Al-Rafidain Journal of Computer Sciences and Mathematics (RJCM)

www.csmj.mosuljournals.com

The Multilevel Encryption Model: A Review

Mais Irreem A kamal[1,] *, Ibrahim, Laheeb Mohammad[2]

[1,2] *Software Department, College of Computer Science and Mathematics, University of Mosul, Iraq*
Emails: maisirreem_alsaigh@uomosul.edu.iq, laheeb_alzubaidy321966@uomosul.edu.iq

Article information

Article history:
Received :24/9/2023
Accepted :21/12/2023
Available online: 25/6/2024

Abstract

Multilevel Encryption is a system that uses a lot of overlapping encryption methods to secure sensitive data and information. This technique seeks to improve security by adding numerous layers of encryption, making it more difficult to decipher data. Different encryption algorithms are applied to the data sequentially while employing the multilevel encryption system. Digital encryption algorithms, for example, can be employed as first layers to encrypt data, and the encrypted data can subsequently be encrypted again using additional encryption techniques. This paper aims to review studies, research, and the studies in the field of multilevel encryption models and proposes a multilevel encryption model for future work to improve security and protection from cyber threats, making it difficult for attackers to break all overlapping layers of encryption.

Keywords:
encryption model, multilevel encryption model, cybersecurity, information security.

Correspondence:
Author: Mais Irreem A kamal
Email:
maisirreem_alsaigh@uomosul.edu.iq

1. Introduction

Encryption can be defined as one of the major parts of the current global information security which will make the virtual world a safer place, preferably where users need high performance encryption algorithms such as AES, DES, RSA and 3DES algorithms, see **Fig. 1**, where the scientist William Stallings defines cryptography as "the type of operations used to convert plain text into cipher text, the number of keys used, and the way plain text is processed"[1].

It is, therefore, any Encryption model that consists of plain text (an unencrypted message), Encryption method, Key Encryption, Encryption text (generated from plain text message by the encryption key), improving the efficiency of encryption algorithms which has been the goal of many researches by proposing the multilevel encryption model [2-3].

The Multilevel Encryption Model is a model that uses several layers of encryption to secure data and information. When using this model, each layer encrypts the data in its own way and provides an additional level of security. The advantage of this model is to provide greater data protection, as it is difficult for hackers to access the data due to the number of security layers that must penetrate. In addition, the multilevel

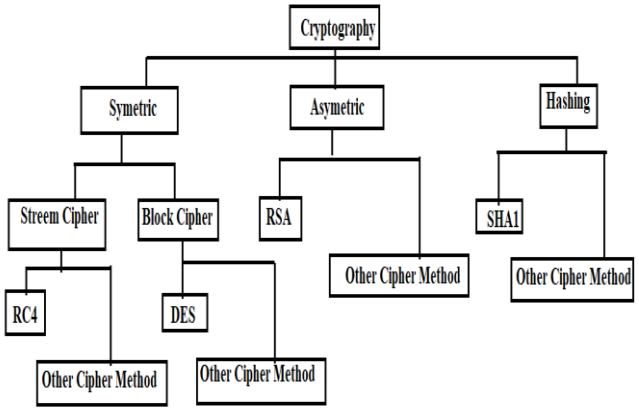

Fig. 1. Encryption Methods.

model ensures that data is secured during transmission and storage on devices [3-5].

Although this model increases the level of complexity, it also increases the level of security, and is suitable for systems that require protection of important and sensitive data such as financial and medical information, as well as multiple and important application areas, including voice communication security, cloud security, e-commerce security, and safe electronic transactions, as the multilevel encryption model has several benefits that include increasing the level of protection. The multilevel encryption model increases the level of protection for encrypted data, and more than one layer of different ciphers are used to protect data. It also increases the difficulty of piracy, as the use of the multilevel encryption model increases the difficulty of hacker attempts to penetrate the system and access the protected data, but there are several problems in the multilevel encryption system, and the most important of these problems is that the use of several layers of encryption that may lead to a negative impact on the speed of communication and the overall performance of the system [6-7].

2. Multilevel Encryption Model

The multilevel encryption model is defined as the application of a computer system that deals with information with inconsistent confidentiality, such as (different security levels), to allow access by users with varying security permissions and knowledge requirements, and to prevent users from accessing information that do not have permission to access.

There are two scenarios in which multilevel encryption is used: The first is to be referred to a trustworthy encryption technique that is suitable for safeguarding information from tampering, the second scenario that a multilevel encryption can be implemented to secure data stored in various environments, such as cloud storage or databases. [8-9]

As the complexity of the encryption algorithm increases, the execution duration can be lengthened and it; therefore, significantly improves the data's security. Hence, Lena's multilevel encryption system is the solution to increase the level of data protection. An example of a multilevel encryption algorithm is the combination of Blowfish, Digital Encryption Standard (DES, Triple DES) and encryption algorithms. In this system, for example, The DES algorithm is used to generate the first level of encryption, then the RSA algorithm and the Blowfish algorithm are applied sequentially to the hidden output. The DES is used to create the second level of encryption., and the third on the encrypted output from RSA - the same process is used to decrypt using the reverse algorithms Blowfish, DES, and RSA. Note **Fig. 2** and **Fig. 3** [8, 9, 10].

