IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A TRIVIAL AND COST EFFECTIVE ELECTRONIC AND ENCRYPTED DOCUMENT SHARING FOR USERS THROUGH SECURED CLOUD STORAGE

[1]Sujith Revilla, [2]Challa Sai Yaswanth, [3]N Sai Janardhan [4]Natarajan P

[1]revilla.sujith2017@vitstudent.ac.in, 2challasai.yaswanth2017@vitstudent.ac.in, [3]sai.janardhan2017@vitstudent.ac.in, [4]pnatarajan@vit.ac.in

[1]Student at VIT, [2]Student at VIT, [3]Student at VIT,[4]Associate Professor

ABSTRACT

Sharing of components on the cloud might be achieved on a large scale since it is cost effective and location independent. However, the demand surrounding cloud computing, organizations are still reluctant to deploy their businesses within the cloud computing environment due to concerns in secure resource sharing and authentication. Sharing digital records on public cloud storage facilitates customers to get or share documents of high quality and efficiency.

Anyway, problems that are data privacy and security, simple data sharing, efficient authority delegation [1], computation speed optimization, are remaining towards achieving practical access control within the Electronic Document Sharing. Proposed project is an innovative access control system and a fine-grained data sharing process for data sharing system, which parallelly achieves the all required features and is suitable for resource-based devices. This project consists of mail notifications for OTP(One Time Password) sharing to provide better security and data privacy. And auto deletion option provided in this system to delete the file automatically based on expire date given by user, so that memory will be optimized. The access control mechanism will be deployed on realistic environment, including public cloud storage, a laptop, and an inexpensive local server with constrained resources. The practical results indicate that the process is efficient, feasible, and economical. Proposed algorithm is AES256 [2] algorithm to encrypt and decrypt the data.

The proposed application was implemented in java technology and using MYSQL database. The above technologies chosen because these are open source and more secure.The objective is to provide simple, secure, and more efficient system to share the document among the employees in an organization.

Keywords: Encryption, AES 256, Decryption, Secured File Sharing

1 INTRODUCTION

1.1 Cloud Computing Definition

Cloud computing is that the utilization of registering assets (equipment and programming) that are conveyed as an assistance over a system (normally the Internet). The name originates from the traditional utilization of a cloud-formed image as a mirrored image for the unpredictable foundation it contains in framework charts. Cloud computing endows far away administrations with a client's information, programming, and calculation. Cloud computing comprises of kit and programming assets made accessible on the web as over saw outsider administrations. These administrations regularly give access to leading edge programming applications and top of the road systems serverPCs.

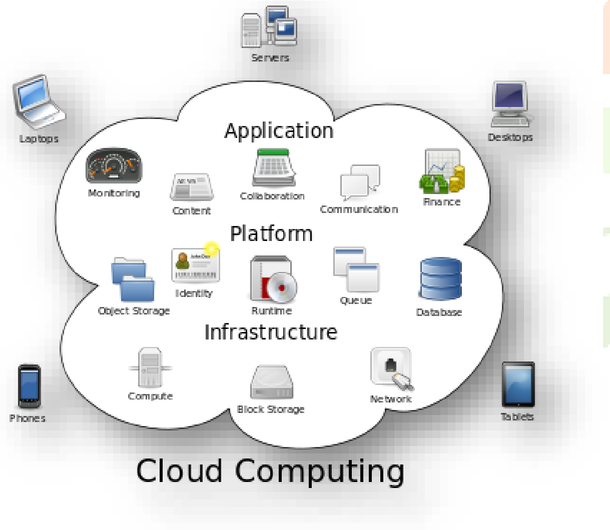


Fig Structure of cloud computing

The objective of cloud computing is to use conventional super figuring, or elite registering power, typically utilized by military and exploration offices, to perform many trillions of calculations for every second, in buyer arranged applications, for instance, monetary portfolios, to convey customized data, to offer information stockpiling or to regulate enormous, vivid PC games.

1.2 Cloud Computing Benefits

Accomplish economies of scale – increment volume yield or efficiency with less individuals. Your expense per unit, undertaking or item dives.

Decrease spending on innovation framework. continue simple access to your data with negligible forthright spending. Pay more only as costs arise (week by week, quarterly or yearly), in sight of interest.

