AMERICAN JOURNAL OF MANAGEMENT AND IOT MEDICAL COMPUTING
Peer Reviewed, Referred & Indexed Journal
E-ISSN: 3069-0110
Vol.5, No.1(2026)
www.ajmimc.com

Dual Encryption Scheme-based Secure Group Key Management for IoMT Communication Networks

S. Bhuvaneswari[1*], T. Pramananda Perumal[2]
[1]Research Scholar (PT), Dept. of Computer Science, Presidency College, Chennai-600 005
[2]Principal (Retired), Presidency College, Chennai-600 005
***Corresponding Author:** Email: bhuvanaparthi@gmail.com

Abstract

The Internet of Things (IoT) plays a vital role in modern communication, where security is a major concern. This paper proposes a group key management approach using a dual encryption scheme (AES and RSA) to ensure secure communication in an Internet of Medical Things (IoMT) environment. Doctors and patients /devices act as network members in a group, exchanging data securely by using group keys. A group key is valid for 72 hours to enhance security and prevent unauthorized access. This proposed group communication system is implemented /simulated using NS3 simulator and its performance is evaluated by using metrics such as packet delivery ratio, throughput and delay. Results show that the proposed system provides secure and efficient communication in IoMT environment.

Key words: IoT, Group Key, RSA, AES, IoMT, NS3

1. Introduction

The Internet of Things (IoT), when applied in healthcare for acquiring bio-signals such as ECG and EEG, along with physiological parameters including blood pressure, body temperature, heart rate and blood oxygen levels, is referred to as the Internet of Medical Things (IoMT). IoMT plays a significant role in modern healthcare systems by enabling continuous monitoring and real-time data exchange among medical entities. This domain has become essential for delivering efficient medical services. Secure group communication among IoMT members such as doctors, patients and healthcare devices is highly important. Establishing a group key is necessary to ensure secure communication among these entities. However, in current network environments, communication among doctors, patients, caretakers and devices is often vulnerable and lacks sufficient security mechanisms.

In recent years, various cryptographic approaches have been proposed to enhance authentication and security in IoMT networks. Hyper Elliptic Curve-based public key cryptography has been utilized for group key agreement in IoT healthcare systems [1]. Decentralized lightweight group key management schemes have been introduced to ensure secure data distribution in IoT environments[2]. Identity-based encryption techniques have also been proposed to mitigate malicious attacks in large-scale networks [3]. In highly dynamic networks such as VANETs, frequent changes in group membership make challenging key update process. To address this issue, lightweight multicast scalable group key management protocols have been developed [4].

The RSA algorithm has been widely used as a cryptographic technique for encryption and decryption processes [5]. Additionally, RSA has been used for secure video transmission [6] and speech data encryption [7]. Comparative studies of RSA, AES and DES algorithms have shown their effectiveness in secure data transmission [8]. Furthermore, comparisons between AES and RSA in image encryption indicate that AES often provides better performance [9]. Hybrid cryptographic approaches combining RSA with other algorithms such as Blowfish have been proposed for improved cloud security [10].Multi-phase hybrid cryptographic techniques incorporating AES, DES

Received: 02-02-2026 | Accepted: 10-03-2026 | Published: 16-03-2026 | www.ajmimc.com

and modified RSA have also been implemented in wireless sensor networks for enhanced security[11]. It effectively minimizes computational complexity while ensuring high grade protection and making it suitable for highly secure data environments [12]. The AES and RSA algorithm increase the security of the data and upgrade the speed of encryption and decryption process [13].

In the healthcare domain, extensive studies have been conducted on IoMT systems integrating big data, IoT and cloud computing to provide secure e-health services [14]. Key management techniques such as mutual authentication and secret key agreement have been proposed to establish secure communication in IoT-based healthcare systems [15]. Research has also explored the applications, benefits and challenges of IoMT to support future developments [16]. Additionally, various security threats, attacks and countermeasures in IoMT have been analysed to develop lightweight security mechanisms [17].

To address the existing challenges, this study proposes a secure group key management approach for IoMT environments using a dual encryption scheme.

This paper is organized as follows. Section 2 gives the overview of AES and RSA algorithms. Section 3 presents the proposed system and dual encryption method. Section 4 discusses the performance evaluation using NS3 simulation and metrics such as packet delivery ratio, throughput and delay. Section 5 highlights conclusions.

2. Overview of AES and RSA algorithms

In this section, the AES and RSA cryptographic algorithms are discussed below.

2.1 AES Algorithm

AES (Advanced Encryption Standard), also known as the Rijndael algorithm, is a **symmetric** block cipher that operates on 128, 192 or 256-bit data blocks [18]. It is significantly faster than Triple DES and provides stronger security due to larger key sizes. AES operates using a substitution–permutation network. It processes 128-bit data blocks as 16 bytes arranged in a 4 × 4 matrix. The number of rounds depends on the key size:

- 10 rounds for 128-bit keys
- 12 rounds for 192-bit keys
- 14 rounds for 256-bit keys [19, 20]

Each AES round consists of four main steps:

- **SubBytes:** Byte substitution using an S-box
- **ShiftRows:** Row-wise shifting of data
- **MixColumns:** Column-wise transformation
- **AddRoundKey:** XOR operation with the round key

The AES Algorithm working process is described in Fig.1.1.

