Volume 13 Number 02 June 2023

Secured Data Transfer with Multi Layered Secured Encryption Standards Using Onion Protocol

M. Sumithra[1], B. Buvaneswari[2], Mohan Raj S[3], Jagadesh E[4], Ganesh N[5]

[1, 2] Professor, Department of Information Technology, Panimalar Engineering College, Chennai
[3, 4, 5] Department of Information Technology, Panimalar Engineering College, Chennai

[1]sumithram.id@gmail.com [2]buvanrajan16@gmail.com [3]mohanrajsrinivasan27@gmail.com
[4]jagadeshezhil74@gmail.com [5]ganeshzane@gmail.com

Abstract: Because of the increased reliance on technology and the internet. With so much personal and sensitive information being exchanged over networks, the risk for cyber assaults and data breaches is greater than ever. This paper aims to increase the security of data against various attacks in a network. A multi-layered secured encryption standard using onion protocol was proposed in this paper to improve the security of data. This model would first choose the optimum path to deliver the data. The data is first encrypted at the source end using the RSA technique, then it is sent to the subsequent node where decryption occurs, which finally goes to the destination. The result shows that for larger files, our model's decryption process is faster than the encryption process. Since multilayer encryption is used, even if one layer of encryption is broken, the data remains encrypted and secured by the other levels of encryption. So this model can be an effective approach to in-crease the security of data against several attacks compared to other encryption schemes.

Keywords: Network Security, Privacy, Onion Protocol, RSA Algorithm, Multi-layered Encryption

I. Introduction

The practises and regulations used to prevent and maintain records of unauthorised use of a network and its services are referred to as network security. Security of a network depends on the authorization of data access, which is managed by the network administrator. By selecting or obtaining an ID, passcode, or other authentication information, users can get access to information and programmes under their control. Public and private computer networks that are used in daily business activities, such as processing the transaction and facilitating communications between businesses, governmental organisations, and individuals, are all included in the scope of network security. Public networks can coexist with private networks, such those inside a company. Network security is an issue for all organisations, businesses, and other types of institutions. It accomplishes precisely what its name suggests: it protects and monitors activity while also securing the network. The most well-known and simple way to protect a network infrastructure is to assign it a special name along with a password.

1.1 Need for the Study

The main concern in the current environment is that data transported over networks is readily hacked and altered or manipulated. In the current scenario, data loss is also a major concern. If a packet is dropped in the midst of a message, the recipient must ask the source node again for the message to be sent, which cost time and traffic. Take into account the several Nodes communicating with one another; packet loss lengthens both duration and traffic.

Onion routing is a mechanism that can present data packets with many levels of encryption as they transit across the network. Because attackers would have to get through many levels of encryption, intercepting or decrypting the data would be significantly more difficult. We can gain a better knowledge of how to construct stronger encryption techniques that safeguard data more efficiently by researching this methodology.

One of the fundamental advantages of onion routing is that it may assist users maintain their anonymity. Data becomes increasingly more difficult to trace back to its original source when it gets encrypted and routed via several nodes in the network. This can be useful for users who want to safeguard their online privacy, as well as journalists, activists, and others who may be subject to monitoring or censorship.

By researching onion routing and multilayer encryption, we may learn how to build more secure networks and apps. This is particularly critical in today's environment, as cyber-attacks are growing more prevalent and sophisticated.

Onion routing and multilayer encryption are becoming increasingly widespread in new technologies such as block chain and the dark web. We can better understand how these technologies function, their advantages, and their concerns by researching them.

The use of onion routing and multilayer encryption involves fundamental ethical concerns, as with any technology. We may gain a better knowledge of the possible hazards and advantages of these treatments by studying them and making more educated judgements regarding their usage.

1.2 Objective of the Study

In this paper, we construct secure data transfer between the origin and the destination across a network. We make sure that data travels through several nodes securely in order to get to its destination. Only once we have the primary key and ID of the node can we send encrypted packets to that nodes for transmission. Using numerous layers of encryption, each added by a separate node in the network, the approach creates a chain of encrypted communications that can only be decoded by the intended receiver. As a result, a highly secure communication channel that is impervious to eavesdropping and manipulation is created. The efficiency of onion encryption can be affected by the protocol employed, as well as network circumstances and user behaviour. As a result, academics have looked at many elements of onion encryption, such as performance, weaknesses, and usability. Moreover, the legal and ethical aspects of onion encryption have been debated, since it may be used to mask unlawful activity while still protecting legitimate internet communication. Ultimately, the goal of this research is to get a better knowledge of onion encryption and its possible uses in improving online privacy and security.

