IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305546 |

Multi-Layer Protection in Cloud using Hybrid Cryptography

Mrs. D. Supriya, S. Sai Lokesh Reddy, R. Sai Raghu Ram, V. Pallavi, P. Gourav Deepu

Assistant Professor, Department of Cyber Security, Malla Reddy University, Hyderabad, Telangana, India

Department of Cyber Security, Malla Reddy University, Hyderabad, Telangana, India

ABSTRACT: The suggested model shows great potential in meeting the critical security needs of cloud data centers. It uses AES, DES, and RSA encryption methods to protect file segments effectively, offering rapid encryption and decryption times when compared to other symmetric algorithms. At the heart of the model's success is its use of data splitting and merging, enhancing conventional security measures by breaking data into smaller, more manageable pieces. This method not only improves data durability but also greatly increases the difficulty of unauthorized access, thus adhering closely to the fundamental principles of data security. The adoption of this hybrid approach in cloud environments strengthens the security of remote servers, increasing users' confidence in cloud service providers. This tactic tackles the essential issue of protecting sensitive information and managing access rights, leading to enhanced data security and privacy. Cryptography converts original information into a format that is unreadable, preserving its confidentiality. It includes two primary types: symmetric key cryptography and public key cryptography, utilizing keys to convert data into a secure format. Thus, only authorized individuals can retrieve data from the cloud server. The encrypted data, or ciphertext, remains visible to all owners and users.

KEYWORDS: Owner, Cryptography, User, Data Security, Cloud, Hybrid Approach

I. INTRODUCTION

Distributed computing has evolved from the basics of large-scale distributed processing technologies. As defined by the National Institute of Standards and Technology (NIST), cloud computing is described as a model that allows for straightforward, on-demand access to a shared pool of configurable computing resources (such as networks, storage, applications, and services). These resources can be quickly allocated and released with little management effort or service provider interaction.

In cloud computing, neither the data nor the software are entirely contained on the user's local computer. This decentralized architecture raises concerns about file security because both the user's applications and programs reside on the cloud provider's premises. This setup introduces potential vulnerabilities as sensitive data may traverse networks and systems beyond the user's direct control.

To mitigate these security risks, cloud providers often employ encryption algorithms to safeguard files stored within their infrastructure. Encryption involves converting plaintext data into ciphertext using cryptographic keys, rendering it unintelligible to unauthorized users. By encrypting files, cloud providers add an additional layer of protection to sensitive data, even if unauthorized parties gain access to the underlying infrastructure.

Encryption methods like AES (Advanced Encryption Standard), DES (Data Encryption Standard), and RSA (Rivest-Shamir-Adleman) are widely used in cloud computing environments to encrypt files. These techniques leverage complex mathematical formulas to provide strong security and data confidentiality. Through the use of encryption, cloud service providers can address concerns about file security and assure users regarding the protection of their data in the cloud. It is crucial for both providers and users to diligently handle encryption keys and access controls to preserve file integrity and confidentiality throughout their lifecycle in the cloud. Furthermore, continuous improvements in encryption technologies and security protocols are essential for consistently enhancing file security within cloud computing environments.

II. LITERATURE SURVEY

This paper introduces a novel document security model aimed at tackling the complex security challenges inherent in cloud environments. Utilizing a hybrid encryption strategy, it combines Blowfish encryption for file security with a

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305546 |

Secure Remote Neural Network (SRNN), a modified version of RSA, to ensure secure communication between users and servers. Within cloud platforms, traditional security mechanisms struggle due to their inability to adapt to the dynamic nature of these environments. Issues such as dynamic scalability, transparency, and multi-tenancy pose significant hurdles, making it difficult to establish fixed security boundaries and identify vulnerable resources. Moreover, the involvement of multiple service providers further complicates matters, as conflicts of interest hinder the implementation of unified security measures. Additionally, the shared, virtualized nature of cloud resources introduces risks related to data confidentiality and privacy, as user data may be accessed by unauthorized parties. To address these challenges effectively, innovative security models are imperative, capable of adapting to the dynamic nature of cloud environments while ensuring robust protection for both data and communication channels.

