Enhanced Data Security Framework Using Lightweight Cryptography and Multi-Level Encryption

Projjal Chakrabarty
School Of Computer Science & Engineering
Lovely Professional University
Phagwara - Punjab, India
projjal07@gmail.com

Tiyas Sarkar
School Of Computer Science & Engineering
Lovely Professional University
Phagwara - Punjab, India
info.tiyasofficial11901657@gmail.com

Manik Rakhra
School of Computer Science & Engineering
Lovely Professional University
Phagwara - Punjab, India
akhramanik786@gmail.com

Kapil Jairath
Department of Sciences
Trinity College
Jalandhar
Punjab, India
jairathkapil@yahoo.com

Vikrant Sharma,
SMIEEE Computer Science and Engineering
Graphic Era Hill University
Adjunct Professor
Graphic Era Deemed to be University
Dehradun, Uttarakhand, India.
vsharma@gehu.ac.in

2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE) | 979-8-3503-6684-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/IC3SE62002.2024.10593191

***Abstract*—Network security is essential for individuals as well as organizations in the modern day, since the majority of enterprises and organizations store their data on clouds. Therefore, a way to guarantee data security during network transmission needs to be discovered. Data security also heavily depends on device level security. These days, it's necessary to protect data at the device, network, and application levels simultaneously. The developers of the suggested concept use multi-level encryption techniques and lightweight cryptography algorithms to attempt to safeguard data on all three levels.**

This paper proposes multi-level cryptography as a fix for the previously noted issue that compared to normal encryption, which uses different keys for each round of encryption, resulting in a complex or powerful algorithm, multi-level encryption protects data more thoroughly.

Keywords—Healthcare, Multilevel Encryption, Lightweight PRESENT, Lightweight RSA, Cryptography

I. INTRODUCTION

This Data security is essential since a lot of stuff is transferred via networks these days. Employing a suitable privacy transformation methodology is the most effective way to secure data transferred across networks. Various tactics are employed to protect the private information. Most data these days is secured via encryption and certificate technologies [1]. Most methods are based on cryptography. A new concept known as multi-level encryption is used to make the system more secure than earlier cryptosystems. Leveraging the same as well as different keys, plain text is encrypted once or more times in the multi-level encryption approach. It makes the process more powerful and intricate than it was previously.

With an increasing number of IoT devices connecting to the internet and exchanging data, lightweight cryptography has become more and more important. To be secure, sensitive data needs to be encrypted. The use of cryptographic techniques and protocols in resource-constrained environments, such as embedded systems [2], smart cards, & Internet of Things devices, is known as lightweight cryptography. These systems have limited memory, energy, and processing capacity; therefore, they require cryptography particularly built for them. PRESENT is a very thin block cipher that was introduced as a privacy-enhanced reduced-sized block cipher. The cipher was designed [3] with high security, minimal energy use, & compact code size in mind. Since its release, the present has grown in popularity within the cryptography, which is used in a wide range of applications today, including wireless sensor networks, RFID tags, and smart cards.

II. BACKGROUND

A. Security outline of lightweight Cryptographic Algorithm

Cryptographic algorithms are used to secure data. Cryptography is the process of encrypting data into code for secure transmission. Cryptographic ciphers fall into two categories: symmetric & asymmetric ciphers. Symmetric key encryption encrypts and decrypt data using the same key. This encryption method is quite safe and reasonably rapid. The exchange of the private key between communication parties is the main disadvantage of symmetric key encryption. An attacker can compromise the data's encryption if they manage to gain the key. Symmetric key algorithms ensure data integrity and confidentiality but not authentication. Examples of conventional symmetric [4] key ciphers are (AES, DES, 3DES & BLOWFISH) among others. Asymmetric encryption offers confidentiality, integrity, and authentication. The transmitter encrypts data with its public key, & the recipient decrypts it with his private key, guaranteeing secrecy and integrity. To ensure authentication, the sender encrypts data using his private key. The recipient uses the sender's public key to decrypt the data and confirm its authenticity [5]. The fact that asymmetric cryptography permits key sharing and all other security techniques is one of its advantages. The

979--83503-6684-6/24/$31.00 ©2024 IEEE

magnitude of the keys is the only negative, as it increases complexity and slows down encryption. The three most often utilized methods are elliptic curve cryptography (ECC), Deffie-Hellmen key exchange (DHKE) & RSA by Rivest, Shamir, and Adleman.

