IJNRD.ORG ISSN : 2456-4184

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

International Research Journal IJNRD Research Through Innovation

CRIME DATA STORAGE USING CRYPTOGRAPHY BASED SECURITY SYSTEM

[1]Sruthi Nanam, [2]T Keerthi, [3]L Teja Sree, [4]K Kusuma Latha

[1]UG Student, [2]UG Student, [3]UG Student, [4]Asst. Professor Department of Electronics and Computers
SREE NIDHI INSTITUTE OF SCIENCE AND TECHNOLOGY, HYDERABAD, INDIA

Abstract: The main goal of our project is to guarantee the safe transmission of data. To accomplish this, we have developed a solution that utilizes Hybrid Cryptography. When a sender wants to send crime data to a receiver, the data is first encrypted using symmetric encryption and a symmetric key. Normally, the receiver would receive the symmetric key and use it to decrypt the data. However, our approach adds an additional layer of security by encrypting the symmetric key using asymmetric encryption. Both the encrypted symmetric key and encrypted crime data are then sent to the receiver. The receiver, who has the private key, can then decrypt the encrypted symmetric key and use it to decrypt the encrypted crime data. This ensures that the crime data is securely transmitted to the receiver.

This approach combines the strengths of both symmetric and asymmetric encryption to provide a robust and secure solution for transmitting sensitive data. By encrypting both the crime data and the symmetric key used to encrypt it, we add an additional layer of protection against potential security threats. This ensures that even if an unauthorized party intercepts the transmission, they would not be able to access the sensitive crime data without also possessing the private key.

Overall, our solution provides a comprehensive and secure approach to transmitting sensitive crime data, ensuring that it reaches its intended recipient safely and securely.

***Keywords**: Hybrid Cryptography, Symmetric Encryption, Asymmetric Encryption, Symmetric Key, Private Key, Data Security.*

1. INTRODUCTION

In law enforcement agencies and various governmental organizations, highly confidential data pertaining to criminals, such as their background, records, prison details, and information about the officers involved, is securely stored in cloud systems. However, when transferring this sensitive information between departments for official purposes, unauthorized entry or tampering by people helping the criminals is a possibility. To address this security concern, we propose implementing a Hybrid Cryptography solution. Using methods of cryptography is one of the most crucial ways to protect cloud data [11]. This approach combines the strengths of multiple cryptographic methods, enhancing the protection of sensitive data during transmission between departments. By employing Hybrid Cryptography, law enforcement and government organizations can ensure the integrity and confidentiality of their critical information, safeguarding it from potential cyber threats and data breaches. Safeguarding data privacy and confidentiality in remote storage locations presents significant challenges due to the inherent complexities of maintaining user information securely [9].

The nature of cloud storage services makes them insecure. There is an inherent risk of (a) data exposure (*confidentiality*), (b) data manipulation (*integrity*) and (c) denial of access to data (*availability*). [4] Cloud storage has become increasingly popular among individuals and businesses for its enhanced protection and scalability features [5].

2. LITERATURE SURVEY

Cloud technology is employed across diverse sectors, including industry, military, and academia, to provide a range of services and store vast quantities of data [8]. Cloud computing offers numerous benefits, including cost-efficiency and easy access to knowledge via the internet. However, securing cloud computing is crucial, as users often entrust sensitive data to potentially untrusted storage providers in the cloud environment [10]. Users can access this data on-demand. However, securing data in the cloud presents numerous challenges, and several methods have been developed to address them. Popular methods for strengthening data security include steganography and cryptography.