II. Literature Review

Multilayer encryption, a method of combining many layers of encryption to improve the security of data, is thoroughly reviewed by this author. The writers go through many forms of multilayer encryption algorithms, their advantages and disadvantages, and how they are used in diverse fields [1].

Joshi, R. C. et al. propose using multilayer encryption for wireless sensor network communication security. The authors use both asymmetric and symmetric encryption methods to improve data transport security. By simulating the proposed method and comparing it to other encryption algorithms, the effectiveness of the recommended strategy in boosting security is evaluated [2].

A multilayer encryption method for data stored in the cloud security was proposed by Saluja, S. S. et al. The authors use a key administration system together with both asymmetric and symmetric encryption techniques to boost the integrity of data saved to the cloud. Simulated results are used to evaluate the recommended algorithm's effectiveness in boosting security and to compare it to other encryption techniques [3].

In [4], the authors proposed a multilayer encryption system built on the foundation of chaotic maps and the Advanced Encryption Standard (AES). The authors create encryption keys with the use of chaotic maps, which they then combine with AES to increase data transmission security. The efficiency of the suggested strategy in enhancing security is assessed through simulation and comparison with different encryption techniques.

For improved security in wireless sensor networks, Mohapatra, S. K., and Rath, S. K. suggested a multilayer encryption method employing DNA computing in [5]. The authors create encryption keys using DNA computing, which are then combined with symmetric encryption techniques to improve data transmission security. The efficiency of the suggested strategy in enhancing security is assessed through simulation and comparison with different encryption techniques.

In [6], a unique multilayer encryption system based on several chaotic maps was proposed by Li, L., and Zhou, W. The authors create encryption keys using a variety of chaotic maps, which are then used with symmetric encryption methods to boost data transmission security. The efficiency of the suggested approach in enhancing security is assessed through simulation and comparison with different encryption schemes.

Z. Wu, et al. proposed a multilayer encryption system in [7] to safeguard the confidentiality of medical data stored in the cloud. To provide safe and effective data transfer in cloud computing settings, the suggested approach makes use of various encryption layers, including symmetric key encryption, public key encryption, and homomorphic encryption. The suggested scheme's effectiveness is further evaluated in the study using simulation tests, which demonstrate that it offers more security and efficiency when compared to current encryption techniques.

In [8], W. Wang and L. Gao proposed a multilayer encryption technique for network security based on Huffman encoding and chaos mapping. The suggested approach improves the security of data transmission in networks by employing various levels of encryption, such as Huffman encoding, bit-level permutation, and chaos mapping. Using simulated studies, the study assesses the performance of the suggested algorithm and demonstrates that it offers more security and efficiency when compared to current encryption techniques.

In [9], the authors propose a layered encryption system based on RSA and chaotic maps for wireless sensor

networks to provide safe communication. The suggested method offers high levels of security and effectiveness in wireless sensor networks by employing various layers of encryption, including RSA encryption and chaotic map-based encryption. Using simulated studies, the study assesses the performance of the suggested method and demonstrates that it offers more security and efficiency when compared to current encryption techniques.

A multilayer encryption system has been proposed by M. Islam and colleagues for safe data transfer in wireless body area networks (WBANs) in [10]. In order to offer safe and effective data transmission in WBANs, the suggested approach makes use of numerous encryption layers, including a symmetric key encryption layer, a public key encryption layer, and a chaotic map-based encryption layer. Using simulated studies, the study assesses the performance of the suggested method and demonstrates that it offers more security and efficiency when compared to current encryption techniques.

In [11], an overview of the security problems that cloud computing faces, including concerns about data privacy, confidentiality, and integrity, is given by Wang, Y., Xu, S., Jia, L., & Wang, Y. The authors review a number of methods, such as encryption, access control, and intrusion detection systems, for maintaining data security in cloud computing.

In [12], Shieh, C. et al. discuss how block chain technology might improve data security and privacy protection. The authors give a general review of block chain technology and its salient characteristics and investigate several applications for block chain based data security, such as in the fields of banking, healthcare, and supply chain management.

Almorsy, M. et al. present a detailed analysis of the big data security difficulties, including issues relating to data privacy, confidentiality, and integrity in [13]. The authors review a number of methods, such as data masking, access control, and encryption, for maintaining data security in large data.

