International Journal for Modern Trends in Science and Technology, 8(07): 11-17, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0807002
Available online at: http://www.ijmtst.com/vol8issue07.html

Hybrid Cryptography Approach for Providing Advanced Security on Cloud

Rajaram Jatothu[1] | Dharmapuri Vaishnavi[2] | Milin Manker[2] | Naralachetty Navitha[2] | Ragula Chakradhar[2]

[1]Professor, Dept of CSE,Teegala Krishna Reddy Engineering College,Hyderabad,Telangana,India.
[2]Dept of CSE,Teegala Krishna Reddy Engineering College,Hyderabad,Telangana,India.

To Cite this Article
Rajaram Jatothu, Dharmapuri Vaishnavi, Milin Manker, Naralachetty Navitha and Ragula Chakradhar. Hybrid Cryptography Approach for Providing Advanced Security on Cloud. International Journal for Modern Trends in Science and Technology 2022, 8(07), pp. 11-17. https://doi.org/10.46501/IJMTST0807002

Article Info
Received: 25 May 2022; Accepted: 24 June 2022; Published: 27 June 2022.

ABSTRACT

Cloud computing is used in many areas like industry, military, colleges etc., to store huge amounts of data. We can retrieve data from the cloud at the request of the user. To store data on the cloud, we have to face many issues. To give the solution to these problems, there are several number of ways. Cryptography is more popular nowadays for data security. The use of a one algorithm is not as effective for high-level security to information in cloud computing. In this paper, we are introducing a new security mechanism using a Symmetric key cryptography algorithm. We expect to safely store data into the cloud, by parting information into a few pieces and putting away pieces of it on the cloud in a way that jelly information privacy, respectability and guarantees accessibility. Sharing information securely while safeguarding information from an untrusted cloud is as yet a difficult issue. Our methodology guarantees the security and protection of customer touchy data by putting away information across a single cloud, utilizing AES, Triple DES and Blowfish algorithms using Hybrid Cryptography.

KEYWORDS : Hybrid, Blowfish, AES, Triple DES, Cryptography, Symmetric key, data security, privacy.

1. INTRODUCTION

Nowadays cloud computing is used in many areas like industry, military colleges etc. to store huge amounts of data. We can retrieve data from the cloud on request of the user. To store data on the cloud we have to face many issues. To provide the solution to these issues there are n number of ways. Cryptography is more popular nowadays for data security. Use of a single algorithm is not effective for high level security to data in cloud.computing. In this paper, we have introduced a new security mechanism using symmetric key cryptography algorithm. Cryptography method makes an interpretation of unique information into garbled structure. Cryptography method is separated intosymmetric key cryptography and public key cryptography. Thisprocedure utilizes keys for make an interpretation of information into muddled structure. So just approved individual can get to information from cloud worker. Symmetric key cryptography calculations are AES, DES, 3DES, IDEA, BRA and blowfish.Hybrid cryptography algorithm present by author A. Shaded. AES and RSA algorithms are used into hybrid algorithm. AES algorithm require a single key. In hybrid algorithm three keys are used. For data upload on cloud mandatory keys are AES secret key and RSA public key. Private Key of RSA and AES secret key are essential to

download data from cloud. Whenever user makes an effort to upload data on cloud first that file stored onto directory for short time. In encryption process first AES algorithm is applied on file after that RSA algorithm is applied on encrypted data. Reverse process is followed for decryption. After applying keys that file covert into encoded form and stored on cloud server. Advantages of hybrid algorithm are data integrity, security, confidentiality and availability. Disadvantage of RSA algorithm is large amount time essential for data encode and decode.In security model symmetric algorithm uses chunk level encryption and decryption of data in cloud computing. Key size is 256 bits. Key is rotated to achieve high level security. For data integrity purpose hash value is generated. Hash values are garneted after encryption and before decryption. If both hash values match than that data is in correct form. In this security model only, valid user can access data from cloud. Advantages of security model are integrity, security and confidentiality. Three algorithms are used for implementation of hybrid algorithm. User authentication purpose digital signature is used. Blowfish algorithm is used to produce high data confidentiality. It is symmetric algorithm. It uses single key. Blowfish algorithm need least amount of time for encode and decode. Sub key array concept is used into blowfish algorithm. It is block level encryption algorithm. The main aim of this hybrid algorithm is achieved high security to data for upload and download from cloud. Hybrid algorithm solves 2 the security, confidentiality and authentication issues of cloud.To reduce the complexity our application can considerably reduce the computational complexity while reducing the storage space. Our proposed system lays a foundation for future attribute-based secure data management and smart contract development Privilege-Based Access: Data is shared in a hierarchical manner based on user privileges. Data users with more privileges (ranked at the higher levels of the hierarchy) are granted access to more sensitive parts than those with fewer privileges (ranked at the lower levels of the hierarchy). Data Confidentiality: completely protected from unprivileged data users (including the storagespace).A Privilege-based Multilevel Organizational Data sharing scheme (P-MOD) that allows data to be shared efficiently and securely on the cloud. P-MOD partitions a data file into multiple segments based on user privileges and data sensitivity. Each segment of the data file is then shared depending on data user privileges. Fine-grained access control: The data owner has the capability to encrypt any part 3 using any set of descriptive attributes he/she wishes, limiting access to only authorized data users. The set of descriptive attributes is defined by the data owner at the time of encryption and can be selected from an infinite pool. Collusion resistant: Two or more data users at the same/different level cannot combine their private keys to gain access to any part of F they are not authorized to access independently.

