e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 6, Issue 12, December 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.54

International Journal Of Multidisciplinary Research In Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 12, December 2023 |

| DOI:10.15680/IJMRSET.2023.0612024 |

CLOUD HYBRID CRYPTOGRAPHY

Vidya S Godbole[1], Santosh Ajitrao Korde[2]

Department of Computer Technology, Y.B.Patil Polytechnic, Akurdi, Pune, India

ABSTRACT: Cloud Computing has played a vital part in the field of computing. It has revolutionized how computing is used in the assiduity from first setting up the structure and also using it to just spinning up the coffers as demanded from different pallvendors.It's also used in different diligence for colorful services and storehouse of data. The data stored on the pall can be recaptured as per the stoner's request but the concern of numerous druggies is the security of theirdata.In this proposed system AES and Blowfish algorithms are used to give security. Then the encryption is divided into three corridor. Each part is translated with different encryption algorithms and deciphered using the different keys when needed. This system of encryption and decryption guarantees better security of data to the druggies by storing translated data on a single pall garçon, using 3DES and Blowfish.

KEYWORDS: Blowfish,3DES, AES, encryption

I. INTRODUCTION

The end of this design is to develop and apply advanced pall ways like p- hash to automatically identify and exclude Duplicate image on the Cloud from multiple source like Organization and particular use. The primary thing is to exclude the indistinguishable images for large storehouse and effectiveness and enhance online safety and cover druggies, particularly children and vulnerable individualities, from dangerous, unequivocal, or deceiving material. This design seeks to produce a more secure and responsible online terrain by furnishing content temperance tools that can be employed by content platforms, service providers, and druggies to insure a safer and further ethical onlineexperience.In pall computing, both lines and software aren't completely contained on the stoner's computer. train security enterprises arise because both stoner's operation and program are abiding in provider demesne. The pall provider can break this problem by cracking the lines by using encryptionalgorithm.Our design idea presents a train security model to give an effective result for the introductory problem of security in pall terrain. In this model, mongrel encryption is used where lines are translated by blowfish coupled with train splitting and AES is used for the secured communication between druggies and the waiters.

pall computing is began from earlier large- scale distributed calculating technology. NIST defines pall computing as a model for enabling accessible on demand network access to a participated pool of configurable computing coffers(like network, storehouse, operation and services) that can be snappily provisioned and released with minimum operation trouble or service provider commerce. In pall computing lines and software aren't completely contained on the stoner's operation and Program are abiding in provider demesne. The pall provider can break this problem by encryption the lines by using encryption algorithm. This paper presents a train security model to give an effective result for the introductory problem of security in pall terrain. In this model, mongrel encryption is used where lines are translated by train splitting and RSA is used for the secured communication between druggies and the waiters.

II. METHODOLOGY

1. The proposed software product is liable to meet the needed security requirements of data center of pall. Blowfish used for the encryption of train slices takes minimal time and has maximum outturn for encryption and decryption from other symmetric algorithms.
2. The idea of splitting and incorporating adds on to meet the principle of data security. The mongrel approach when stationed in pall terrain makes the remote garçon more secure and therefore, helps the pall providers to cost further trust of their druggies.
3. Data security issues

Due to openness andmulti-tenant characteristics of the pall, the traditional security mechanisms are no longer suitable for operation and data in pall. Some of the issues are as following Due to dynamic scalability, service and position translucency features of pall computing model, all kinds of operation and data of the pall platform have no fixed structure and security boundaries. In the event of security breach, it's delicate to insulate a particular resource that has been compromised. According to service delivery models of pall computing, coffers and pall services may be possessed

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 12, December 2023 |

| DOI:10.15680/IJMRSET.2023.0612024 |

by multiple providers. As there's a conflict of interest, it's delicate to emplace a unified security measure. Due to the openness of pall and sharing virtualized coffers by multitenant, stoner data may be penetrated by other unauthorized druggies.