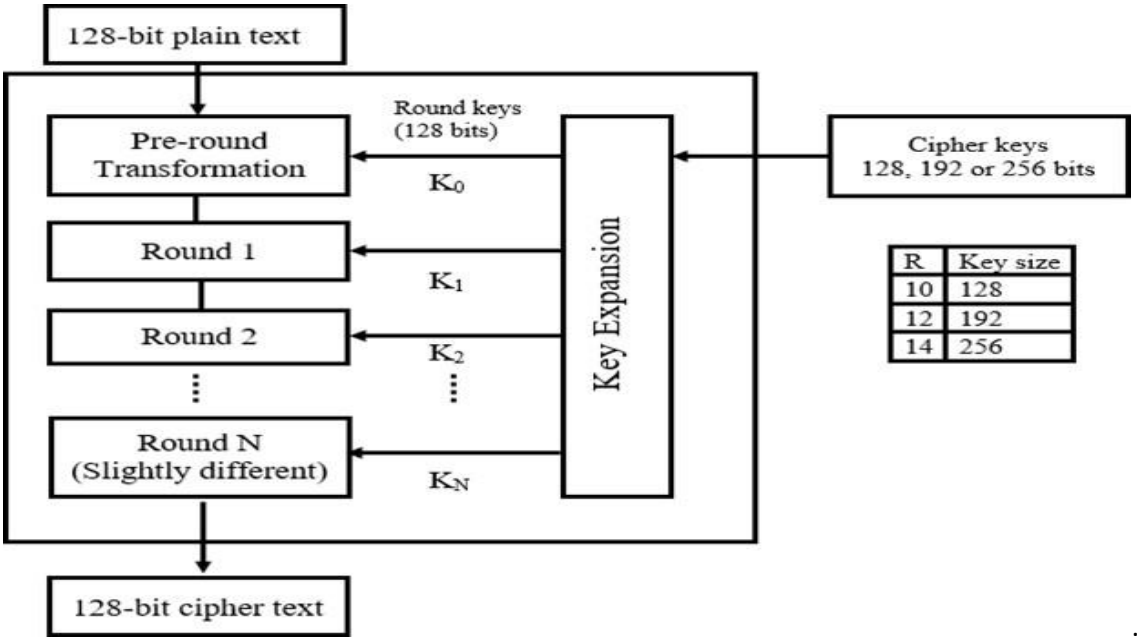

Fig.1. AES Algorithm working process

2.2 RSA Algorithm

RSA (Rivest-Shamir-Adleman) is an **asymmetric** cryptographic algorithm that uses a pair of public and private keys for secure communication. There are three steps involved while implementing this algorithm [19].

Step 1: Two prime numbers (a and b) are selected and multiplied to obtain the modulus (N = a × b).

Step 2: A derived number (E) is chosen such that it is greater than 1 and less than (a−1) and (b−1).

Step 3: The public key consists of N and E, which is used for encryption.

The sender encrypts the message by using the public key. S is a message which will be a plain text. If the size of S (in bytes) exceeds N, it is divided into smaller parts, encrypted and then recombined. The cipher text [C] is generated by using the formula, $C = S^E \bmod N$.

The diagrammatic representation of RSA is shown in Fig.2.

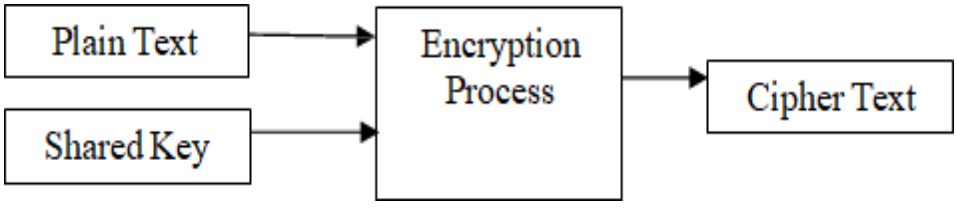

Fig.2. RSA Encryption Process

3. Details of Proposed work

In this study, group key management plays an important role in enabling secure group communication. It involves group key generation and the use of a group manager to distribute and maintain secure keys among members.

3.1 Proposed Group Key Generator Model

The Key Distribution Center (KDC) is typically responsible for providing cryptographic keys in secure systems. However, to enhance the security of group communication, this proposed work replaces the traditional KDC with a self-designed Group Key Generator (GK_G) using a dual encryption scheme. This model is implemented in an IoMT environment. The proposed system follows a two-tier architecture consisting of doctors and devices/patients. Sensors are attached to all members of the communication network. When a new member joins the IoMT environment, it is categorized accordingly [21]. The dual encryption scheme which combines AES and RSA algorithms is applied to generate secure keys.

The Group Manager (GM) initializes the network by assigning unique IDs to doctors and devices/patients, as illustrated in Fig.3. The GM generates encrypted cryptographic keys, referred to as Group Keys (GK) and distributes them to all members. Whenever a member joins or leaves the group, the GM updates the group key to maintain security. The GM ensures forward and backward secrecy. Forward secrecy prevents former members from accessing future keys, while backward secrecy ensures that newly joined members cannot access previously used keys [21]. Doctors can access patient or device information only by sending requests to the GM. The GM verifies both the doctor's ID and the group key before granting access to the requested data.

