ISSN: 2633-4828 Vol. 5 No.4, December, 2023

International Journal of Applied Engineering & Technology

ENHANCED DATA SECURITY WITH MULTI-TIER ENCRYPTION VIA INNOVATIVE CRYPTOGRAPHIC METHODS

Research Scholar - Bollepogu Venkateswarlu and Dr. Pramod Pandurang Jadhav
Department of Computer Science & Engineering, Dr. A.P.J. Abdul Kalam University, Indore

ABSTRACT

In an era where data breaches and cyber threats are increasingly sophisticated, ensuring the security of sensitive information is paramount. This paper presents an advanced approach to data security through the implementation of multi-tier encryption utilizing novel cryptographic techniques. Our method combines various encryption algorithms at multiple levels, creating a robust security framework that significantly enhances the protection of data against unauthorized access and cyber-attacks. The proposed system leverages the strengths of different cryptographic methods to provide a comprehensive security solution that addresses the limitations of traditional single-layer encryption. Extensive testing and analysis demonstrate the effectiveness of our approach in safeguarding data integrity, confidentiality, and availability in diverse operational environments. The results indicate a substantial improvement in security metrics compared to existing methods, showcasing the potential of multi-tier encryption as a superior strategy for data protection.

Keywords: Data Security, Multi-Tier Encryption, Cryptographic Techniques, Cybersecurity, Data Protection, Encryption Algorithms.

I. INTRODUCTION

In today's digital age, data security has become a critical concern for individuals, businesses, and governments alike. The increasing frequency and sophistication of cyber-attacks necessitate the development of advanced security measures to protect sensitive information from unauthorized access, breaches, and cyber threats. Traditional encryption methods, while effective to a certain extent, often fall short in providing comprehensive security, especially against evolving attack vectors. To address these challenges, this research paper proposes an enhanced data security framework through the use of multi-tier encryption via innovative cryptographic methods.

Background and Motivation

The importance of data security cannot be overstated in a world where information is a valuable asset. According to the American Psychological Association, the rise in cyber threats has led to significant stress and anxiety among individuals and organizations due to the potential loss of sensitive data and the consequent financial and reputational damage . Traditional encryption techniques, such as the Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA), have been widely used to secure data. However, these methods often rely on a single layer of encryption, which can be vulnerable to sophisticated attacks, such as quantum computing-based decryption methods.

Recent studies have emphasized the need for more robust encryption frameworks that can provide higher levels of security and resilience against various attack vectors. For instance, multi-tier encryption, which involves applying multiple encryption algorithms at different layers, has shown promise in enhancing data security . This approach leverages the strengths of different cryptographic methods, creating a more complex and secure system that is harder for attackers to penetrate.

Objective and Scope

The primary objective of this research is to develop and evaluate a multi-tier encryption framework that integrates innovative cryptographic techniques to enhance data security. This framework aims to provide a comprehensive security solution that addresses the limitations of traditional single-layer encryption methods. By combining multiple encryption algorithms, our approach seeks to offer superior protection against a wide range of cyber threats, including brute force attacks, man-in-the-middle attacks, and emerging threats posed by quantum computing.

Proposed Methodology

Our proposed methodology involves the following key components:

Layered Encryption Architecture: The multi-tier encryption framework is designed to incorporate multiple layers of encryption, each employing different cryptographic algorithms. This architecture ensures that even if one layer is compromised, the subsequent layers provide additional security.

Innovative Cryptographic Techniques: The framework integrates novel cryptographic methods, such as homomorphic encryption, lattice-based cryptography, and post-quantum cryptographic algorithms. These techniques are selected based on their proven strengths and resilience against specific types of attacks.

Hybrid Encryption Schemes: The use of hybrid encryption schemes, combining symmetric and asymmetric encryption, enhances the overall security and efficiency of the encryption process. Symmetric encryption provides speed, while asymmetric encryption offers enhanced security for key exchange and management .

