Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 3, pp. 779–791
DOI : 10.47974/JDMSC-1754

Securing networked image transmission using public-key cryptography and identity authentication

V. Dankan Gowda *
Department of Electronics and Communication Engineering
BMS Institute of Technology and Management
Bangalore
Karnataka
India

Pullela SVVSR Kumar †
Aditya College of Engineering
Surampalem
Andhra Pradesh
India

J. Latha §
C. Selvakumar ‡
Lecturer Electrical Section
University of Technology & Applied Science
Shinas
Sultanate of Oman

R. Shekhar @
Department of Computer Science and Engineering
Alliance University
Bangalore
Karnataka
India

* *E-mail:* dankan.v@bmsit.in (Corresponding Author)
† *E-mail:* pullelark@yahoo.com
§ *E-mail:* lathasendhil@gmail.com
‡ *E-mail:* selvahere0607@gmail.com
@ *E-mail:* shekhar.r@alliance.edu.in

© Taru Publications

Abhay Chaturvedi [#]
Department of Electronics and Communication Engineering
GLA University
Mathura
Uttar Pradesh
India

Abstract

Nowadays, the data transmission in the network is working with the latest technology including 3G, 4G, and 5G. These technologies are replacing old technologies including 2G. Many techniques were proposed and implemented by different researchers in the directions of encryption, decryption, digital signatures, secure routing, WSNs, and cryptographic algorithms. Even though, no systems provide a better result as per the real world requirement. For this purpose, a new model is designed and implemented in this research work. Moreover, it provides data security while performing data transmission in WSN with the incorporation of steganography and digital signatures. The different cryptosystem is the novelty of different algorithms is proposed for providing security services. In this field, there are many combinations with different result were classified under various types. However, in the existing scheme, accommodate their type that forms the algorithms into cryptography oriented methods and other different techniques combined to get a high secured image. Moreover, the various related works in this direction were discussed under all types.

Subject Classification: *14G50 Applications to coding theory and cryptography of arithmetic geometry, 94A60 Cryptography ,54H30, 94A08 Image processing.*

Keywords: *Image processing, Steganography, Digital signatures, Cryptosystem, Encryption and decryption.*

1. Introduction

Developments in wireless communication and digital electronics have made possible the creation of sensor nodes that serve several purposes, are inexpensive, and use very little energy. Spread out in different locations, these sensor nodes operate together in a cooperative fashion to transmit data gathered from the monitored region across established network links. Whether or whether the destination node plans to utilise the consolidated data locally depends on the nature of the other sensor networks with which it communicates [1]. The basic operation of a WSN is shown in Figure 1. channel provides a medium which is used for exchanging the message and extracted from the sensor nodes to the external world that might be an inter-node communication process and the computer

[@] *E-mail:* **abhaychat@gmail.com**

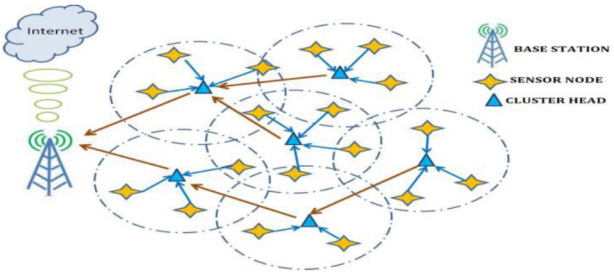


Figure 1

Basic wireless sensor architecture

network. For this purpose, the sensor node's energy is used in a productive mode for enhancing the net's lifetime. In such a scenario, energy-efficient communication of the data collected by the sensor nodes is a challenging design issue for reliable data collection and communication. Moreover, the security attacks in such sensor nodes and the links connecting the nodes will decrease the performance of the network communication and will result in increased congestion, delay, and energy consumption. In addition, the packet delivery ratio will be affected leading to the reduction in network throughput [2]. Hence, it is necessary to propose efficient techniques for data collection and the secured delivery of the collected data. Security to WSN is provided in different ways such as access control, encryption, and decryption techniques, the introduction of intrusion detection and prevention mechanisms and effective key management schemes [3]. However, for image and video communication, steganography based security mechanism is more suitable and hence it is necessary to propose effective security mechanisms based on steganography and cryptography.

