Security Enhancement Using AES Algorithm for Emergency Situation Detection System

Vidya S.[1] and Deepa T.[2]

[1]Electronics and Communication Department, MGM College of Engineering and Pharmaceutical Science,
Valanchery, Kerala, India

[2]Electronics and Communication Department, MGM College of Engineering and Pharmaceutical Science,
Valanchery, Kerala, India

Abstract

To mitigate the challenge in emergency situation detection and data transmission, this paper proposes a secure data transmission using AES algorithm (Advanced Encryption Standard Algorithm). The transfer of data which were obtained from weak and old age people during emergency situation provides security using AES cryptographic method with the help of Ambient Assisted Living (AAL). AAL is a new concept which assists a person with engaging the day today living as well as working environment and to stay dynamic for longer with the utilization of data and correspondence innovation (ICT). Security of digital information is the fundamental concern in the present time. Particularly when somebody is sending information over the internet there is a risk of data misuse. Cryptography plays an important role in our highly daily life. The principal key arrangement and authentication scheme ensures anonymity and untraceability for both sensors (wearable device) and mobile relay nodes, and depends on symmetric key-based operations to work under resource-constrained conditions. Mobile relay and wearable device are connected using Bluetooth Low Energy (BLE) communication technology. This paper focuses on the code implementation and the encryption and decryption procedure using AES algorithm is provided in detail. Strong security can be provided using the AES cryptographic algorithm.

Keywords: *Ambient assisted living (AAL), Bluetooth Low Energy (BLE), Cryptography, AES algorithm, Information Entropy, Correlation Coefficient.*

1. Introduction

Ongoing advancements in IoT based procedures have made a huge effect on current modern technological applications including continuous (e.g. patients) monitoring and medical services. Weak and elderly people aged have fearful life, due to their unbalanced body: if they fall, they may lie on the floor for hours, until someone comes to know their situation and a doctor is reached. An IoT based system automatically detects dilemmas like this and send information to the responsible person. This facility allows them to live an independent life. Fall may cause fracture and which is the major injury in case if an old man falls down and there is likewise a specific chance to get coma, brain trauma, and paralysis.

Fall detection technologies empower fast detection and intercession for people who have experienced a fall. This could reduce the after effect caused by the fall as well as the time after a fall before disclosure. IoT based techniques enormously affect present day technological applications including consistent monitoring. The improvements in these techniques would be very supportive for older individuals with chronic conditions. The upgrades in these techniques would be extremely supportive for older people with chronic conditions. Often, they should be really taken a look at in view of the checked information on the monitored data.

Progress of technology conveys more possibilities to help us with safeguarding the old. Low power usage parts make it possible to recognize wearable checking gadget. An IoT based arrangement is accommodated the patient to remotely screen. This strategy is cost effective, flexible, mobility supported and power efficient approach to spreading out major areas of strong patient observing. Patients with chronic disease conditions and older individuals can get support from BLE wearable sensors to their wellbeing.

This paper will make sense of how the gathered information can be communicated securely through the environment utilizing AES algorithm. Information security is due to the individual data it carries, the need is much more significant. Thus forward, worries with regards to data protection and security are winding up a limit to the greater take-up of cloud-computing services. To be successful, cloud data security depends upon more than basically applying reasonable information security techniques and countermeasures. PC based security measures generally underwrite with respect to client authorization and confirmation.

Cloud security is a wide subject and mix of strategies, technologies, and controls to protect information, infrastructure and services from possible attacks. Cloud Computing appears as a computational paradigm as well as a circulated design and its major objective is to give secure, rapid, helpful data storage and net computing service, with all computing resources imagined as services and delivered over the Internet.

The essential need of security is the protection of the PC and computerized data from intruders. By mean of security, one can conceal his/her information from irrelevant users. Fig.1 shows the relation among different security principles.

