Ascii_{(Ch)} \quad (25)$$

Finally, predict the anonymized data for securing the personal information. If only authentication user can de-anonymized the data and can efficiently use the personal information otherwise can't retrieve the original information. The proposed NAA procedure is as follows:

Novel Anonymization Algorithm

Input : *Patient Personal details i.e. (Name, Age, etc…)*
Output : *Anonymized Information*

Step 1*: Consider alphabetic*
Step 2*: for* $i = 1: N$
Step 3*: Assign* In_{Str}=Atr_i
Step 4*: Convert the String to a set of characters using equation (22);*
Step 3*: for* $j = 1: size\ (Ch_{inp})$
Step 4*: Compute the* $Ascii_j$*from using equation (23);*
Step 5*: for k=1: size (*$Ascii_j$*)*
Step 6*:Compute the* $Ascii_k$*from using equation (24);*
Step 7*: find ASCII value of k name:*
Step 8*: Compute the* $Ascii_k$*from using equation (25);*
Step 9*: Then Convert the set of Char into string;*
Step 10*: for* $p = 1;\ length\ (Ascii_k)$*;*
Step 11*: End for p;*
Step 12*: Anonymized Data*

V. PERFORMANCE ANALYSIS

This section discusses the effectiveness of proposed system by comparing with the existing key agreement[5], key management [4]methodologies, and the privacy preservation[17] techniques in terms of key generation time, security evaluation, execution time, and the strength of security. The sensor dataset to validate the proposed system efficiency in secure manure regarding the authentication.

A. Key Agreement versus Time

The key agreement is defined as the total time taken for generating a secret key that must satisfies the key confirmation. If one of the party is guaranteed that all other parties actually have proprietorship of a specific secret key. Table II represents the different algorithm key agreement time

TABLE II
KEY AGREEMENT TIME

Methods	**Key generation time (ms)**
ECDH	108
RSA	889
DH	87
NM(DH-ECC)	57

From the table, clearly shows that the proposed (DH-ECC) algorithm is compared with the existing DH, ECDH, and the RSA cryptographic techniques. The proposed algorithm produces lower generation time in terms of milli seconds. The proposed algorithm nearly 30% improvements than the existing DH algorithm. Hence, it is outperforms than other techniques.

B. Security Level versus Time

The security level is defined as the give protection against the attacks that affects the patient personal information. The security level is compared with the time in milli seconds. Fig. 5 represents the security level versus time measurement.

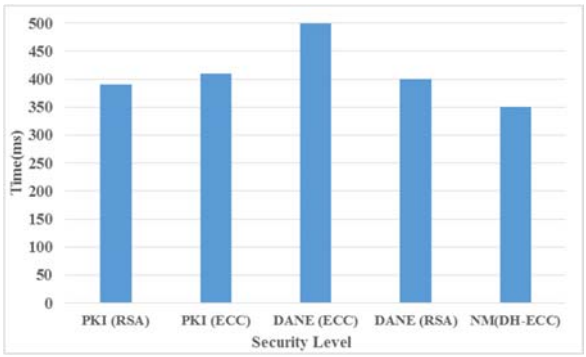

Fig. 5 Security Level

From the graph, it clearly observed that the proposed NM (DH-ECC) algorithm is compared with the existing PKI (ECC), PKI (RSA), DANE (ECC), and the DANE (RSA) algorithm. The proposed NM (DH-ECC) algorithm security level develops stronger than other, meanwhile the networking expectancies yields a substantial percentage. Therefore, the proposed NM (DH-ECC) represents the lower delay time when compared to the existing techniques. Hence, the proposed NM (DH-ECC) algorithm produced the minimal key setup time as 350ms.

C. Security Strength

The security strength is defined as the number of operations performed in an accompanying way to reject the cryptographic security system. The numbers of bits are taken for considerations as a set of {80, 112, 128, 192, and 256}. Table III represents the security strength comparison.