In [14], an overview of numerous strategies for assuring data security in cloud computing is provided by Kumar, P., Singh, K., & Singh, P. The writers go over a number of methods, including as encryption, access control, and intrusion detection systems, for maintaining data privacy, confidentiality, and integrity.

In [15], Chen, Y., et al. provide a summary of privacy and security of data problems in the IoT. The authors discuss several techniques for ensuring privacy and security of data in the IoT such as cryptography, access control, and intrusion detection systems. They examine the challenges in protecting IoT systems, networks, and devices while highlighting promising areas for further research.

In [16], Patil and Narote provide an improved multilayer encryption method that uses a Hill cipher and chaotic map to ensure safe communication. Before using the Hill cipher technique, the plaintext message is first encrypted using the chaotic map. By contrasting their strategy with other encryption methods, the authors illustrate how successful it is and how much more secure and effective it is.

For text communications, Othman, Aziz, and Tham describe a safe multilayer encryption system that makes use of DNA-based steganography. The suggested method uses a substitution approach to embed the plaintext into a DNA sequence after first using the Caesar cypher to encrypt it. The Blowfish technique is then used to further encrypt the obtained DNA sequence. The authors demonstrate how their strategy offers robust protection against several assaults in [17].

For safe picture transmission, Pramono, Nugroho, and Purnomo suggest a multilayer encryption system that makes use of a chaotic map and DNA encoding in [18]. The suggested method first turns the picture into a matrix, which is then chaotically mapped to make it unpredictable. Then, a DNA encoding method is used to translate the scrambled matrix into DNA sequences. Advanced Encryption Standard (AES) encryption is then applied to the obtained DNA sequence. The authors demonstrate how their method offers great security and resilience against attackers.

A multilayer encryption method for text data employing the Hill cypher, AES, and Blowfish is proposed by Sudarsana, Darmawan, and Setiawan in [19]. The Hill cypher is used to initially encrypt the plaintext message, then the AES and Blowfish algorithms are then used to further encrypt the cipher text produced. The authors demonstrate that their method offers more security and is quicker to compute than previous encryption methods.

A multilayer encryption system for safe data transfer in a cloud setting is presented by Saboor, Mehmood, and Ullah in [20]. The suggested method uses the RSA algorithm for key exchange and the Blowfish technique to encrypt the plaintext data after that. A symmetric key produced by a chaotic map is used to further encrypt the cipher text that results from this process. The authors com-pare their strategy to existing encryption methods and show that it offers greater security and efficiency to prove the strategy's efficacy.

III. Proposed Work

This study suggests a multi-layered safe encryption standard based on the onion protocol. After registering with the server, each node will receive a decryption key, a primary key, a secondary key and an id. Data is first encrypted using the RSA technique, and then using a master key that corresponds to each hop. The intermediary node's ID is likewise hashed for confirmation. The data being transmitted is initially encrypted using the (RSA) technique in the suggested model, then the same data is secretly encoded using the public key of the target

node, "E" and then the same cipher text is once again encoded using the public keys of the intermediary node "C", assuming "C" is chosen as the best access point connecting "A" which is the source node and "E" the target node. Data that has been multiple encrypted will be sent to intermediary node "C". The Private Key and ID of the "C" Node are now validated. After verification, the initial layer of encryption on the data is decoded. It is then sent to Node "E" its ultimate destination. The second layer may now be decoded by looking up E's private key. The last layer is decrypted with "E" Node's Secret Key. At the end, the original data is delivered to the Destination Node "E".