In the realm of cloud computing, the primary concerns revolve around maintaining confidentiality and ensuring the integrity of information stored in cloud-based data repositories. These threats arise due to the inherent nature of the cloud environment, which allows for the storage and processing of vast amounts of data across distributed systems. As a result, safeguarding sensitive information and preserving the accuracy and consistency of this data becomes a critical aspect of cloud-based solutions. Addressing these challenges requires the implementation of robust security measures and data management practices to minimize potential risks and vulnerabilities associated with cloud storage systems. [5]

Cloud computing, as an advanced technology, is classified according to the diverse range of services it offers. These services, designed to address varying requirements and preferences, enable users to fully harness the potential of cloud-based solutions. By ensuring a comprehensive understanding of these categories, organizations and individuals can efficiently utilize the appropriate services to meet their specific needs, ultimately leading to a more streamlined and effective approach to computing.[15]

Cryptography fundamentally operates on mathematical principles that form the foundation for developing various algorithms, commonly referred to as cryptographic algorithms. These algorithms play a crucial role in securing communication and ensuring the privacy of sensitive information. By leveraging complex mathematical concepts and techniques, cryptographic algorithms create robust encryption and decryption methods, which safeguard data from unauthorized access and tampering. As a result, cryptography has become an essential component in the field of information security, providing a reliable means of protecting data in diverse applications and industries.[13]

Encryption methods are widely regarded as highly effective approaches for ensuring data security. They function by encoding information in a manner that makes it virtually impossible to access or decipher without the appropriate decryption key.[16]

Preserving user data privacy and confidentiality becomes a significant challenge when storing and maintaining information at remote locations. This issue arises due to the inherent complexities associated with securing sensitive data in offsite storage facilities. As a result, it is crucial to implement advanced security measures and protocols to guarantee the protection of user data from unauthorized access, breaches, and potential vulnerabilities. By addressing these concerns proactively, remote storage solutions can continue to provide users with a reliable and secure environment for their data management needs.[9]

Since cloud computing has become an integral aspect of daily life, spanning various sectors such as healthcare, finance, real estate, and defense, researchers have shown a growing interest in enhancing data security within cloud computing. This includes exploring encryption methods and strategies to accelerate the encryption process.[11]

Encryption algorithms utilize a designated parameter or key for data transformation [14]. To encrypt or decrypt text, an encryption algorithm and key are needed together. Even though a key may appear meaningful, as with a character string used as a password, its usefulness lies in the fact that it is a string of bits that defines how plain text is mapped to cipher text [6].

Regarding security, individuals and organizations utilizing cloud services often lack direct control or influence over the server infrastructure employed. This infrastructure, managed by third-party cloud service providers, may introduce potential security concerns or challenges for users who must rely on the provider's security measures and protocols to safeguard their data and applications. Consequently, it is crucial for cloud users to thoroughly evaluate and understand the security policies and practices of their chosen cloud service providers in order to mitigate potential risks and ensure the protection of their valuable assets[4] . The Data Encryption Standard (DES) and RSA are used to enable various levels of encryption and decryption at both the source and recipient sides of communications in order to increase the security of cloud storage. [7].

Each method has a 128-bit key size, and the system can additionally use AES, Blowfish, RC6, and BRA to offer block-wise data security. The file section, encryption algorithm, and key are all secured using the LSB steganography technique. It splits the file into eight pieces. The file is encrypted using a new technique for each section. The multithreading approach is used to simultaneously encrypt every component of a file[1]. In the file security paradigm, the idea of a hybrid encryption technique is used to satisfy security requirements. Files are encrypted and decoded on cloud servers using blowfish and a modified version of RSA. It is also looked at in a cloud environment [2].

A novel online transaction security protocol can be developed by integrating symmetric and asymmetric cryptographic methods. Elliptic Curve Cryptography (ECC), the Dual-RSA method respectively, to achieve the three key properties of this protocol: integrity, confidentiality, and authentication. [3].The RSA decryption process utilizes the Chinese Remainder Theorem (CRT) by performing calculations in p and q, and then combining the results to obtain the solution in ZN.

This approach reduces computational expenses in two ways:

1. Zp and Zq operations go more smoothly due to smaller element sizes compared to ZN.
2. According to Lagrange's Theorem, when d exceeds prime integers, it is possible to substitute the private exponent d with dp = d mod (p - 1) in Zp and dq = d mod (q - 1) in Zq. This substitution effectively minimizes the computational expense of power operation. These exponents are commonly used terms. [12]

3. EXISTING METHODOLOGY

Maintaining the confidentiality and security of crime records is crucial for police departments, as these records hold sensitive information. Presently, cloud databases store these records, making them vulnerable to breaches, hacking, and tampering during data transfers between departments.