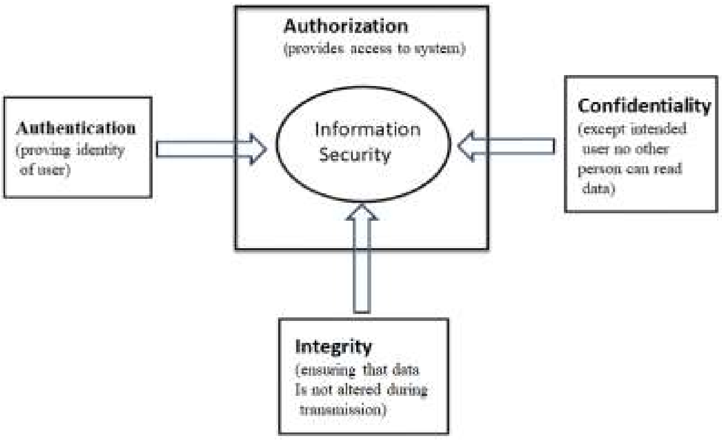
Authorization
(provides access to system)
Authentication
(proving identity of user)
Information Security
Confidentiality
(except intended user no other person can read data)
Integrity
(ensuring that data Is not altered during transmission)

Fig.1 Principles of Security

Cryptography is one of the most common and popular computer-based security mechanisms. The word cryptography comes from Greek words kryptós which means “hidden or secret” and graphein which means “to write or study”. In this way, cryptography can be called as “the study of hidden secrets”.

One method to execute cryptography is "Encryption". Encryption is the process of converting plain text message into some encoded message or cipher text which is in unreadable forms. The cipher text is totally different from the original plain text message. In order to do, encryption, a key and corresponding algorithm is needed. Key has a major part in encryption process. Data security depends on the key strength and how complicated the mechanism to retrieve the plain text from cipher text. It will be easy for the intruder to retrieve data if we use weak keys for encryption.

1.1) TYPES OF CRYPTOGRAPHY

Cryptography is method of securing data and communications through utilization of codes so that only those individual for whom the data is intended can understand it and process it. In Cryptography the methods which are used to protect data are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert original plain text to coded cipher text which is hard to retriever for intruders.

Features of Cryptography are as follows:

- Confidentiality
- Integrity
- Non-repudiation
- Authentication

In general there are three classification of Cryptography:

- Symmetric Key Cryptography (Secret Key)

In Symmetric key Cryptography, sender and receiver use single common key to encrypt and decrypt the message. It is simpler and faster but the issue is that the key needs to be exchanged between the sender and receiver for the encryption and decryption process. The most popular symmetric key cryptographic algorithm is AES.

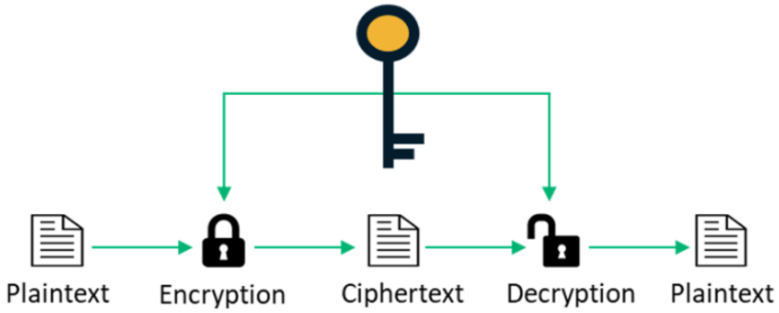

Fig.2 Symmetric Key Encryption/Decryption

- Asymmetric Key Cryptography (Public Key)

Pair of keys is used in asymmetric key cryptography. A public key is used for encryption and a private (Secret) key is used for decryption. Public key is shared with all the parties but private key is provided only to the intended recipient for the decryption process.