B. Lightweight Algorithm Approaches

Our daily lives are filled with low-power devices, from medical equipment to digital companions to household appliances. Requiring an acceptable level of security is necessary because these gadgets often function on low power and hold valuable private information about us. Conventional encryption methods don't always work well on these kinds of devices because of possible restrictions in the software (i.e. processing speed) and hardware (i.e. memory) [6]. Because devices lack the computing power of laptops and smartphones, for example, low power with little power will suffer if a huge stream of data needs to be safeguarded quickly, such as a video stream. When trade-offs are chosen in a low-power system, security suffers since there is more restricted power available. for instance, are preferred in such a situation, as doing so could lower the security level of the system [7]. Therefore, the objective of lightweight cryptography aims to provide a certain level of security while utilizing the least amount of memory, computing power, or extra assets possible.

There might be software restrictions on memory capacity, processor speed, and latency for lightweight devices. Hardware that is lightweight may have restrictions on its performance, size, and power usage. When used in these situations, a lightweight cryptographic method that can offer a respectable degree of safety in a range of applications is necessary [8].

C. Lightweight RSA Algorithm

The RSA asymmetrical key encryption mechanism is based on the hard-to-find factor of big integers assumption. While a private key under RSA is kept confidential, the public key is shared with every framework participant. Three steps make up the RSA algorithm [9]: message encryption, message decryption, and key creation. The steps that follow are shown as shown as Fig. 1.

Figure 1. Framework Lightweight RSA algorithm step-wise approaches

III. PRESENT RSA ALGORITHM

With a symmetric key, the PRESENT scheme is a block cipher. It began to grow in the orange laboratory in 2007. The globally recognized organization created it in 2012 as an (ultra-lightweight block cipher) appropriate for lightweight encryption in resource-constrained environments. Devices with limited storage or low power consumption, such as network of things devices, use this method. Data and keys are used in the implementation of this algorithm [10].

64 bits make up a single chunk of data that is fed into the decryption as well as encryption procedure. Either 80 or 128 bits can make up the executable key. According to other studies, the security degree of the application determines the key size of the existing techniques. The 80-bit key was prioritized over the 128-bit key because some researchers had already implemented it or anticipated that the 128-bit key wouldn't be useful in real-world applications. A significant advancement in lightweight cryptography was brought about by the PRESNT algorithm [11] in 2007 with the introduction of numerous lightweight models, leading to the creation of a lightweight block cipher as shown as Fig. 2.

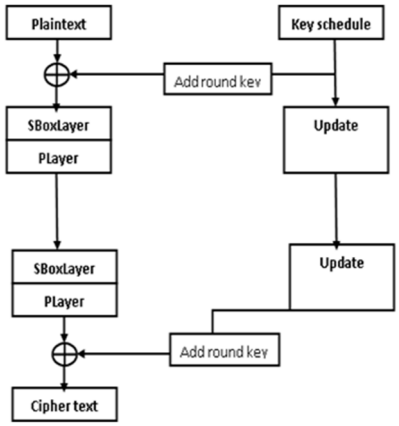

Figure 2. Presenting Process of RSA algorithm

The PRESENT algorithm is described by the following pseudocode:

ProduceRoughKeys()
End for addRoundKey (STATE, K32), AddRoundKey (STATE, Ki) for i=1 to 31 & State-specific s-BoxLayer and pLayer. Here is how the encryption process works:

a. AddRoundKey: XOR the 64-bit input and the round key.

b. S box: Every state 4-bit word is subject to an independent, non-linear substitution process called the S-box transformation.

c. Player: a permutation modification that operates on a 64-bit environment.