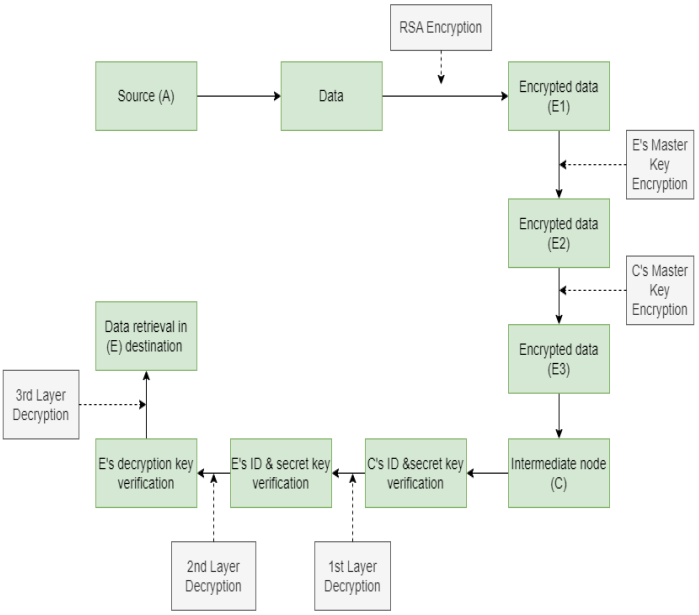

Fig. 1. General architecture of multi-layer encryption model

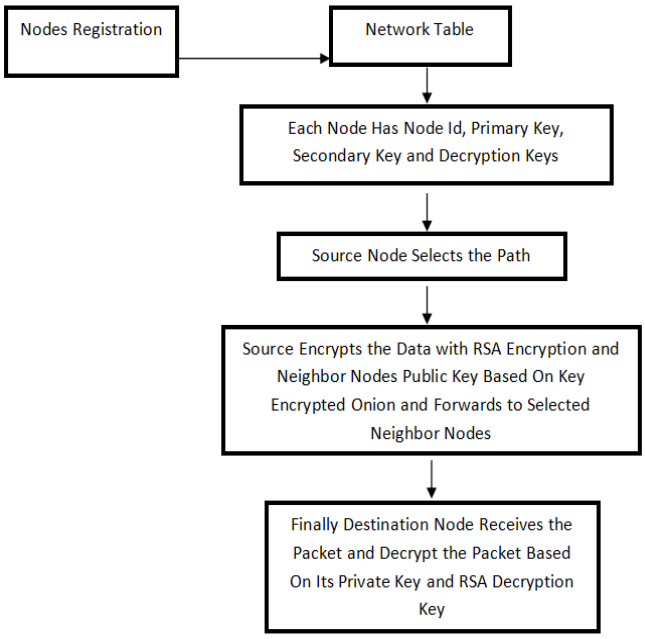

Fig. 2. Data Flow Diagram of multi-layer encryption model

3.1 The Process of RSA Algorithm

Public-key cryptosystems are characterised by the use of two distinct keys a public key and a private key for encryption and decryption, and by the fact that the secret key cannot be inferred from the public key. This enables the disclosure of the public key without running the danger of the information being compromised. RSA is the most significant kind of public key encryption and has so far proved to be almost immune to password attacks.

The value n, which is the result of multiplying two different primes, p and q, is used by the RSA cryptosystem to complete the following lines of operation These are the RSA algorithm's specifics.

i. Key Generation

a. Choose two K/2 bit long random primes, p & q.

b. Determine the modulus (n).

$$n = p*q \quad (1)$$

c. Determine the totient, φ(n), by using the formula

$$\varphi(n) = (p-1) * (q-1) \quad (2)$$

d. Choose an integer e, such that gcd (e, φ(n)) =1 and 1< e <φ(n).

e. The private exponent (d), is calculated. This may be accomplished using the extended Euclidean approach.

$$d \equiv e^{(-1)}(\text{mod } \varphi(n)) \quad (3)$$

f. The modulus (n) and the public exponent (e) make up the public key. The modulus (n) with the secret exponent (d) make up the private key.

ii. Encryption

a. Choose a plaintext message (M) and convert it to a numerical value using a specified encoding scheme.

b. Calculate the cipher text value (C).

$$C \equiv Me \text{ (mod } n)$$

(4)

iii. Decryption

a. Calculate the plaintext value (M).

$$M \equiv Cd \pmod{n} \quad (5)$$

b. Convert the numerical value back into the original message using the encoding scheme.

IV. Module Description

4.1 Network Construction

The first step in doing so is to build a network with "n" nodes. So that the nodes of the network can ask other nodes for information We may expect that the nodes are moving around the network since they possess the mobility attribute. The network stores all node details, including nodes id and other data. There are master and backup keys for every node. Also, the network will keep track of every node's communication for security reasons.

