ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Data Security Using Public Distribution in Cloud Storage

Vamsi Krishna K.V.
Department of Computer Science & Engineering,
SRM University, Kattankulathur, Kancheepuram District- 603203, India.

Siddharth Chilukuri
Department of Computer Science & Engineering,
SRM University, Kattankulathur, Kancheepuram District- 603203, India.

Mrs. T. Y. J. Nagamalleshwari
Department of Computer Science & Engineering,
SRM University, Kattankulathur, Kancheepuram District- 603203, India.

ABSTRACT

This project aims at demonstrating how security and privacy of shared data in the cloud can be obtained by distribution and encryption of file using multiple cloud storage after splitting the file. Security has always been an issue to be concerned with while dealing with operations in the cloud. In the proposed system, we implement the concept of multiple cloud storage along with enhanced encryption through using encryption technique and storing the file after splitting into multiple files. The storage of files in the cloud storage can be achieved through creation of multiple virtual cloud storage. The current system of cloud storage is based on storing the file in a single storage space after encryption and retrieving the file after decryption. Attacks are difficult to prevent on the single server storage with mere encryption. Public distribution in cloud storage uses Advanced Encryption Standard to encrypt the file and splitting before storage and Message Digest algorithm MD5 is used to verify the confidentiality of the file before retrieval.

I. INTRODUCTION

A computer cloud is a target-affluent environment for pernicious individuals and criminal organizations. Security is a primary concern for subsisting users and potential incipient users of cloud computing applications. Due to astronomically immense infrastructure costs, organizations are gradually switching to cloud technology. In cloud computing, files and software is not stored in user's computer and the user is generally concerned about the integrity and privacy of his data. Data security is the primary concern in cloud storage since they are maintained in cloud storage provider's servers. Confidentiality and security of the data stored in the cloud is at potential threat by various types of attacks.

Objective of the project:

The objective of the project is to design a cloud storage system for confidentiality, integrity and functionality. We present with the distributed cloud storage architecture to add additional security to the files along with encryption and verify the files before retrieval for any loss or corruption of data. Files can be modified or altered by external attacks in a single server. The data is encrypted to prevent any knowledge of the file. The multiple server storage is difficult to access simultaneously by sources other than the user. When the data is corrupted or modified, it is difficult to identify by the user and requires the storage servers to protect the data or inform the user during any modification. The system tells the user if the data stored in multiple servers is modified or corrupted by external user. The key used to encrypt the data is particular to the user and the files cannot be accessed or decrypted by any other way.

Introduction to Encryption and Decryption:

Encryption is the process of transforming information into an unrecognized format which is meant to secure the data from the external persons other than the intended user and recipient. Encryption is encoding an particular type of information using various encryption algorithms. Decryption is the process of decoding the encrypted data

Cite this article as: Vamsi Krishna K.V., Siddharth Chilukuri & Mrs. T. Y. J. Nagamalleshwari, "Data Security Using Public Distribution in Cloud Storage", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 7 Issue 2, 2020, Page 40-48.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

into normal information .Data is encrypted and decrypted using various keys which can be either public or private. A key is provided by the user to encrypt the data by converting into cipher texts which can be decoded only through the key used to encrypt or any combination of keys which encrypted the data. Various algorithms for encryption are AES, DES, RSA, DSA, IDEA. Encryption of files can be based on two types of keys like Asymmetric (Public key) or Symmetric (Private key). Asymmetric key uses a private key to encrypt the data along with the user's key. DSA,RSA are types of asymmetric encryption, Symmetric key uses the key given by user to both encrypt and decrypt the data .AES, Blowfish, IDEA are types pf symmetric encryption.

Different cryptographic methods can be utilized for encryption and decrypting of information, concretely for information security in distributed computing applications:

- RSA technique in which encryption key is open and varies from the unscrambling key which is kept as unknown.
- DES or Data Encryption Standard in which there is the utilization of symmetric key for encryption and decryption.
- SSL or Secure Socket Layer which is customarily utilized convention for dealing with the security of a message transmission on the Internet and it utilizes open and private key encryption framework.
- Mixed encryption which comprises of different methodologies that are associated together and lead to improved results which significantly higher levels of security.

II. LITERATURE SURVEY

Cloud Computing:

Now a days, Cloud processing is used to give functionalities to large storage and different undertakings and joint effort over a system by a gathering of remote servers. It is a conceptual collection of PCs on cloud used to give enormous, appropriated capacity and handling abilities, which can be accessed by any Internet-associated PC that has a web program. Distributed computing can provide the devices to facilitate late advances in programming, systems administration, memory, and preparing innovation applications. Distributed computing is advanced by significantly enormous IT organizations where these most recent mechanical improvements occur, and these organizations have a personal stake in advancing the nascent innovations. A cloud comprises a homogeneous arrangement of equipment and programming assets in a solitary regulatory area. In this setup, protection, security, asset administration, mistake resilience, execution and productivity of settlement are less testing than in a heterogeneous domain with assets in a wide range of managerial and technological areas. Thus, the clients do not have to possess their resources which lead to huge savings in purchasing as well as maintaining costs and financial requirements.