Such security compromises can have serious consequences, including enabling criminals to attack transport vehicles, manipulate evidence, and potentially be released back into society, posing a threat to public safety.

To address these concerns and safeguard our communities, we recommend designing and implementing a secure system employing hybrid cryptography for data transfer. This cutting-edge security approach would utilize multiple cryptographic algorithms, offering enhanced protection against potential risks.

The implementation of a hybrid cryptography system is crucial for maintaining the security of crime records in policedepartments. This advanced system aims to:

- Preserve the integrity of crime records
- Deter unauthorized access
- Reduce the risk of data breaches

By achieving these goals, the system ensures that evidence presented in court is accurate, promoting the conviction of criminals and preserving public safety. In summary, adopting a secure hybrid cryptography system is vital for protecting sensitive crime data, preventing evidence tampering, and fostering a safer, more just society for all.

1. Obtain input from a text file.
2. Utilize cryptographic algorithms, such as Data Encryption Standard (DES) and Rivest-Shamir-Adleman (RSA), to encrypt the input text.
3. Throughout this encryption process, the original input text is transformed into a cipher text, ensuring secure communication through cryptography. This cipher text conceals the original information, rendering it unreadable without the appropriate decryption keys. Utilizing both symmetric and asymmetric encryption methods, the process provides an additional layer of security for the transmitted data.

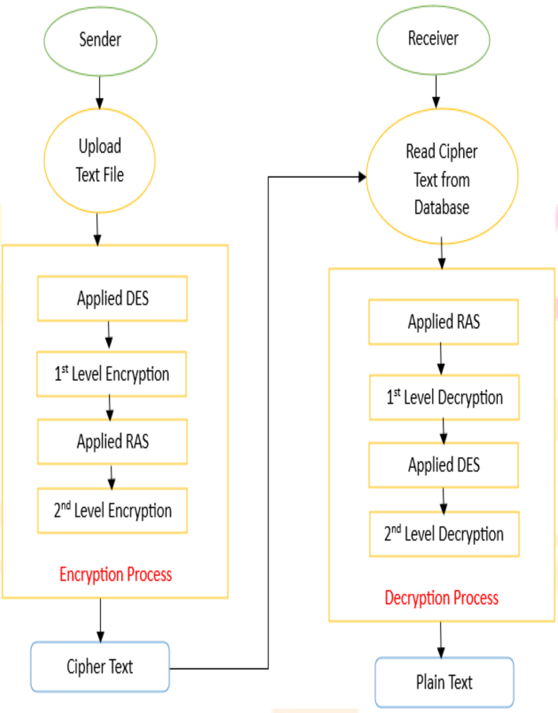


Fig (3) Flow chart depicting the existing methodology

4. PROPOSED SYSTEM

4.1 Overview

The process of secure communication begins with the utilization of symmetric encryption, specifically employing the Data Encryption Standard (DES) algorithm. This technique is used to guarantee the message's confidentiality as it is transmitted. The symmetric key, which is essential for the successful decryption of the message, is then encrypted using an asymmetric encryption technique known as the Rivest-Shamir-Adleman (RSA) algorithm. This step is crucial to safeguard the symmetric key from unauthorized access.

Afterward, the designated receiver of the communication offers their unique public key, which serves a crucial purpose in encoding the symmetric key. This vital step ensures that exclusive access to decrypt the symmetric key is granted only to the intended receiver, thereby upholding the security and credibility of the entire communication process. Once this phase is complete, both the ciphered message and the encoded symmetric key are conveyed securely to the receiving party. By implementing such a robust system, the integrity of sensitive information is protected, and unauthorized access is effectively prevented.

Upon acquiring the encoded correspondence, the receiver utilizes their confidential private key to decipher the encrypted symmetric key through the implementation of the RSA algorithm. This crucial procedure enables the recipient to access the unaltered symmetric key, which plays a significant role in decoding the transmitted data. After successfully decrypting the symmetric key, the receiver can move forward with the decryption process for the encoded message by employing the DES algorithm.

