iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.45107

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Secure Data Sharing Using 3DES Algorithm

Pranjali Prajwal M
Department of Master of Computer Applications, RV College of Engineering

Abstract: ***The Triple Data Encryption Algorithm, also known as Triple DES (Data Encryption Standard), 3DES, TDES, Triple DEA, or TDEA, is a symmetric key-block cypher that uses the DES cypher in triplicate by encrypting with key 1 (k1), decrypting with key 2, and encrypting with key 3 (k3) (k3). There is a two-key variation as well, where k1 and k3 are identical. The Data Encryption Standard, created by IBM in the early 1970s and adopted by NIST with minor adjustments in 1977, is the foundation of the 3DES cypher suite. The system consists of a Data Owner, Network Storage, Aggregate Key and User. The data owner uploads the file which is encrypted by making use of 3DES algorithm, once the data has been encrypted blowfish is applied to convert the whole data into data blocks which is stored in network storage or the drop box. When the authorized user provides the secret key that is the aggregate key the data is decrypted and original data is available for the user. Admin will be a superuser who will manage different things like uploaded files and registered users. Admin will be having permissions to remove users if found invalid. The secure data sharing system using 3DES algorithm is developed with the Java technologies. Encryption is done using triple standard encryption standard. Agile methodology is used to develop the system and MySQL Database is used to store the data. The system is able to efficiently store the data uploaded by the data owner after encrypting it using blowfish algorithm and 3DES technology. After the storage of the data the system will also be able to securely transfer the saved data within the trusted set of people without any other person able to access the file.***
Keywords: 3DES, cypher, blowfish, encryption, secure data sharing

I. INTRODUCTION

Sharing data is a key component of cloud storage. It exemplifies how to exchange data with others in cloud storage in a safe, effective, and adaptable way. It provides brand-new public-key cryptosystems that produce constant-size ciphertexts, enabling effective decryption rights delegation for any collection of cypher texts. The breakthrough lies in the ability to combine any collection of secret keys into a single key that possesses the full power of all the individual keys. To put it another way, the owner of the secret key can release a constant-size aggregate key for cloud storage flexibility in cipher text sets while maintaining the privacy of the other encrypted files outside the set. It is simple to email or store this brief aggregate key.

To ensure that the algorithm used for the file's encryption technique is not chosen by one person, the document can be uploaded while taking probabilistic algorithm usage into consideration. Following data upload, keys are produced for each file based on the random algorithms used to encrypt the content. The algorithm used to produce the key determines how unique it will be for each and every file. When files are uploaded in a batch, both individual file keys and an aggregate key are generated.

The aggregate key is only valid for that specific batch, and the keys are kept by the person who uploaded the data. The file can be opened using either the key generated specifically for it or the key generated collectively by that batch of files. If a user wants to share a file with other users, he or she can send the file and grant access by mentioning the keys produced with the file.

II. LITERATURE SURVEY

In this study authors recommend a simple data-sharing method for cloud computing systems. It takes use of the ciphertext-policy, attribute-based encryption access control technology and adapts the access control tree structure to suit mobile cloud environments. By way of external proxy servers, the lightweight data sharing scheme moves a substantial portion of the computationally taxing ciphertext-policy, attribute-based encryption access control tree transformation from mobile devices. Attribute description fields have also made it easier to implement lazy-revocation, a difficult issue in program-based ciphertext-policy, attribute-based encryption access systems. The experimental results show that, when users share data in mobile cloud environments, a lightweight data sharing scheme can successfully reduce the overhead on the mobile device side [2].

The authors of this paper focused on developing a practical, safe, and computationally Diffie-Hellman secure technique for the random oracle model. We assess the performance of our system through theoretical comparisons with related schemes and implementations at various security levels, using NIST recommended elliptic curve settings. The outcomes demonstrate that cloud-based data exchange may be accomplished using our strategy [3].

©IJRASET: All Rights are Reserved

In this method, they have identified ciphertexts by a number of target properties, whereas a user's access credentials are specified by a multi-attribute access structure. A delegator can change the original ciphertexts into proxy ciphertexts encrypted by the delegate's characteristics without divulging any private information to the cloud server. If his credentials are in accordance with the delegate's access policy, a delegate may also submit a search request for the ciphertexts. According to security research, our ABPRE-KS is private and keyword semantic secure under the BDBH assumption. [4].

