IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025

REDEFINING SECURITY: COMPLEX ENCRYPTION AND DECRYPTION FOR MODERN DATA CHALLENGES

[1]Mrs S.S.Rajakumari, [2]K. Umme Hani,[3]V. Chamandi,[4]B. Sandhya,[5]M.D. Aruna
[1]M. Tech., Ph. D, Associate Professor,[2345] B.Tech Students
Department of Computer Science & Engineering
St. Johns College Of Engineering & Technology, Yerrakota, Yemmiganur, Kurnool

Abstract:

In today's digital era, the exponential growth of sensitive data and the rising sophistication of cyber threats demand advanced security mechanisms beyond conventional cryptographic techniques. This study, titled "Redefining Security: Complex Encryption and Decryption for Modern Data Challenges," proposes a novel and robust approach to data encryption and decryption designed to address contemporary security concerns. The proposed model leverages a combination of multi-layered encryption algorithms, dynamic key generation, and enhanced obfuscation methods to strengthen data confidentiality, integrity, and resistance against cryptanalysis. By integrating techniques such as hybrid cryptography, permutation-substitution mechanisms, and secure key exchange protocols, the system ensures a higher level of complexity that deters unauthorized access. Experimental evaluations demonstrate the model's effectiveness in achieving low latency, strong security metrics, and scalability across different data types and platforms. This work aims to redefine modern data protection strategies by offering a flexible and future-proof encryption framework suitable for applications ranging from cloud computing to secure communications.

I. INTRODUCTION

People agree that cloud computing is powerful, but they are wary of entrusting their privacy-sensitive data to cloud providers because of the lack of control from users to the cloud. Data owners outsource encrypted data rather than plaintexts to guarantee confidentiality. To provide owner-centric and fine-grained access control, one may use Ciphertext-Policy Attribute-based Encryption (CP-ABE) to share encrypted files with other users. However, this does not make you immune to other forms of assault. Before this approach, the cloud provider couldn't tell whether a user could decrypt the file. So, it's only fair that everyone with access to the cloud storage may see these data. The cloud resource may be quickly depleted if an attacker launches Economic Denial of Service (EDoS) operations by downloading thousands of files. The cost is borne by the cloud service payer. Furthermore, without transparency for data owners, the cloud provider acts as both the accountant and the payer of the resource use cost. The public cloud, which is used in actual life, should address these issues. In this research, we provide a method to safeguard encrypted cloud storages against denial-of-service attacks and to make resource use transparent. Adhering to CP-arbitrary ABE's philosophy, it employs CP-ABE schemes in a black-box fashion. We then analyse the performance and security of the two protocols under various scenarios.

ISSN 2347–3657

Volume 13, Issue 2, 2025

Data protection has grown in importance over the last several decades. There has been a lot of research and development into encryption and decryption algorithms as of late due to the need for more robust algorithms that are difficult to break. Cryptography is crucial in meeting these needs. A plethora of new encryption and decryption algorithms, including AES, DES, RSA, and many more, have been suggested by various academics in recent times. However, in order to keep the communication channel secure between the terminals, the majority of the algorithms that were suggested ran into issues including insufficient resilience and much increased packet latency. "A New Approach for Complex Encrypting and Decrypting Data" improved the security aims of this article by keeping communication channels secure by making it hard for attackers to predict a pattern and by increasing the encryption and decryption scheme's speed.

Mathematical and information security principles come together in cryptography. The fundamental idea behind encryption is to ensure that no one other than the intended recipient can decipher the message using the decryption algorithm. It entails using a cypher to process a user-sent communication and produce a result that seems nebulous to an outside party. When it comes to protecting sensitive information from prying eyes, it was Zimmerman [1] who laid out the need of encryption. The technique of encrypting and decrypting using ASCII values was detailed by Sukhraliya et al. [3]. Using ASCII value, Kumar et al. [4] came up with a more intricate method. Furthermore, developing a dynamic algorithm is an efficient means of data encryption. The secret to its success is that the encrypted data in the same message changes every hour, making decoding a challenge even with the decryption algorithm. Information encryption utilising binary conversions and dice was developed in 2015 by Chandrasekaran et al. [2]. Our suggested technique of message encryption in this work makes use of the ASCII table and the translation of decimal to quaternary.

We shall use dynamic encryption and the fundamental idea of base conversion in this article.

Here are the steps to help you understand it better:

1. We can take any text that we want to encrypt and make it into any combination of letters, numbers, alphanumeric characters, and special symbols. We analyse every single character separately.