This multi-layered approach to secure communication not only strengthens the protection of sensitive information but also ensures that the intended recipient alone can access the content. The employment of the RSA and DES algorithms together creates a strong framework for preserving the secrecy and accuracy of the transmitted data, eventually protecting it against unauthorized access and potential manipulation.

As a result of this layered encryption process, the recipient gains access to the original message, ensuring the confidentiality, integrity, and authenticity of the communication. This method effectively mitigates the risk of unauthorized access to sensitive information and promotes secure information exchange between parties.

4.2 Proposed Methodology

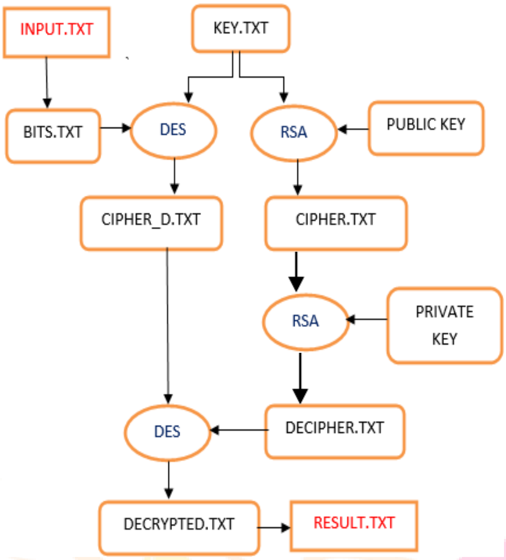
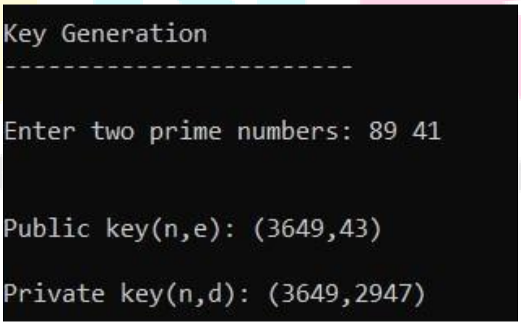


Fig (4.2) Flowchart depicting the proposed methodology.

4.3 Working of proposed system

1. The system initially obtains input text from the user and proceeds to convert this text into a binary format, represented as aseries of bits.
2. Following the conversion, the bit sequence undergoes a transformation into cipher text utilizing the Data Encryption Standard (DES) algorithm.
3. To commence the key generation process, the user is prompted to provide two distinct numerical inputs.
4. Within the context of hybrid cryptography, the encryption and decryption processes are facilitated through the generation oftwo separate keys: a public key and a private key.
5. The Rivest-Shamir-Adleman (RSA) algorithm is employed to perform the encryption and decryption tasks, leveraging the generated keys.
6. In particular, the private key is saved for decryption operations while the public key is reserved for encryption objectives. This approach ensures a secure and efficient means of managing sensitive information within the hybrid cryptography framework.
7. Ultimately, the input data is securely transferred into the resultant file, safeguarded from unauthorized access or intrusion. This is achieved through the meticulous implementation of the hybrid cryptography framework, ensuring the reliable and confidential management of sensitive information throughout the process.

5. RESULTS



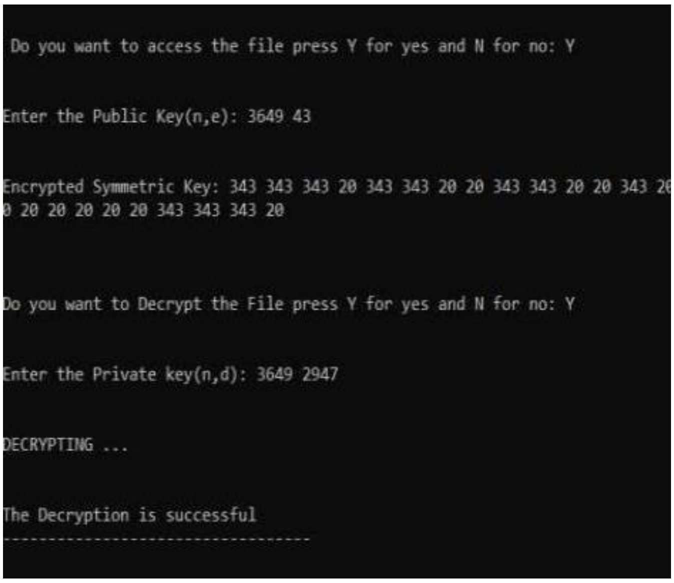
```
Key Generation
------------------------

Enter two prime numbers: 89 41


Public key(n,e): (3649,43)

Private key(n,d): (3649,2947)
```