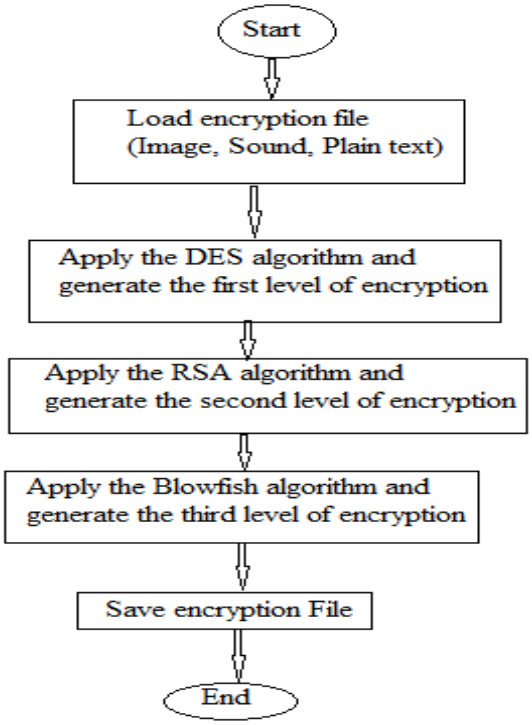

Fig. 2. Flow Chart for Encryption Model

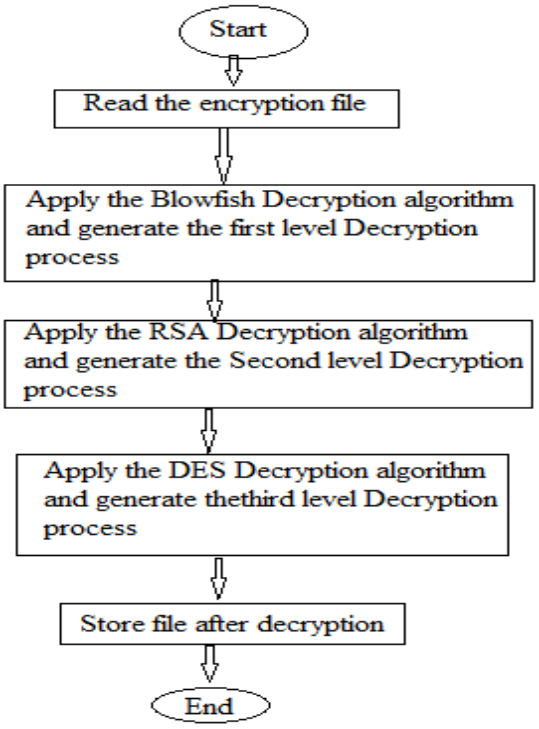

Fig. 3. Flow Chart for Decryption Model.

3. Previous studies

The main objective of this study is to understand the multilevel encryption model, and many studies were reviewed in the field of multilevel encryption model.

Bh, Sumita, et al. in 2012, suggested a multilevel encryption model using (Byte – Rotation Encryption Algorithm BREA) to encrypt files. The investigation makes most of the advantages of the BREA minimization of Habits. A fragrance grievance that ignores the front-end can be used in any network security services. The network enhances the concept of block parallel estimation using multithreading technology [2].

G. Himansgu, et al. in Science 2013 designed and implemented a new encoding technique called "multi-path variability. The original data is changed several times using different powerful algorithms for encryption at each stage in this encryption." This complexity in the downsizing technique decreases significantly with the deployment of multi-stage encryption, which is a significant and good step toward developing a network security standard. [3].

S. A. Alawale, et al. in 2015 successfully developed a multilevel change algorithm in the implementation of surrogate estimate with RSA change to obtain a high degree of information security assurance, where the RSA encryption method ensures the message's validity. The application layer implementation of this technique gives a significant benefit for arithmetic RSA keys. The RSA transformation output is used as the input for the substitution transformation, which yields the needed ciphertext. [4].

K Satyanian, in 2016 presented a method that employed multilevel encryption and decryption to increase storage security. Because the suggested algorithm is a multilevel modification method, only the user who is permitted to access the data can do so in the proposed work. Even if an unauthorized user gains access to the data, whether unintentionally or on purpose, the data must be cracked, and decrypting the data at each level is a tough operation without a legitimate key, which is intended to be provided by a federated cipher. When opposed to having a single change level, levels give additional security for cloud storage. [5].

K Mukesh, et al in 2016, in this paper, the researchers focused on protecting the security of files in the cloud. A new approach of multilevel change of Cloud Data Security System (MESCD) is proposed in this approach. Any file is loaded and decrypted by using a level of separate keys, after which the other keys are concatenated into one secure key "K." Decryption solutions are the inverse of encryption, in which the key (K) is inserted in the keys "N", which is then applied to the method of that modification as well as decoding. [6].