This framework AES, RC6, Blowfish and BRA calculations are utilized for block savvy security to information. Proposed framework is hybridization of AES, RC6, Blowfish and BRA. All calculations are symmetric key cryptography. These calculations utilize a solitary key for document encode and disentangle reason. All calculations key size is 128 digits. To conceal key data into cover picture utilizing LSB method. Usage of proposed framework is finished utilizing java language. Document encoding and disentangling time is determined with the assistance of java programming. Record encode and decipher time is determined for just content document with examination of existing AES and Blowfish calculations. Document size is given in MB for AES calculation.

2. EXISTING APPROACH

In existing framework single calculation is utilized for information encode and unravel reason. Yet, utilization of single calculation isn't achieved elevated level security. On the off chance that we utilize single symmetric key cryptography calculation than we need to confront security issue on the grounds that in this kind of calculation applies a solitary key for information encode and interpret. So key transmission issue happens while sharing key into multiuser climate. Public key cryptography calculations achieve high security however most extreme postponement is required for information encode and translate.More information stockpiling needs going over to the cloud, finding a protected and effective information access structure has become a significant exploration issue. Security strategies are not applied in the security of offloaded information from assaults.Once transferred and shared,

the information proprietor unavoidably loses authority over the information, making the way for unapproved information access. Only one algorithm is used for encryption while uploading any file on the cloud.

3. PROPOSED APPROACH

Selectively sharing data files on the cloud becomes a burden on the data owner as the hierarchy grows (the access privileges increase in number) and/or as the access restrictions become more complex due to an increase in the sensitivity of the file segments. A trivial solution involves the data owner to use public key encryption. This solution would require the data owner to encrypt the same part of the data file once for each data user being granted access then upload the resulting cipher texts to the cloud. The data users would then fetch their uniquely encrypted parts of the file from the cloud and utilize their private keys to decrypt them. This method ensures that no unprivileged data user will gain access to any part of the data file even if that user is able to download the cipher texts from the cloud. However, on a large scale, public key encryption becomes an inefficient solution due to the increase in the number of encryptions and large storage spaces required. Therefore, the challenge is to provide the data owners with an efficient, secure and privilege-based method that allows them to selectively share their data files among multiple data users while minimizing the required cloud storage space needed to store the encrypted data segments.

• Requiring less network communication.

• We present multiple data file partitioning techniques that facilitate data sharing in hierarchical settings.

• A new security layer is added to encrypt the data of the task before transferring to the cloud side by using AES and Triple DES encryption technique

A method for securely storing files in the cloud using a hybrid cryptography algorithm is presented In the proposed system. In this proposed system, the user can safely store the file in online cloud storage as these files will be stored in encrypted form in the cloud and only the authorized user has access to their files. The proposed software product is liable to meet the specified security needs of data center of cloud. To store the files safely the user will upload files on the cloud will be encrypted with a user-specific key. Cryptographic technique is used for secure file sharing in the cloud. AES, DES, algorithms are used to implement block-wise security to data for the user file security. Key data security is implemented by using the LSB steganography technique. Specifically sharing information documents on the cloud turns into a weight on the information proprietor as the progressive system develops (the entrance benefits increment in number) as well as the entrance limitations become more intricate because of an expansion in the affectability of the record fragments. A minor arrangement includes the information proprietor to utilize public key encryption. This arrangement would require the information proprietor to scramble a similar aspect of the information record once for every information client being allowedadmittance at that point transfer the subsequent code writings to the cloud. The information clients would then get their extraordinarily encoded pieces of the record from the cloud and use their private keys to decode them. This technique guarantees that no unprivileged information client will access any aspect of the information record regardless of whether that client can download the code messages from the cloud. Be that as it may, for an enormous scope, public key encryption turns into a wasteful arrangement because of the expansion in the quantity of encryptions and huge extra rooms required. In this way, the test is to furnish the information proprietors with an effective, secure and benefit-based technique that permits them to specifically share their information documents among numerous information clients while limiting the necessary distributed storage space expected to store the encoded information portions. Requiring less network communication.We present multiple data file partitioning techniques and propose a privilege-based access structure that facilitate data sharing in hierarchical settings. A new security layer is added to encrypt the data of the task before transferring to the cloud side by using AES encryption technique.