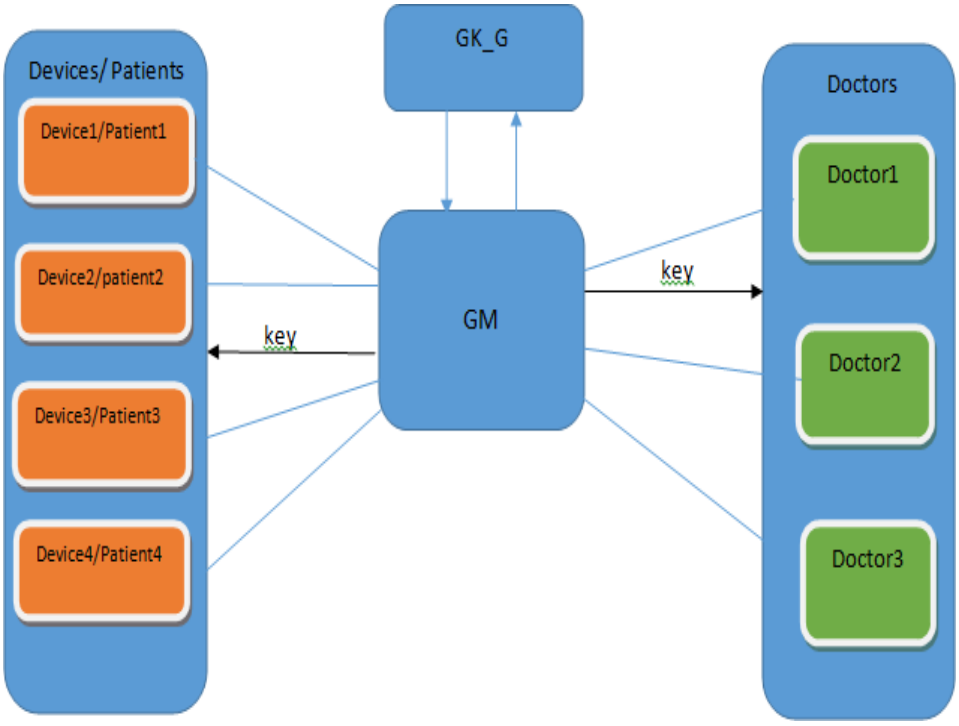

Fig.3. Data Flow Diagram for Group key management framework

3.2 Responsibilities of Group Manager

The Group Manager (GM) performs the following key functions:

When a new member joins: The GM generates a unique user ID, updates the group key and distributes the new key to all members. The shared key is then used for secure communication [21].

When a current member leaves: The GM updates the group key and distributes it to the remaining members. The leaving member is no longer authorized to access the system [21].These responsibilities ensure secure and dynamic group communication, as shown in Fig.4.

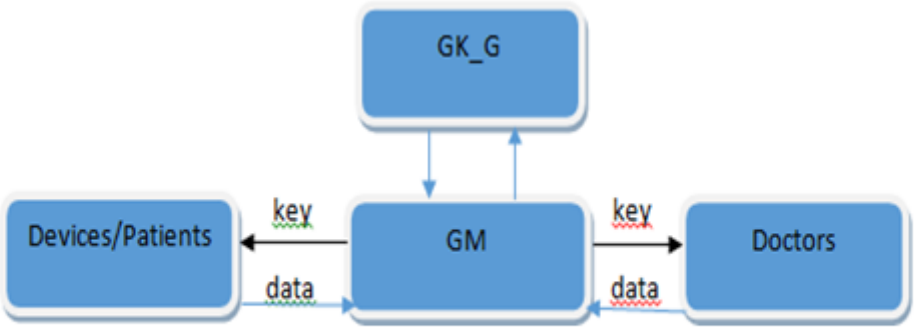

Fig.4. Responsibilities of Group Manager

3.3 Dual Encryption Scheme

This study proposes a dual encryption approach combining AES and RSA algorithms to achieve secure group communication in IoMT environments.

Proposed Dual Encryption Algorithm

In the proposed dual encryption scheme, the plaintext message is divided into two parts: left (L_Part) and right (R_Part). The left part is encrypted using AES with key AK, producing a 128-bit encrypted output. The right part is encrypted using RSA with public key RPu, also producing a 128-bit output. Both encrypted parts are combined to form the full encrypted message (256 bits). The encrypted message and keys are further compressed using a hash function. Now the group key is distributed to all the members of the group by the group manager. The group key is stored by the GM for the safety purpose [22].

The mathematical representation of the dual encryption process is given as follows [23]:

$C = \{E_{AES}, E_{RSA}, M_{left}, M_{right}, K_{left}, K_{right}, AK, RPu\}$
$K_{left} = \{E_{AES}\ (M_{left}, AK)\}$
$K_{right} = \{E_{RSA}\ (M_{right}, RPu)\}$
$E_{Key} = (AK, RPu)$

Algorithm: Dual (AES & RSA) Encryption Scheme

Input: Plain message (text/numeric data)
Output: Cipher message, key K
Begin
1. Divide the message into L_Part and R_Part
2. Generate AES key (AK)
3. Encrypt L_Part using AES
4. Generate RSA public key (RPu)
5. Encrypt R_Part using RSA
6. Combine encrypted parts
7. Generate EncryptKey = (RPu, AK)
8. Apply hash function to encrypted message and key
9. Return final encrypted message

End

The generated group key is 256 bits and is used for secure communication among network members. This eliminates the need for frequent key generation, thereby improving communication speed.

3.4 NS3 Simulator

The proposed group communication system is implemented in an IoMT environment. This is simulated using NS3 software in order to show the communication among the nodes available in the IoMT environment. This simulation includes 50 network nodes representing devices, patients and medical professionals. The proposed system supports remote patient monitoring, healthcare data transmission and access by physicians for diagnosis and treatment planning.