Globalize your workforce for barely anything. Individuals worldwide can get to the cloud if they need an online association.

1.3 Information Deduplication

Information deduplication implies diminish the copy information in distributed storage. Information deduplication has been displayed to be a viable strategy in Cloud reinforcement and documenting applications to decrease the reinforcement window, improve the additional room effectiveness and system transfer speed usage. Ongoing investigations uncover that moderate to high information repetition obviously exists in VM (Virtual Machine), endeavor and High-Performance Computing (HPC) stockpiling frameworks.

1.4 Encryption and Decryption

Encryption is that the way toward interpreting plain content information (plaintext) into something that provides off an impact of being arbitrary and unimportant (ciphertext). Decoding is that the way toward changing over ciphertext back to plaintext.

To encode quite a modest quantity of data, symmetric encryption is employed. A symmetric key utilized during both the encryption and decoding forms. To unscramble a touch of ciphertext, the key that was utilized to scramble the knowledge must be utilized.

The objective of every encryption calculation is to form it as troublesome as conceivable to unscramble the produced ciphertext without utilizing the key. within the event that an honest encryption calculation is employed , there's no strategy essentially better than deliberately attempting each conceivable key. For such a calculation, the more drawn out the key, the more troublesome it's to decode a touch of ciphertext without having the key.

It is hard to make a decision the character of an encryption calculation. Calculations that watch promising a number of the time find yourself being quite simple to interrupt , given the simplest possible assault. While choosing an encryption calculation, it's a sensible thought to select one that has been getting used for quite while and has effectively opposed all assaults.

2 OBJECTIVES OF THE PROJECT

The main objective of the project is to provide more efficient and secured cloud storage for employees to store and share their data one another easily. The main objectives are providing security, user friendliness, sharing environment, memory optimization and finally improve the performance. This project developed for the company employees to manage their data and files globally.

3 PROBLEM DEFINITION

The problems faced in cloud computing are security, ease of data sharing from one another, information privacy, efficient authority management, computation speed optimization, storage and they are remaining towards achieving practical access control in the Electronic Document Sharing. Proposed application is an innovative access control system and a fine-grained data sharing process for data sharing system, which parallelly achieves the all required features and is suitable for resource-based devices for employees in a company.

4 REQUIREMENTS

This chapter contains requirements that are needed to complete the project without any hassle. Need to consider the hardware and software requirements for project and also functional and non-functional requirements of the project.

4.1 Software Requirements

Operating System	-	Windows
Coding Language	-	Java
Front End-		HTML, CSS, JavaScript, Jquery, Bootstrap
Back End-		MySQL and DriveHq Cloud Storage
Server	-	Apache Tomcat

4.2 Hardware Requirements

Processor	-	Intel
RAM	-	4 GB (min)
Hard Disk	-	160 GB
Keyboard	-	Standard Windows Keyboard
Mouse	-	Two or Three Button Mouse

4.3 Functional Requirements

1. Document Sharing System for efficient sharing of documents through cloud storage.

2. It consists of auto time-based deletion option to optimize the storage.

3. Fine grained access control through OTP for deletion and downloading.

4. Secure data sharing implemented using AES256 Encryption Algorithm

5. Employee Authentication

6. Data Sharing among the employees

7. Admin monetization on employees

4.4 Non-Functional Requirements

1. High Security

2. High Performance

3. User Friendly

4. Memory Optimized

5 SYSTEM ANALYSIS

System analysis consists of the various existing systems, disadvantages in them, proposed system with advantages and the feasibility study for this project.

5.1 Existing System

In existing system company employees are using mails and online drives to share the data and files from one another. Its not safe and secure for company privacy and information. In this they are not using any encryption techniques to protect the data from unauthoirzed access. Even they did not maintain the user levels and protection measures so the data can be stolen easily.

5.2 Disadvantages

The main drawbacks in existing system are:

1. Less Secure and authentication problem
2. Memory wastage due to no optimization in memory usage
3. More storage required
4. Depends on proxy so that they may misuse the company's data
5. Employee may be misusing the data and may corrupt the data.

5.3 Proposed System

Proposed Model is Document Sharing System for efficient sharing of documents through cloud storage. It consists of auto time-based deletion option to optimize the storage. Fine grained access control through OTP for deletion and downloading. Secure data sharing implemented using AES256 Encryption Algorithm. Proposed system contains of authentication module to reduce the unauthorized access. For OTP generation random function used in this system.