Cloud computing is centredon enterpriseprocessing; its selection by modern associations, financial establishments, social insurance associations, thus on has a conceivably tremendous effect on the economy. A cloud gives the hallucination of infinite figuring assets; its versatility liberates application planners from the confinement of a solitary framework. A cloud takes out the requirement for in advance financial responsibility, and it depends on a compensation as-you-go approach. This can possibly draw in new applications and new clients for existing applications, inciting another period of all-inclusive innovative headways. There can be various models of distributed cloud computing however it is comprehensively separated into three classifications:

- IaaS (infrastructure as a service): redirects the equipment working behind it and authorizations clients to expend foundation as a convenience with no burden about the fundamental issues.
- PaaS (platform as a service): expands upon IaaS and gives customers access to the basic working programming and discretionary suppliers to create and utilize programming applications without programming establishment.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

- SaaS (software as a service): empowers the customers to get to online applications and programming that are facilitated by CSPs.

The arrangement model of distributed cloud computing include:

- Open cloud: possessed by settlement supplier and its assets are leased or sold to the general population.
- Private cloud: It is claimed or purchased by an organization.
- Group Cloud: It is similar to the private cloud yet cloud assets are shared among some groups.
- Mixed cloud: It displays the property of two or more arrangement models.

Data Security in Cloud:

Data security has always been a major issue for any person or organization dealing with sensitive data. Network attacks, hacking, listening to communication as well as unauthorized access to data can cause serious security risks. The data can be accessed even by the insiders who are a part of the organization and who can access that data even when they are not expected or allowed to do so. Thus, security of data is one of the major concerns for such organizations. If data gets compromised, it can not only lead to loss of important information but also cause major financial losses and thus huge risks and hazards are inflicted on the organizations that owned the data.

Cloud Computing has provided businesses with a great platform to store large amounts of data and provide tools and platform for performing multiple kinds of operations. It saves money in the form of resources as well as overheads of transferring and sharing data between multiple users belonging to that organization. It also allows multiple users to collaborate and work together in a more effective manner. However, the data that is stored in cloud faces serious issues related to privacy and security. In such cases, the amount of security provided to that data becomes the responsibility of the host cloud, not of the users or organization that uploaded the data. Also, the fact that these clouds do not allow outsiders to check and manage their security techniques may result in a monopoly that can be a threat to the clients who uploaded the data because they have to depend on the Cloud Service Providers for that.

Once the data is uploaded to the cloud, the owner of the data files loses control on it, and it goes public because the cloud is accessible to anyone who can provide authentication. Many issues related to this are:

- Sometimes, it is possible for outsiders to use fake accounts with copied or stolen authentication information to access the data stored in Public Clouds.
- In Private Clouds, security is higher but still it is possible for attackers to obtain the authentication and authorization information somehow via unfair means and gain access to the data uploaded by the members of the cloud owner organization.
- Another very important issue is the external connection through which the data is uploaded to the cloud. Even if the data is secure internally, as soon as it leaves the secure private networks or Virtual Private Networks (VPN) of that organization, the external connection might not be secure enough to keep the file safe from external threats that can hack into or listen to the data being transferred towards the cloud.

Insider threats are also very significant sources of risk. Insiders can be of two types:

- Insiders present in the organization network who are authenticated as members of the network but are not authorized to access the data without permission from the owners of the data or organization's management.
- Insiders present in the cloud who have access to the cloud storage of the organization but are not authorized to access certain uploaded files.
- Insiders present in the cloud who were previously allowed to access those files but

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

whose status was updated by the organization but the information needed to eliminate such users was not propagated to the cloud.

Existing System:

In traditional public-key cryptography, a message is encrypted for a specific user using the user's public-key. The existing system of cloud storage is based on encryption of the file and storage in an single server after the user provides a key for encryption. The file is decrypted and retrieved from the single server with the key.

Existing System Disadvantages:

- A single server storage is easy to access or modify by external attacks.
- Data is secured only through encryption using a public key provided by the user.
- Data is entirely lost or corrupted if the single server is accessed.

Proposed System:

The proposed system is based on distributed storage of the file after encryption and additional splitting of the file, in multiple storage locations. The file will be combined and decrypted using the user's key for retrieval. Various virtual server storages are created in the cloud storage to increase the difficulty in identifying the storage location of the file. The encrypted file is divided to append security. If a single storage server is lost or hacked or the file is modified, the data cannot be used by the hacker and the proposed system identifies the attempt of corrupting or accessing the data by non-user.