4. Results and Discussion

4.1 Group Key Generated by Dual Encryption Scheme

The group key values are generated using the proposed dual encryption scheme and each generated key is unique. The time duration required for generating sample group keys is presented in Table 1.

Table.1. Key sample values used in the Group communication

S. No.	Time stamp t (sec)	Group Key sample values
1	1.567	55ecfcda4e3f3b51c1854ffb6e8225f1b6815c3f14caa7a192687594bc3160d596b50 b8b0840c5bb0828c2e539abe07088ed60b92d6a8bd56d17264c92f69f6e2fe667639 0b83241832967e69a06072db2b8c3d0e915f82c3ee4c0ff66f28ea27935db686dd24e aed4c2dc946e34606c63d1312066209eb1ad60cc6dfac59585h
2	1.565	268c5d7cb01bdcbaa179f694ca78e2998382e4094a3e3803c858e526d99224c238 82dc77d2a34065982c35d732c2ced4eb417556e5f6034430b73c98e35a4143203d 5ba001abe30e1d647023c35e425bd4818a192927916b36a82bfdc3fe3ddfda10839 c5f56010343e051fc98c6ff35eb6661356ab3c2854bca5a6e8d0f699bh
3	1.563	761d536faada91e5c851ef8fc4fc88a65736494118e3e1b4abb7722f50d794e9f1e07 52d732c18170f7577e4fe67c6f1d6b17766c386588354af928d5fc02d21310c2435 f3d3b13f5afc6a9194b89f5e802db8a92c7e2afb525470751cce0b4d596be73ac45a 19a9c2b955259759ec323520b4b4a36a470ac03102cf16f2d514h

In the IoMT environment, strong authentication by the Group Manager (GM) and the use of highly secure keys are helping to prevent the security threats such as data theft, eavesdropping, privacy loss etc. Additionally, the authentication mechanism must be efficient and fast without compromising security levels. A 256-bit encryption key is considered highly secure and is widely used in applications such as online banking, e-commerce and government communications [1].

In the proposed system, a 256-bit group key is generated using the dual encryption scheme. The AES algorithm contributes 128 bits, where brute-force attacks would require testing up to 3.403×10^{38} combinations, with an estimated breaking time of 3.19×10^{14} years [24]. The remaining 128 bits are secured using RSA encryption, further enhancing the difficulty for attackers. Moreover, attackers are unlikely to predict the use of a dual encryption mechanism combining two different algorithms. Further to strengthen security, the system enforces a key update policy where a new group key is generated for every 72 hours if the group key is not updated so far.

Security threats are categorized into external and internal attacks. External attackers may attempt to interrupt communication between the Group Manager and the Group Key Generator or obtain keys from group members. However, these attacks are mitigated by the dual encryption scheme and the implementation of forward and backward secrecy [21]. Internal attackers may attempt to access information from other group members [25]. This is prevented by restricting communication such that members interact only through the Group Manager. Therefore, the proposed dual encryption scheme effectively safeguards against both internal and external threats, ensuring secure group communication in IoMT environments.

4.2 Simulation Results

4.2.2 IoMT Environment Simulation Using NS3

The proposed group communication system is implemented /simulated by using the NS3 simulator after the generation of a group key. In this simulation process, the NS3 network consists of 50 nodes representing IoMT members, including patients, devices and healthcare professionals. Sample group key distribution scenarios are illustrated in Figs. 5, 6 and 7.