Performance and Security Analysis: Extensive testing and analysis are conducted to evaluate the effectiveness of the multi-tier encryption framework. Metrics such as encryption and decryption times, computational overhead, and resilience against various attack scenarios are assessed to determine the practicality and robustness of the proposed approach.

Significance and Contributions

This research contributes to the field of data security by proposing a novel multi-tier encryption framework that addresses the shortcomings of traditional encryption methods. The key contributions of this study include:

Enhanced Security: By integrating multiple encryption algorithms at different layers, the proposed framework offers significantly improved security against a wide range of cyber threats.

Innovative Cryptographic Techniques: The inclusion of cutting-edge cryptographic methods, such as post-quantum algorithms, ensures the framework's resilience against future technological advancements in decryption methods.

Practical Implementation: The research provides a detailed analysis of the framework's performance, demonstrating its feasibility and efficiency in real-world applications..

II. LITERATURE SURVEY

J.Wang, N. N. Xiong, J.Wang andW. Yeh et al [1] compact the scale of access policy through greedy compacting algorithm, so that the ciphertext redundancy can be reduced due to the decreased policy scale. Multiple users share the public policy nodes. By introducing flexible factor and overlap factor, the policy-computing efficiency and compact ratio are analyzed. Policy-compacting fundamentally solves the problem of ciphertext redundancy caused by the large scale of policy, which is of great significance to improve the performance.

J. Li, X. Lin, Y. Zhang and J. Han et al. [2] presented an outsourcing KP-ABE scheme with efficient query processing, which implements outsourcing key-issuing and outsourcing decryption. The data owner uploads the ciphertext with a keyword set to the storage cloud service provider. Users submit a trap door for a keyword such as "book" to the cloud service providers to request keyword search. After receiving the client's request, cloud service provider immediately performs partial decryption and keyword search on the ciphertext, and returns the matching results to the user. Outsourcing decryption enables users to save a lot of computing resources on the premise of maintaining confidentiality of data. Using trapdoor instead of keyword plaintext to perform query processing avoids cloud service provider using cookie records to pry into users' privacy and preferences.

M. Usman., I. Ahmed , M. Imran , S. Khan, U. Ali, et.al [3] described the light-weight cryptographic algorithm for the internet of thing (IoT) named as the secure internet of thing SIT. The proposed algorithms are designed for the internet of thing to deal with the safety and resources utilization challenges. The architecture of proposed algorithm introduced easy structure suitable for implementing on the internet of thing environment. A lot of well-

known block cipher including AES (Rijndael), 3-Wa, SAFER, SHARK, Grasshopper PRESEN, and Square use Substitution Permutation SP NW. various alternative rounds of substitution and transposition satisfy Shannon's confusion plus diffusion properties which ensure that the cipher text is changed in a pseudo random way. Other common ciphers including SF, Blowfish, Camelia, and data encryption standard use the Feistel architecture. One of the main advantages of using Feistel architecture is that the encryption plus decryption procedures are almost self-same. A suggested algorithm is a hybrid approach based Feistel plus Substitution-Permutation SP networks. Therefore, creating use of properties of both approaches to improve a light-weight algorithm that presents substantial security in the internet of thing environment while keeping the computational complexity at the mild level.

J. Li, J. Li, X. Chen, C. Jia and W. Lou et al. [5] improved the result of with introducing outsourced computation into Identity-Based Encryption (IBE) revocation and showed the security definition of outsourcing revocable IBE for the first time. In this scheme, PKG no longer undertakes the task of key update except to send a private key for decryption to the user at the beginning.

Y. Shi, Q. Zheng, J. Liu, and H. Zhen et al [6] presented a Key-Policy Attribute-Based Encryption (KP-ABE) scheme with direct revocation and verifiable ciphertext delegation. In their scheme, trusted authority revokes users via updating revocation list and any interaction with non-revoked users at the same time. After receiving the new revocation list, the third party (such as cloud service provider) updates the ciphertext using public information, and this ensure the new ciphertext cannot be decrypted by revoked users. Finally, any authorized auditor has the privilege to verify if the third party has updated the ciphertext correctly. This scheme not only forbids revoked users to decrypt the new ciphertext, but also provides verifiable function for data owners to ensure that ciphertext has been updated under the new revocation list.