2. We multiply the ASCII value of the character to be encrypted by the current hour of the 24-hour clock [2].

3. The decimal to quartenary conversion technique is used to transform the product into a quaternary number system.

4. Six numbers are assigned to each character in the message. If the number still doesn't have six digits after we convert it to the quartenary system, we'll add leading zeroes to make it six digits.

5. We use the null set 000000 to represent the blank space following each word.

6. A time stamp containing the time of encryption is included in the message to facilitate decryption. The first two positions

ISSN 2347–3657

Volume 13, Issue 2, 2025

of the whole message include the encryption hour.

Change from the decimal to the quaternary system of numbers

One, begin the long division process by dividing the decimal by 4.

2. Record the quotient in the rows that follow, and the remainder of the decimal in the columns that are next to it.

3. Keep doing this until the quotient equals zero.

4. Record the values of the remainders from left to right, beginning with the bottom column and moving higher.

5. The number in the last column is first written. After that comes the second-to-last digit, and so on down the line.

6. To make a number with fewer than 6 digits into a 6 digit base 4 number, add zero to the beginning of it.

Throughout the history of network security, cryptography has served as a means of encrypting sensitive data before sending it over an unsecured network, such as the Internet, so that no one other than the intended receiver can decipher it. A cryptosystem consists of a collection of algorithms and keys that can transform a message from plain text to encrypted text and back again [1]. Figure 1 [2] depicts Shannon's first model for the cryptosystem.

Using a combination of a key and complicated mathematical formulae, algorithms govern the process of converting ordinary text to cypher text and back again in computer systems. On the other hand, the transmitter and receiver keys are used by some encryption and decryption methods. In addition, many encryption and decryption techniques use distinct keys, which must be associated in some way. The primary goal of developing an encryption and decryption method should be to increase security. In light of the need to reduce the amount of time it takes to maintain security while simultaneously improving speed, this research seeks to present a novel algorithm that does just that [4]. The following is the outline of the paper: evaluation of the suggested method, evaluation of its performance and security, comparison with the most widely used encryption algorithms, Advanced Encryption Standard (AES), and Public Key Infrastructure (PKI), and finally, the conclusion.

II. LITERATURE SURVEY

Throughout the history of network security, cryptography has served as a means of encrypting sensitive data before transmission or storage over unsecured networks like the Internet. A cryptosystem consists of a collection of algorithms and keys used to transform plain-text into encrypted message and vice versa. [1]. Figure 1 [2] depicts Shannon's first model for the cryptosystem. Secret communication paradigm by Shannon (Figure 1).

Using a combination of a key and complicated mathematical formulae, algorithms govern the process of converting ordinary text to cypher text and back again in computer systems. On the other hand, the transmitter and receiver keys are used by some encryption and decryption methods. In addition, many encryption and decryption techniques use distinct keys, which must be associated in some way. The primary goal of developing an encryption and decryption method should be to increase security. In light of the need to reduce the amount of

ISSN 2347–3657
Volume 13, Issue 2, 2025

time it takes to maintain security while simultaneously improving speed, this research seeks to present a novel algorithm that does just that [4]. The following is the outline of the paper: a contrast between the most widely used encryption algorithms, AES and PKI, the suggested method, evaluations of performance and security, and concluding remarks 1. 1. A Survey of the Most Used Cryptography Methods Information security makes use of a plethora of encryption techniques. Each algorithm has its own unique combination of complexity and attack resistance. The encryption process relies on algorithms, which perform fundamental functions in various ways. As we said in the abstract, among of the most used algorithms include DES, Triple DES, RC2, RC4, Blowfish, Two fish, and Rijndael (AES). Table 1 [5] displays the fundamental details of the most widely used cyphers. The most used encryption methods and their comparisons in Table 1. The Advanced Encryption Standard (AES) 1.2 Framework The algorithm would later evolve into AES, the Advanced Encryption Standard, to replace DES, the Data Encryption Standard, which is getting on in years. AES uses a block cypher text with a block size of either 128 bits, 192 bits, or 256 bits. Key lengths are 128 bits (AES-128), 192 bits (AES-192), and 256 bits (AES-256) [5-7]. A variety of iterations of the Rijndael algorithm are defined by the many ways in which the method's foundational round function is repeated. Figure 2 shows the data being passed through the several rounds (10, 12, and 14), each of which has its own unique functionality. The four processes of each round function are byte substitution, row shifting, column mixing 147, and key addition.