In the field of cryptography, keys are generated using the key generation method. It doesn't matter what kind of data is being encrypted or decrypted; here, a key is utilised as a secret key to do both tasks. For this, we use a tool known as a key generator to produce new keys [4]. DES and AES, both symmetric key algorithms, are utilised in current cryptographic systems, whereas the existing RSA technique is used for public-key cryptography. Different cutting-edge algorithms were created to transmit the privacy needed to produce a unique shared key for each session.

2. Related work

A framework for transmitting the data is developed by author's [5]. The data using Steganographic methods are secured and in which hides

the data while performing the data communication between the nodes in networks. They have considered the issue of applying steganography widely through a network protocol. For this purpose, they analyzed the possibilities and proposed a new model called warden to hinder the utilization of communication channels in the network. Finally, they have achieved better performance in terms of delay in data communication between the nodes of the network. In [6] author's developed a key generator and further it combines resource allocation along with key generation and a new stream-based authentication mechanism is created for maintaining the best possible video quality. When ensuring energy efficiency and security in wireless area sensor networks. A novel security algorithm developed and dedicated to initiating cryptographic techniques in which the work is developed and combined to give asymmetric and asymmetric cryptographic techniques for providing a high degree of data security with reduced key maintenance[7]. The algorithm is guaranteed for three security principles - data authentication, data integrity, and data confidentiality. The algorithm is combined with ECC and AES for providing encryption. It uses the MD5 algorithm used for data integrity. A new ECC based encryption technique and homomorphic encryption for securing the data transmission process in WSN [8]. Moreover, their approach is developed based on the GASONeC algorithm that applies a genetic algorithm for building the exact clusters in the network. They increased the network lifetime, less communication overhead, and less energy consumption. The modified techniques on this research are initiated and developed an ECC based encryption method [9]. This method focuses on the homomorphic encryption for securing data transmission in sensor networks. In [10] author's designed a robust authentication model to functioning other security processes such as semantic segmentation, data hiding and the chaotic encryption for performing authentication remotely. The hidden technique developed and recommended a novel approach to share their secret images by applying an existing scheme called the NP-threshold scheme along with the extra characteristics of steganography and authentication processes [11]. In their work, they processed a secret image into an 'n' number of shares in hidden mode and selected the equal number of hidden images. Moreover, their method recommended that to choose these hidden images for holding the famous data or information like most popular characters of images for increasing the effect of steganographic to protect the data. In their work, each of the hidden images is considered as stego-images. In [12] author's explained the various steganography based works that are proposed by various researchers in the past along with the

disadvantages. Moreover, they also reviewed that few hidden encryption techniques implications by using various tools. In [13] author's presented and developed a new method that method is used by performing the feature mining process and the pattern classification for detecting the Least Significant Bit matching over the grayscale images that is a big issue in stego analysis. They have proposed five different types of features and compared with the famous feature sets that are rarely mentioned in stego analysis and also identified the best feature.

3. Digital signature

A digital signature is different from a manual signature used by human beings for performing authentication. In bank transactions, human signatures were verified to check the authentication of the user[14]. In Automatic Teller Machines (ATMs), two types of authentication mechanisms are applied. The first authentication technique is the verification of the card. If the card used by the customer is not a valid card or expired card then the ATM rejects the card. In this case, the user is denied permission to carry out the transaction. In addition to this, the user is asked to type the PIN. The user is successful in providing a PIN number and ATM card correctly then the ATM machine allows the user to perform the transaction.