TABLE III
SECURITY STRENGTH COMPARISON

Methods	**Integer Factorization Cryptography**	**Size of extension field**	**Size of Bits**
AES	1024	2048	7680
DH	1024	2048	7680
NMECC	106	224	256

From the table, illustrates that the proposed system security strength is compared with the number of bits taken. The security strength of the existing AES, DHand the proposed NMECC is compared. Therefore, the proposed system key size is lower than the existing systems.

D. Encryption / Decryption Time

The encryption and decryption time is the process of calculating the total time taken for the conversion of original text into cipher text as well as cipher text into original text format. Fig. 6 represents the encryption or decryption time.

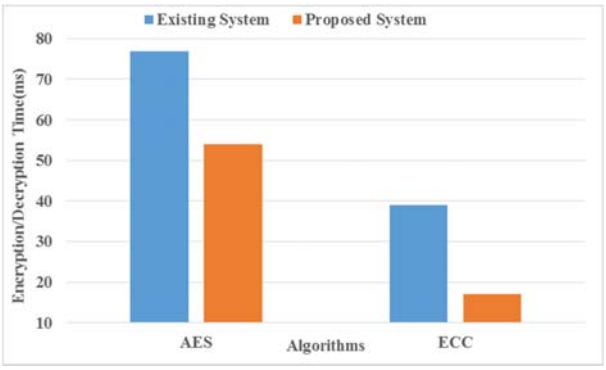

Fig. 6 Encryption / Decryption Time

The graphical representation of the proposed system encryption/decryption time is compared with the existing system. The comparison between existing and the proposed work describes that the proposed system takes lower time for encrypting or decrypting the text. Hence, the proposed system outperforms than the existing methods.

E. Outsourcing Time

The outsourcing time is defined as the total time taken for completing the overall process. It shows the efficacy of the proposed system. Fig. 7 represents the outsourcing time measured in milli seconds.

The graphical representation of the outsourcing time is the comparison diagram of the traditional with the proposed system.The proposed system produces the minimal outsourcing time than the existing system. Hence, the proposed system takes lower delivery time and it outperforms than the existing methods.

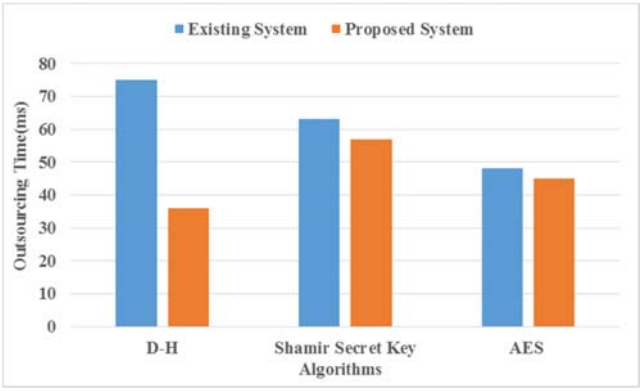

Fig. 7 Outsourcing Time

F. Execution Time

The execution time is defined as the total time taken for completing the task and it measured in terms of milli seconds. Fig. 8 represents the overall execution time.

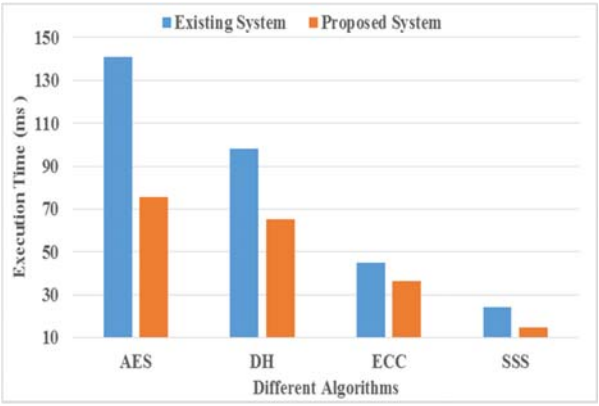

Fig. 8 Execution Time

From the graph shows that the proposed algorithms overall execution time. The proposed system utilized algorithms such as AES, DH, ECC and the SSS algorithms are produces 75.52ms, 65ms, 36.25ms, and the 14.56ms respectively. Hence, the proposed system outperforms than the existing methods.