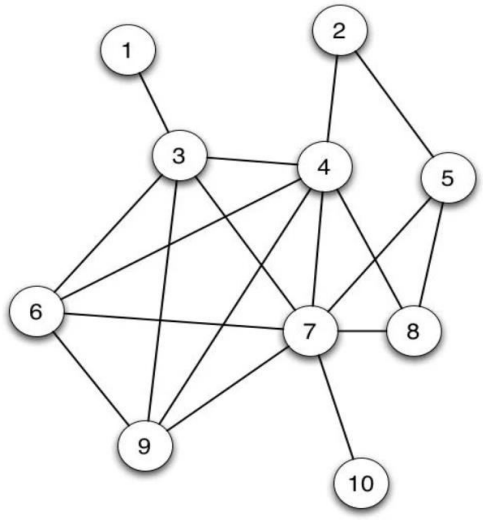

Fig. 3. Network construction of nodes

4.2 First Level Encryption

The data that has to be communicated from the source is encrypted in this module before it is sent to the target. With this module, data security is assured. This encryption procedure serves as the first layer of protection before being followed by many layers of encryption.

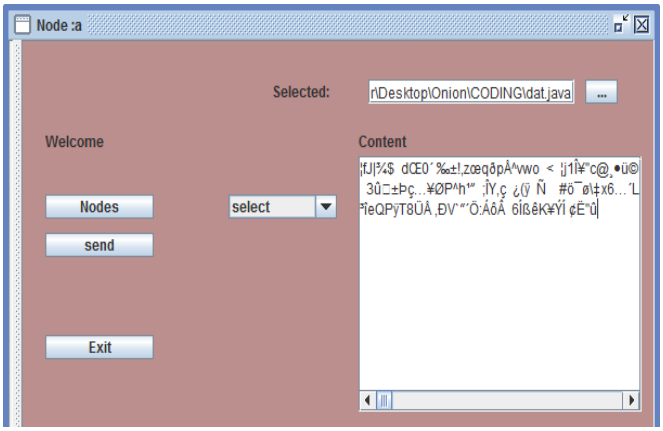

Fig. 4. Output of first level encryption of plain text

4.3 Multi-Layered Encryption Model

The main project's multi-layer security implementation is accomplished with this Module. After the first level of encryption, the identical data is encrypted once again using the intermediary node's and recipient master keys. The intermediate node is receiving data that has been multi encrypted. The Intermediary Network node Private Key and ID will now be verified by our system. The data's first layer of encryption is decrypted after verification. After that, data is sent to the final Node. The second layer is now decoded by confirming the destination node's secret key. Finally, using Destination's Decryption Key, the single layer is decrypted. Eventually, the Destination Node receives the Original data back.

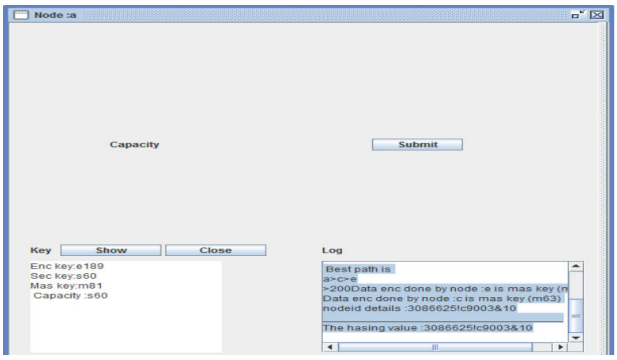

Fig. 5. Best path selection for transfer of data

4.4 Decryption Process

In this module, the data is sent to the target node after being initially decoded by the neighbour node. The destination node then uses both its secret key as well as the AES decrypt key to decode the message. The destination node may now view the original data. As the capacity of the pathways will change dynamically, the paths will

change according to the network's data transfer. As a result, it improves the packet delivery rate and cuts down on the typical end-to-end latency.

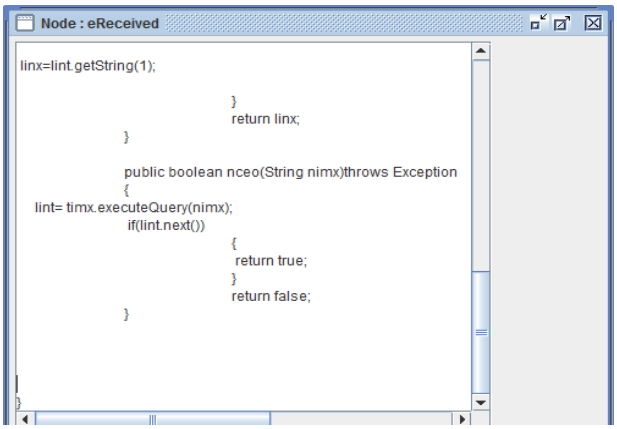

Fig. 6. Decryption at the destination node

V. Results and Discussion

This study proposes a multi layered security system to protect client data and server traffic in a network. Moreover, the data acquisition process will be more securely conducted. In this case, onion layer encryption is used to safeguard client confidentiality. The data cannot be altered or modified by attackers. The encryption and decryption time analysis for multilayer encryption model is shown in (Fig. 7), in which key size of 1024 bits is used. The results may differ depending on a number of parameters, including key size, computer processing capability, and algorithm implementation.