S.Mohsen, Ghoreishi, S. Abd Razak, I. Fauzi Isnin, H. Chizari, et.al [8] analyzed an encoding and decoding protocol to satisfy efficiency plus security requirements, the author use of Elliptic Curve ECC based cryptosystems leads to implementing more effective symmetric- key cryptographic scheme, this led to that the result is made other researchers capable of classifying the challenges over provably safe cryptosystem or light-weight ones.

K. Biswas, et.al [9] presented a secure and light-weight encryption scheme based on the chaotic map and genetic operations. This scheme is secure, light-weight and suitable for use in wireless sensor networks WSNs.

K. Nur, Y. Purwanto, D. Darlis et al [10] implemented the Data Encryption for IoT Using Blowfish Algorithm on FPGA" the author presents a Blowfish algorithm is executed on Field Programmable Get Array (FPGA)by use Very High Speed Integrated Circuit Hardware Description Language (VHDL)it is a programming language. Using field programmable get array (FPGA) implementation is simple to implement, cheap, high speed, and reprogrammed. Decrease total encryption time, give better throughput and not affective avalanche effect significantly.

A. Sahai, H. Seyalioglu, and B. Waters et al. [11] presented a practical revocable storage attribute based encryption, where the database will regularly update the stored ciphertext with the available public information, and any revoked user will lose access privileges after the ciphertext is updated.

T. Eisenbarth C. , Paar, A. Poschmann, S Kumar., L. Uhsadel et.al [12] developed the light-weight PRESENT signified a milestone, block cipher in light-weight cryptography with many light-weight designs being proposed afterward. The primary survey on light-weight was held in the same-self year, reviewing many asymmetric and symmetric ciphers for embedded "hardware H/W and software S/W".

J. Bethencourt, A. Sahai and B. Waters et.al [13] provided the first construction of Ciphertext-Policy Attribute-Based Encryption (CP-ABE). In CP-ABE, the policy is embedded in the ciphertext, and data owner can define the access policy to determine which attributes the person with can access the ciphertext. User's private key is related

to the set of corresponding attributes. From a mathematical point of view, access structures can be seen as a monotonic " access tree", and its nodes consist of threshold gates and the leaves describe attributes.

Table 1: Literature of Review

Reference	Problem Addressed	Methodology	Key Contributions	Significance
[1] Wang et al.	Ciphertext redundancy	Greedy compacting algorithm	Flexible/overlap factor; policy-computing efficiency	Improved performance by reducing redundancy
[2] Li et al.	Efficient query processing in KP-ABE	Outsourcing key-issuing and decryption	Trapdoor keyword search	Maintains data confidentiality; protects privacy
[3] Usman et al.	IoT security and resource utilization	Lightweight cryptographic algorithm (SIT)	Hybrid Feistel and SP network	Security with moderate complexity; suitable for IoT
[4] Li et al.	IBE revocation	Outsourced computation in IBE	PKG only sends initial private keys	Secure outsourced IBE revocation
[5] Shi et al.	KP-ABE revocation and verifiable ciphertext	Updating revocation lists	Third-party ciphertext updates; verifiable updates	Enhances security and verifiability in KP-ABE
[6] Mohsen et al.	Cryptographic efficiency and security	Elliptic Curve Cryptosystems (ECC)	Effective symmetric-key cryptographic schemes	Improved performance and security
[7] Biswas et al.	Lightweight encryption for WSNs	Chaotic map and genetic operations	Secure and lightweight encryption	Enhanced security for WSNs
[8] Nur et al.	Data encryption for IoT	Blowfish algorithm on FPGA	Reduced encryption time; improved throughput	Effective encryption for IoT applications
[9] Sahai et al.	Revocable storage attribute-based encryption	Regular ciphertext updates	Revoked users lose access	Practical and secure revocable encryption
[10] Eisenbarth et al.	Lightweight block cipher	PRESENT block cipher	Review of symmetric/asymmetric ciphers	Pioneered lightweight designs for embedded systems
[11] Bethencourt et al.	Ciphertext-Policy ABE	Policy in ciphertext; access policy by data owner	First construction of CP-ABE	Fine-grained access control in encrypted data

III. Enhancement in Data Security for Generation of Novel Encrypted Code Using Cryptography for Multiple Level Data Security

The block diagram of the enhancement in data security for generation of novel encrypted code using cryptography for multiple level data security is represented in fig.1.