Fig (5.1) Image showing the public and private key generation with the help of input prime numbers



```
 Do you want to access the file press Y for yes and N for no: Y


Enter the Public Key(n,e): 3649 43


Encrypted Symmetric Key: 343 343 343 20 343 343 20 20 343 343 20 20 343 2
0 20 20 20 20 20 343 343 343 20



Do you want to Decrypt the File press Y for yes and N for no: Y


Enter the Private key(n,d): 3649 2947


DECRYPTING ...


The Decryption is successful
----------------------------------
```

Fig (5.2) Image showing the encryption and decryption of the input text file

6. CONCLUSION

Utilizing a hybrid cryptographic approach, we can significantly enhance the security and protection of sensitive information. Instead of relying entirely on one technique, this is accomplished by integrating the advantages of both asymmetric and symmetric encryption. The suggested blended approach separates the plaintext and employs two different strategies to thwart possible attackers.

Firstly, the protocol harnesses the power of both symmetric and asymmetric cryptographic methods by employing the Data Encryption Standard (DES) and RSA algorithms. This dual approach increases the robustness of the encryption process and makes it more challenging for potential attackers to compromise the data. Secondly, the use of a combination of algorithms provides a higher degree of security, as it is more resilient to potential attacks. This is particularly advantageous when compared to existing security protocols, as it offers superior protection with reduced encryption and decryption times, as well as a smaller cipher text size. As a result, hybrid protocol minimizes processing overhead and achieves lower memory consumption, making it suitable for a wide range of applications.

In summary, the hybrid cryptographic protocol offers a more secure and efficient solution for safeguarding sensitive information. It offers a strong defence against prospective attackers while minimising processing overhead and consumption by combining the benefits of symmetric and asymmetric cryptography. This innovative approach sets a new standard for data protection and ensures that critical information remains secure across various applications.

7. FUTURE SCOPE

As technology continues to advance, the storage of sensitive data becomes increasingly important, especially when it comes to crime data. The need for secure and confidential storage systems has led to the emergence of cryptography-based security systems. These systems use encryption techniques to transform data into a format that is unreadable by unauthorized parties. The future scope for crime data storage using cryptography-based security systems is vast, as advancements in technology continue to provide new opportunities for enhancing security and privacy.

Quantum cryptography exploits the characteristics of quantum mechanics to generate secret keys, making it hard to intercept or tamper with data. In contrast to classical cryptography, which depends on mathematical procedures.

Another future scope for crime data storage using cryptography-based security systems is the use of blockchain technology Blockchain represents a distributed ledger system designed to chronicle transactions securely and with complete transparency. By employing this cutting-edge technology in the realm of crime data storage, records can be safeguarded against tampering and unauthorized access. The decentralized nature of blockchain ensures that the stored data remains both secure and verifiable, thereby significantly reducing the risk of manipulation or corruption. Consequently, this advanced method of data storage serves as an invaluable tool in maintaining the integrity and reliability of crime-related information. Additionally, blockchain provides a transparent record of all activities related to the data, making it easier to track any attempts at unauthorized access or manipulation.

The use of artificial intelligence (AI) and machine learning (ML) algorithms in cryptography-based security systems for crime data storage has the potential to greatly enhance their capabilities. These technologies can be used to analyze crime data and identify patterns and anomalies, allowing law enforcement agencies to detect and prevent criminal activities more effectively. Additionally, AI and ML algorithms can be used to improve encryption algorithms, making them more secure and robust. This can help to ensure that sensitive crime data is protected from unauthorized access. By leveraging the power of AI and ML, cryptography-based security systems for crime data storage can become even more effective in the fight against crime.