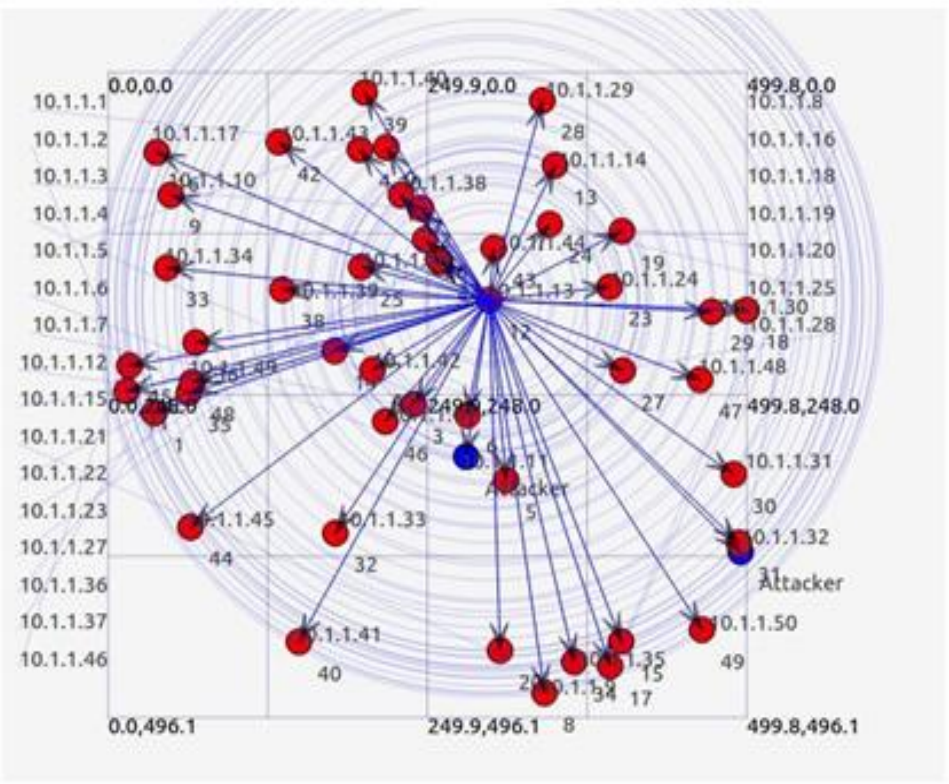

Fig.5. Sample group key distribution in the network from 12th node

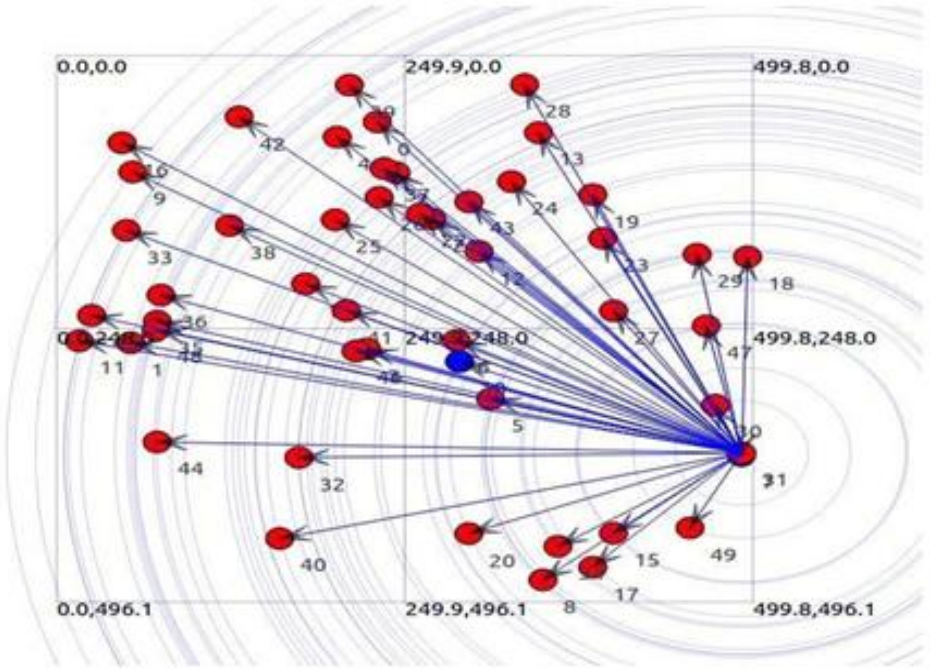

Fig.6. Sample group key distribution in the network from 31st node

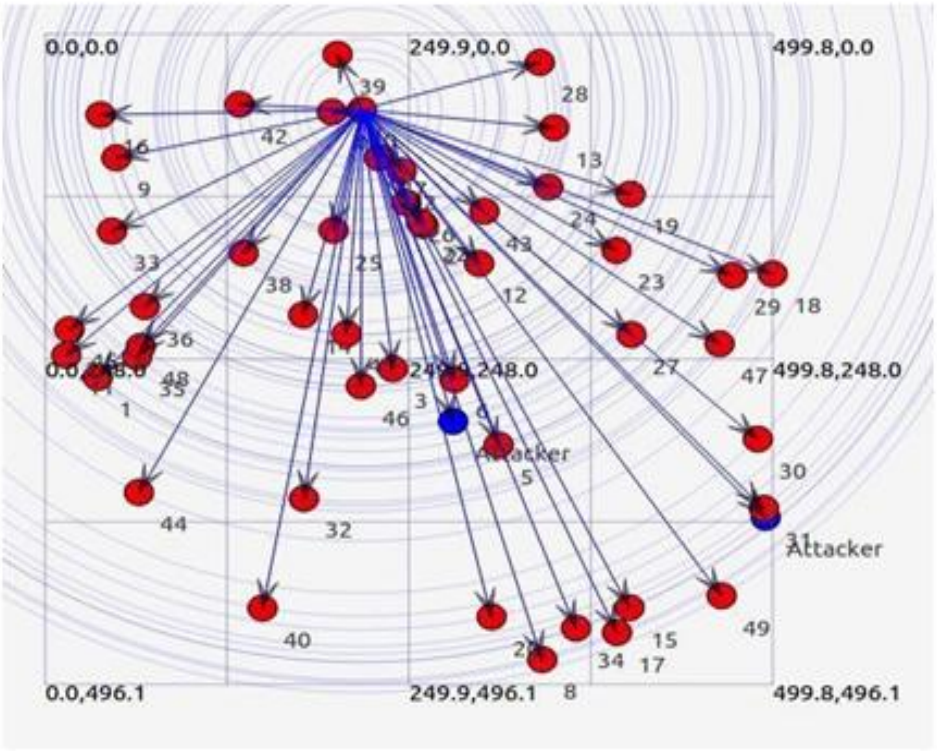

Fig.7. Sample group key distribution in the network from 39th node

4.2.3 Evaluation of Performance Metrics

The performance of the proposed dual encryption scheme is evaluated using performance metrics such as packet delivery ratio (PDR), throughput and delay. The proposed group key is compared with the traditional KDC-based key approach.

a) Packet Delivery Ratio (PDR):

PDR is defined as the ratio of successfully received packets to the total number of transmitted packets is depicted in Fig.8.The proposed scheme demonstrates higher PDR due to efficient path selection with minimal interference and congestion, outperforming the KDC-based approach [26,27].