III. METHODOLOGY

To bolster file security in the cloud, a hybrid cryptosystem is in use. This system operates under the assumption that the remote server is trustworthy, allowing it to encrypt files which are then stored on the server itself. The hybrid cryptosystem employs both the Blowfish Algorithm and a File Splitting and Merging mechanism. Known for its efficiency and effectiveness, the Blowfish Algorithm is a symmetric-key block cipher that encrypts and decrypts data in blocks using a secret key. In this setup, it encrypts files before they are stored on the remote server. The use of symmetric-key encryption streamlines the process and ensures that only authorized individuals with the key can access the files.

The File Splitting and Merging mechanism works by dividing files into smaller parts, or slices, which are then encrypted separately using the Blowfish Algorithm. This division enhances security by making it difficult for unauthorized users to access a complete file. Moreover, the merging mechanism enables the reassembly of these encrypted slices back into the original file when needed. Combining the Blowfish Algorithm with the File Splitting and Merging mechanism provides a comprehensive security solution for files in the cloud. This system ensures that files are safeguarded against unauthorized access and adds an additional security layer by complicating attempts to compromise the entire file. Furthermore, with encryption handled by a trusted remote server, users can feel secure about the safety of their data stored in the cloud.

3.1 Proposed System

The stored image file is completely secured, as the file is being encrypted not by just using one but three encryption algorithm which is AES, DES and RC6. The proposed system represents a significant advancement in the realm of cloud data security, offering a comprehensive and effective solution for protecting sensitive information in cloud environments. By leveraging advanced encryption techniques, file fragmentation, robust key management, compatibility, usability, and stringent security measures, the system empowers users to safeguard their data assets against evolving threats and vulnerabilities. As the digital landscape continues to evolve, the importance of robust security measures cannot be overstated, and the proposed system stands as a testament to the commitment to protecting data integrity, confidentiality, and availability in the cloud. Data is kept secured on cloud server which avoids unauthorized access.

3.2 Encoding and Decoding

Encoding involves the transformation of original data, such as file slices, into an illegible format using encryption algorithms like AES, DES, and RSA. This encryption ensures data security by rendering it incomprehensible to unauthorized users.

Decoding, conversely, entails the reversal of this process, where encrypted data (known as ciphertext) is converted back into its original, readable format through decryption. Authorized users can securely access and utilize the data through this process. The decryption process is facilitated by the user, who possesses the decryption keys provided via email.

3.3 JDBC

Java Database Connectivity (JDBC) serves as the JavaSoft-defined standard application programming interface (API) enabling Java applications to interact with database management systems. This JDBC API encompasses a collection of interfaces and classes coded in the Java programming language. By leveraging these standardized elements, developers can create applications capable of establishing connections with databases, executing queries written in Structured Query Language (SQL), and handling the returned results. Notably, owing to its standardized nature, any Java program utilizing the JDBC API can establish connections with various database management systems (DBMS), provided a compatible driver exists for the targeted DBMS.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305546 |

3.4 Blow fish algorithm along with Splitting and Merging :

The hybrid cryptosystem utilizes a combination of the Blowfish Algorithm along with a File Splitting and Merging mechanism. The Blowfish Algorithm is a symmetric-key block cipher known for its speed and effectiveness in encryption. It operates on blocks of data and employs a secret key to encrypt and decrypt information. In this hybrid cryptosystem, the Blowfish Algorithm is utilized to encrypt files before storage on the remote server. By using symmetric-key encryption, the process is efficient and ensures that only authorized parties with the encryption key can access the files. File Splitting and Merging mechanism involves dividing files into smaller segments, or slices, before encryption. These slices are then individually encrypted using the Blowfish Algorithm. By splitting files into smaller parts, security is enhanced as it becomes more challenging for unauthorized users to access the complete file.