D. Shweta, in 2016 designed an algorithm to hide the image with more financial and secure using a multilevel encryption model, The image is the focus of attention here since it is commonly utilized on the Internet and in mobile systems. The Linear Significant Bit (LSB) method is simple to tweak and does not degrade the image much. Due to the security of the summed LSB approach, enhanced LSB utilizing multilevel Hadamard transform looks to be a more acceptable algorithm for steganography. Secret communications can exchange securely via a public channel. Because it is dependent on the number 1 in the antagonistic value of the key, the suggested approach is much safer than the prior method, which employs merely basic shura. [7].

K Surinder, in 2017 proposed the implementation and monitoring of notable parameters such as time and memory. Multilevel encryption is implemented utilizing metric export bots (DES) and multistage RSA. After utilizing different primes, the values for a parameter are averaged. The main principal of DES is the finite size of the key. It can be decoded by multiple digits, requires RSA, and multilevel DES over this defect by signaling the DES key, making it more complex and mutilated. The time to encoding significantly increases with the number of primes, but compared to them the encoding time increases at a much slower pace as well. Memory usage increases and decreases instead of the transition from 2 to 10 primes under the protection of DES and Ahulti-Prime RSA. To make your data more secure [8], it focused on the broad security issues related to the use of Amazon File World from public cloud service provider indexes. The work is performed to design and implement a system that is used to create a home and public security analysis on the Amazon 2 platform with additional security of flags and a detailed implementation frequency of it, specifically Amazon storage associated with user credentials and PEM security file to access to cloud storage, and use Amazon3 to meet client demands. User can get the uploaded file in unmetered form if the user creates a container in which the file is guarded in alienated form and where the data can be kept in hexadecimal form [9].

K. Khaitul, et al. in 2018 gave information on multilevel encryption, which encrypts data in a more secure manner than typical types of encryption since it includes many rounds of encryption and decoding, making it difficult. Multilevel encryption is a perplexing method to data and information protection that is crucial in current encryption. Multilevel encryption refers to the increased security and integrity of secret data as a result of various encryption procedures. The main benefit of multilevel encryption is that it provides greater protection because even if certain secret keys or ciphers are cracked or parts of cipher scripts are broken, multi-encryption may still protect the secrecy and privacy of the original material. Multilevel encryption significantly improves data security. [10].

A. Habboush, in 2018 suggested a highly computational multilevel encryption system that incorporates symmetry strength, cryptographic algorithm [Advanced Encryption Standard (AES)], Feistel network, crossover and mutation genetic algorithm approaches, and HMAC. The framework was tested and compared to a collection of typical symmetric encryption techniques, including RC5, DES, and 3-DES. The algorithms were tested on a comparable platform and their performance parameters of runtime, throughput, and an avalanche effect security measure were compared. The findings reveal that the suggested framework outperforms the traditional symmetric encryption algorithms evaluated in terms of throughput and uptime, and it meets the collapse effect condition. [11].

Y. Mehmet, et al in 2019 proposed a novel privacy-preserving multilevel encryption technology that is reversible,

enables identification at various privacy levels, and can successfully obtain data, encryption, and data anonymity by integrating multilevel encryption with pressure sensing. The suggested approach's efficacy in protecting users' identities has been validated utilizing the quality of reconstruction and strong anonymization of faces. [12]

Sh. Jinan, et al. in 2019 presented a design for a multilevel security cloud storage model mixing AES symmetric encryption with an improved identity-based proxy re-encryption (PRE) method. The researchers' enhancements include support for microcontrollers and increased performance. The researchers introduced a fine-grained control factor to the process using a mixture of attribute-based encryption approaches, where each permission is only valid for one factor. They improved performance by lowering the amount of two-line mappings, which can be the most time-consuming procedure. Finally, they enabled safe data exchange among diverse cloud systems. The proposed multilevel security cloud storage system provides services like direct data storage, transparent AES encryption, PRE protection that permits heterogeneous conversion and ciphertext, and other features. [13].

Sh.Amna, et al in 2020 introduced a Multilevel Video Security (MuLViS) monitoring system was created for privacy-protected cameras. First, Smart Surveillance Security Systems (SSSO) was included into MuLViS with the purpose of autonomously identifying the amount of privacy according to playback device hardware specifications and network capabilities. Generally, when combined with hardware security, the technology allows for reasonably quick indexing and retrieval of surveillance video. Second, the data in the videos is encrypted at several stages during recording, streaming, and storage. Show the overall evaluation of the system by visual examination and statistical analysis of experimental video data, such as encryption space ratio (ESR), suitability for security level assignments. The system is suitable for protecting surveillance footage, which can be made compliant with the General Data Protection Regulation (GDPR), ensuring that legal access to data respects the privacy rights of individuals. [14]

K. T. Sampath, et al in 2020 proposed a multilevel security system that provides more security than any type of current process based on single level encryption. The suggested solution, in particular, assures that only pre-authorized users may access cloud data, and another advantage of the researcher's algorithm is that it is quicker and more secure in various directions, such as when uploading and downloading a specific file. [15]

J. Rami, in 2021 in his dissertation, introduced a novel method named (LWCD). In which he showed how DNA sequence was used as the encryption key by the researcher. To accommodate IoT devices, this technique regulates the number of encryption roles and the size of information segmentation prior to encryption. Two main encryption processes were used: the switching process and the five-position switching process, and they were compared with two well-known algorithms, the Triple Data Encryption Standard (3DES) and the Advanced Encryption Standard (AES). The proposed algorithm obtained the best results in terms of encryption speed, image noise ratio, and the amount of randomness in the image encrypted [16].