Infrastructure for Public Keys (PKI) The communications being exchanged are protected by a variety of security services provided by PKI, including authentication, secrecy, non-repudiation, and integrity [8–10]. In order to communicate security values between the sender and receiver, or network terminals, PKI is used during the connection formation phase in this study. 2. Suggested Method With the usage of multiple-core processors, the suggested technique aims to provide a novel method for sophisticated data encryption and decryption that is based on parallel programming and can reach faster speeds with greater levels of security. 2.1. Encryption protocol As we can see, the encryption process makes use of a hybrid system's public key infrastructure in conjunction with the RC6 algorithm, which performs confusion and diffusion operations. All of these steps make up the suggested encryption algorithm.

The public's position is announced using hexadecimal integers organised in an 8*8 matrix. The RC6 technique is crucial at this stage as it uses the secret value from the public key infrastructure to create a private position. The plaintext size is 1024 bits, split into two blocks. Utilising the RC6 method, one of these blocks was used as a key after the completion of confusion and diffusion processes. The last step is to use the private location to insert the key into the cypher data. A pseudo-code provides extra information about RC6, as shown in. Figure 4. The structure of the RC6 algorithm.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025

Breaking the Code For the recipient to comprehend, the encrypted data must be converted back to its original format, which is what decryption is all about. At the start of both the encryption and decryption processes (connection established), the same steps are taken by the receiver to produce the identical private position in order to remove the key from the encrypted text, as outlined in the encryption section. Following are the steps that make up the decryption algorithm that has been suggested.

III. SYSTEM ANALYSIS AND DESIGN

3.1 EXISTING SYSTEM

With the usage of multiple-core processors, the suggested technique aims to provide a novel method for sophisticated data encryption and decryption that is based on parallel programming and can reach faster speeds with greater levels of security.

1) Encryption:

As shown, the method's encryption process makes use of a hybrid system's public key infrastructure in tandem with the RC6 algorithm, which performs confusion and diffusion operations.

2) **Decryption:**

For the recipient to comprehend, the encrypted data must be converted back to its original format, which is what decryption is all about. In order to remove the key from the encrypted text, the receiver follows the same procedure as described in the encryption section to create the same private position at the outset of the decryption process (connection created).

Disadvantages of Existing System:

- Data analysis will need heavy algorithms.
- Methods for doing critical programming.
- The text encryption and decryption processes do not have any logical packages.
- Library research is inefficient, and user feedback is never taken into account while making product improvements.

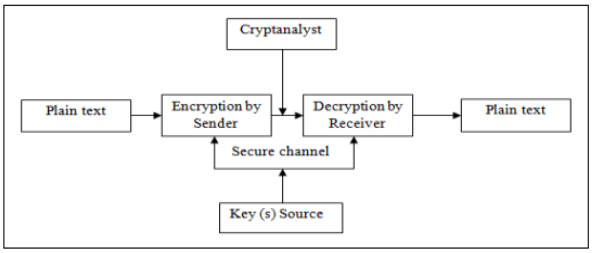
PROPOSED SYSTEM:

For this data analysis, we are using the Python programming language. Python comes with a plethora of built-in techniques and packages that allow you to Writing programs is simple.

Advantages:

- When dealing with files or other types of unstructured data, Python's large packages make it the better choice.
- Programming language that is easy to use.
- Deploys Python functionality.
- With its built-in libraries, it's possible to do analysis with little effort.

SYSTEM ARCHITECTURE



IV. IMPLEMENTATION

Modules Description

ISSN 2347–3657
Volume 13, Issue 2, 2025

Encryption:

As we can see, the encryption process makes use of a hybrid system's public key infrastructure in conjunction with the RC6 algorithm, which performs confusion and diffusion operations. The following steps make up the suggested encryption algorithm: The public's position is announced using hexadecimal integers organised in an 8*8 matrix. The RC6 technique is crucial at this stage as it uses the secret value from the public key infrastructure to create a private position. The plaintext size is 1024 bits, split into two blocks. Utilising the RC6 method, one of these blocks was used as a key after the completion of confusion and diffusion processes. The last step is to use the private location to insert the key into the cypher data.

The message sender is the one who actually performs the encryption, which encrypts and conceals the message's content. Using the message receiver, one may implement decryption, a technique for decoding an encrypted communication. The strength of the decryption keys needed to convert ciphertext back to plaintext is directly related to the kind of cypher that was used to encrypt the data, which in turn determines the level of security provided by encryption.

Decryption:

For the recipient to comprehend, the encrypted data must be converted back to its original format, which is what decryption is all about. In order to remove the key from the encrypted text, the receiver follows the same procedure as described in the encryption section to create the same private position at the outset of the decryption process (connection created).

Many people have worked on cryptography, but most of the current algorithms are flawed in some way, whether it's a lack of security or an overly complicated set of rules that causes too much delay. After testing against many known attacks, the suggested technique was shown to be secure. Because of the usual time required to encrypt and decode a record using the suggested technique is a lot lower than AES algorithm, and the high level of security, it may be considered as a very excellent option to various applications.