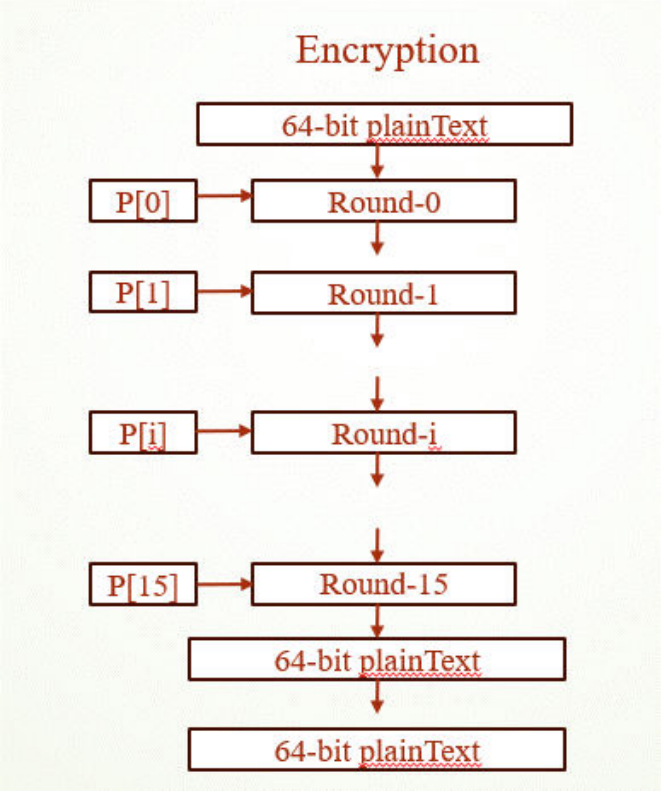


Fig 3.4.1: Blow Fish Algorithm

IV. IMPLEMENTATION

4.1 Project Architecture

The architecture of our project consists of three layers i.e,
1) User Interface layer 2) Functional layer 3) Data Storage layer

1) **User Interface layer :** The user interface (UI) layer acts as a bridge between the user and the underlying system, enabling interaction and data exchange. Graphical elements include all aspects of presentation and interaction, including control and feedback mechanisms. Through design and usability, the UI layer tries to improve the user experience by providing clear instructions, useful instructions, and efficient operations. It encompasses the visual and interactive components of a software application to ensure that users can easily understand and interact with key functions, creating a seamless and engaging user experience.

2) **Functional layer :** The operating system is an important part of the software architecture and is responsible for certain functions such as encryption and decryption. During this process, encryption algorithms convert plaintext data into encrypted format so that without the decryption key the data becomes unintelligible. The decryption function reverses this process, converting the encrypted data to its original form. These capabilities are critical to ensuring data security and privacy in a variety of applications, including telecommunications, financial transactions, and data storage

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305546 |

solutions. By integrating encryption and decryption capabilities into operations, software systems can prevent unauthorized access to data and protect the integrity of data transmission.

3) **Data Storage layer :** The data storage layer acts as a storage location for encrypted content and information regarding the owners and users of the software system. It is responsible for securely storing encrypted messages, including user credentials, personal details, and private details. Encrypting data ensures confidentiality and integrity and reduces the risk of unauthorized access or interception. This system uses strong encryption techniques such as symmetric or asymmetric encryption algorithms, hash functions, and key processes to protect sensitive data. The data storage layer stores content encrypted at rest, ensuring that encrypted data is protected even if an unauthorized party accesses the stored data, thus protecting the privacy and security of owner and user data.

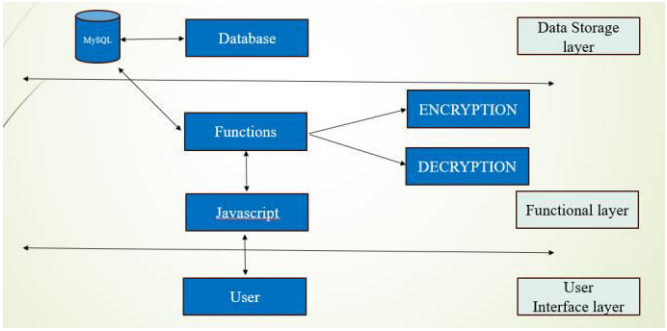


Fig 4.1.1: Project Architecture

4.2 Sequence Flow

1) In order to upload the files, one need to register into it.
2) After registering, one need to login into it with the given credentials.
3) After successful login, upload the files which owner want to upload.
4) Admin/Owner need to split the uploaded file in order to encrypt the file splits.
5) At view files, we can see the three different regarding three encryptions.
6) Check if any user is requesting for the files or not.
7) If there is any request, Owner can send the file to the users.