4. Hybrid Cryptosystem Scheme:

Hybrid Cryptography concept is used for securing storage system of cloud. Two different approaches are used to show the difference between less secure and more secure systems. The first approach uses RSA and AES algorithms; RSA is used for key encryption and AES is used for text or data encryption. In the second or we can say more secured approach, AES and Blowfish algorithms are used. In this approach, these two algorithms provide double encryption over data and key which provides high security compared to the first one. I. In this proposed system three step procedures is used. Firstly, Diffie Hellman is used for exchanging keys. Thereafter authentication is performed using digital signature scheme. Finally, data is encrypted using AES and then uploaded to the required cloud system. For decryption reverse procedure is implemented. II. Combination of RSA algorithm and MD5 to assure various security measures such as confidentiality, data integrity, no repudiation etc. It uses RSA key generation algorithm for generation of encrypted key for encryption and decryption process. MD5 digest is used for accepting an input of length up to 128 bit and processing it and generating an output of padded length for encryption and decryption process. III. Implementation of Trusted Storage System using Encrypted File System (EFS) and NTFS file system drive with help of cache manager for securing data files. EFS encrypt stored files by automatically using cryptographic systems. The process takes place as follows, firstly application writes files to NTFS which in turn places in cache and return backs to NTFS. After this NTFS asks EFS to encrypt files and heads them towards the disk. IV. Cloud Storage Security Service is provided by using separate servers viz. User Input, Data Storage and User Output. Three different servers are used to ensure that failure of any of the servers doesn't harm the data. User Input server is used for storing user files and input data by providing user authentication and making sure the data is not accessed by any of the unauthorized means. Data storage server is the place where the encryption using AES is performed to secure user input and then the encrypted files are transferred to User Output server. User Output Server is the place from where user gets the output file or the decrypted file and uses it for further use.

Blowfish:

Blowfish is a symmetric block cipher which uses a Fiestal network, 16 rounds of iterative encryption and decryption functional design. The block size used is of 64-bits and key size can vary from any length to 448.Blowfish cipher uses 18 sub arrays each of 32-bit commonly known as P-boxes and four Substitution boxes each of 32-bit, each having 256 entries. The algorithm design is shown in figure. It consists of two phases: one is Key Expansion phase another is Data Encryption phase. In Key expansion phase, key is converted into several sub-keys and in Data Encryption phase, encryption occurs via 16-round networks. Each round consists of a key dependent permutation and a key and data dependent substitution.

Advanced Encryption Standard (AES) The AES algorithm is related to Rijndael`s encryption. Rijndael is a family of encryption algorithms with different keys and block sizes. It consists of a continue serial operations, some of them involve the input of certain outputs (substitutions) and others the mixing of bits (permutations). All AES calculations algorithm is executed in bytes instead of bits. Therefore, for Advanced Encryption Standard, 128 bits of plain data is considered as a block of 16 bytes These 16 bytes are arranged in a 4x4 matrix for the processing.

III. MODULE DESCRIPTION

In order to ensure file security on cloud, hybrid cryptosystem is being used. We assume that the remote server is trusted, so files are encrypted by server and finally encrypted files are stored at the server end. The hybrid cryptosystem uses a combination of:

- Blowfish Algorithm coupled with File Splitting and Merging mechanism
- AES Algorithm
    - SHA256

In a hybrid scheme, the performance of symmetric algorithm is integrated with security of asymmetric algorithm. The symmetric algorithm (Blowfish) used in hybrid cryptosystem has best practice to avoid data misuse when compared with other symmetric algorithms. Also, in terms of throughput, Blowfish has best performance.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 12, December 2023 |

| DOI:10.15680/IJMRSET.2023.0612024 |

IV. PROBLEM STATEMENT

The main aim of this system is to securely store and retrieve data on the cloud that is only controlled by the owner of the data. Cloud storage issues of data security which we can solve using cryptography and steganography techniques. Data security is achieved using Blowfish and AES algorithm

V. LITERATURE SURVEY

[1]. To make the centralised cloud storage secure ECC(Elliptic Curve Cryptography) algorithm is implemented. This approach uses single key for encryption and decryption and complete process takes place at the client side. This methodology performs steps such as: a.Authentication, b.Key generation operation, c.Encryption, d.Decryption.

[2]. In this proposed system three step procedure is used. Firstly, Diffie Hellman is used for exchanging keys. Thereafter authentication is performed using digital signature scheme. Finally data is encrypted using AES and then uploaded to the required cloud system. For decryption reverse procedure is implemented.

[3]. Combination of RSA algorithm and MD5 to assure various security measures such as confidentiality, data integrity, nonrepudiation etc. It uses RSA key generation algorithm for generation of encrypted key for encryption and decryption process. MD5 digest is used for accepting an input of length up to 128 bit and processing it and generating an output of padded length for encryption and decryption process.