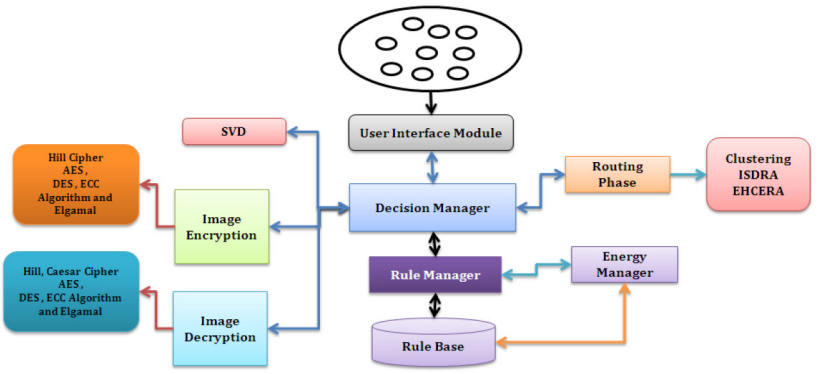
4. Data hiding

Data hiding is a method that is used for embedding the data namely text data, image data, audio data or video data into the different kinds of media like audio, image, and video. This data hiding is playing a major role in the military for sharing their secret information in the form of text, image, audio, and video securely. The intelligent agents are used in data hiding for performing the communication for the data hiding process and to ensure data security [15]. After the development of internet technology, it helps to store the data in the World Wide Web and also facilitates data communication between the nodes present on the internet. Therefore, every user is uploading their information on the web and hence the volume of web data is increasing continuously and the data are stored and communicated in different data types namely text, image, audio, and video. Therefore, data communication requires the use of high-speed networks that are connected as a part of the internet[16]. Even though data transmission is not secure through the internet due

to the leakage of transferred data, it leads to a serious impact on society. Therefore, it is necessary to hide the transferring data secretly as digital data with different formats are used in the transmission. In this secured data transmission process, data integrity is a very important issue to be considered. Many algorithms were proposed and implemented in the past to protect the data from hackers [17]. The classical data hiding techniques include cryptography, steganography, and watermarking. These techniques contain a variety of features such as robustness, payload, security, reliability, and high capacity. However, the degree of data security in each data transmission is different according to the various techniques [18]. Due to the presence of malicious users and attackers in the network, the challenges of developing a suitable and efficient data hiding process is becoming a complex task. Any "holes" present in the data to be communicated will make the compression algorithm to provide a lossy compression. However, it is necessary to provide a non-loss compression by designing suitable keys and constraints [19]. The key is useful for finding the most successful holes in the data hiding process which are also not suitable to perform the exploitation process by applying the standard compression techniques [20]. Therefore, digital signatures can be used to perform the verification of genuine users and to avoid malicious users.

5. Secure data communication system architecture

A new secure data communication model is recommended which uses cryptographic techniques for wireless sensor networks. Figure 2



Figuer 2

Secure data communication system architecture

shows the complete design of the proposed security model. The design consists of ten key working mechanisms. They are User interface module, Decision manager, Rule manager, Rule base. The specific scenario is created for conducting the experiments with sufficient minimum energy level for data communications.

These sensor nodes can transmit the data between them securely with the help of the proposed secured data communication model that uses cryptographic and steganography methods in this research work. It provides sufficient detail about the sensor node's energy level to the decision manager and it also confirms the required energy for every node in all kinds of situations. The energy status of the nodes will be updated in the rule base frequently. The single value decomposition is a method that is used to compress the input images by applying the standard decomposition algorithm in this research work. Based on the decision manager input, this method works and produces the resultant values to the decision manager. The resultant value is to be forwarded into the right destination node through the decision manager. The routing phase is playing a crucial role in the secured data communication process of this proposed secured data communication model. It applies the various algorithms such as the clustering algorithm, ISDRA, and EHCERA for performing the data routing process effectively. First, it performs a clustering process over the various participated sensor nodes in the WSNs. After performing the clustering process, the routing algorithm is applied over the clustered nodes data communication activities in this research work. The decision manager will decide the secured routing algorithm to be applied for the specific data communication process in the network. The decision manager is responsible for selecting the encryption algorithm, decryption algorithm, secured routing algorithm and the single value decomposition algorithm in this research work. The decision manager is an overall controller for this secured data communication model. It is responsible for initiating a data transmission until it reaches the data to the destination node carefully. Moreover, it selects the suitable routes with the help of the routing phase and also the various rules from rule base through rule manager in this work. The decision manager might be of any role such as system administrator, program manager, base station controller, network administrator or database administrator. They have access to our secured data and initiate the data communication. The rule base is a database that contains a variety of rules related to the node's energy level and the individual node's status in terms of energy and reliability. This rule base supplies the various rules. The different kinds

of rules are useful for making the decision over the routing algorithm selection process, single value decomposition algorithm, encryption algorithm selection, and the decryption algorithm selection processes. The overall system architecture shows the entire working flow of the proposed secured data communication model.