N. Zaid, et al in 2022, created a system based on two different branches of text coding. The initial branch involves the development of a new mathematical model for generating and exchanging keys. The suggested key exchange approach enhances the Dave-Helmann method. It is a paradigm for new mathematical operations based on prime numbers and the potential of utilizing integers to exchange keys. This proposal's second branch is a multi-key encryption algorithm. The present method allows for the usage of more than two keys. The keys can be any sort of integer (at least one of which must be a prime number), and they do not have to have the same length. The encryption procedure is based on turning text characters into recommended integers, which are then changed to other numbers several times using a multilevel mathematical model. The number of levels is determined by the number of keys used, but cracking the encryption is a one-level procedure in which one key is used as the primary key and the other keys as secondary keys. Before the encryption procedure, the message's values are modified. It is possible to utilize ASCII code or a recommended method. The suggested approach may employ an infinite number of keys with very high sizes exceeding 7500 bytes, at least one of which is a prime number. [17].

R.Mahdi, et al. in 2022 illustrated how classical cryptographic primitives are widely used in IoT security solutions. These primitives provide sufficient safety but do not protect privacy and do not provide enhanced functionality. They are also unduly reliant on trustworthy third parties owing to design restrictions. The researchers then demonstrate how multilevel encryption systems connect the connections and explain how certain advanced encryption systems may achieve lofty objectives. Describe briefly the heterogeneous, multi-tiered Internet of Things architecture that supports cloud, edge, fog, and blockchain technologies, as well as the assumptions and capabilities of each layer. They also show the fundamentals of advanced cryptography, including wildcarded encryption, glassbreaking, proxy re-encryption, registry-based cryptographic schemes, and IoT-compatible cryptographic pools. The researchers demonstrate how they may enhance the aforementioned capabilities while still satisfying the criteria of the Internet of Things architecture. [18]

Y. Minghao, et al. in 2022 provided an accelerator device with the ability to allow the use of multi-key fully symmetric encryption. In addition to accelerated symmetric encryption, cloud-based solutions such as KLP18 and THL21, in which each user utilizes single-key encryption, and the process of turning wide public encryption into multi-key encryption are used. This might possibly be a solution. The cloud executes the process of extending the ciphertext as the size of the stretched ciphertext rises, which can decrease bandwidth loss. As a result, the researchers believe that users need only upload encrypted data, and the cloud outfitted with the symmetric hardware accelerator will be ready to conduct a huge number

of symmetric operations. Hardware accelerators based on a trusted execution environment can be utilized to improve security if possible. [19].

Zh. Yuzhou, et al. in 2022, based on coupled chaotic systems and Otsu threshold segmentation, suggested an effective multilevel encryption technique for medical holograms. The medical stereoscopic picture is first separated into upper, middle, and bottom image sections in this manner. Furthermore, Otsu threshold segmentation is used to separate each fragment into background areas and regions of interest, which boosts coding efficiency by 40% when the background region is ignored. Second, the proposed linked chaotic system outperforms current chaotic systems in terms of efficiency and unpredictability; all NIST SP800-22 test data surpass 0.01. Third, using Meyer wavelet transform redirection and singular value decomposition, the researchers created a robust watermarking technique. Furthermore, in the region of interest, the watermarking technique implanted 2D doctor and patient information. Finally, the experimental results show that the proposed algorithm has good encryption and watermarking performance, that the graph and scatter graphs have nearly uniform distribution, and that the NPCR and UACI plaintext sensitivity and key sensitivity are close to 99.6094% and 33.4635%, respectively, in terms of robustness to noise and slash attacks. [20].

M. Emil M. in 2023 proposes a framework for integrating encryption technologies while taking into account multilevel encryption architecture. Coding techniques were developed as classes to describe their major characteristics, test their flexibility, and assess their suitability for consideration in higher level approaches. For comparative purposes, the resultant application parameters are defined, and they take into consideration numerous factors for certain blades. Important features of network creation are given in relation to the spin-network encoding approach. Several testing have been conducted, and an app that merges the aforementioned categories is in the works. [21].

Table 1. Previous studies in the field of multilevel encryption models.