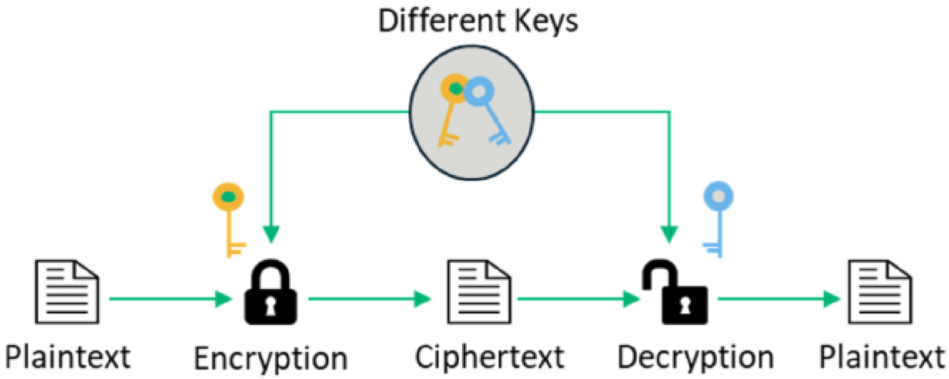

Fig.3 Asymmetric Key Encryption/Decryption

- Hash Functions

In hash function there is no usage of keys. A hash value with a fixed length is calculated according to the original message (plain text), this makes it difficult to recover the original message.

AES algorithm is an example for symmetric key cryptography. It is the more popular and widely used algorithm. AES can be implemented both in software and hardware. It uses a common secret key for both the encryption and decryption. Overall implementation is easy and it is a cryptographic algorithm accepted worldwide.

In this way, encryption is done by the Cloud service provider and decryption is done by the Cloud user. The information is encrypted and decrypted with the Secret-Key for encryption and decryption.

Pavel Lozhnikov et al.[2], proposed several variations of fuzzy extractors which is used to generate cryptographic keys and passwords based on parameters of keystroke dynamics. The key is generated by typing continuous text of acceptable length (minimum 1500 symbols). A method of generating a key with 192 bits is developed based on keystroke dynamics which is recorded while typing a continuous text of 1500 symbols.

In [3] A.J and K.D introduced an iris-based and fingerprint-based approach to obtain a secure encryption key and has three procedures: extract features, create a biometric template, and create an encryption key. Initially, iris images and fingerprints are analyzed to get the required features. All these features are mixed together to develop a complex feature thus a 256 bits secure biometric encryption key is created.

In [4], Shakeeba S. Khan et al. proposed different security provisions for cloud computing. Cloud is being implemented with different algorithms to give the data security. In this paper, different algorithms tried in cloud both symmetric and asymmetric. As the cloud computing is a vast area, this paper opens up for novel algorithms to implement further for better cloud security.

Penchalaiah et al. [5], analyzed the structure and design of DES (Data Encryption Standard) and AES. The aim of this study is to find out the similarities and dissimilarities of DES and AES.

Dongjiang et al.[6], proposed a method for generating a public key encryption system. Here, a generator is used to generate a random number, then uses an algorithm called Miller Rabin's algorithm to do preliminary test and then used the Stain algorithm to generate public and private keys.

2. SYSTEM DESIGN

Remote patient monitoring system is implemented based on IoT. It provides maximum ease of mobility to the patients and the gathered data securely transmit using AES algorithm to the intended mobile numbers or email IDs (care takers/relatives/doctors) via cloud server. The system architecture is shown below (Fig.4).

The system has four main sections. A BLE sensor node is used to gather the required patient data. The collected data from the sensors are forwarded to a mobile relay but mobile relay has no provision to process or store data, but mobile attaches its location details to calculate the approximate patient location along with the collected patient information.

To transfer the data to the cloud server for further processing, mobile relay uses its internet connection. For providing the data security certain algorithm is used called AES algorithm. And the system requires certain protocol to follow to transfer the collected patient’s information. Hence a secure communication established between mobile relay and cloud server. Complete data processing and information storage perform in cloud server (CS). CS sends notification to the authorized mobile numbers or email IDs (care takers, relatives or doctors) as SMS or email in case of any emergency. After the connection authenticated by CS, the data transfer from BLE sensor begins. The original message would be encrypted using AES algorithm so that the mobile relay cannot identify the cipher text. This would be decrypted using the same private key in order to extract the original information. This improves the security and privacy to the collected information from the patients.