6. Proposed Signature verification system architecture

The signature verification architecture is shown in Figure 3. The proposed signature verification architecture consists of ten components namely sender, distribution centre, receiver, medical image, decision manager, compression using SVD, decryption module, encryption module, rule manager, and rule base. The sender sends the image to the decision manager and it forwards to the image compression using SVD for compressing the images. The compressed image is sent to the encryption module for encrypting the image data by applying symmetric image encryption and the public key encryption. Here, the symmetric image encryption incorporates the existing AES and Hill-Cipher algorithms for performing the encryption process. And, the public key encryption uses RSA, Rule-based RSA, and Hill Cipher for performing the additional encryption process.

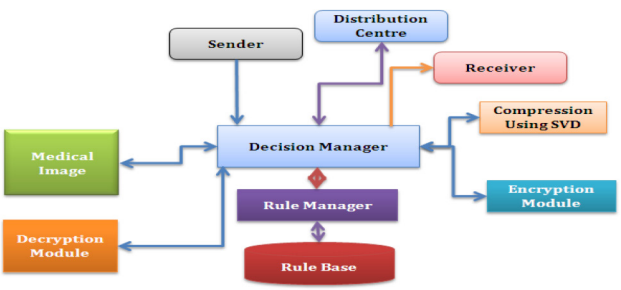
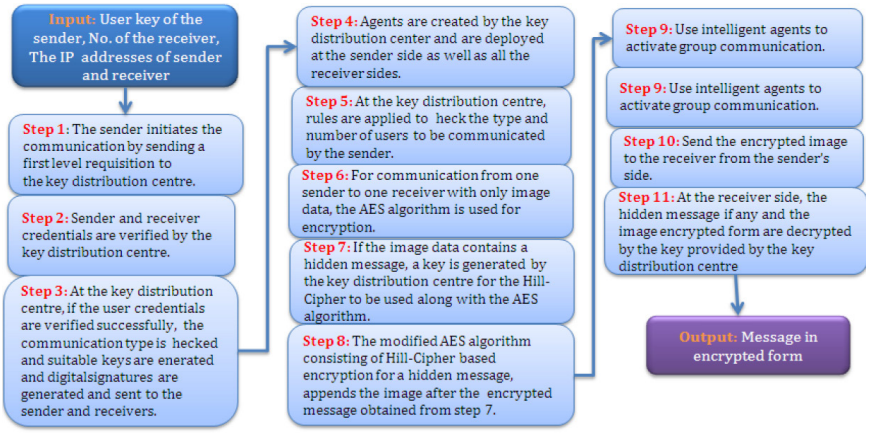


Figure 3

Signature verification system architecture

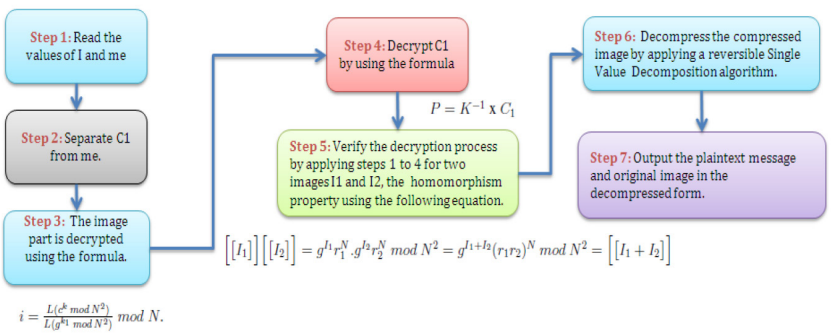
Encryption algorithm

Moreover, the encrypted image is sent to the decryption module for performing the decryption process. The decryption module applies Modified AES and the Reversible SVD. The decision manager refers to the rules from the rule base for deciding on the image data set. The decision manager acts as the overall coordinator for the entire system architecture.



It can send the image data and receive it. Here, the medical image is used for carrying the data in a hidden manner secretly.

Decryption Algorithm with Public Key



7. Results and discussion

In order to ensure the accuracy of this work, it was put to the test on 800 images taken from the UCI repository's collection of medical photographs. Java was used to implement the algorithms, while Java Sockets were used for the communication. Rules were implemented in Java with the help of Aglet-based mobile agents to facilitate efficient data exchange between the network's nodes.