TABLE I
PERFORMANCE MEASURE OF MULTI-LAYER ENCRYPTION MODEL

File Size (Kbits)	Encryption Time (ms)	Decryption Time (ms)
10	202	204
50	500	410
100	680	620
200	1160	1100
512	1600	1500
1024	2040	1800

The data from (TABLE I) shows that the time required for both encryption and decryption grows as the file size does as well. This is due to the fact that processing bigger files takes longer and more computationally intensive. The fact that the decryption process requires more calculations than the encryption process contributes to the fact that the decryption time is often a little bit longer than the encryption time.

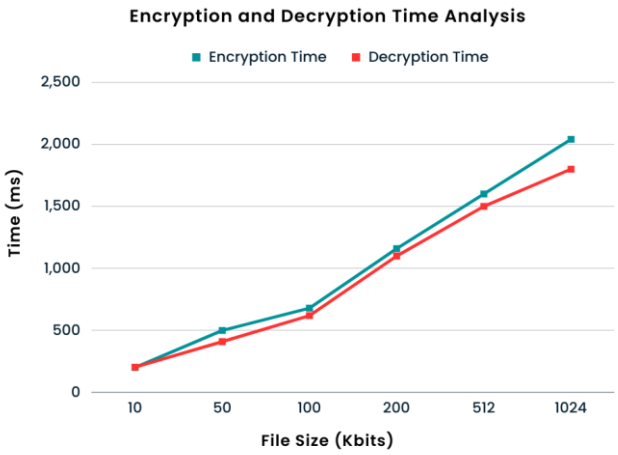

Fig. 7. Encryption and Decryption Time Analysis of Multi-Layer Encryption Model

Also, from (Fig. 7) it can be seen that as file size grows, the ratio of decryption to encryption time drops, suggesting that for bigger files, the decryption procedure is computationally less demanding than encryption. In general, the information in the table may be used to evaluate how well the multilayer encryption model performs for various file sizes. Since multilayer encryption is used, even if one layer of encryption is broken, the data remains encrypted and secured by the other levels of encryption. So this can be an effective approach to increase the security of data against several attacks compared to other encryption schemes like Symmetric and Asymmetric encryption.

Attacks involving forgery are impossible since we employ the SHA-256 hashing algorithm in this instance for client authentication. Only authorised clients are allowed access to the data server. So the model is efficient against fabrication attacks.

The server won't accept requests made by attackers who attempt to alter the route path. Because every intermediate in a server route only knows the intermediate before and after it Because of onion encryption, they are unsure about what will happen next. So the model is efficient against route modification attacks.

Attacks involving the modification of client data are not possible on the server, due to the fact that we encrypt the data using RSA algorithm. When an attacker tries to add data, they must first compute hashes and then have all clients on the server validate the addition before it can be made. So the model is efficient against data modification attacks.

With DoS and DDoS attacks, attackers try to block the route in order to produce unauthorized traffic. Several requests will be sent to the server by the at-tacker. By

verifying each request in this case to safeguard the data server, we reduce the effect of the assault. So the model is efficient against Dos and DDos attacks.

VI. Conclusion

In the proposed work, we implemented a multi-layer security system with multi-hop connection to effectively transfer data from the source to the destination. For extremely secure data communication, we developed a Complicated Multilayer Secured Protocol. Apart from Multi-Layer Encryption, we also used RSA to encrypt data. Finally, the multilayer encryption project is a complicated system that delivers high-level data protection. To safeguard the data from illegal access and hacking attempts, the project employs numerous levels of encryption methods such as RSA and SHA-256. The use of several encryption levels adds another degree of defence against assaults and helps to guarantee that data remains safe even if one layer is compromised. This project's next development will involve connecting routes dynamically in case an intermediate node fails. In addition to capacity calculations, we may take into account throughput and energy while deciding on the best route or hop for data transfer.

VII. References

[1] S. K. Srivastava and S. S. Bedi, "Multilayer Encryption: A Review". International Journal of Computer Applications, vol. 80, no. 7, 2013, pp. 32-36.