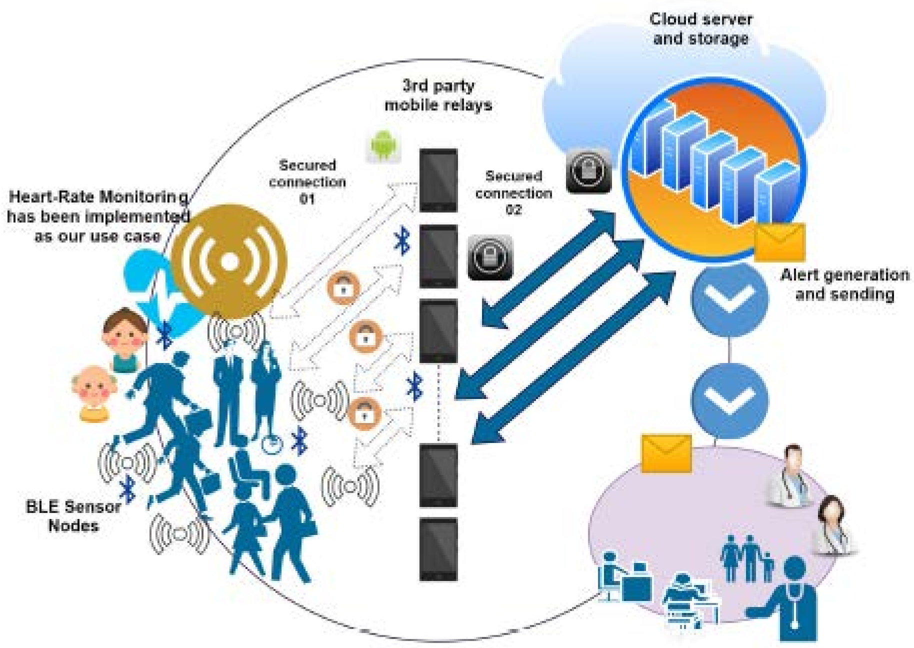

Fig. 4 System Architecture

2.1) PROTOCOL

i. Single mobile relay node BLE connection

The **Fig. 5** shows the message flow of protocol for a single mobile in the relay**.**

This protocol has of five phases.

Phase 1: The mobile relay node connects with the CS. The registration phase initiates, BLE sensor and mobile relay have to be registered with cloud server. Upon successful registration, CS issues a dynamic value a_f an advertisement ID.
Phase 2: The received advertisement ID starts advertise by the mobile relay and the mobile starts scanning for the same advertisement ID from the BLE sensor. Meanwhile BLE sensor also scanning for mobile relays with the same ID. Then BLE sensor and mobile relay establish a connection with this ID.
Phase 3: BLE sensor can initiate a connection the CS, and the mobile relay would forward this to CS. The connection has been validated and approved by CS.
Phase 4: After the approval of connection, BLE sensor initiates the data transmission to mobile relay. This information is encrypted using AES algorithm so that the mobile relay cannot eavesdrop the patient’s data. Encryption and decryption using AES algorithm explains in the next session. Once a fixed amount of information is moved, the sensor anticipates an encoded acknowledgment form CS. If the acknowledgement is sent, then BLE sensor can continue the data transfer, else the sensor terminates the connection with mobile relay.

Phase 5: The mobile relay can set a maximum threshold of information that a BLE sensor can send. Once the threshold reaches, it can cease the connection from CS. The CS will send an acknowledgement to BLE sensor and terminates the connection with the mobile relay. Then BLE sensor restart the process from phase 2, and it starts scanning for the mobile relay with the same advertisement ID for sending another set of data.