5.4 Advantages

The main advantages in proposed system are:

1. More Secure and authenticated system
2. Memory Usage Optimized by deleting files automatically from cloud by maintaining expiry date.
3. No proxy required to maintain the data
4. High Performance through reducing storage wastage
5. Employee can easily share the date one another by single click.
6. This will incredibly improve their productivity, streamline their activity line the board, and eventually upgrade the system performance

6 ALGORITHM(AES256)

To provide the higher and powerful security to the project data, here it's implemented encryption algorithm AES 256. Whenever employee upload the filing system will encrypt it then stored into the cloud. And even passwords also stored within the sort of cipher text only. Encryption is one among the foremost common ways to guard sensitive data. Encryption works by taking plain text and converting it into cipher text, which is formed from seemingly random characters. Only those that have the special key can decrypt it. AES uses symmetric key encryption, which involves the utilization of just one secret key to cipher and decipher information.

The Advanced Encryption Standard (AES) is that the first and only publicly accessible cipher approved by the US National Security Agency (NSA) for shielding top secret information. AES was first called Rijndael after its two developers, Belgian cryptographers Vincent Rijmen and Joan Daemen.

256-bit encryption may be a data/file encryption technique that uses a 256-bit key to encrypt and decrypt data or files.

The following diagram shows how symmetric key encryption works:

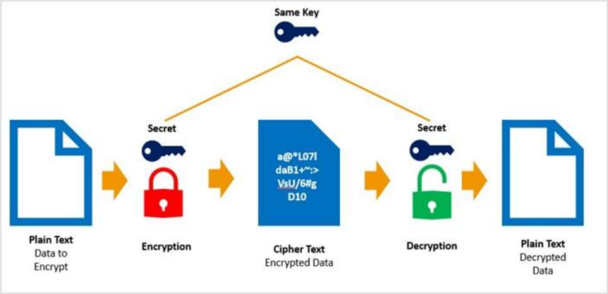


Fig Encryption Process

It is one among the foremost secure encryption methods after 128- and 192-bit encryption, and is employed in latest encryption algorithms, protocols and technologies including AES and SSL.

256-bit encryption is refers to the length of the encryption key wont to encrypt a knowledge stream or file. A hacker or cracker would require 2^{256} different combinations to interrupt a 256-bit encrypted message, which is virtually impossible to be broken by even the fastest computers.

7 MODULES

7.1 Administration

This module consists administration activities like admin can moniter cloud uploads, cloud downloads, login history, manage users, file security response, view feedback, view problems, key generation to mails, view transactions, change password, change secret key etc.

7.2 Employee Management

In this module employee can register, login and upload and download the files and share the files and employee can send request for owner and admin for key, employee can send key to others request, post feedback, post problems to admin.

7.3 OTP Required For Login

In this module the main goal is otp comes to mail when admin and employee want lo login to their account. Along with password they required otp to login in their account. Random otp will generate every time and we have to login in 30 sec only.

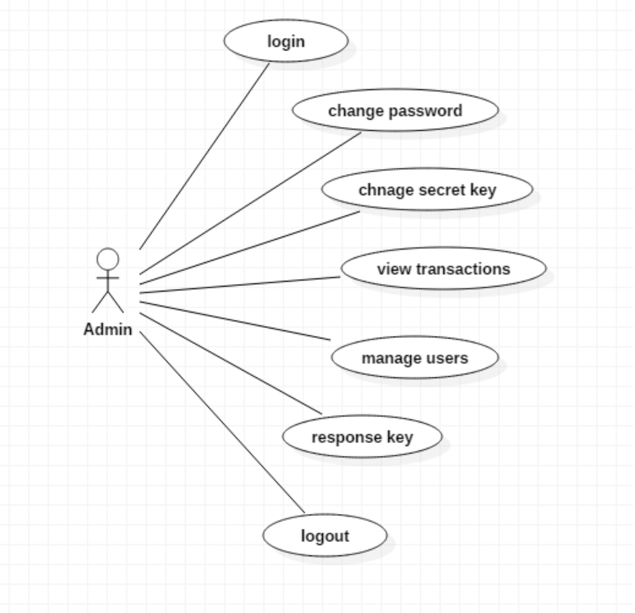
7.4 Data Auto Deletion

In this module the main goal is auto deletion of files once expiry date is reached.