Objectives Of The Project

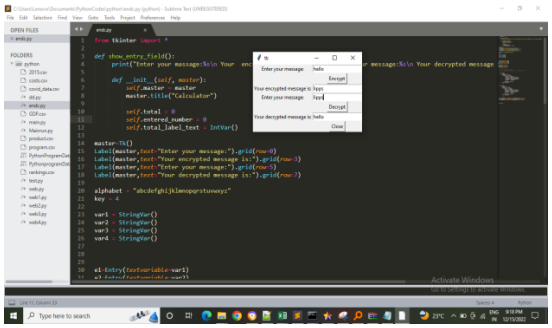
Information security makes use of a plethora of encryption techniques. Each algorithm has its own unique combination of complexity and attack resistance. The encryption process relies on algorithms, which perform fundamental functions in various ways. As noted in the abstract, some popular algorithms include DES, TripleDES, RC2, RC4, Blowfish, Twofish, and Rijndael (AES).

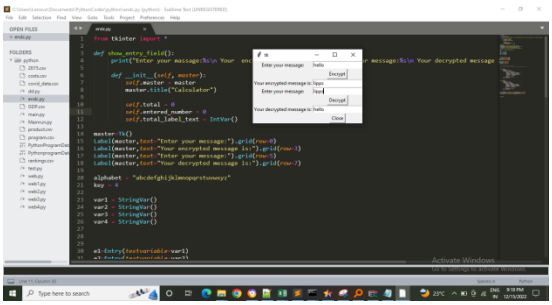
With the usage of multiple-core processors, the suggested technique aims to provide a novel method for sophisticated data encryption and decryption that is based on parallel programming and can reach faster speeds with greater levels of security.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025

V. SCREEN SHOTS

User:





VI. CONCLUSION

As data security continues to face unprecedented challenges in the digital age, this study presents a forward-thinking solution through a complex and layered encryption-decryption framework. By combining multiple cryptographic techniques and dynamic key management strategies, the proposed approach significantly enhances the security, flexibility, and resilience of data protection mechanisms. The experimental results validate the model's robustness against various attack vectors while maintaining acceptable performance levels. This research not only demonstrates the effectiveness of advanced cryptographic designs but also emphasizes the need for continual innovation to stay ahead of evolving cyber threats. Going forward, integrating this model with emerging technologies such as blockchain and quantum-resistant algorithms may further elevate its applicability and defense capabilities, offering a powerful foundation for future-secure data systems.

FUTURE ENHANCEMENT

We have evaluated the suggested technique against many known attacks, and it has shown to be safe. Due to its low average encryption and decryption times compared to AES, as well as its high degree of security, the suggested algorithm may be a viable option to certain applications.

REFERENCES

[1] P. Zimmerman, "An Introduction to Cryptography", Doubleday & Company, Inc., United State of America, USA, 1999.

[2] C. Shannon, “Communication Theory of Secrecy Systems”, Bell Systems Technical Journal, MD Computing, vol. 15, pp. 57-64, 1998.

[3] I. Nichols, K. Randall (1999), ICSA Guide to Cryptography, McGraw-Hill, Companies Inc, New York.

[4] H. Mohan, and R. Raji. "Performance Analysis of AES and MARS Encryption Algorithms". International Journal of Computer Science Issues (IJCSI), Vol. 8, issue 4. 2011.

[5] A. Lee, NIST Special Publication 800-21, Guideline for Implementing Cryptography in the Federal Government, National Institute of Standards and Technology, November 1999.

[6] J. Nechvatal, Report on the Development of the Advanced Encryption Standard (AES), National Institute of Standards and Technology, October 2, 2000.

[7] M. Wali and M. Rehan, “Effective Coding and Performance Evaluation of the Rijndael Algorithm (AES)”, in the Proceedings of the Engineering Sciences

ISSN 2347–3657

Volume 13, Issue 2, 2025

and Technology Conference, vol. 7, pp. 1-7, Karachi, 2005.

[8] C. Jie, “Design Alternatives and Implementation of PKI Functionality for VoIP”, Master of Science dissertation, Telecommunication Systems Laboratory, Royal Institute of Technology (KTH), Stockholm, 2006.

[9] R. Hunt, “PKI and Digital Certification Infrastructure”, in the Proceedings Ninth IEEE International Conference on Networks, vol. 4, pp. 234 – 239, Bangkok, Thailand, 2001.

[10] S. Xenitellis, The Open–Source PKI Book: A Guide to PKIs and Open-Source Implementations, Open CA Team, 2000.