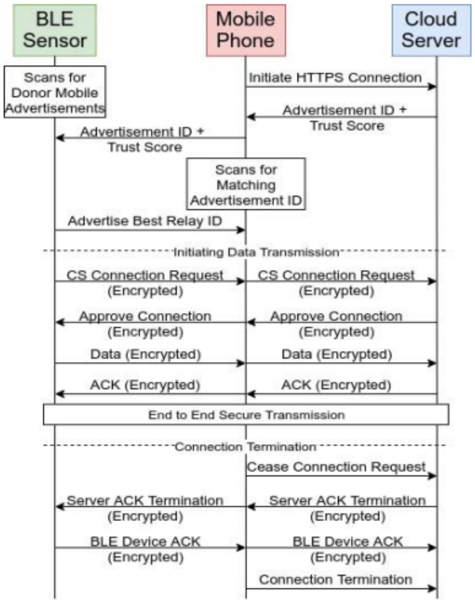
BLE Sensor
Mobile Phone
Cloud Server
Scans for Donor Mobile Advertisements
Initiate HTTPS Connection
Advertisement ID + Trust Score
Advertisement ID + Trust Score
Scans for Matching Advertisement ID
Advertise Best Relay ID
Initiating Data Transmission
CS Connection Request (Encrypted)
CS Connection Request (Encrypted)
Approve Connection (Encrypted)
Approve Connection (Encrypted)
Data (Encrypted)
Data (Encrypted)
ACK (Encrypted)
ACK (Encrypted)
End to End Secure Transmission
Connection Termination
Cease Connection Request
Server ACK Termination (Encrypted)
Server ACK Termination (Encrypted)
BLE Device ACK (Encrypted)
BLE Device ACK (Encrypted)
Connection Termination

Fig. 5 Message flow of the proposed protocol

2.2) AES Algorithm

AES is private key cryptography, wherein a single key is used to get information in cloud. It is otherwise called the Symmetric cryptography because of the utilization of single key both by the receiver and sender. In AES algorithm, the block size of plaintext varies from 128 to 256 bits. 128 bit, 192 bit and 256 bits keys are used for encryption and decryption. It uses 10, 12, 14 rounds which depends on the type of key used for encryption and decryption. Such as if 128-bit key is used then 10 round encryption and decryption process is used. Likewise, for 192-bit key 12 round encryption and decryption is used and for 256-bit key 14 rounds is used.

Initially, user information is encrypted and then it is stored in the CS. whenever required, user places a request for the information to the CS and CS validates the user authenticity and delivers the required information.

AES is an iterative rather than Feistel Cipher. AES is based on two common techniques to encrypt and decrypt data called substitution and permutation network (SPN). It is a number of mathematical calculations used in block cipher algorithm. AES utilizes a particular structure for encryption to secure the data. For that it relies on a number of rounds and each round comprises of four sub-process.

AES algorithm involves four steps:

- **Substitute Bytes or Sub-bytes Transformation:** This step is the initial stage of each round. AES uses 128-bits block of data. In sub-bytes transformation, each bit of data gets transformed by other data using 8-bit substitution box or also called s-box. As per diffusion and confusion Shannon's principles for cryptographic algorithm design it has important roles to get more security.

- **ShiftRows Transformation:** The second step is ShiftRow. This step is to shift bytes of the state cyclically to the left in every row instead of row number zero. In this process the bytes of row number zero will not change and does not carry out any permutation. The bytes of data in three rows are shifted in a left cycle way. In second row one-byte circular left shift is done and in third and fourth row two and three bytes left shift is done.

- **MixColumns Transformation**: This is a crucial step in AES algorithm. In mixColumns transformation, each column is multiply with a stable matrix. Every row of matrix transformation must multiply by every column of the state. The results of these multiplication are used with XOR to generate a new four bytes for the next state. In this step, size of the matrix remains unchanged.

- **AddRoundKey Transformation**: In this stage, XOR operation is performed among 128-bits of the current state and 128-bits round key. Both the key and the state are structured in a 4x4 matrix of bytes. AddRoundKey has the ability to give more security during encryption. This operation is based on creating the relationship between the key and the cipher text. The cipher text is coming from the previous stage.

The AES decryption process is similar to the encryption process, but only difference is that which is in the reverse order and both sender and receiver have the same key to encrypt and decrypt data. The decryption process is based on the key that was received from the sender of the data. The last round of a decryption stage consists of three stages such as InvShiftRows, InvSubBytes, and AddRoundKey as shown in Fig. 6.