Fig. 3 which is included below and is suggested in this paper—flowcharts the suggested RSA algorithm.

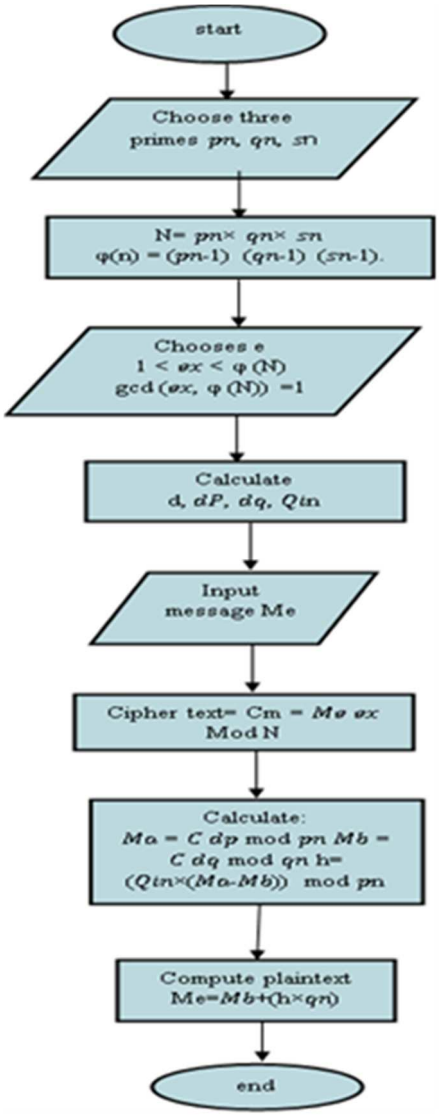

Figure 3. Stepwise approaches of process LW RSA Algorithm

IV. Improvement Of The Present S Box

A 4-bit S-box is used by the PRESENT cipher and is an essential part of its non-linear substitute level. This S-box is usually less in size since it is implemented more effectively than an 8-bit S-box. A table of hexadecimal symbols represents the capabilities of the S-box. Taking out plagiarism, let me explain briefly: A small 4-bit S-box is used in the non-linear substitution layer of the PRESENT cipher. This solution is significantly less in size while maintaining all of the capabilities of an 8-bit S-box. A hexadecimal sign table is usually used to indicate how the S-box operates. Desirable s-box successes include nonlinear behaviour, differential consistency, immune correlation, avalanche affecting, and avoidance of fixed or anti-fixed locations. This work generates optimized s-boxes (s-box S1 & S-box S2) with rate of diffusion by designing S-boxes using a genetic algorithm. This eliminates an anti-fixed-point challenge in the PRESENT s-box. Better s-boxes can be shown in Tables 2 and 3.

TABLE I. Present's S-Box

X	0	1	2		3	4	5	6	7	8	9	A	B	C	D	E	F
S(X)	c	5	6		B	9	0	A	D	3	E	F	8	4	7	1	2

TABLE II. Augmentation Of Sbox - S1

A	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(A)	C	6	1	4	9	0	A	D	3	E	F	8	B	7	5	2

TABLE III. Augmentation Of Sbox - S2

A	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(A)	2	5	E	9	1	D	0	B	4	3	7	C	F	6	A	8

The improved techniques applied on research make use of the concepts of crossover as well as mutation in the genetic algorithm. In pairs, these crossover regulators are utilized to transfer genetic information among members of bigger groupings.

V. Related Work And Proposed Methodology

Three layers make up the most common and well-known architectural design. The IoT study was initially conducted in its infancy. It indicates three levels: application, network, and perception layer [12].