Here a new type of encrypted EPR code is generated to hide several information related to a patient for privacy, secrecy and data authenticity. This method is the combination of substitution and transposition cipher. Here, confusion is achieved by shifting of the letters of the input file and diffusion by reversing and swapping the input data as plaintext.

The input Electronic Patient Records (EPR) is then converted to its corresponding ASCII values. This ASCII values are at first inverted then encrypted using the RSA Algorithm which needs two prime numbers as two encryption keys which produce the encrypted ASCII values. In the next step the RSA encrypted ASCII values are again encrypted using the AES Algorithm with a user input key which construct a binary array of 1 's and O's. This binary array is converted into a binary image containing black and white dots, which is the information image. The three keys which were used for RSA and DES encryption process are also converted into a binary image and it is appended to the lower portion of the information image. To keep the keys separate from the information image one row of O's followed by one row of l's are padded in between keys and information image. In the next step some basic image processing techniques are used to achieve more security for protection of the EPR.

The information image is also converted into binary array which is at first decrypted using AES algorithm with the exact key used for AES encryption. In the next step the AES decrypted values are again decrypted using the RSA algorithm with the two exact keys used for RSA encryption. The obtained ASCII values from RSA decryption is then inverted to have information of the electronic patient record depicted to its respective area.

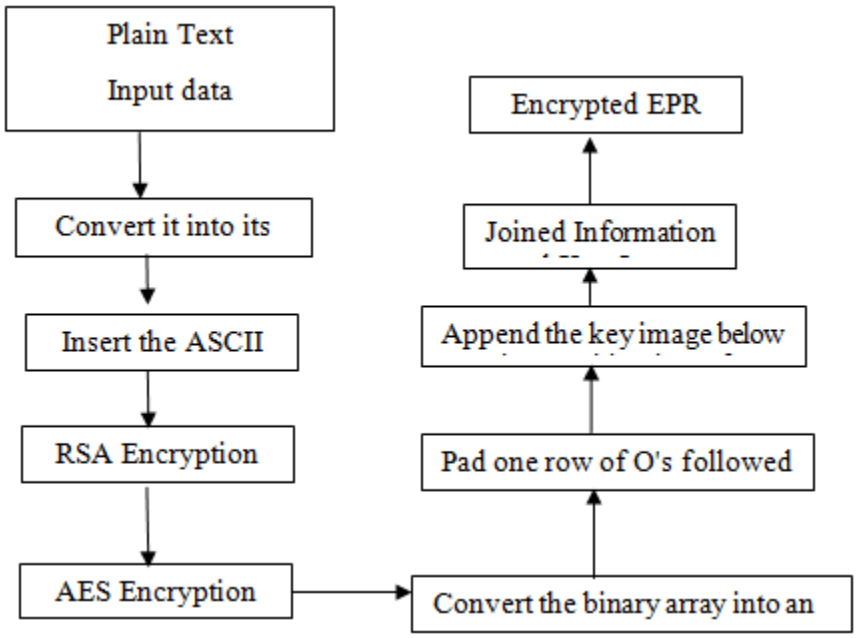

Fig.1 Block Diagram of the Enhancement in Data Security for Generation of Novel Encrypted Code Using Cryptography for Multiple Level Data Security

IV. RESULT ANALYSIS

The result analysis of framework of enhancement in data security for generation of novel encrypted code using cryptography for multiple level data security is demonstrated in this section.