The future of crime data storage using cryptography-based security systems is promising. By integrating multiple encryption techniques, such as symmetric-key encryption, public-key encryption, and hash functions, a hybrid encryption system can be created. This type of system provides a more robust and secure way to store crime data than using any single encryption technique alone. By combining the strengths of different encryption methods, a hybrid system can provide enhanced security and protection against potential threats.

8. REFERENCES

[1] Maitri, P. V., & Verma, A. (2016, March). Secure file storage in cloud computing using hybrid cryptography algorithm. In *2016 international conference on wireless communications, signal processing and networking (WiSPNET)* (pp. 1635-1638). IEEE.

[2] Swarna, C., & Eastaff, M. S. (2018). Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm. *Iaetsd Journal for Advanced Research in Applied Science*.

[3] Subasree, S., & Sakthivel, N. K. (2010). Design of a new security protocol using hybrid cryptography algorithms. *IJRRAS*, *2*(2), 95-103.

[4] Nepal, S., Friedrich, C., Henry, L., & Chen, S. (2011, December). A secure storage service in the hybrid cloud. In *2011 Fourth IEEE International Conference on Utility and Cloud Computing* (pp. 334-335). IEEE.

[5] Mata, F., Kimwele, M., & Okeyo, G. (2017). Enhanced secure data storage in cloud computing using hybrid cryptographic techniques (AES and Blowfish). *Int. J. Sci. Res*, *6*(3), 1702-1708.

[6] Stallings, W. (2006). Cryptography and network security, 4/E. Pearson Education India.

[7] Kumar, S., Karnani, G., Gaur, M. S., & Mishra, A. (2021, April). Cloud security using hybrid cryptography algorithms. In *2021 2nd international conference on intelligent engineering and management (ICIEM)* (pp. 599-604). IEEE.

[8] Kumar, U., & Prakash, J. (2020). Secure File Storage on Cloud Using Hybrid Cryptography Algorithm. International Journal of Creative Research Thoughts, 8(7), 334-340.

[9] El-Attar, N. E., El-Morshedy, D. S., & Awad, W. A. (2021). A New Hybrid Automated Security Framework to Cloud Storage System. *Cryptography*, *5*(4), 37.

[10] Jogar, S., & Handral, D. S. (2022). Secure File Storage on Cloud Using Hybrid Cryptography. International Journal of Advanced Research in Science, Communication and Technology, 2(2), 540. https://doi.org/10.48175/IJARSCT-5861

[11] Bermani, A. K., Murshedi, T. A., & Abod, Z. A. (2021). A hybrid cryptography technique for data storage on cloud computing. *Journal of Discrete Mathematical Sciences and Cryptography*, *24*(6), 1613-1624.

[12] Dubai, M. J., Mahesh, T. R., & Ghosh, P. A. (2011, April). Design of new security algorithm: Using hybrid Cryptography architecture. In *2011 3rd International Conference on Electronics Computer Technology* (Vol. 5, pp. 99-101). IEEE.

[13] Gupta, R. K., & Singh, P. (2013). A new way to design and implementation of hybrid crypto system for security of the information in public network. *International Journal of Emerging Technology and Advanced Engineering*, *3*(8), 108-115.

[14] Abbas, M. S., Mahdi, S. S., & Hussien, S. A. (2020, April). Security improvement of cloud data using hybrid cryptography and steganography. In *2020 international conference on computer science and software engineering (CSASE)* (pp. 123-127). IEEE.

[15] Chinnasamy, P., & Deepalakshmi, P. (2018, April). Design of secure storage for health-care cloud using hybrid cryptography. In *2018 second international conference on inventive communication and computational technologies (ICICCT)* (pp. 1717-1720). IEEE.

[16] Orobosade, A., Aderonke, T., Boniface, A., & Gabriel, A. J. (2020). Cloud application security using hybrid encryption. *Communications*, *7*, 25-31.