As a result, the authors relocate to the blockchain rather than a central server in this work and they develop an ABE algorithm that may be used in a multicenter scenario. Additionally, IoT devices often cannot afford complicated encryption computations due to their low computing power. We create an obfuscating policy that shifts encryption calculations from terminals to the cloud in order to remedy this. In this way, IoT devices may encrypt data at low processing costs. The method we developed can efficiently and safely reduce the computational demands on IoT terminals during the data encryption and decryption stages, according to security studies and simulations [5]. In this study, the authors introduce the Secure Data Sharing in Clouds technique, which enables data sharing (forwarding) without the requirement for computationally expensive re-encryption, insider threat security, forward and backward access control, and data confidentiality and integrity. One encryption key is used by the Secure Data Sharing in Clouds technique to encrypt a file. Two unique key shares are generated for each user, but only one share is given to each user. A single share of a key can be used in the Secure Data Sharing in Clouds method to mitigate insider risk. The other key share is kept on the encryption server, an unbiased third party. Both stationary and mobile cloud computing environments can benefit from the Secure Data Sharing in Clouds technique. A functioning system prototype was created by them [6]. This study's goal is to safeguard cloud storage data and offer a complementary cloud storage security strategy. By examining the security difficulties with user data in cloud storage and tackling a topic of relevant security technology based on the structural elements of cloud storage systems, these were merged with the results of earlier academic research [10]. The researchers undertook a thorough examination of the literature on data security and privacy issues, data encryption methods, and related countermeasures in cloud storage systems for this work. First, let's look over the definitions, categories, architecture, and applications of cloud storage. In the second section, we go into great detail about the issues with and requirements for data security and privacy protection in cloud storage systems. The final section provides an overview of data encryption technology and defence tactics. We conclude by talking about a few current topics of research for cloud storage data security [11].

III. EXISTING SYSTEM

In the current configuration, relying on the server to perform access control after authentication is a common way to safeguard the privacy of the data, but also means that any unanticipated privilege escalation will reveal all the data. In a shared-tenancy cloud computing context, things substantially worsen. A number of cryptographic techniques exist that enable a third-party auditor to assess file availability on the data owner's behalf without disclosing any information about the data or risking the identity of the data owner. The ability of the cloud server to preserve secrecy is also unlikely to inspire confidence in cloud consumers. a cryptographic solution that has been proven to be secure and is based on number-theoretic assumptions. The disadvantages of the existing system are:

1) With the number of decryption keys to be shared, the prices and difficulties often rise.
2) In public key encryption, the encryption and decryption keys are distinct.

IV. PROPOSED SYSTEM

The suggested solution will be able to boost a decryption key's strength without increasing its size by allowing it to decrypt several ciphertexts. To offer a trustworthy public-key encryption system with flexible delegation, which allows any subset of the ciphertexts it generates to be unlocked using a constant-size decryption key produced by the owner of the master-secret key. Authorized users can decode a file using the aggregate key provided by the data owner over a secure email by employing key-aggregate cryptosystems, a sort of public-key encryption. The advantages of the proposed system are:

1) The extracted key could be an aggregate key, which is as little as a single-class secret key.
2) The aggregate key can be used to easily conduct decryption delegation.

V. ARCHITECTURE

Fig 1 describes that based on the algorithm used to produce the key, each key is generated for every file and is unique in nature. When files are uploaded in a batch, both the individual file key and the aggregate key for the entire batch of files are generated. The user who uploaded the files retains the aggregate key, which is only valid for that specific batch. The key generated for the file or the aggregate key generated by that batch of files can be used to open the file. The user can transfer the file and grant access to it by other users when he wants to share a file with them.

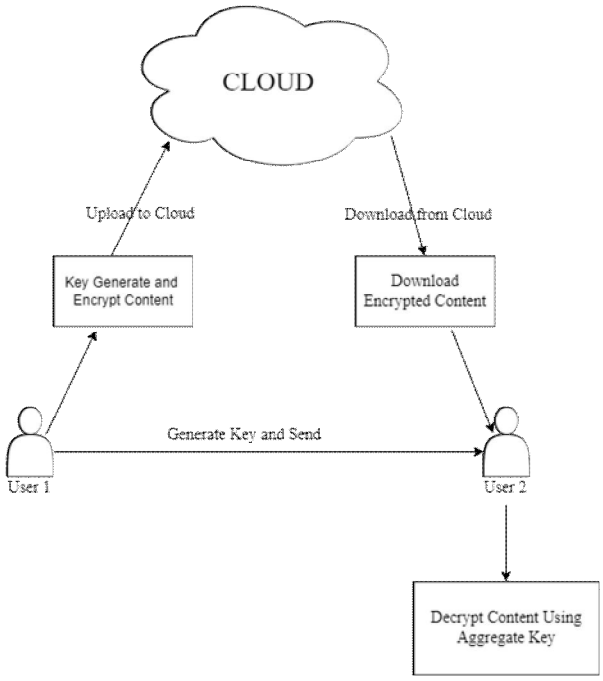


Fig. 1 Architectural Design of Secure Data Sharing System

VI. SYSTEM REQUIREMENTS

A. Hardware Requirements

Table 1
Hardware Requirements

Hardware Requirements	Specifications
Processor	Dual-core 1.6GHz or higher
RAM	8GB or more
Hard Disk	10GB or more