A. Application Layer

The user interface layer is in charge of making it easier for consumers to interact with software resources. One example of this is a smart home app that allows users to click a button to control appliances like coffee makers. This layer gives users access to resources that are relevant to their application, enabling a range of features designed for particular uses such as intelligent houses, intelligent cities, including smart healthcare.

B. Network Layer

The data which these gadgets gather must be shared and stored. This is the responsibility of the network layer. It links these intelligent and smart objects to other intelligent and clever objects. It also includes data transfer in its jurisdiction. The network layer connects servers, networked gadgets, and smart objects. It is also used for distribution and analysis of sensor data.

C. Perception Layer

The perception layer is the term used to describe the physical layer underlying IoT architecture. It is mostly made up of embedded systems and sensors that gather a lot of data based on requirements. Additionally, this layer makes it possible for edge devices, detectors, and actuators to communicate with the outside world. It also has the ability to recognize particular spatial factors and recognize

other intelligent items in the surrounding environment and Multi-level Architecture as shown as Fig 4.

Both the current technique and lightweight RSA have been used to perform multi-level encryption on the healthcare dataset that was gathered from Kaggle. In contrast to the current approach, which used a 44-bit key, compact RSA encryption was created using a 64-bit key over three rounds. The smallest and largest dataset sizes utilized to determine the complexity of space and time are 3.51 MB and 27 MB, respectively.

For key generation, the lightweight RSA technique uses a GCD computing unit and a pseudo-random number generator unit. This guarantees the encryption process's effectiveness and security. The goal of the encryption procedure is to protect medical records while keeping time and space complexity under control.

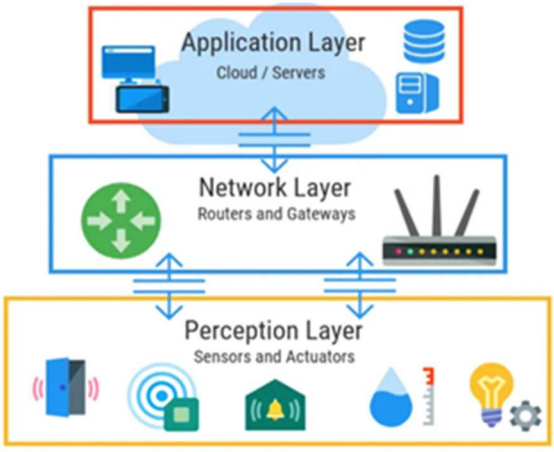

Figure 4. Framework of Multi level Architecture

VI. Comparative Results And Implementation

Algorithms are used to two distinct sizes of health care information in accordance with the suggested technique. The LW RSA comparing results and presented algorithms in the form of tables and graphs are shown below [13].

A. Comparison of the LWRSA algorithm's and the current algorithm's time complexity on 3.51 MB of small-scale healthcare data

TABLE IV. Time Complexity

Algorithm used	Index	Time expressed Sec	
		Encryption	Decryption
LW - RSA algorithm	L1	0.0292	0.0351
	L2	0.0239	0.0239
	L3	0.0159	0.0239
PRESENT algorithm	L1	0.483	0.605
	L2	0.501	0.613
	L3	0.487	0.599

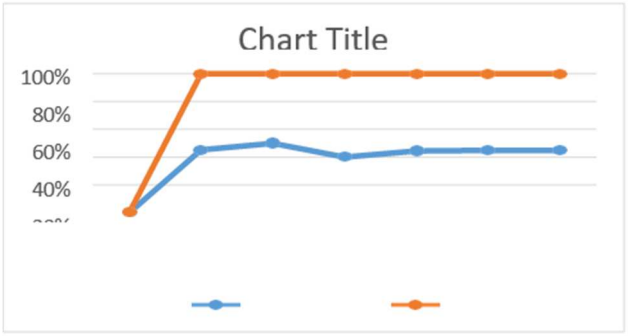

Figure 5. Graph plotting based on LW-RSA Algorithm Vs Present Algorithm Computational time using Multi level Encryption.