VI. CONCLUSION

In this article, the Certificate-less Group Key Management scheme with Anonymization (CGKMA) system is utilized to secure the patient health information. Initially, the patient health information is in two forms such as medical sensor data and the personal data. The patient personal data is secured with the Novel Anonymization Algorithm (NAA) to effectively preserve the information. If the registered user only can de-anonymized the anonymized data and the patient medical sensor data is secured with the help of Novel Modified Diffie Hellman with the Elliptic Curve Cryptography (NM-DHECC) algorithm. A Novel Modified Diffie Hellman algorithm is used to pairing the secret key between the patient and the base station. A NMECC is utilized to encrypt and decrypt the sensor information and is preserved by an AES algorithm. Then, utilized the Novel Shamir Secret Sharing (NSSS) model to share the key with a provable security manure. Hence, the proposed system is compared with numerous existing cryptographic techniques in terms of key agreement, security level, security strength, execution time, encryption/decryption time, and the outsourcing time. Thus, it achieves greater performance than the existing methods.

REFERENCES

[1] V. Mainanwal, M. Gupta, and S. K. Upadhayay, "A survey on wireless body area network: Security technology and its design methodology issue," in *Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on*, 2015, pp. 1-5.

[2] R. Cavallari, F. Martelli, R. Rosini, C. Buratti, and R. Verdone, "A survey on wireless body area networks: Technologies and design challenges," *IEEE Communications Surveys & Tutorials*, vol. 16, pp. 1635-1657, 2014.

[3] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, pp. 1658-1686, 2014.

[4] S.-H. Seo, J. Won, S. Sultana, and E. Bertino, "Effective key management in dynamic wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, pp. 371-383, 2015.

[5] E. Cho, M. Park, and T. Kwon, "TwinPeaks: A new approach for certificateless public key distribution," in *Communications and Network Security (CNS), 2016 IEEE Conference on*, 2016, pp. 10-18.

[6] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wireless Networks*, vol. 17, pp. 1-18, 2011.

[7] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE transactions on parallel and distributed systems*, vol. 24, pp. 131-143, 2013.

[8] S. N. Ramli, R. Ahmad, M. F. Abdollah, and E. Dutkiewicz, "A biometric-based security for data authentication in wireless body area network (wban)," in *Advanced Communication Technology (ICACT), 2013 15th International Conference on*, 2013, pp. 998-1001.

[9] P. Belsis and G. Pantziou, "A k-anonymity privacy-preserving approach in wireless medical monitoring environments," *Personal and ubiquitous computing*, vol. 18, pp. 61-74, 2014.

[10] N. Tirthani and R. Ganesan, "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography," *IACR Cryptology ePrint Archive*, vol. 2014, p. 49, 2014.

[11] H.-V. Dang, T.-S. Tran, D.-T. Nguyen, T. V. Bui, and D.-T. Nguyen, "Efficient privacy preserving data audit in cloud," in *Advanced Computational Methods for Knowledge Engineering*, ed: Springer, 2015, pp. 185-196.

[12] 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," *Information Sciences*, vol. 314, pp. 255-276, 2015.

[13] D. He, S. Zeadally, and L. Wu, "Certificateless public auditing scheme for cloud-assisted wireless body area networks," *IEEE Systems Journal*, 2015.

[14] S. Li, H. Zhong, and J. Cui, "Public auditing scheme for cloud-based wireless body area network," in *Proceedings of the 9th International Conference on Utility and Cloud Computing*, 2016, pp. 375-381.

[15] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, 2016.

[16] M. Ma, D. He, M. K. Khan, and J. Chen, "Certificateless searchable public key encryption scheme for mobile healthcare system," *Computers & Electrical Engineering*, 2017.

[17] H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren, and A. Alamri, "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility with Pairing-Based Cryptography," *IEEE Access*, 2017.