MODULES:

- Data Owner
- Data User
- Admin
- Cloud

MODULES DESCRIPTION:

Data Owner (DO): Owner uploads the data on a cloud server. File is split into octet. Every part of the file is encoded simultaneously using multithreading technique. Encoded file is stored on cloud server. Keys used for encryption are stored into the cover image. Cloud computing is the multi user environment.

Data User (DU): Cloud user request for file. On request of the file user also gets a key using email which consists of key information. Reverse process is used to decode the file.

Cloud: Cloud module can operate by the admin in cloud module having all the registered users and owners details and owner uploaded file details and user downloaded details.

Admin: Admin login with username and password, the entered username and password is correct then only admin enter into the home page, if entered details are incorrect admin can't login to home page, after entered into the home page admin act like owner of this application and admin activate and deactivate the user and owner and admin can view all uploaded file details and request details.

ADVANTAGES OF PROPOSED SYSTEM

More data storage needs turning over to the cloud, finding a secure and efficient data access structure has become a majorresearch. Security techniques are applied in the protection of offloaded data from attacks. Once uploaded and shared, the data owner will not loses control over the data, opening thedoor to authorized data access.sufficient and specifications documentationenlists the sufficient and necessary requirements that are used for the development of the project.

A software requirement specification (SRS) is a detailed explanation of a software system to being developed, specifying the functional and non-functional requirements (Non-functional supplements impose constraints on the plan or implementation such as quality standards, or design constraints). The specification may also include a set of use cases that describe interactions the user will have with the software. Software requirement specification establishes the basis for agreement between customers and contractors or suppliers (in market-driven projects, these roles may be played by marketing and development division) on how the software product should work as well as how it is not expected to work. Software requirement specification permits a correct assessment of requirements before design can begin and reduces work of redesign. It should provide supply a practical basis to guess the product costs, risks and schedules. The software product To procure the requirements, we need to get the clear understanding of the requirements to be developed or being developed. This is attained and clarified with detailed and thorough communications with the project members and customer till the results of the software.

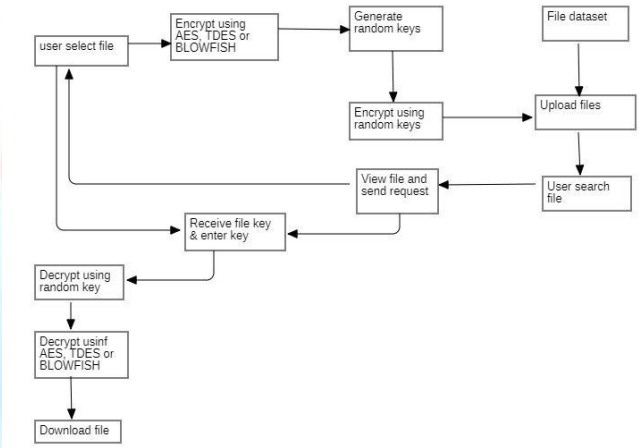

Fig 1 : Software Architecture

Procedure :

- Start
- Admin will be managing all the system operations. Cloud Admin will just see the members, uploaded files and downloaded files.
- Data Owner will upload the file which is encrypted with double encryption using(AES, Blowfish & Triple DES) algorithms.
- First encryption will be done by using AES and second encryption will be done using Blowfish & triple DES based on the size of the file.
- After that the file is divided into 7 fragments and will be saved in real time cloud(Firebase).
- Data User will not able to see any files after he login then data user will request to see the files then admin will request, when he accept data user will see the files but not able to see the information in it.