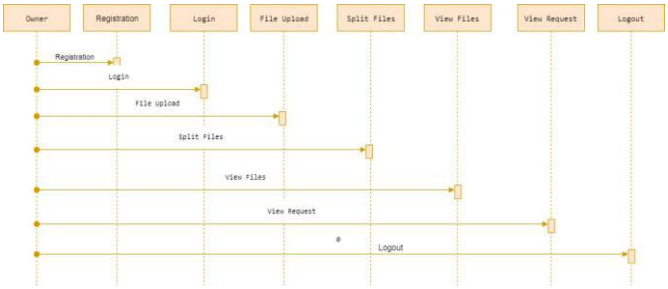


Fig 4.2.1: Sequence Flow (Owner/Admin)

1) In order to get the files from the owner, user need to register into it.
2) After registering, user need to login into it with the given credentials.
3) After successful login, user can view the files which the owner uploads into it.
4) If user want that particular file, user can send the request to that owner.
5) After accepting user's request user can get the decrypting keys through the mail.
6) User need to use that keys to get the actual file, user can also download the file.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305546 |

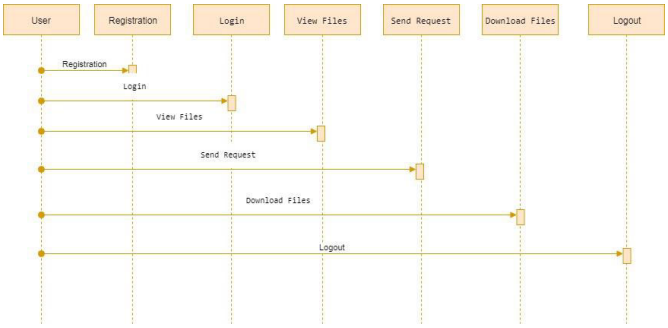
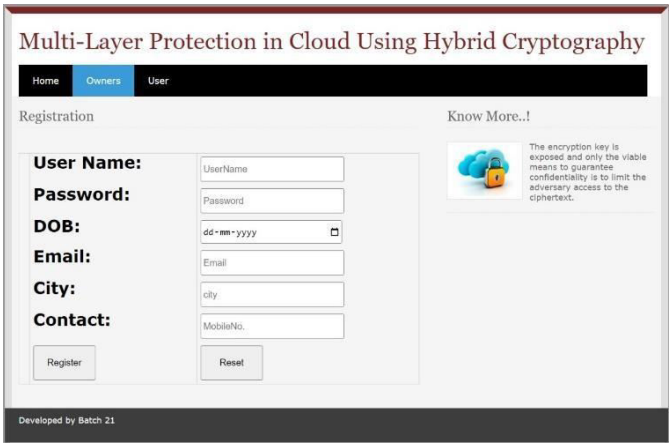


Fig 4.2.2: Sequence Flow (User)