[2] R. C. Joshi and A. Kumar, "Multilayer Encryption for Secure Communication in Wireless Sensor Networks". International Journal of Computer Science and Network Security, vol. 16, no. 7, 2016, pp. 98-103.

[3] S. S. Saluja and A. Kumar, "A Multilayer Encryption Algorithm for Data Security in Cloud Computing". International Journal of Computer Science and Information Security, vol. 15, no. 2, 2017, pp. 133-139.

[4] X. Ma and Y. Wang, "Multilayer Encryption Based on a Combination of AES and Chaotic Maps". Journal of Information Security, vol. 4, no. 4, 2013, pp. 202-209.

[5] S. K. Mohapatra and S. K. Rath , "Multilayer Encryption Using DNA Computing for Enhanced Security in Wireless Sensor Networks". Journal of King Saud University - Computer and Information Sciences, vol. 29, no. 2, 2017, pp. 266-275.

[6] L. Li and W. Zhou, "A Novel Multilayer Encryption Scheme Based on Multiple Chaotic Maps". Mathematical Problems in Engineering, pp. 1-9.

[7] Z. Wu, et al , "A Multilayer Encryption Scheme for Protecting Medical Data Privacy in Cloud Computing". Journal of Medical Systems, vol. 41, no. 12, 2017, pp. 1-11.

[8] W. Wang and L. Gao, "A Multilayer Encryption Algorithm Based on Huffman Encoding and Chaos Mapping for Network Security". International Journal of Distributed Sensor Networks, vol. 11, no. 9, 2015, pp. 1-8.

[9] K. C. Gupta and S. K. Singh, "A Multilayer Encryption Scheme Based on RSA and Chaotic Maps for Secure Communication in Wireless Sensor Networks". International Journal of Communication Networks and Information Security, vol. 9, no. 3, 2017, pp. 50-60.

[10] M. Islam, et al, "Multilayer Encryption for Secure Data Transmission in Wireless Body Area Networks". Journal of Medical Imaging and Health Informatics, vol. 6, no. 4, 2016, pp. 971-978.

[11] Wang, Y., Xu, S., Jia, L., & Wang, Y, "A Survey on Data Security in Cloud Computing". Journal of Network and Computer Applications, vol. 103, 2018, pp. 1-17.

[12] Shieh, C., Lee, C., Lee, C., & Wu, T "Blockchain-based Data Security and Privacy Protection". IEEE Communications Magazine, vol. 57(9), 2019, pp. 104-109.

[13] Almorsy, M., Grundy, J., & Müller, I, "Security in Big Data: A Review". IEEE Access, vol. 4, 2016, pp. 6587-6708.

[14] Kumar, P., Singh, K., & Singh, P, "A Review on Cloud Data Security Approaches". Journal of King Saud University-Computer and Information Sciences, vol. 29(4), 2017, pp. 362-376.

[15] Chen, Y., He, W., & Chen, S. (2020). "Data Security and Privacy Protection in Internet of Things: A Review". Journal of Network and Computer Applications, 152, 102528.

[16] S. K. Patil and S. P. Narote. "Enhanced Multilayer Encryption Using Chaotic Map and Hill Cipher for Secure Communication". Wireless Personal Communications, vol. 117, no. 1, pp. 101-119 (2021).

[17] M. Othman, N. A. Aziz, and W. Y. Tham. "Secure Multilayer Encryption with DNA-Based Steganography for Text Messages". Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 6, pp. 5345-5358 (2021).

[18] A. Pramono, M. A. Nugroho, and M. H. Purnomo. " Multilayer Encryption with Chaotic Map and DNA Encoding for Secure Image Transmission". Journal of Telecommunication, Electronic and Computer Engineering, vol. 13, no. 3, pp. 57-62 (2021).

[19] G. D. Sudarsana, R. D. Darmawan, and A. Setiawan. "Multilayer Encryption of Text Data Using Hill Cipher, AES, and Blowfish Algorithms". Bulletin of

Electrical Engineering and Informatics, vol. 10, no. 4, pp. 1803-1813 (2021).

[20] S. S. Saboor, A. Mehmood, and M. H. Ullah. "A Multilayer Encryption Scheme for Secure Data Transmission in Cloud Environment". Wireless Personal Communications, vol. 125, no. 3, pp. 1531-1551 (2021).