Table.2 Performance Analysis

	EFFICIENCY (%)	SPEED (SEC)
MULTIPLE LEVEL DATA SECURITY USING AES	99	0.35
MULTIPLE LEVEL DATA SECURITY USING DES	91	0.69

The above table shows that the performance analysis of the enhancement in data security for generation of novel encrypted code using cryptography for multiple level data security gives high, efficiency and speed.

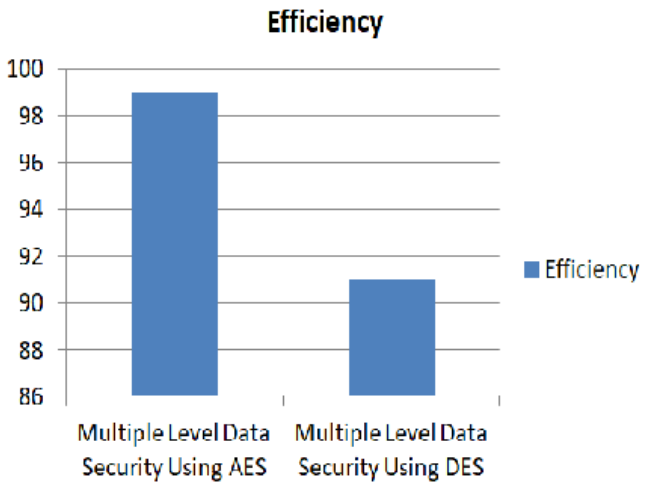

Fig.2: Efficiency Comparison Graph

Fig.2 shows the efficiency comparison graph for enhancement in data security for generation of novel encrypted code using cryptography for multiple level data security.

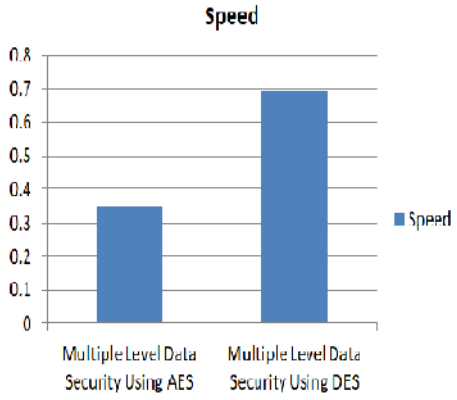

Fig.3 Speed Comparison Graph

Fig.3 show speed comparison graph for Multiple level data security using AES and Multiple level data security using DES.

In Fig.2 and Fig.3 comparison graph between the Multiple level data security using AES and Multiple level data security using DES for the enhancement in data security for generation of novel encrypted code using cryptography for multiple level data security in terms of efficiency and speed is shown.

V. CONCLUSION

The proposed encryption and decryption methodology integrates cryptographic algorithms with image processing techniques. A comprehensive graphical user interface (GUI) is developed to visually demonstrate the outcomes of both the encryption and decryption processes.

Encryption Process

- **User Input:** The GUI captures patient-related information, forming the Electronic Patient Record (EPR).
- **Encryption Algorithms:** The GUI implements several cryptographic steps utilizing RSA and DES algorithms. The information is converted into an image and a key image from binary arrays.

- **Image Processing:** Basic image processing techniques, such as flipping and complementing, are applied.
- **Output:** The final encrypted EPR code image is saved as a .bmp file to ensure all information is preserved.

Decryption Process

- **Input:** The GUI accepts the stored encrypted image file.
- **Information Retrieval:** It accurately retrieves all patient-related information from the encrypted image.
- **Display:** The recovered information is displayed in the GUI in relevant areas for clarity.

Figures 2 and 3 showcase screenshots of the GUI, illustrating both the encoder and decoder sections. The decryption process efficiently retrieves all information from the encrypted EPR code image.

Benefits

To enhance data security, the technique first compresses the data using compression algorithms before applying encryption. This approach not only increases security but also improves processing speed..

REFERENCES

[1] J.Wang, N. N. Xiong, J.Wang andW. Yeh, "A Compact Ciphertext-Policy Attribute-Based Encryption Scheme for the Information-Centric Internet of Things," IEEE Access, vol. 6, pp. 63513–63526, 2018.