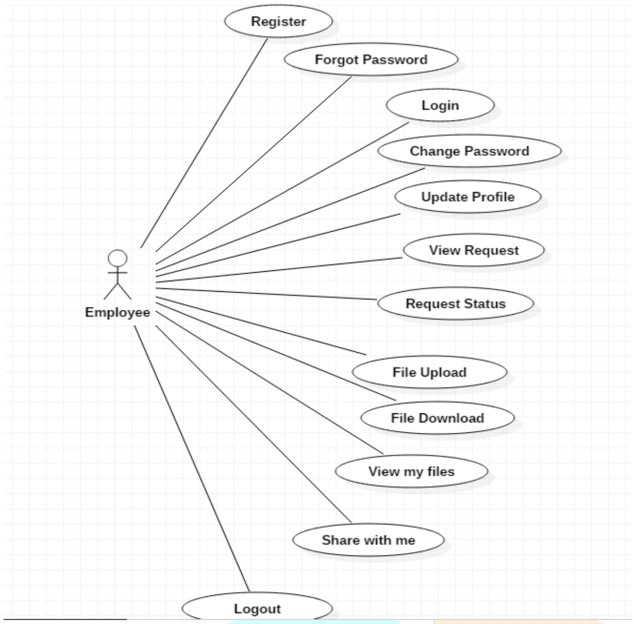
8 USECASE DIAGRAM

A use case diagram within the Unified Modelling Language (UML) may be a sort of behavioural diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. the most purpose of a use case diagram is to point out what system functions are performed that actor. Roles of the actors within the system are often depicted.

Admin Use-Case Diagram:



Employee Use-Case Diagram:



9 CONCLUSION AND FUTURE SCOPE

The Application designed have successfully met the requirements which were presented during the proposal. The algorithm used are indeed helpful in getting the expected results. The goal was providing friendly environment to the employees to share their data one another securely and easily. All specified functional and non-functional requirements completed. In this project AES256 encryption algorithm successfully implemented.

To further extend this for future developments, there are few directions among which the one is to implement the same concept for various applications such as image sharing, digital wallets, and few others.

Another enhancement can be to extend the otp verification with mobile instead of email to provide better identification of user. Further it can be implemented in public domain also.

10 REFERENCES

[1] Qinlong Huang, Member, IEEE, Yixiang Yang and Jingyi Fu -Secure Data Group Sharing and Dissemination with Attribute and Time Conditions in Public Cloud 2018

[2]https://www.techopedia.com/definition/29703/256-bit-encryption

[3]Peng Zeng, Kim-Kwang Raymond Choo, "A New Kind of Conditional Proxy Re-Encryption for Secure Cloud Storage", Access IEEE, vol. 6, pp. 70017-70024, 2018

[4] C. Delerablée, “Identity-based Broadcast Encryption with Constant Size Ciphertexts and Private Keys,” Proc. the 13th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2007), pp. 200-215, 2007.

[5] F. Beato, S. Meul, and B. Preneel, “Practical Identity-based Private Sharing for Online Social Networks,” Computer Communications, vol. 73, pp. 243-250, 2016.

[6] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy Attribute based Encryption,” Proc. the 28th IEEE Symposium on Security and Privacy (S&P 2007), pp. 321-334, 2007.

[7] Z. Wan, J. Liu, and R. Deng, “HASBE: A Hierarchical Attribute-based Solution for Flexible and Scalable Access Control in Cloud Computing,” IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743-754, 2012.

[8] H. Hu, G. Ahn, and J. Jorgensen, “Multiparty Access Control for Online Social Networks: Model and Mechanisms,” IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 7, pp. 1614-1627, 2013.

[9] M. Blaze, G. Bleumer, and M. Strauss, “Divertible Protocols and Atomic Proxy Cryptography,” Proc. Advances in Cryptology EUROCRYPT 1998 (EUROCRYPT '98), pp.127-144, 1998.

[10] D. Tran, H. Nguyen, W. Zha, and W. Ng, “Towards Security in Sharing Data on Cloud-based Social Networks,” Proc. the 8th International Conference on Information, Communications and Signal Processing (ICICS2011), pp. 1-5, 2011.