[21] Prince Roy, Rajneesh Kumar. "Multilevel Security Framework based on An Onion Encryption in Public Cloud Network." 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), 2021, pp. 123-128,

[22] M. Sumithra and Dr. S. Malathi, "A Novel Distributed Matching Global and Local Fuzzy Clustering(DMGLFC) FOR 3D Brain Image Segmentation for Tumor Detection", IETE Journal of Research

[23] B.Buvanswari and T.Kalpalatha Reddy, "A Review of EEG Based Human Facial Expression RecognitionSystems in Cognitive Sciences" International Conference on Enenrgy, Communication, Data analytics and Soft Computing(ICECDS),CFP17M55-PRJ:978-1-5386-1886-8",August 2017.

[24] M. Sumithra and Dr. S. Malathi, " Modified Global Flower Pollination Algorithm-based image fusion for medical diagnosis using computed tomography and magnetic resonance imaging", International Journal of Imaging Systems and Technology, Vol. 31, Issue No.1, pp. 223-235, 2021

[25] K. Sridharan , and Dr. M. Chitra "SBPE: A paradigm Approach for proficient Information Retrieval , Jokull Journal" , Vol 63, No. 7;Jul 2013

[26] M. Sumithra and Dr. S. Malathi, "3D Densealex NET Model with Back Propagation for Brain Tumor Segmentation", International Journal OfCurent Research and Review, Vol. 13, Issue 12, 2021.

[27] B.Buvaneswari and Dr.T. Kalpalatha Reddy,"EEG signal classification using soft computing techniques for brain disease diagnosis",Journal of International Pharmaceutical Research ,ISSN : 1674-0440,Vol.46,No.1,Pp.525-528,2019.

[28] K. Sridharan , and Dr. M. Chitra "Web Based Agent And Assertion Passive Grading For Information Retervial", ARPN Journal of Engineering and Applied Sciences, VOL. 10, NO. 16, September 2015 pp:7043-7048

[29] M. Sumithra and Dr. S. Malathi, "Segmentation Of Different Modalitites Using Fuzzy K-Means And Wavelet ROI", International Journal Of Scientific & Technology Research, Vol. 8, Issue 11, pp. 996-1002, November 2019.

[30] M. Sumithra and S. Malathi, " A Survey of Brain Tumor Segmentation Methods with Different Image Modalitites", International Journal of Computer Science Trends and Technology (IJCST) – Vol. 5 Issue 2, Mar – Apr 2017

[31] B.Buvaneswari and Dr.T. Kalpalatha Reddy, "High Performance Hybrid Cognitive Framework for Bio-Facial Signal Fusion Processing for the Disease Diagnosis", Measurement,ISSN: 0263-2241, Vol. 140, Pp.89-99,2019.

[32] M. Sumithra and Dr. S. Malathi, "A Brief Survey on Multi Modalities Fusion", Lecture Notes on Data Engineering and Communications Technologies, Springer, 35, pp. 1031-1041,2020.

[33] M. Sumithra and S. Malathi, "A survey on Medical Image Segmentation Methods with Different Modalitites", International Journal of Engineering Research and Technology (IJERT) – Vol. 6 Issue 2, Mar 2018.

[34] B.Buvaneswari and Dr.T. KalpalathaReddy,"ELSA- A Novel Technique to Predict Parkinson's Disease in Bio-Facial",International Journal of Advanced Trends in Computer Science and Engineering, ISSN 2278-3091,Vol.8,No.1,Pp. 12-17,2019

[35] K. Sridharan , and Dr. M. Chitra , Proficient Information Retrieval Using Trust Based Search On Expert And Knowledge Users Query Formulation System, Australian Journal of Basic and Applied Sciences, 9(23) July 2015, Pages: 755-765.

[36] B.Buvaneswari and Dr.T. Kalpalatha Reddy, "ACPT-An Intelligent Methodology for Disease Diagnosis",Journal of Advanced Research in Dynamical and Control Systems,ISSN : 0974-5572,Vol.11,No.4,Pp.2187-2194,2019.

[37] Sumithra, M., Shruthi, S., Ram, S., Swathi, S., Deepika, T., "MRI image classification of brain tumor using deep neural network and deployment using web framework", Advances in Parallel Computing, 2021, 38, pp. 614–617.

[38] K. Sridharan , and Dr. M. Chitra "RSSE: A Paradigm for Proficient Information Retrieval using Semantic Web" , Life Science Journal 2013;10(7s), pp: 418-425