B. Software Requirements

Table 2
Software Requirements

Software Requirements	Specifications
Operating System	Microsoft Windows 8 and above
Technologies	CSS3, HTML5, Bootstrap4, JQuery, Spring Boot, Spring MVC
IDE	NetBeans 8.2 and above
Coding Language	Java 8
Database	MySQL

©IJRASET: All Rights are Reserved

VII. CONCLUSION

A technique for implementing secure data sharing in an isolated cloud environment is to use 3DES. A user is the data owner who shares a file with a number of other users. In addition, we developed a network storage module that stores the encrypted data that the data owner submitted and generates and emails the user an aggregate key in order to prevent unauthorized access to the system. Only when the user sends a request to the data owner and the data owner shares the aggregate key through encrypted email with the user will the user be able to access the submitted data.

The proposed method is excellent for hosting data since it is safe and well-organized when it comes to exchanging data files with other parties in a public cloud environment, as well as when it comes to data security and availability. The security of user data privacy is a crucial issue with cloud storage. With the availability of additional mathematical tools, the variety of cryptographic systems is growing, and many applications now make use of multiple keys. It examines the compression of secret keys using public-key cryptosystems that allow key delegation for various ciphertext classes in cloud storage.

The delegate can always receive an aggregate key of a given size, regardless of the power set of classes they choose. Hierarchical key assignment can only lower storage needs if each keyholder has access to the same set of resources, making it less versatile. The maximum number of specified ciphertext classes is referred to as a work restriction. The quantity of ciphertexts in cloud storage typically rises quickly.

VIII. ACKNOWLEDGMENT

The gratification and euphoria that come with the achievement of any work would be unfinished unless we mention the name of the people, who made it possible, whose relentless guidance and support served a beacon light and served our effort with success.

We express our sincere thanks and wholehearted credit to our internal guide Dr. Deepika K, Assistant Professor, Department of MCA, R.V. College of Engineering ®, Bengaluru for her constant encouragement, support and guidance during the seminar work.

REFERENCES

[1] RUIXUAN LI,Chenglin Shen, Heng He, Xiwu Gu, Zhiyong Xu, Cheng-Zhong Xu,"A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing", Publisher: IEEE, April-June2018, pp.344-357, vol.6 DOI, Bookmark: 10.1109/TCC.2017.2649685.

[2] Jiang Zhang; Zhenfeng Zhang, "Secure and Efficient Data-Sharing in Clouds", INSPEC Accession Number: 13852016, DOI: 10.1109/EIDWT.2013.81, Publisher: IEEE, Conference Location: Xi'an, China.

[3] Hanshu Hong, Zhixin Sun,"Towards secure data sharing in cloud computing using attribute based proxy re-encryption with keyword search", 2017 IEEE 2nd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), Date Added to, IEEE Xplore: 19 June 2017, INSPEC Number : 16967088, DOI:10.1109/ICCCBDA.2017.7951914,Publisher:IEEE,Conference Location: Chengdu.

[4] Xin Wei, Yong Yan, Shaoyong Guo, Xuesong Qiu, Feng Qi, "Secure Data Sharing: Blockchain-Enabled Data Access Control Framework for IoT", Published in: IEEE Internet of Things Journal (Volume: 9, Issue: 11, June1, 1 2022), Page(s): 8143 - 8153, Date of Publication: 08 September 2021, DOI: 10.1109/JIOT.2021.3111012, Publisher: IEEE.

[5] Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, Albert Y. Zomaya, "SeDaSC: Secure Data Sharing in Clouds", Published in: IEEE Systems Journal (Volume: 11, Issue: 2, June, 2017), Page(s): 395 - 404, Date of Publication: 13 January 2015, INSPEC Accession Number: 16992950, DOI: 10.1109/JSYST.2014.2379646, Publisher: IEEE.