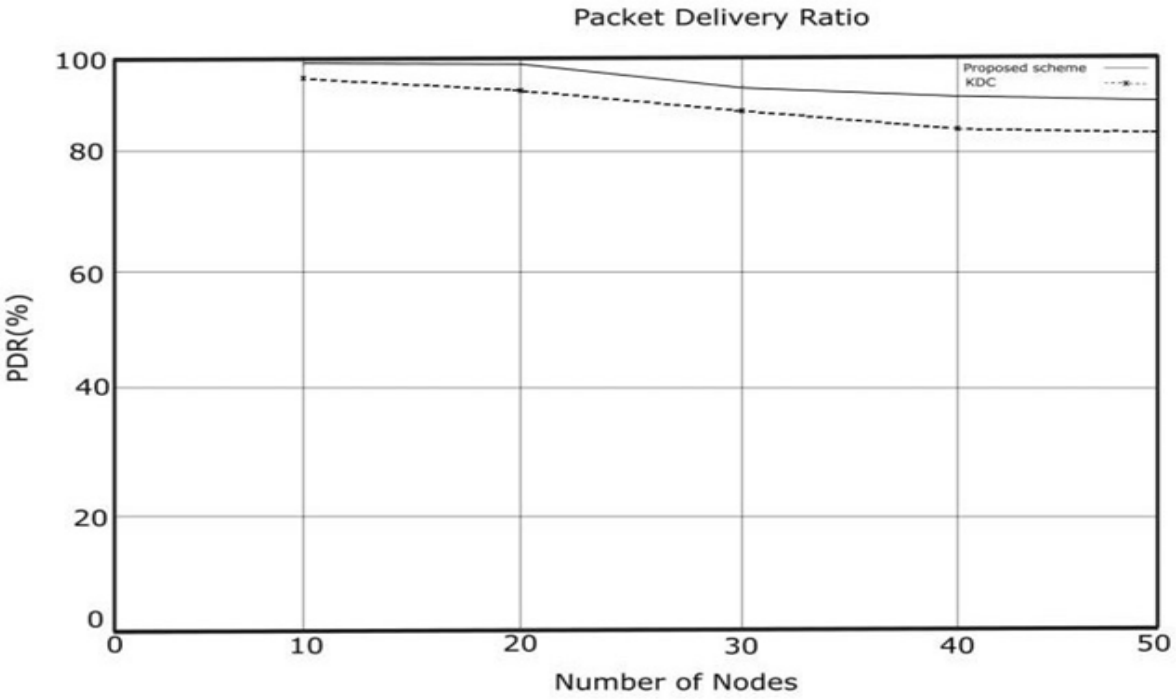

Fig.8. Packet delivery ratio vs number of nodes plot

b)Throughput:

Throughput represents the rate at which data packets are successfully delivered over the network is depicted in Fig.9. The proposed system achieves higher throughput by ensuring faster and more reliable data transmission compared to the KDC method [26, 27].

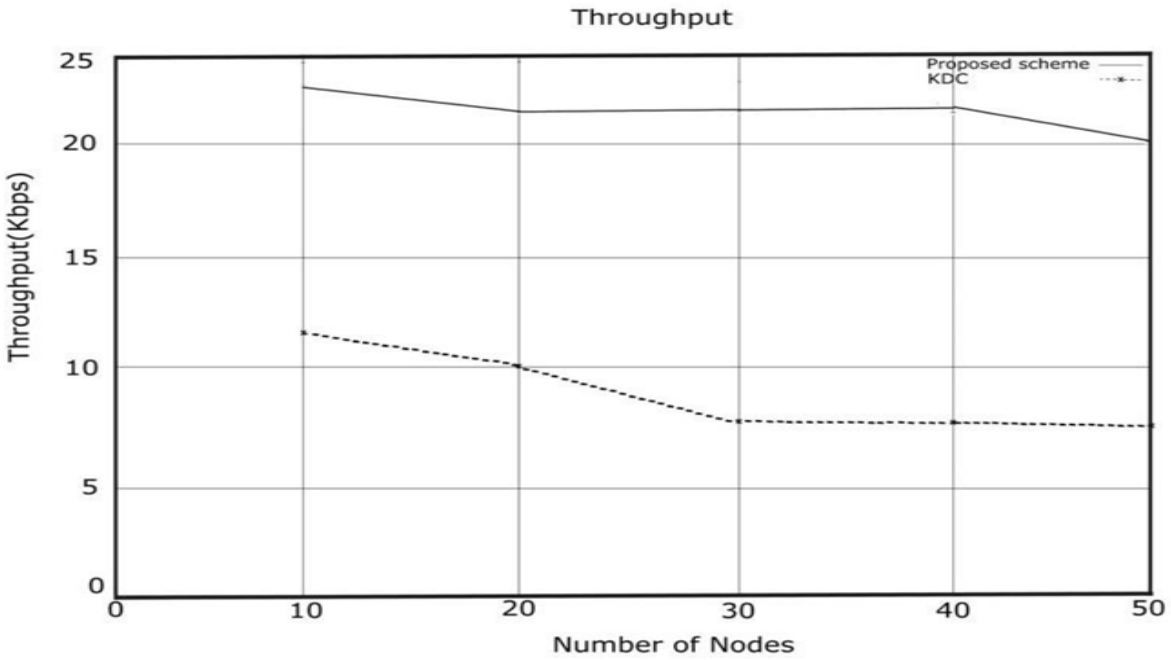

Fig.9. Throughput vs number of nodes plot

c) Delay:

Delay refers to the time taken for data packets to reach the destination is depicted in Fig.10. Increased congestion leads to higher delay, whereas less congestion path reduces it. The proposed scheme minimizes delay by selecting less congested communication paths, thereby improving overall performance [26, 27].