B. Descriptive Analysis

We used the current approach to determine time complexity and Lightweight RSA to apply multilevel encryption to a collection of healthcare data.

C. Time complexity comparison between the current technique and the LWRSA algorithm for large-scale health care records (27 MB)

TABLE V. Time Complexity

Algorithm Used	Index	Time express Sec	
		Encryption Algorithm	Decryption Algorithm
LW-RSA algorithm	L1	0.1094	0.319
	L2	0.162	0.285
	L3	0.199	0.228
PRESENT algorithm	L1	10.101	5.996
	L2	10.398	5.850
	L3	5.210	5.234

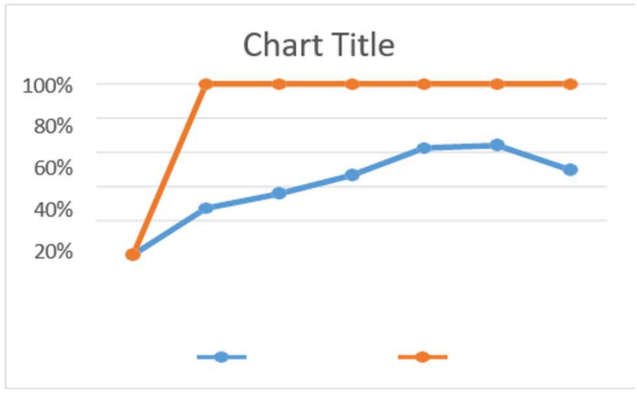

Figure 6. Graph plotting based on LW-RSA Algorithm Vs Present Algorithm Computational time using Multi level Encryption.

D. Descriptive Analysis

We used the current approach to determine time complexity and Lightweight RSA to apply multilevel encryption to a collection of healthcare data [14].

E. Evaluation of LW RSA Algorithms in Comparison

	Level	Data Size (IN MB)	Memory Used (Bytes)	Key Size (Bits)	Key Genration Time (Sec)	No of Rounds	Encryption Time(In Sec)	Decryption Time(In Sec)	Total Time(E+D)
LW RSA algorithm	L1	3.51	722	2048	1.9665	12	0.029	0.035	0.064
	L2	3.51	737	2048	1.9665	12	0.024	0.024	0.048
	L3	3.51	783	2048	1.9665	12	0.016	0.024	0.04
	L1	27	720	2048	2.1473	12	0.1195	0.032	0.1515
	L2	27	783	2048	2.1473	12	0.016	0.029	0.045
	L3	27	753	2048	2.1473	12	0.02	0.023	0.043
	L1	3.51	1545	4096	15.492	13	0.025	0.0819	0.1069
	L2	3.51	1536	4096	15.492	13	0.027	0.0692	0.0962
	L3	3.51	1494	4096	15.492	13	0.019	0.0646	0.0836
	L1	27	1525	4096	5.2873	13	0.0657	0.08	0.1457
	L2	27	1476	4096	5.2873	13	0.016	0.1292	0.1452
	L3	27	1446	4096	5.2873	13	0.0589	0.1159	0.1748

F. Evaluation of PRESENT Algorithms in Comparison

	Level	Data Size (IN MB)	Memory Used (Bytes)	Key Size (Bits)	Key Genration Time (Sec)	No of Rounds	Encryption Time(In Sec)	Decryption Time(In Sec)	Total Time(E+D)
present algorithm	L1	3.51	4896612	2048	1.9748	10	0.484	0.604	1.088
	L2	3.51	4896612	2048	1.9748	10	0.502	0.616	1.118
	L3	3.51	4896612	2048	1.9748	10	0.486	0.6	1.086
	L1	27	38817612	2048	1.169	10	10.009	5.997	16.006
	L2	27	38817612	2048	1.169	10	10.406	5.848	16.254
	L3	27	38817612	2048	1.169	10	5.168	5.239	10.407
	L1	3.51	4896612	4096	1.333	10	0.835	1.269	2.104
	L2	3.51	4896612	4096	1.333	10	0.817	1.033	1.85
	L3	3.51	4896612	4096	1.333	10	1.124	1.379	2.503
	L1	27	38817612	4096	1.9665	10	8.058	5.07	13.128
	L2	27	38817612	4096	1.9665	10	9.168	5.735	14.903
	L3	27	38817612	4096	1.9665	10	7.038	5.292	12.33