2.3) SECURE ANALYSIS

The efficiency evaluation of AES algorithm is calculated using information entropy analysis and correlation coefficient analysis. In the study of statistical analysis such as Information *Entropy factor*, estimating the secure value of a cipher. A secure cryptosystem should be performing a condition on the information entropy that is the cipher text shouldn't give any data about the plaintext.

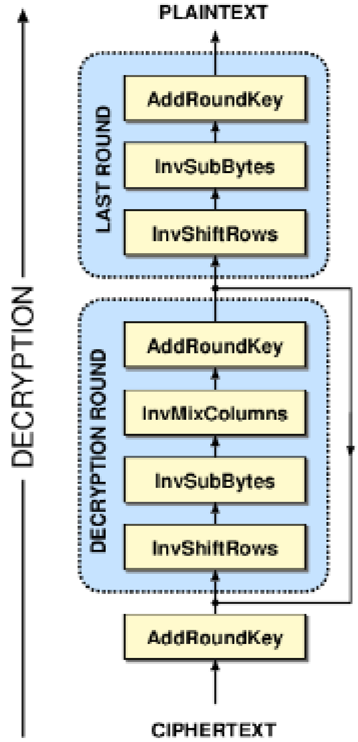

Fig. 6 Decryption Process

Statistical analysis such as *correlation coefficient factor* is utilized to measure the connection between two variables; the plaintext and its encryption. This factor shows how much the proposed encryption algorithm strongly resists statistical attacks. Subsequently, cipher text should be totally different from the plaintext.

Let the correlation coefficient equals one, that implies the plaintext and its encryption is identical. If the correlation coefficient equals zero, that implies the cipher text is totally different from the plaintext (i.e. good encryption). If the correlation coefficient equals minus one that implies the cipher text is the negative of the plaintext. The success of the encryption process means smaller values of the correlation coefficient.

3 EXPERIMENTAL RESULTS

The efficiency evaluation of AES algorithm has been done. The information entropy and correlation coefficient have been evaluated for the AES encrypted information. The information entropy of encrypted data by proposed encryption algorithm AES obtained is about 3.20986.

The correlation coefficient of encrypted data with the proposed algorithm AES is about 0.00962 which is a small value to compare zero value. So, the proposed algorithm AES is a good or secure encrypted data.

The Table.1 below shows the Experimental results.

S. No.	Features	RSA
1	Entropy before Encryption	2.87314
2	Entropy after Encryption	3.20986
3	Correlation Coefficient before Encryption	0.25635
4	Correlation Coefficient after Encryption	0.00962

Table.1 Experimental Results

The information entropy and correlation coefficient result show that the proposed encryption algorithm AES has a strong security.

4 CONCLUSION & FUTURE WORK

IoT can possibly offer an extensive support for AAL to consistently monitor patients and detect emergencies. This paper proposed a BLE relay based sensor emergency situation detection system with enhanced data security using AES algorithm. The high secure and high potential data encryption is provided using AES algorithm. Encrypting sensitive information from the database becomes more and more pivotal for securing from being misused by intruders who bypass conventional access control mechanism and have direct access to the data set. The results show, the information entropy of encrypted data is about 3.20986 and the correlation coefficient values of encrypted fields is about 0.00962 using AES algorithm. This shows that AES enhances the security of data.

For the future work, we intend to extend the work to develop machine learning algorithms to identify emergencies and peculiarities.

5 *REFERENCES*

[1] Shabisha,, Placide, et al. Security enhanced emergency situation detection system for ambient assisted living, IEEE Open Journal of the Computer Society 2 (2021): 241-259.

[2] Lozhnikov, Pavel, et al. Methods of generating key sequences based on keystroke dynamics. Houston, Texas: Gulf Professional Publishing; 2002, 411. 2016 Dynamics of Systems, Mechanisms and Machines (Dynamics). IEEE, 2016.

[3] A.Jagadeesan and Dr. K.Duraiswamy, Secured Cryptographic Key Generation from Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris. (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 2, February 2010.