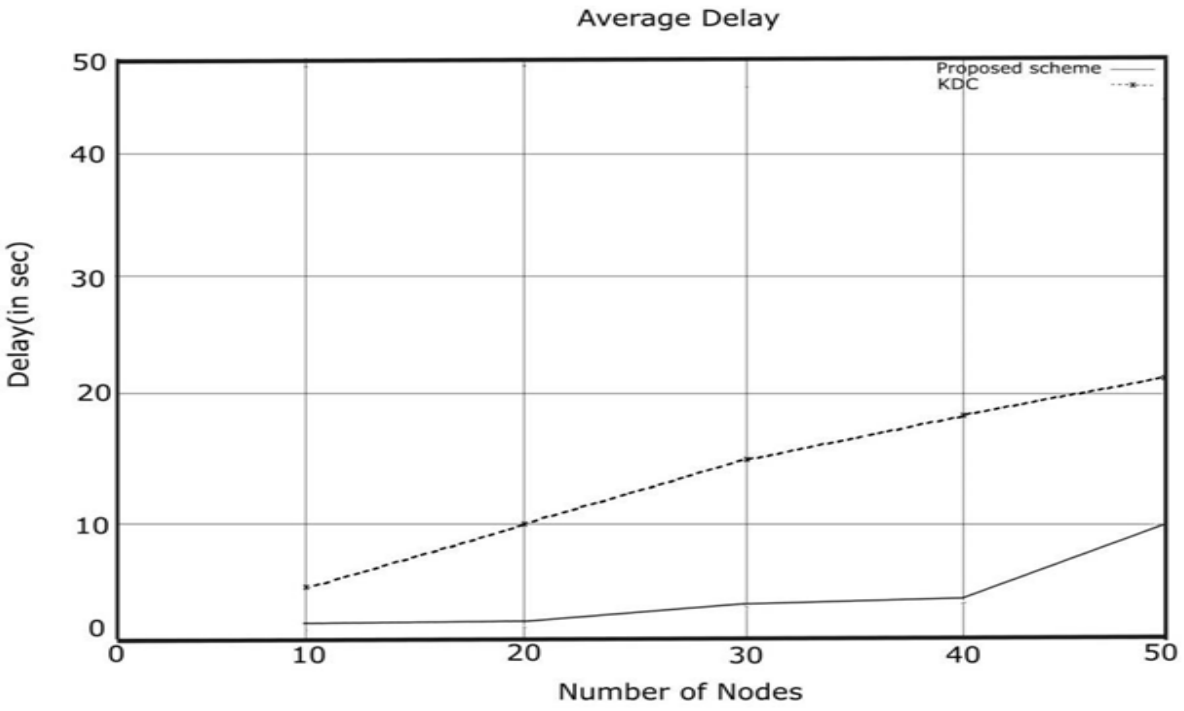

Fig.10. Delay vs number of nodes plot

Overall, the dual encryption scheme demonstrates more performance in generating secure group keys and enabling efficient communication in IoMT environments. The significance of this study is particularly evident in modern healthcare applications such as telemedicine, which has gained more importance after the COVID-19 pandemic. The proposed dual encryption approach ensures secure transmission of sensitive medical data, making it highly suitable for IoMT-based healthcare systems.

5. Conclusions

The Group communication in the Internet of Medical Things (IoMT) has activated as an important area of research. The security plays a critical role, especially when multiple devices and patients interact with the Group Manager. In this study, a dual encryption scheme has been effectively implemented to generate secure group keys for safe communication within the IoMT environment. The proposed system has been implemented and analysed using the NS3 simulator, demonstrating the group communication process among IoMT members. The performance of the system has been evaluated using key metrics such as packet delivery ratio, throughput and delay, confirming its efficiency. Overall, the results indicate that the proposed dual encryption scheme provides a secure and efficient solution for IoMT-based communication. The proposed system can be effectively adopted by healthcare institutions to ensure safe data transfer among authorized users, since this research work proves to be highly reliable and suitable for secure IoMT environments.

Acknowledgements

We would like to express our special thanks to Dr. K. S. Easwarakumar, Professor (Retired), Department of Computer Science, Anna University CEG campus, Chennai for useful discussions, his interest and encouragement. The first author (SB) is very grateful to "**Baby-Perumal Research Institute**" at Chennai for research guidance and supporting us with computing facilities.