- Data User will keep request to file then the request is sent to data owner who is uploaded the file if the data owner accept the request and send the keys to the data user.
- The keys sent by the data owners are not original keys, the keys are like OTP(one time password) it used by particular user and particular time.
- Then data user can download the file by using that keys.
- End

Fig 1: Home page

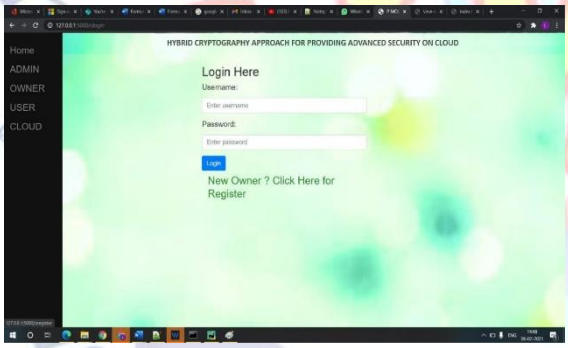

Fig 2: LoginPage

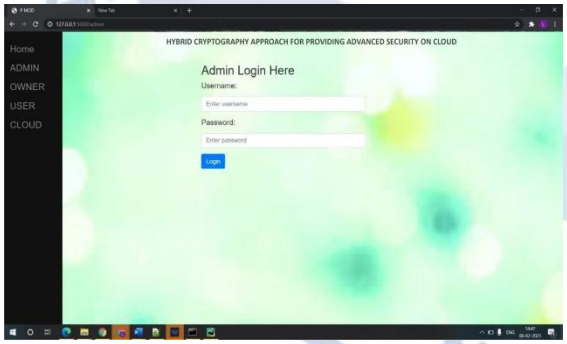

Fig 3: Admin Login page

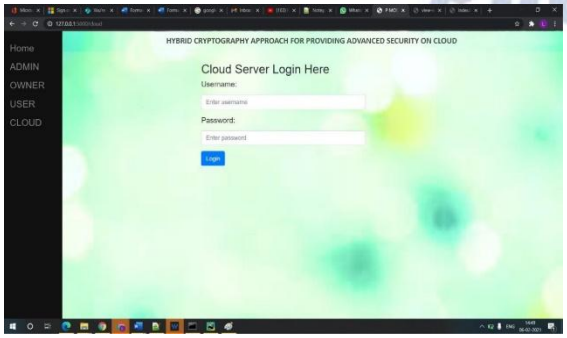

Fig 4: Cloud Server Login Page

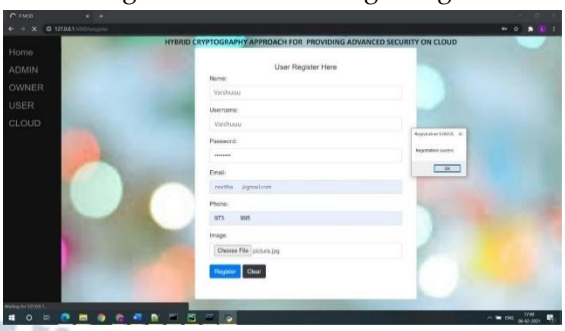

Fig 5: User Registration Page

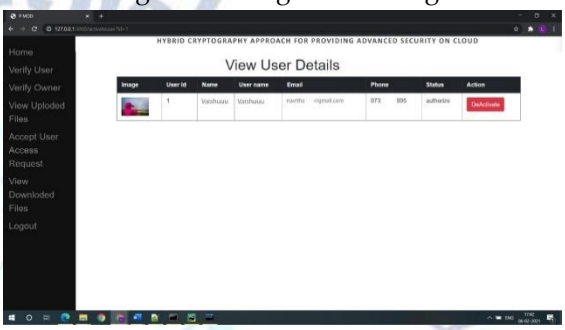

Fig 6: User Details Page

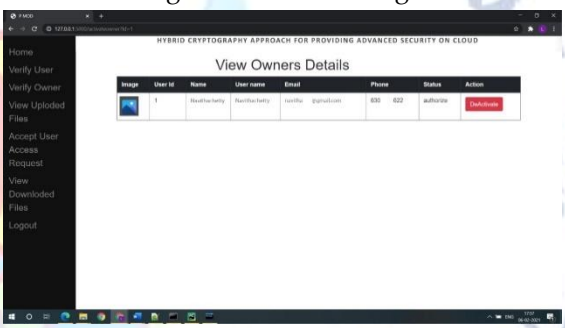

Fig 7: View Owner Details

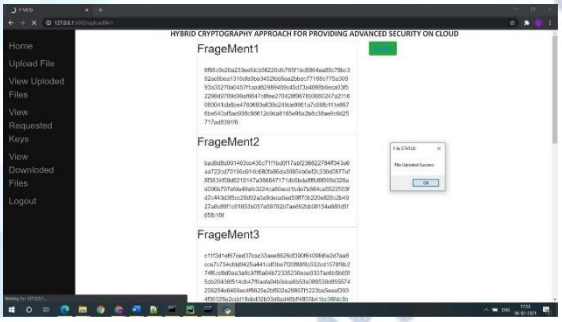

Fig 8:Data being Fragmented

4. INPUT DESIGN AND OUTPUT DESIGN

The input design is the bridge between the information and the user. It consists of the developing specification and the requirements for data preparation and the basic steps are required to put transaction data in to a usable form for processing can be attained by inspecting the computer to read data from a written or printed document or it can occur by having people witnessing the data directly into the system. The input design