[4 Khan, Shakeeba S., and R. R. Tuteja.. Security in cloud computing using cryptographic algorithms., International Journal of Innovative Research in Computer and Communication Engineering 3.1 (2015): 148-155.

[5] N..Penchalaiah and R.Seshadri," Effective Comparison and Evaluation of DES and Rijndael Algorithm(AES)", International Journal on Computer Science and Engineering, Vol. 02, No. 05, 1641-1645, 2010.

[6] Dongjiang, Li, Wang Yandan, and Chen Hong The research on key generation in RSA public-key cryptosystem, 2012 Fourth international conference on computational and information sciences. IEEE, 2012.

[7] Abdalrdha, Zainab Khyioon, Iman Hussein Al-Qinani, and Farah Neamah Abbas, Subject review: key generation in different cryptography algorithm, Int J Sci Res Sci Eng Technol 6.5 (2019): 230-240.

[8] Mousa, Ayman, et al, Security analysis of reverse encryption algorithm for databases. International Journal of Computer Applications 66.14 (2013).

[9] Parthasarathy, P. Rajamohan, et al., Implementation of RSA Algorithm to Secure Data in Cloud Computing, International Journal of Innovative Science, Engineering & Technology 6.4 (2019).

[10] Milanov, Evgeny. The RSA algorithm, RSA laboratories (2009): 1-11.

[11]De Raeve, Nick, et al., Bluetooth-Low-Energy-Based Fall Detection and Warning System for Elderly People in Nursing Homes., Journal of Sensors 2022 (2022).

[12]Wu, Falin, et al. Development of a wearable-sensor-based fall detection system, International journal of telemedicine and applications 2015 (2015).

[13]Dhakar, Ravi Shankar, Amit Kumar Gupta, and Prashant Sharma., Modified RSA encryption algorithm (MREA)., 2012 second international conference on advanced computing & communication technologies. IEEE, 2012.

[14] Segar, T. Chandra, and R. Vijayaragavan Pell's RSA key generation and its security analysis, 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT). IEEE, 2013..

[15] Jogdand, R. M., and Sahana S. Bisalapur, Design of an efficient neural key generation. International Journal of Artificial Intelligence & Applications (IJAIA) 2.1 (2011): 60-69.

[16] Nagar, Sami A., and Saad Alshamma, High speed implementation of RSA algorithm with modified keys exchange. 2012 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT). IEEE, 2012.

[17] A. Makhlouf, I. Boudouane, N. Saadia, and A. Ramdane Cherif, Ambient assistance service for fall and heart problem detection, Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 4, pp. 1527–1546, 2019.

[18] Lord, Stephen R., et al. The effect of an individualized fall prevention program on fall risk and falls in older people: a randomized, controlled trial., Journal of the American Geriatrics Society 53.8 (2005): 1296-1304.

[19] Jonsson, Jakob, and Burt Kaliski., Public-key cryptography standards (PKCS)# 1: RSA cryptography specifications version 2.1. No. rfc3447. 2003.

[20] Kelsey, John, et al., Cryptanalytic attacks on pseudorandom number generators, International workshop on fast software encryption. Springer, Berlin, Heidelberg, 1998

[21] Shakir M. Hussain and Hussein Al-Bahadili, A DNA-Based Cryptographic Key Generation Algorithm, 338 Int'l Conf. Security and Management, SAM'16.

[22] O. G. Abood and S. K. Guirguis,"A Survey on Cryptography Algorithms," International Journal of Scientificand Research Publications, Vol. 8, No. 7, pp. 495-516, 2018.

[23] Md. A.Hossain, Md. B. Hossain, S. Md. Imtiaz and Md. S. Uddin," Performance Analysis of Different Algorithms," International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 6, No. 3, pp. 659-665, 2016.

[24] D. Pugila, H. Chitrala, S. Lunawat and P. M. D. R. Vincent," An Efficient Encryption Algorithm Based on Public Key Cryptography," International Journal of Engineering and Technology, Vol. 5, No. 3, pp.3064- 3067, 2013.

[25] Md. I. Alam and M. R. Khan," Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography," International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 10, pp. 713-720, 2013.