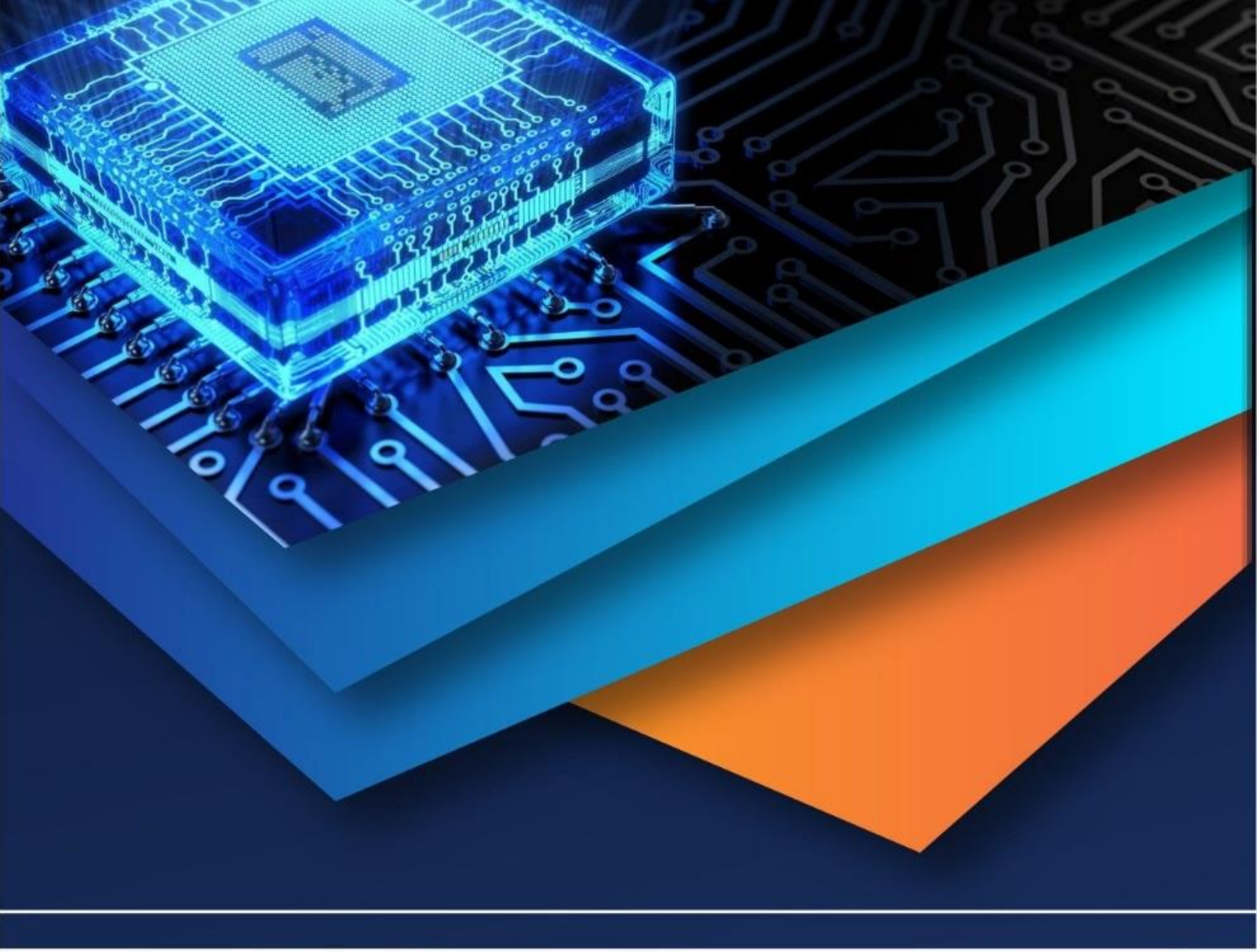
[6] K. Akhil, M. P. Kumar, B. Pushpa, "Enhanced cloud data security using AES algorithm", Published 1 June 2017, Computer Science, 2017 International,Conference on IntelligentComputing and Control (I2C2), DOI:10.1109/I2C2.2017.8321820, Corpus ID: 4113072.

[7] Ms N. Sushma (M.Tech) 2Mr V.N.S Vijay Kumar M.Tech, "A New Approach For Secure Data Sharing in Clouds" , Associative Professor 1,2 Lenora College Of Engineering, Rampachodavaram, East Godavari, Andhra Pradesh, INDIA, Vol 10, Issue 12, Dec /2019 ISSN NO:0377-9254, Journal of Engineering Sciences.

[8] Bandaru Chandrakala, Sanjay Lingareddy, "Proxy Re-Encryption in cloud using ALBC" (adaptive lattice based cryptography), December 2019, Indonesian Journal of Electrical Engineering and ComputerScience 16(3):1455, DOI:10.11591/ijeecs. v16.i3.pp 1455-1463

[9] Diao Zhe, Wang Qinghong, Su Naizheng, Zhang Yuhan, "Study on Data Security Policy Based on Cloud Storage", Published 26 May 2017, Computer Science, 2017 IEEE 3rd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS)

[10] Pan Yang, N. Xiong, Jingli Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey", Published 2020, Computer Science, IEEE Access,DOI:10.1109 /ACCESS.2020. 3009876 Corpus ID: 220835389



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)