Three critical sizes of data—570, 2048, and 4096—have been gathered. We have worked with moderately sized data sets. Applying time complexity to a 2048-bit key results in a decrease in time [16], whereas applying memory complexity results in an increase in memory size. IoT devices, as of now, have little memory.

VII. SECURITY ANALYSIS

To improve data security, the Enhanced Data Security Framework (EDSF) uses multi-level encryption and lightweight cryptography. The purpose of this framework [17] is to handle the changing risks to data confidentiality and integrity. This framework's security is examined as follows:

a. The EDSF is subjected to a thorough security analysis process in order to detect any potential weaknesses or vulnerabilities in its design and implementation.

b. Threat modelling, evaluations of vulnerabilities, penetration testing, and adherence to accepted security norms and best practices are all included in this research.

c. In order to adjust the framework to new dangers and weaknesses in the quickly changing cybersecurity world, ongoing monitoring & updates are necessary.

d. GCD Computing and Pseudo-Random Number Generation (PRNG) - The inclusion of a PRNG unit enhances the randomness of cryptographic keys, making them more resistant to brute-force attacks. The GCD computing unit facilitates the generation of secure key pairs for asymmetric encryption algorithms like RSA.These components contribute to the overall strength of the encryption scheme by ensuring that cryptographic keys are generated securely and efficiently [18].

All things considered [19], the Integrated Data Security Framework, which makes use of multi-level encryption and lightweight cryptography, offers a thorough method of protecting sensitive data from misuse and illegal access. By carefully choosing encryption methods, key lengths, and cryptographic algorithms, it provides a strong defence mechanism appropriate for safeguarding data in a variety of settings and applications.

VIII. CONCLUSIONS

According to the results, Lightweight RSA fared quite well when compared to the current algorithm. Thus, lightweight RSA can be applied to Internet of Things applications such as smart cities. Better performance with multi-level encryption is provided by lightweight RSA. Therefore, for improved device level security, we can either utilize a hybrid method or lightweight RSA in a multi-level setup. In conclusion [20], the Improved Data Security Strategy is a major step forward in data security, providing businesses with a flexible and strong way to reduce risks and secure sensitive data in the increasingly digital and networked world of today. EDSF offers a strong basis for guaranteeing the privacy, integrity, and accessibility of data across a range of applications and contexts by combining lightweight cryptography with multi-level encryption [21].

REFERENCES

[1] Sharma, Isha, and Monika Saxena. "A Review of Lightweight Cryptography Algorithm for Healthcare Using Multi-Level Encryption." Available at SSRN 4700912.

[2] Lin, Junyu, et al. "FGDB-MLPP: A fine-grained data-sharing scheme with blockchain based on multi-level privacy protection." IET Communications (2024).

[3] Sneha Chaturya, A. "Enhancing Data Security through Innovations in AES-FBC Encryption and DWT Steganography." International Journal of Engineering Science and Advanced Technology 24.1 (2024): 43-53.

[4] Asaad, Renas Rajab, and Subhi RM Zeebaree. "Enhancing Security and Privacy in Distributed Cloud Environments: A Review of Protocols and Mechanisms." Academic Journal of Nawroz University 13.1 (2024): 476-488.

[5] Padmapriya, Valluri, and Muktevi Srivenkatesh. "IoT Network based Cyber Attack Mitigation in Digital Twin with Multi Level Key Management Using Enhanced KNN Model." International Journal of Intelligent Systems and Applications in Engineering 12.14s (2024): 49-62.