V. RESULTS

5.1 OWNER



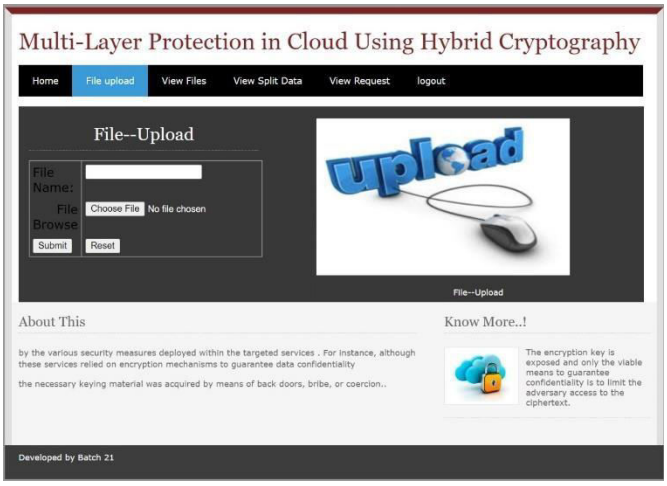
5.1.1 Owner Registration

5.1.2 Owner Login Page

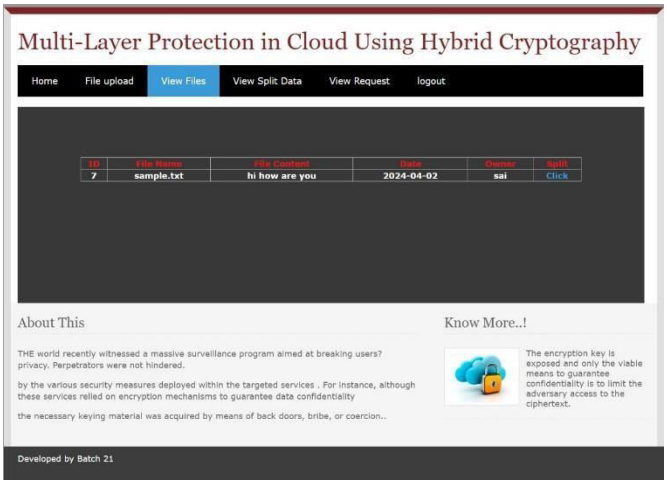
|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305546 |



5.1.3 File Upload Page



5.1.4 View Files

5.1.5 Split Files

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305546 |

5.2 USER

5.2.3 Verify Page (Download)

VI. CONCLUSION

The primary objective is to ensure secure data storage and access in the cloud, particularly in scenarios where the data owner lacks direct control. We leverage elliptic curve cryptography (ECC) encryption techniques to safeguard data files stored in the cloud. Enhancements to the cloud server architecture facilitate improved performance for both storing and accessing data. The utilization of ECC encryption algorithms further enhances performance during encryption and

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305546 |

decryption processes. This approach is presumed to offer heightened security and superior performance compared to traditional methods. Ongoing efforts are directed towards addressing the challenge of group data sharing within the shared data section, where only group members have access. Currently, limitations exist regarding one-to-many, many-to-one, and many-to-many communications within this scheme, which we are actively working to resolve.

REFERENCES

[1] Peter Mel and Tim Grace, "The NIST Definition of Cloud Computing", NIST, 2010.
[2]Achill Buhl, "Rising Security Challenges in Cloud Computing", in Proc. of World Congress on Information and correspondence Technologies ,pp. 217-222, Dec. 2011.
[3]B Yamini, K Sudha, M Nalini, G Kavitha, R Siva Subramanian, R Sugumar, Predictive Modelling for Lung Cancer Detection using Machine Learning Techniques, 2023 8th International Conference on Communication and Electronics Systems (ICCES), pp.1220-1226.
[4]Srinivasarao D et al., "Breaking down the Superlative symmetric Cryptosystem Encryption Algorithm", Journal of Global Research in Computer Science, vol. 7, Jul. 2011
[5] Tingyuan Nye and Tang Zhang "An investigation of DES and Blowfish encryption algorithm" , in Proc. IEEE Region 10 Conference, pp. 1-4 ,Jan. 2009.
[6] Jitendra Singh Adam et al.," Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering ,vol. 2,Aug. 2012.
[7]R.Udayakumar, A. Joshi, S.S. Boomiga, R. Sugumar, Deep Fraud Net: A Deep Learning Approach for Cyber Security and Financial Fraud Detection and Classification, Volume 13, Issue 4, November 2023, pp. 138-157.
[8] Manikandan.G et al., "A changed cryptographic plan improving information", Journal of Theoretical and Applied Information Technology, vol. 35, no.2, Jan. 2012.
[9] Niles Maintain and Subhead Bhingarkar, " The examination and Judgment of Nimbus, Open Nebula and Eucalyptus", International Journal of Computational Biology , vol. 3, issue 1, pp 44-47, 2012.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details