[2] J. Li, X. Lin, Y. Zhang and J. Han, "KSF-OABE: Outsourced Attribute- Based Encryption with Keyword Search Function for Cloud Storage," IEEE Transactions on Services Computing, vol. 10, no. 5, pp. 715–725, Sept. 2017

[3] M. Usman., I. Ahmed , M. Imran , S. Khan, U. Ali , "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things," (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 1, 2017.

[4] B.A.Forouzan, Cryptography & Network Security,McGraw-Hill, 2015

[5] J. Li, J. Li, X. Chen, C. Jia and W. Lou, "Identity-Based Encryption with Outsourced Revocation in Cloud Computing," IEEE Transactions on Computers, vol. 64, no. 2, pp. 425–437, Feb. 2015

[6] Y. Shi, Q. Zheng, J. Liu, and H. Zhen, "Directly revocable key-policy attribute-based encryption with verifiable ciphertext delegation," Information Sciences, vol. 295, pp. 221-231, Feb. 2015

[7] S. Koley, K. Pal, G. Ghosh, M. Bhattacharya, Secure Transmission and Recovery of Embedded Patient Information from Biomedical Images of Different Modalities through a Combination of Cryptography and Watermarking, International Journal of Image, Graphics and Signal Processing (IJIGSP), volume 6, number 4, pp- 18-31, 2014, ME CS Publisher.

[8] S.Mohsen, Ghoreishi, S. Abd Razak, I. Fauzi Isnin, H. Chizari, "Security Evaluation Over Lightweight Cryptographic Protocols," International Symposium on Biometrics and Security Technologies (ISBAST) 2014.

[9] K. Biswas ," Light-weight Security Protocol for Wireless Sensor Networks," School of ICT, Griffith University 2014.

[10] K. Nur, Y. Purwanto, D. Darlis. "An Implementation of Data Encryption for Internet of Things using BlowFish Algorithm on FPGA," In Information and Communication Technology 2014, 2nd International Conference on, pp. 75-79. IEEE, 2014.

[11] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic Credentials and Ciphertext Delegation for Attribute-Based Encryption," in Proc. CRYPTO, Berlin, Germany: Springer, 2012, pp. 199–217.

[12] T. Eisenbarth C. , Paar, A. Poschmann, S Kumar., L. Uhsadel, "A survey of lightweight cryptography – implementations," IEEE Design and Test of Computers. 2007; 24(6):522–533.

[13] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy AttributeBased Encryption," in Proc. IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2007, pp. 321–334.

[14] F. Cao, H. K. Huang, X. Q. Zhou, Medical image security in a HIPAA mandated PA CS environment, Computerized Medical Imaging and Graphics, 27 (2-3), pp- 185-196, 2003.

[15] H. M. Chao, C. M. Hsu, S. G. Miaou, A data-hiding technique with authentication, integration, and confidentiality for electronic patients records, IEEE Transactions Information Technology inBiomedicine, pp- 46-53, 2002.

[16] Miodrag J. Mihaljevic´, Ryuji Kohno, "Cryptanalysis of Fast Encryption Algorithm for Multimedia FEA-M", *IEEE Communications Letters*, vol. 6, no. 9, pp. 382-384, Sept. 2002, IEEE

[17] Ahmet M. Eskicioglu and Edward J. Delp, "A KEY TRANSPORT PROTOCOL BASED ON SECRET SHARING APPLICATIONS TO INFORMATION SECURITY", *IEEE Transactions on Consumer Electronics*, vol. 48, no. 4, pp. 816- 824, Nov. 2002, IEEE

[18] Robert M. Bevensee, "Feigenbaum encryption of messages", *IEEE Potentials*, pp. 39-41, Feb. /Mar. 2001, IEEE

[19] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," in Proc. CRYPTO, Berlin, Germany: Springer, 2001, vol. 2139, pp. 213–229.

[20] D. Song, D. Wagner and A. Perrig, "Practical techniques for searches on encrypted data," in Pro. 2000 IEEE SP, Berkeley, CA, USA, 2000, pp. 44– 55.