No.	Researchers	Algorithms	Result	Comments
1	Bh. Sunita et al, 2012 [2]	BREA	The BREA algorithm idea of block parallel encryption employing multithreading technology increases the encryption system's performance while still providing enough security. As a result, the system is justified in employing it to safeguard files.	Propose a good strategy to make the most of the advantages of the BREA algorithm while trying to get rid of the constraints. The developed system that ignores the front end can be used in any network services for network security
2	G. Himanshu et al, 2013[3]	DES, IDEA, RC5 BLOWFISH	Implementing multilevel encryption is a significant and beneficial step toward establishing a network security standard.	The researchers designed and implemented a new encryption technology called "multilevel encryption". where the original data is encrypted multiple times with different strong encryption algorithms at each stage
3	S.Olawale et al,, 2015 [4]	RSA	They effectively build multilevel approaches employing RSA and replacement ciphers. The use of alternative encryption with the RSA cipher has resulted in a high level of information security assurance.	Because big primes are factored while using this approach, it gives a significant benefit for computing RSA keys. The use of big primes can be viewed as a substantial security benefit. The RSA transformation output is used as the input for the substitution conversion, and the needed ciphertext is acquired as a result.
4	K. .Satyanarayana , 2016 [5]	RSA, DES	Using multilevel encryption provides security for the cloud storage than using a single level encryption	He presented a solution that employs multilevel encryption and decryption to improve cloud storage security.
5	K. Mukesh, et al, 2016 [6]	3DES	The experimental result showed that the "MESCD" scheme proposed by the researchers is suitable for encoding as well as decoding	In this paper, the researchers focus on protecting the security of files in the cloud. A new multilevel encryption approach for Cloud Data Security System ("MESCD") has been proposed.

6	D. Shweta, et al, 2016 [7]	Improved LSB algorithm using Hadamard transform	With the upgraded LSB method, confidential messages may be sent securely over a public channel. The suggested approach is more secure which just utilizes a basic cipher, because it is entirely dependent on the amount of 1s in the key's corresponding binary value.	By using multilevel encryption, the image masking approach is more effective and safe. The image is the focus of attention here since it is frequently used on the internet.
7	K. Surinder, 2017 [8]	DES and a modified RSA	Implement and control notable parameters such as time and memory to perform multilevel encryption using standard, multi-stage RSA. After utilizing a variable number of prime numbers, the values for each parameter are averaged.	Using a multilevel encryption system that provides two-factor protection using DES and Multi-Prime RSA, data becomes more secure
8	R. Sandeep et al, 2018 [9]	Amazon S3	The researchers implementation of the planned work to provide cloud security utilizing cryptographic technologies based on client requirements. With Amazon S3, the user may construct a container in which the file is encrypted.	Investigate the general security issues related with utilizing Amazon File Server from public cloud service provider catalogs.
9	Khaitul, et al ,2018 [10]	AES, DES, 3DES, RSA	The fundamental benefit of multilevel encryption is that it gives more security even if certain secret keys are compromised, cipher or part of cipher scripts are broken. Multilevel encryption enhances data security tremendously	Multilevel encryption refers to the increased security and integrity of secret data as a result of numerous encryption operations.
10	Habboush, 2018 [11]	Encryption Algorithms AES Advance Encryption Standard, Feistel Network, Intersection and Mutation Techniques of Genetic Algorithm and HMAC	The findings shown that the suggested framework outperforms the evaluated typical symmetric encryption algorithms in terms of throughput and runtime, as well as passing the collapse effect condition.	The framework was evaluated and compared to a number of popular symmetric encryption approaches, including RC5, DES, and 3-DES. The algorithms were compared using uptime and throughput performance parameters, as well as the Avalanche Impact safety metric, on a comparable platform.
11	Y. Mehmetl, 2019 [12]	Use a perturbation matrix to selectively blur specific metrics regarding sensitive parts of the images to preserve privacy.	The effectiveness of the proposed approach in protecting the identity of the users was verified using the quality of the reconstruction and the strong anonymization of the faces	By merging multilevel encryption with pressure sensing, a new privacy-preserving technology was introduced that is reversible, enables identification at various privacy levels, and can successfully collect data, encryption, and data anonymity.
12	Sh. Jinan, 2019 [13]	AES , PRE	The researchers reduced time costs permission, and for decoding.	The suggested multilevel security cloud storage system provides features such as direct data storage, AES, PRE protection that allows heterogeneous conversion and ciphertext.
13	Sh. Amna, 2020 [14]	AES-OFB with a 128-bit key real-time eXclusive OR cipher	The examination of the system, including visual inspection of experimental video data confirmed the sufficiency of the security level assignments. The technology is appropriate for safeguarding surveillance footage.	The researchers built a multilevel Video Security monitoring system for privacy-protected cameras. First, Intelligent Monitoring Security Systems (SSSO) are integrated into MuLViS, with the goal of independent determination of the level of privacy matching playback device hardware specifications and network capabilities.
14	K. Sampath, 2020 [15]	hessian curve cryptography, TDES AES, and ECC.	They propose a multilevel security approach that is more secure than single-level encryption-based algorithms.	The approach that was suggested ensures that only pre-authorized users may access cloud data