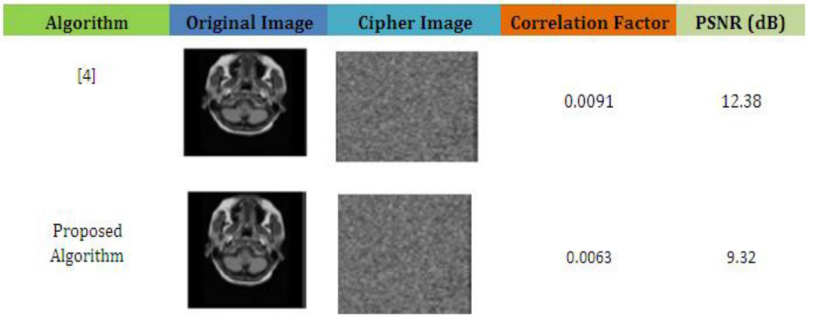


Figure 4

Analysis of PSNR and correlation coefficients for use in public-key image encryption

In this study, uses asymmetric key encryption methods for unicast communications where the key is agreed upon by both the sender and the receiver to encrypt images. In this section, we evaluate the proposed model's privacy features against those of similar current solutions. Figure 4 shows the results of a comparison between two metrics used by the authors of [4] the correlation factor and the PSNR value. Figure 4 shows that the correlation factor is small for both the baseline and the suggested work, demonstrating a good level of privacy. The suggested work, however, has a smaller correlation factor than the current work, and therefore the secrecy is raised in the proposed work to improve security. The PSNR value is also poor in both the current and suggested work, but it is somewhat better in the latter. This demonstrates that both the baseline model and the suggested approach have very good system security. Even

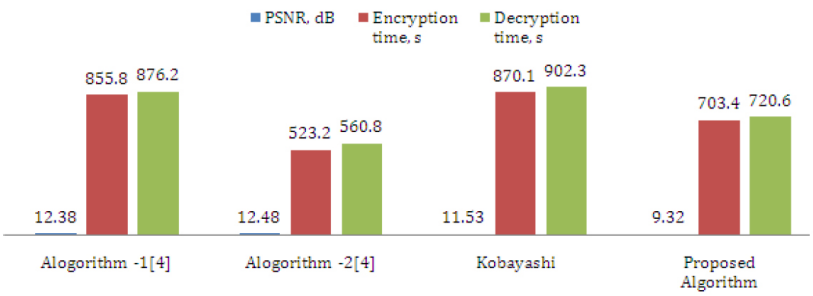


Figure 5

Comparison of the quality and speed of encryption using the Kobayashi scheme

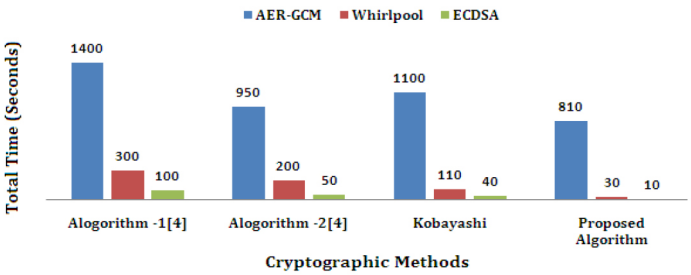


Figure 6

Time Analysis

though the suggested model employs a modified AES algorithm, it has a lower PSNR value than the current model.

By comparing the results of the proposed encryption algorithm to those of other methods, as shown in Figure 5, it becomes clear that the suggested algorithm achieves impressive results. This is because conventional authentication and encryption techniques are being used. The main features that can be identified and differentiate from one algorithm to another. The result might be varied and they are to show its ability and performance to secure the protected data against attacks and its speed and efficiency can be focused and do in all algorithms. Time comparisons were carried out between the proposed algorithms and the current techniques, with both the encryption and decryption processes being taken into account. Specifically, we have implemented the AES-GCM, Whirlpool, and ECDSA cryptographic algorithms. The different cryptosystem is the novelty of different algorithms is proposed for providing security services. In this field, there are many combinations with different result were classified under various types. However, in the existing scheme, accommodate their type that forms the algorithms into cryptography oriented methods and other different techniques combined to get a high secured image. Moreover, the various related works in this direction were discussed under all types. Figure 6. shows the Time Analysis of existing method with the proposed approach.