focuses on how to control the amount of input required, rectifying the errors, avoiding delay, avoiding extra steps and keeping the process understandable. The input is planned in such a way so that it ensures security and ease of use with retaining the privacy. Input Design is the process of converting a user-oriented specifications of the input into a computer-based system. This plan is important to rectify errors in the data input process and show the correct direction to the management for getting genuine information from the system It is attained by creating user-friendly screens for the data entry to handle piles of data. The data entry system is designed in such a way that all the data manipulates can be performed easily. It also provides record viewing facilities. When the data is presented it will check for its usability. Data can be entered with the help of 22 screens. Appropriate messages are given as when needed so that the user will not be in a problem of instant. Thus, the aim of input design is to create an input layout that is easy to implement.A quality result is one, which meets the specifications of the end user and presents the information clearly. In any system output of processing are presented to the users and to other system through results. In output design it is shown how the information is to be displaced for immediate need and also the hard copy output. It is the most key and direct source information to the user. Efficient and intelligent result design improves the system's relationship to help user in clear decision-making. Designing computer results should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that user will find the system that is easy to use and effective. When analysis design computer output, they should identify the specific result that is needed to meet the specifications.

5. CONCLUSION AND FUTURE WORK

The various benefits gave by the cloud have driven numerous huge staggered associations to store and share their information on it. This paper starts by calling attention to significant security concerns information proprietors have when sharing their information on the cloud. Next, the most generally executed and explored information sharing plans are briefly examined uncovering purposes of shortcoming in each. To address the worries, this paper proposes a Privilege-based Multilevel Organizational Data sharing plan that permits information to be shared efficiently and safely on the cloud. Parcels an information file into numerous sections dependent on client advantages and information affectability. Each section of the information file is then common relying upon information client advantages. We officially demonstrate that is secure against adaptively picked plaintext assault accepting that the DBDH presumption holds. Our extensive presentation and reproduction examinations with the three most delegate plans show that can significantly decrease the computational multifaceted nature while limiting the extra room. 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 are solved using cryptography and steganography techniques. Data security is achieved using Blowfish, 3DES and AES algorithms. Less time is used for the encryption and decryption process using multithreading technique. With the help of the proposed security mechanism, we have accomplished better data integrity, high security, low delay, authentication, and confidentiality. As a future enhancement, we can accomplish high level security using hybridization of public key cryptography algorithms.Our proposed conspire establishes a framework for future characteristic based, secure information the executives and savvy contract improvement. As a future enhancement, we can accomplish high level security using hybridization of public key cryptography algorithms.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Y. Yang, X. Liu, R.H. Deng, "Multi-user Multi-Keyword Rank Search over Encrypted Data in Arbitrary Language". IEEE Transactions on Dependable and Secure Computing, 2018, publish online, DOI: 10.1109/TDSC.2017.2787588.

[2] W. Sun, S. Yu, W. Lou, Y. Hou and H. Li, "Protecting Your Right: Verifiable Attributebased Keyword Search with Fine grained.

[3] K. Liang, W. Susilo, "Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage," IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 9, pp. 1981- 1992.

[4] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE cipher texts," in USENIX Security Symposium, ACM, 2011, pp. 34-34.
[5] Rajaram Jatothu, published a paper on Detect and Classify the Unpredictable
[6] Cyber-Attacks by using DNN Model Turkish Journal of Computer and Mathematics Education Vol.12 No.6(2021), 74-81, Accepted: 27 December 2020; Published online: 05 April 2021.
[7] Rajaram Jatothu,published a paper on Detection of URL Based Phishing Attacks Using Machine Learning International Journal of Modern, Engineering and Research Technology Volume 6, Issue3, July, 2019, ISSN: 2348-8565.
[8] Rajaram Jatothu,Dr.R.P.Singh, Published a paper on Distributed Protocol Using Quantum Cryptography For Secure Communication In Ad hoc Networks International Journal of Pure and Applied Mathematics Volume 116 No. 23 2017, 253-260 SSN: 1311-8080
[9] Rajaram Jatothu, paper on an efficient Cloud Based Healthcare Services Paradigm for Chronic Kidney Disease Prediction Application Using Boosted Support Vector Machine Concurrency and Computation: Practice and Experience.