15	Rami J. Al-D, 2021 [16]	The LWCD algorithm is based on the use of the DNA sequence as the encryption key	The results showed that the best encoding time and the amount of randomness in the encoded image were using 128-bits size.	To fit IoT devices and the sensitivity of the information acquired, this technique regulates the number of encryption roles as well as the ability to adjust the quantity of shredding information before encryption.
16	N. Zaid, et al, 2022 [17]	The researchers suggested a two-strategy for text encoding. The first strategy involves the development of a new mathematical model for creating and transferring keys. The suggested key exchange approach enhances the Dave-Helmann method. The second strategy, is a multi-key encryption scheme.	The proposed method achieved good results	The suggested strategy can employ an infinite number of keys with extremely large sizes. To add intricacy, the ace is also utilized for keys.
17	R. Mahdi, et al, 2022 [18]	Advanced cryptographic fundamentals algorithms, wildcarded, glassbreaking, IoT-compatible cryptographic pools, proxy re-encryption, and registry-based cryptographic schemes	The proposed method met the requirements of the Internet of Things architecture.	The researchers show that interdisciplinary cryptographic systems
18	Y. Minghao, 2022, [19]	Fully symmetric multi-key encryption algorithms. Plus accelerated symmetric encryption	Accelerators depend on execution environment can be utilized to improve security.	Each user employs single-key encryption, and transforming wide public cipher to multi-key cipher stored in the cloud is another option. The cloud executes the process of extending the ciphertext as the size of the stretched ciphertext rises, which can decrease bandwidth loss.
19	Zh. Yuzhou, et al., 2022, [20]	Development of a watermarking model depends on wavelet Meier transform redirection and singular value decomposition.	The experimental findings reveal that the suggested technique has good encryption and watermarking performance.	The Model depend on chaotic systems and developed an efficient multilevel coding strategy for medical holograms.
20	M. Emil, 2023 [21]	Rotary network encryption method algorithms	Numerous tests have been done and the app integrating the categories	It introduces a framework aimed at integrating encryption methods, considering a layered encryption architecture. Coding methods were implemented as classes in order to define their main features, check their flexibility and evaluate the opportunity for consideration in higher level approaches.

After reviewing the research and studies in the field of multilevel "as shown in **Table 1**" Encryption using encryption techniques to protect data from unauthorized access when there are high security requirements. The general conclusion of reading studies and research in this field is to increased security where the multilevel encryption helps increase the level of security of sensitive data and sensitive information by applying several layers of encryption to the data, making it difficult for attackers to crack and decrypt. By using multilevel encryption model, the system's resistance to various types of cyber-attacks, such as hacking, also different layers of encryption are used in different ways to increase the complexity and difficulty of breaking a security system. These layers can involve the use of different encryption keys and different key lengths, and multiple layers of encryption that may affect the overall system performance and may require more computing resources to fully process encrypted data.

4. Methodology for a Proposed Future Work

After reviewing previous work in the field of multilevel encryption, a future proposal work was reached for a multilevel encryption model to ensure the security of data and information and to improve data security, the proposed multilevel encryption architecture for future work employs many layers of encryption/decryption techniques that are executed successively. Each layer employs a separate encryption algorithm, which adds an extra degree of security by employing Triple Digital Encryption Standard (3DES), Diffie-Hellman Message Digest 5 (MD5) algorithms, as seen in **Fig. 4:**

1- Pre-processing of data before to encryption: Data is prepared for encryption by performing any necessary pre-processing processes, such as data normalization or formatting.
2- The first level of encryption (symmetric encryption) is as follows: An algorithm for a symmetric encryption, such as Triple Digital Encryption Standard (3DES), is used in the initial layer of encryption. Symmetric encryption encrypts and decrypts data using a single key. This layer's key is often a randomly generated secret key. The output of this level is first level cipher text
3- Key generation: A new encryption key is created for the second level of encryption. This key must be unique and secure.
4- The second encryption level (Asymmetric encryption): Asymmetric encryption algorithms, such as Diffie-Hellman, are implemented in the second layer of encryption. Asymmetric encryption uses a pair of keys for encryption and decryption: a public key for encryption and a private key for decryption. At this layer, data is encrypted using the receiver's public key, guaranteeing that only the person who intended it may decode it using their private key. The output of this level is the second level cipher text.
5- The third encryption level (hash): The last layer of encryption includes hashing approaches such as Message Digest 5 (MD5), that changes data into a fixed-length character string that is called a hash. This layer secures data integrity and assists in the detection of illegal tampering or change. The output of this level is the third level cipher text
6- Salting and Key Strengthening: In this layer, additional approaches are used to strengthen the encryption process. Salting is the process of adding a random value (salt) to data before encryption to make the encryption more difficult to crack. Key-strengthening approaches entail raising the complexity of cryptographic keys, such as by utilizing key-spanning algorithms or increasing key size, in order to make it more difficult for attackers to guess or break keys.
7- Decryption: When it is necessary to access encrypted data, the decryption method is carried out in reverse order. Until the original data is retrieved, each encryption layer is decrypted using the associated decryption key.

It is extremely important to keep in mind that deploying a multilevel encryption architecture necessitates careful consideration of variables such as performance, key management, and the use case's overall security needs.