[6] Sami, Teba Mohammed Ghazi, Subhi RM Zeebaree, and Sarkar Hasan Ahmed. "A Novel Multi-Level Hashing Algorithm to Enhance Internet of Things Devices' and Networks' Security." International Journal of Intelligent Systems and Applications in Engineering 12.1s (2024): 676-696.

[7] Kanani, Pratik, et al. "Lightweight multi-level authentication scheme for secured data transmission in IoT-Fog context." Journal of Combinatorial Optimization 45.2 (2023): 59.

[8] Budati, Anil Kumar, et al. "Secure multi-level privacy-protection scheme for securing private data over 5G-enabled hybrid cloud IoT networks." Electronics 12.7 (2023): 1638.
[9] K Santhi, Sri. "A COMPARATIVE ANALYSIS ON THE COMBINED MULTI LEVEL FUNCTIONALITY FRAMEWORK IN CLOUD ENVIRONMENT WITH ENHANCED DATA SECURITY LEVELS FOR PRIVACY PRESERVATION." Journal of Theoretical and Applied Information Technology 101.9 (2023).
[10] Wu, Wei, et al. "A Secure and Efficient Data Transmission Method with Multi-level Concealment Function Based on Chaotic Compressive Sensing." IEEE Sensors Journal (2023).
[11] Lin, Junyu, et al. "FGDB-MLPP: A fine-grained data-sharing scheme with blockchain based on multi-level privacy protection." IET Communications (2024).
[12] Sneha Chaturya, A. "Enhancing Data Security through Innovations in AES-FBC Encryption and DWT Steganography." International Journal of Engineering Science and Advanced Technology 24.1 (2024): 43-53.
[13] Aghili, Seyed Farhad, et al. "MLS-ABAC: Efficient multi-level security attribute-based access control scheme." Future Generation Computer Systems 131 (2022): 75-90.
[14] Shifa, Amna, et al. "MuLViS: Multi-level encryption based security system for surveillance videos." IEEE Access 8 (2020): 177131-177155.
[15] Kanani, Pratik, et al. "PIRAP: Lightweight Multi-Level Authentication Scheme for Secured Data Transmission in IoT-Fog Context." International Journal of Cooperative Information Systems (2022).
[16] Dhall, Sakshi, Saibal K. Pal, and Kapil Sharma. "A chaos-based multi-level dynamic framework for image encryption." Internet of Things (IoT) Concepts and Applications (2020): 189-217.
[17] Hasan, Mohammad Kamrul, et al. "Lightweight encryption technique to enhance medical image security on internet of medical things applications." IEEE Access 9 (2021): 47731-47742.
[18] K Santhi, Sri. "A COMPARATIVE ANALYSIS ON THE COMBINED MULTI LEVEL FUNCTIONALITY FRAMEWORK IN CLOUD ENVIRONMENT WITH ENHANCED DATA SECURITY LEVELS FOR PRIVACY PRESERVATION." Journal of Theoretical and Applied Information Technology 101.9 (2023).
[19] Shifa, Amna, et al. "Fuzzy-logic threat classification for multi-level selective encryption over real-time video streams." Journal of Ambient Intelligence and Humanized Computing 11 (2020): 5369-5397.
[20] Christhu Raja, S., N. Jafer Gani, And Mohammed Uveise. "Three Level Authentication And Lightweight Encryption For Hybrid Cloud–Iot Environment." (2021).
[21] A. Durgapal and V. Vimal, “Prediction of Stock Price Using Statistical and Ensemble learning Models: A Comparative Study,” 2021 IEEE 8th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering, UPCON 2021, 2021, doi: 10.1109/UPCON52273.2021.9667644.
[22] V. Vimal, T. Singh, S. Qamar, B. Nautiyal, K. Udham Singh, and A. Kumar, “Artificial intelligence-based novel scheme for location area planning in cellular networks,” Comput Intell, vol. 37, no. 3, pp. 1338–1354, Aug. 2021, doi: 10.1111/COIN.12371.