8. Conclusion

In this paper a new novel framework is developed for image transmission using public-key cryptography and identity authentication. To perform a better level of security this method is initiated. The Proposed

steganography method that applies multilayer embedding which can improve the data hiding performance. The results proved that better performance than other methods in terms of providing good quality image and low computational complexity. When compared to current methods, the suggested approach for transmitting medical images is superior. A new image compression method might be developed in the future to improve the efficiency of medical image transmission.

References

[1] Amir M, A. and Maryam, A. 'A novel secret image sharing with steganography scheme utilizing optimal asymmetric encryption padding and information dispersal algorithms', *Signal Processing: Image Communication* 74, pp.78–88 (2019).

[2] Ayesha, S. and Masilamani, V., 'A novel digital watermarking scheme for data authentication and copyright protection in 5G networks', *Computers and Electrical Engineering* 72, pp.589–605 (2018).

[3] Bakar, A. and Ismail, R., 'An agent based rough classifier for data mining', Eighth International Conference on Intelligent Systems Design and Applications 6, pp.145–151 (2018).

[4] Blinowski, G. and Szczypiorski, K., 'LuxSteg: First practical implementation of steganography in VLC', IEEE Access 6, pp.74366–74375 (2018).

[5] Cao, J., Ma. and Liu, X. 'Eghr: Efficient group-based handover authentication protocols for mmtc in 5g wireless networks', *Journal of Network and Computer Applications* 102, pp.1–16 (2018).

[6] Chia-Chun, W. and Min-Shiang, H., 'A high-quality image sharing with steganography and adaptive authentication scheme', *Journal of Systems and Software* 84(12), pp. 2196–2207, (2019).

[7] Fatnassi, A. and Bouamama, S., 'A new hybrid steganalysis based approach for embedding image in audio and image cover media', IFAC-papers online 49(12), pp.1809–1814 (2017).

[8] Guanglou, Z. and Subhas Chandra, M., 'A critical analysis of ECG-based key distribution for securing wearable and implantable medical devices', *IEEE Sensors Journal* 19(3), pp.1186–1198 (2019).

[9] Huang, C. and Prucnal, P., 'Robustness of optical steganographic communication under coherent detection attack', *IEEE Photonics Technology Letters* 31(4), pp.327–330 (2019).

[10] Juan,W. and Yiming, X., 'A novel natural languagesteganographic framework based on image description neural network', *Journal of Visual Communication and Image Representation* 61, pp.157–169 (2019).

[11] Kouzehzar, and Torkzadeh, P., 'A high data rate pipelined architecture of aes encryption/decryption in storage area networks', Electrical Engineering (ICEE), Iranian Conference on pp. 23–28 (2018).

[12] S. B. Sridhara, M. Ramesha, "Recent advances in graph theory and its applications," *Advances in Mathematics: Scientific Journal*, vol. 10, no. 3, pp. 1407–1412 (2021).

[13] Li, L., Liu, L. and Cheng, S., 'Flexible and secure data transmission system based on semitensor compressive sensing in wireless body area networks', *IEEE Internet of Things Journal* 6(2), pp.3212–3227 (2019).

[14] Avinash Sharma, M. Nagabushanam, H. G. Govardhana Reddy & K. Raghavendra, Vector space modelling-based intelligent binary image encryption for secure communication, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:4, pp.1157-1171 (2022).

[15] Muhammad and Baik, S., 'Secure surveillance framework for IoT systems using probabilistic image encryption', *IEEE Transactions on Industrial Informatics* 14(8), pp.3679–3689 (2018).

[16] A. P, A. Sharma, A. Sharma, K. S and M. R. Arun, "Priority Queueing Model-Based IoT Middleware for Load Balancing," 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 425-430 (2022).

[17] Philip Chen, C. and Benjamin, M. R., 'A pattern recognition system for jpeg steganography detection', *Optics Communications* 285(21–22), pp.4252–4261 (2016).

[18] Safwan El, A. and Mousa, F., 'A new chaos-based image encryption system', Signal Processing: Image Communication 41, pp.44–157 (2018)

[19] Shin, S. and Kwon, T., 'Two-factor authenticated key agreement supporting unlinkability in 5g-integrated wireless sensor networks', IEEE Access 6, pp.11229–11241 (2018).

[20] A. P, A. Sharma, A. Singla, N. Sharma, "IoT Group Key Management using Incremental Gaussian Mixture Model," 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC), pp. 469-474 (2022).