To address all security issues related to data integrity and protect users' privacy, we strongly recommend that we consider the following proposed multilevel encryption model with model components. The proposed multilevel encryption model consists of multiple layers of Encryption/ Decryption algorithms applied sequentially to enhance data security. Each layer uses a different encryption technology, which adds an additional level of protection using Triple Digital Encryption Standard (3DES), Diffie-Hellman Message Digest 5(MD5), as following, see **Fig. 4**:

Data pre-processing before encryption: Data is prepared for encryption by applying any necessary pre-processing steps, such as data normalization or formatting.

The first level of encryption (symmetric encryption): The first layer of encryption uses a symmetric encryption algorithm, such as Triple Digital Encryption Standard (3DES), Symmetric encryption encrypts and decrypts data with a single key. A key used for this layer is usually a randomly generated secret key.

Key generation: For the second level of encryption, a new encryption key is generated. This key must be unique and secure.

The second level of encryption (asymmetric encryption): The second layer of encryption uses an asymmetric encryption algorithm, such as Diffie-Hellman. For encryption and decryption, asymmetric encryption uses a pair of keys: a public key for encryption and a private key for decryption. Data is encrypted using the receiver's public key at this layer, guaranteeing that only the intended recipient may decode it

using their private key.

The third level of encryption (hash): The third layer of encryption includes hashing algorithms, such as Message Digest 5 (MD5) where the hash converts the data into a fixed-length character string called a hash. This layer ensures data integrity and helps detect any unauthorized tampering or modifications.

Salting and Key Strengthening: This layer involves incorporating additional techniques to strengthen the encryption process. Salting refers to adding a random value (salt) to the data before encryption, which makes the encryption difficult to crack. Key-strengthening techniques involve adding complexity to cryptographic keys, such as using key-spanning algorithms or increasing key size, to make it more difficult for attackers to guess or crack keys.

Decryption: When the encrypted data needs to be accessed, the decryption process is performed in reverse order. Each encryption layer is decrypted with the corresponding decryption key until the original data is recovered.

It is important to note that implementing a multilevel encryption model requires careful consideration of factors such as performance, key management, and the overall security requirements of the use case.

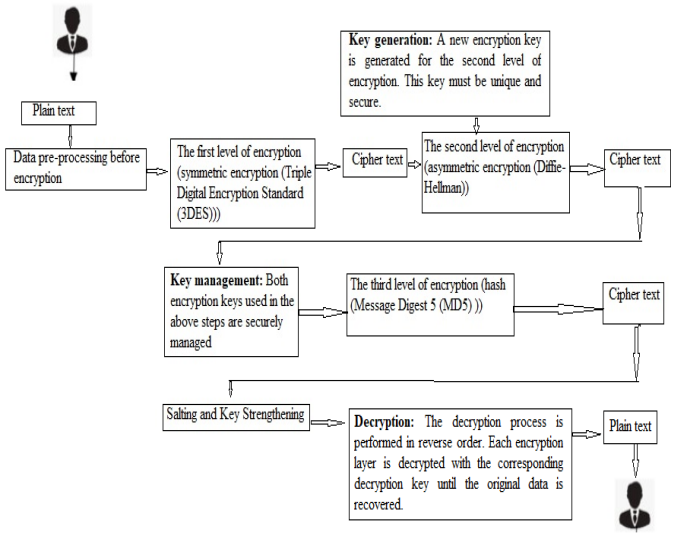

Fig. 4. Methodology for a proposed work

5. Conclusion

The multilevel encryption model is important for the following reasons:

- Improving the performance of the encryption model: Using a multilevel encryption model improves the performance of the encryption system because it does not increase resource consumption and works reliably, efficiently, and with great security.
- Compatibility of multilevel encryption model with other systems: Because multilevel encryption model is compatible with many other existing systems, it can be used in a variety of sectors.
- Mistakes: Using many levels of encryption increases the risk of mistakes in the of multilevel encryption model, making it more vulnerable to hacking and cyber-attacks. Problems in the system might be difficult to comprehend and identify, making them difficult to resolve fast.
- Privacy Protection: The model provides privacy protection for encrypted data by masking the real identity of the data sender or receiver and limiting the ability to determine the origin of the data.
- Cost of data encryption: If many layers are utilized, the cost of data encryption may rise since the requisite hardware and software must be acquired.

Finally, a future work is proposed to encrypt data based on a multilevel encryption/decryption model that includes the following algorithms by employing Triple Digital Encryption Standard (3DES), Diffie-Hellman Message Digest 5 (MD5) algorithms

Acknowledgement

The authors would express they're thanks to the College of Computer Sciences and Mathematics - University of Mosul, for supporting this paper.

References

[1] J. Hussam Ali, M. Talib Jawad and H. Zuhair, "Data Security Using Random Dynamic Salting and AES Based on Master-Slave Keys for Iraqi Dam Management System," Indonesian Journal of Electrical Engineering and Computer Science., vol. 23, no. 2, pp. 1018-1-2029, 2021, doi: 10.11591/ijeecs.v23.i2.

[2] Bh. Sunita, Bh. Anita and S. Sharma, "A New Approach towards Encryption Schemes :Byte – Rotation Encryption Algorithm," Proceedings of the World Congress on Engineering and Computer Science 2012 (WCECS), vol. 2, 2012 .