[4]. Implementation of Trusted Storage System using Encrypted File System (EFS) and NTFS file system drive with help of cache manager for securing data files. EFS encrypts stored files by automatically using cryptographic systems. The process takes place as follows, firstly application writes files to NTFS which in turn places in cache and return backs to NTFS. After this NTFS asks EFS to encrypt files and heads them towards the disk.

[5]. Cloud Storage Security Service is provided by using separate servers viz. User Input, Data Storage and User Output. Three different servers are used to ensure that failure of any of the servers doesn't harm the data. User Input server is used for storing user files and input data by providing user authentication and making sure the data is not accessed by any of the unauthorized means. Data storage server is the place where the encryption using AES is performed to secure user input and then the encrypted files are transferred to User Output server. User Output Server is the place from where user gets the output file or the decrypted file and use it for further use.

VI. SYSTEM ARCHITECTURE

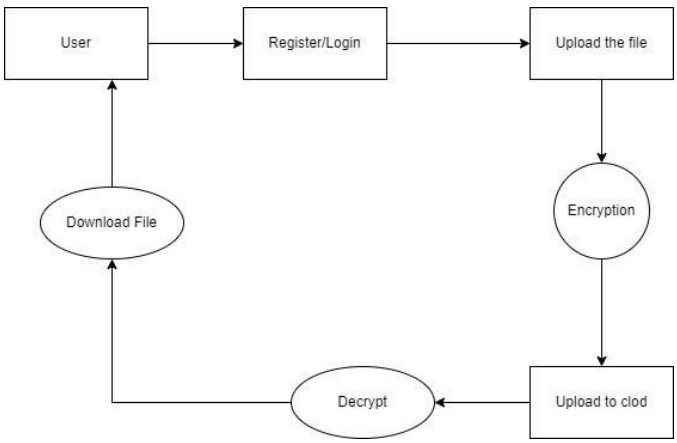

Fig 1. System Architecture

1. The user signs in if already registered, or signs up to register themselves by providing their details such as name, email id, phone number, password for account etc.
2. The user then selects the file that is to be uploaded by browsing from local storage.
3. The user then selects the encryption algorithm that they want to use. The proposed system provides the choice between using a combination of AES and RSA or AES and Blowfish.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly Peer Reviewed & Referred Journal |

| Volume 6, Issue 12, December 2023 |

| DOI:10.15680/IJMRSET.2023.0612024 |

4. The selected file gets uploaded after getting encrypted using the selected encryption algorithm combination.
5. The user also has the option of viewing the files that they have uploaded or have access to and downloading them.
6. On selecting a file to download it, the user is sent the decryption key on their email id that was entered on registration or sign-up.
7. Using this key, the user can download the decrypted or original file.
8. The system also provides a comparison with respect to security between the two hybrid encryption algorithm combinations AES and Blowfish combination.

VII. CONCLUSION

The users equipped with mobile phones or PDA's interact with the sensors through Wi-Fi.GPS is inadequate for indoor location positioning. Wi-Fi is a technique used for location tracking with wireless access points(AP's).

REFERENCES

[1] Kumar, A., Lee, B. G., Lee, H., & Kumari, A. (2012). Secure storage and access of data in cloud computing. 2012 International Conference on ICT Convergence (ICTC).
[2] Rewagad, P., & Pawar, Y. (2013). Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. 2013 International Conference on Communication Systems and Network Technologies.
[3] Ping, Z. L., Liang, S. Q., & Liang, L. X. (2011). RSA Encryption and Digital Signature. 2011 International Conference on Computational and Information Sciences.
[4] Sunita Sharma,Amit Chugh:'Suvey Paper on Cloud Storage Security'.
[5] Rawal, B. S., & Vivek, S. S. (2017). Secure Cloud Storage and File Sharing. 2017 IEEE International Conference on Smart Cloud (SmartCloud).
[6] 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.
[7] Srinivasarao D et al., "Breaking down the Superlative symmetric Cryptosystem Encryption Algorithm", Journal of Global Research in Computer Science, vol. 7, Jul. 2011
[8] Tingyuan Nye and Tang Zhang "An investigation of DES and Blowfish encryption algorithm", in Proc. IEEE Region 10 Conference, pp. 1-4 ,Jan. 2009.
[9] 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.
[10] Manikandan.G et al., "A changed cryptographic plan improving information", Journal of Theoretical and Applied Information Technology, vol. 35, no.2, Jan. 2012.
[11] 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

Impact Factor
7.54

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com