References

1. S.Kavitha, P.J.A.Alphonse, Y.Venkataramana Reddy. (2019), "An Improved Authentication and Security on efficient Generalized Group Key Agreement Using Hyper Elliptic Curve Based Public Key Cryptography for IoT Health Care System", *Journal of Medical Systems*, 43: 260, pp.1-6.
2. Maissa Dammak et al. (2020), "Decentralized Lightweight Group Key Management for Dynamic Access Control in IoT Environments", *Transaction on Network and Service Management*, 1932- 4537, pp.1-15.
3. Rajeev Kumar Gupta et al. (2022), "An Improved Secure Key Generation Using Enhanced Identity- Based Encryption for Cloud Computing in Large-scale 5G", *Wireless Communication and Mobile Computing*, Article Id 7291250, pp.1-14.
4. Ahmad Mansour, Khalid M.Malik. (2020). "ALMs: Asymmetric Lightweight Centralized Group Key Management Protocol for VANETs", *IEEE Transaction on Intelligent Transportation Systems*, 1524- 9050, pp.1-16.
5. Xin Zhou, Xiaofei Tang. (2011), "Research and implementation of RSA algorithm for encryption and decryption", *2011 6th international forum on strategic technology, IEEE*, 978-1-4577-0399-7/11, pp.1118-1121.
6. Aman Chadha et al. (2015), "Dual-Layer Video Encryption using RSA Algorithm", *International Journal of Computer Applications*, 116 (1), pp.33-40.
7. Md.Mijanur Rahman, Tushar Kanti Saha, Md.Al-Amin Bhuiyan. (2012), "Implementation of RSA Algorithm for Speech Data Encryption and Decryption", *IJCSNS International Journal of Computer Science and Network Security*, 12(3), pp.74-82.
8. Dr.Prena Mahajan, Abhishek Sachdev. (2013), "A study of Encryption Algorithms AES, DES and RSA for Security", *Global Journal of Computer Science and Technology Network, Web & Security*, 13(15), pp.15-22.
9. Dalia Mubarak Alsaffar et al. (2020), "Image encryption based on AES and RSA algorithms", *In 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS), IEEE*, 978- 1-7281-4213-5/20, pp.1-5.
10. Viney Pal Bansal, Sandeep Singh. (2015), "A Hybrid Data Encryption Technique using RSA and Blowfish for Cloud Computing on FPGAs", *2015 2nd International Conference*

on Recent Advances in Engineering & Computational Sciences (RAECS), IEEE, 978-1-4673-8253-3/15.

11. Pooja, R.K.Chauhan. (2020), "Triple phase hybrid cryptography technique in a wireless sensor network", *International Journal of Computers and Applications*, ISSN: 1206-212X.
12. Juvi Bharti and Sarpreet Singh (2014), "A Hybrid Approach Using AES-RSA Encryption for Cloud Data Security", *International Journal of Intelligent Systems and Applications in Engineering (IJISAE*), 12(21s), pp.62-69.
13. Sa'idu Sani. (2022), "An Improved Cryptographic Scheme Using AES & RSA Algorithms for Maximum Security in File Encryption and Decryption", *International Journal of Scientific Development and Research (IJSDR),*7(6), pp.494-500.
14. V.Jagadeewari et al. (2018), "A study on medical Internet of Things and Big Data in personalized healthcare system", *Health Information Science and Systems*, 6(14), pp.1-20.
15. Bayu Anggorojati and Ramjee Prasad. (2018), "Securing Communication in the IoT-based Health Care Systems", *Jurnal Ilmu Komputer dan Informasi (Journal of a Science and Information)*, 11 (1), pp.1-9.
16. Gulraiz J.Joyia et al. (2017), "Internet of Medical Things (IOMT): Applications, Benefits and Future Challenges in Healthcare Domain", *Journal of Communications, Research Gate*, DOI:10.12720/jcm.12.4.240-247, pp.240-247.
17. Maria Papaioannou et al. (2019), "A Survey on Security threats and Countermeasures in Internet of Medical Things (IoMT)", *Trans Emerging Tel Tech.2020*; e4049, pp.1-15.
18. William Stallings, "Cryptography and Network Security Principles and Practices", Book Fourth Edition, 2005.
19. K.R.Monisha. (2015), "Secure Cloud Computing using AES and RSA algorithms", *20th IRF International Conference*, pp.12-17.
20. Komal Rege et al. (2013), "Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA", *International Journal of Computer Applications*, 71(22), pp.10-13.
21. Yi-Hsuan Kung and Hsu-Chun Hsiao. (2018), "GROUPIT:Lightweight Group Key Management for Dynamic IoT Environments", *IEEE INTERNET OF THINGS Journal*, X(X), pp.1-11.
22. M Sravani,R Sreenivasulu, P C Praveen Kumar. (2022), "Secured Medical Data Transmission Model for Health Care Systems", *Journal of Engineering Science*, 13(01), pp.308-311.
23. Mohamed Elhoseny et al. (2018), "Secure Medical Data Transmission Model for IoT-Based Healthcare Systems", *IEEE Access. Information Security solutions for Telemedicine Applications*, vol.6, pp.20596- 20608
24. Abdullah Al-Mamun et al. (2017), "Security Analysis of AES and Enhancing its Security by modifying S-Box with an Additional Byte", *International Journal of Computer Netwoks & Communications (IJCNC)*, 9(2), pp.69-88.
25. Yi Sun et al. (2012). "An Authenticated Group Key Transfer Protocol Based on Secret Sharing", *International workshop on Information and Electronics Engineering (IWIEE), ELSEVIER, Procedia Engineering* 29, pp.403-408.
26. Manu Elappilaa, Suchismita Chinara, Dayal Ramakrushna Parhi.(2027), "Survivable Path Routing in WSN for IoT applications", *Journal of Pervasive and Mobile Computing*, http://doi.org/ 10.1016/j.pmcj.2017.11.004, pp.1-20.
27. Kavita Jaiswal, Veena Anand. (2019), "An Optimal QoS-aware multipath routing protocol for IoT based Wireless Sensor Networks", *Proceedings of the Third International Conference on Electronics Communication and Aerospace Technology [ICECA 2019], IEEE*, pp.857-860.