[3] G. *Himanshu and Sh. Vinod* , "Multiphase Encryption: A New Concept in Modern Cryptography," International Journal of Computer Theory and Engineering (IJCTE), vol. 5, no. 4, pp. 638-640, 2013, doi: 10.7763/IJCTE.2013.V5.765

[4] S. Olawale Adebayo, O. Morufu and N. Joel Ugwu, " Implementation of N-Cryptographic Multilevel Cryptography Using RSA and Substitution Cryptosystem,", MIS Review, vol. 20, no 02, pp. 57-76, DOI: 10.6131/MISR.2015.2002.03 2015 .

[5] K. Satyanarayana, "Multilevel Security for Cloud Storage using Encryption Algorithms," International Journal Of Engineering And Computer Science (IJECS), vol. 5, no.7, pp. 17338-17346, 2016 .

[6] Jh. Mukesh Kumar and V. Shrivastava, "Multi Level Encryption Approach To Secure Cloud Data," International Journal of Engineering Sciences & Research Technology (Ijesrt), vol. 05, pp. 532-541, DOI: 10.5281/zenodo.168443, 2016 .

[7] Sh. Dahiya, "Multilevel Data Encryption Using Hadamard Transform Based Image Steganography", IJEDR , vol. 04, no. 4, pp. 317-323, 2016 .

[8] K. Surinder, "Study of Multilevel Cryptography Algorithm: Multi-Prime RSA and DES," I. J. Computer Network and Information Security, pp. 22-29, DOI: 10.5815/ijcnis.2017.09.03, 2017.

[9] R. Sandeep , and B.R. Pushpa. "An Approach to Provide Multilevel Security for Cloud Using Cryptography Algorithms ," Jour of Adv Research in Dynamical & Control Systems, vol. 10, no. 05-Special Issue, pp. 1815-1820,2018.

[10] A. Khaitul, S. Sandeep., Z. Majid and A.Muheet, " A Review On Multilevel Encryption ," Journal of Emerging Technologies and Innovative Research (JETIR) , vol. 5, no. 8, pp. 484-492, 2018.

[11] A. Habboush, "Multilevel Encryption Framework," International Journal of Advanced Computer Science and Applications(IJACSA), vol. 9, No. 4, pp. 130-134, 2018.

[12] Y. Mehmet, A. Mete, P. Nikolaos, R. Jenni, S. Bulent , and G. Moncef, "Reversible Privacy Preservation using Multilevel Encryption and Compressive Sensing," 27th European Signal Processing Conference (EUSIPCO), IEEE, 2019, DOI: 10.23919/EUSIPCO.2019.8903056

[13] Sh. Jinan, D. Xuejian, and X. Zhenwu, "Multi-security-level cloud storage system based on improved proxy re-encryption," EURASIP Journal on Wireless Communications and Networking , (2019) 2019:277 . https://doi.org/10.1186/s13638-019-1614-y

[14] Sh. Amna, N. Mamoona, F Martin, K. Nadia, S. Mohammad, L. Brian, H. Marco, And Q. Yuansong, "Mulvis: Multilevel Encryption Based Security system For Surveillance Videos," IEEE., vol. 8, pp 171131-171155, 2020.

[15] K. T. Sampath, and B. Manjula, "Competent multilevel encryption methods for implementing cloud security," ICRAEM 2020IOP Conf. Series: Materials Science and Engineering 981 (2020), doi:10.1088/1757-899X/981/2/022039, 2020.

[16] J. Rami, "New Symmetric Lightweight Encryption Algorithm Based on DNA for Internet of Things Devices," A Master Thesis, Middle East University , June, 2021.

[17] Kh. Zaid, N. Ahmed, and K. Nidhal, "Text Multilevel Encryption Using New Key Exchange Protocol," Baghdad Science Journal, vol. 19, no. 3, pp: 619-630, 2022.

[18] R. A. Mahdi and M. Atefeh, "Advanced encryption schemes in multi-tier heterogeneous internet of things: taxonomy, capabilities, and objectives," The Journal of Supercomputing, vol. 78, pp:18777–18824, 2022.

[19] Y. Minghao, W. Dongdong, Zh, Feng, W. Shenqing, Ji. Shan, and R. Yongjun, "An Examination of Multi-Key Fully Homomorphic Encryption and Its Applications," MDPI, Mathematics, Https://doi.org/10.3390/math10244678

[20] Zh. Yuzhou, X. Hongwei, S. Jingyu, and Zh. Hao, "An Efficient Multilevel Encryption Scheme For Stereoscopic Medical Images Based On Coupled Chaotic System And Otsu Threshold Segmentation," Computers in Biology and Medicine., vol. 146, 2022.

[21] M. O. Emil, "Multi-layer encryption flexible integrating algorithm, " SPIE Proceedings vol. 493 :Advanced Topics in Optoelectronics, Microelectronics, and Nanotechnologies XI, 124931X (2 March 2023); doi: 10.1117/12.2643224, 2023