Proposed System Advantages:

- The file is stored in multiple locations after splitting and increases security.
- The file cannot be used or accessed before joining and decrypting the data if it's retrieved by a non-user from a single storage location.
- Any process of access by non-user is identified through the system.
- Data loss or corruption is identified by MD5 Hashing.

III. PROJECT DESCRIPTION

Data security has been the most important requirement since the data is stored on cloud servers. General encryption of data to protect has become vulnerable and the requirement of additional levels of security has grown in demand for cloud storage.

Therefore we focus on the file security where the normal access to storage location of the file does not reveal the data inside to the other users. We ensure that the data is secured multiply and guarded if there's a potential risk or access.

Problem definition

Storage of data in a single server is always not secure because the storage location is always available to different users and the file is entirely saved as a whole in the location along with the encryption provided by the user's key. The server's data can be hacked or corrupted easily and the information can be retrieved. The server can be down causing the user loss of data and the user can not know if the data is modified.

Algorithms used:

AES Algorithm

The Advanced Encryption Standard (AES) is an encryption algorithm for securing delicate however unclassified material by U.S. Government organizations and, as a reasonable result, may in the long run turned into the true encryption standard for business exchanges in the private division. (Encryption for the US military and other grouped correspondences is taken care of by independent, mystery algorithms.)In January of 1997, a procedure was started by the National Institute of Models and Technology (NIST), a unit of the U.S. Trade Department, to locate a more powerful trade for the Data Encryption Standard (DES) and to a lesser degree Triple DES.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The particular required a symmetric calculation (same key for encryption and unscrambling) utilizing piece encryption (see block figure) of 128 bits in size, supporting key sizes of 128, 192 and 256 bits, as a base. The calculation was required to be sans sovereignty for use worldwide and offer security of an adequate level to ensure information for the following 20 to 30 years. It was to be anything but difficult to actualize in equipment and programming, and also in limited situations (for instance, in a smart card) and offer great protections against different assault techniques.The whole determination procedure was completely open to open investigation and remark, it being chosen that full perceivability would guarantee the most ideal investigation of the outlines.

AES is based on a design principle known as a Substitution permutation network. It is fast in both software andhardware. Unlike its predecessor, DES, AES does not use a Feistelnetwork.AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits. The blocksize has a maximum of 256 bits, but the key size has no theoretical maximum. AES operates on a 4×4 column-major order matrix of bytes, termedthe state (versions of Rijndael with a larger block size have additional columns in the state).

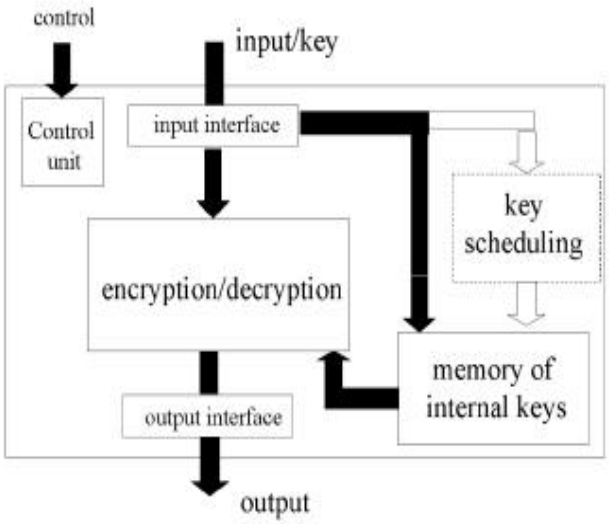


Fig.1 Hardware implementation of AES

Most AES calculations are done in a special finite field.The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

MD5 Algorithm

MD5 is an algorithm that is utilized to check information integrity through the production of a 128-piece message digest from information (which might be a message of any length) that is guaranteed to be as novel to that particular information as a unique mark is to the particular person. MD5, which was produced by Professor Ronald L. Rivest of MIT, is planned for use with computerized signature applications, which require that substantial documents must be compacted by a safe technique before being encoded with a mystery key, under an open key cryptosystem.

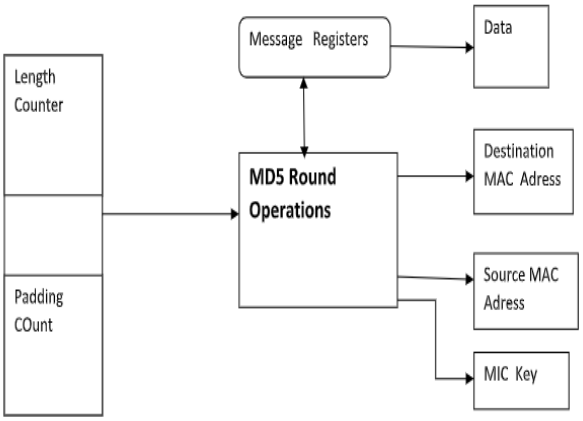


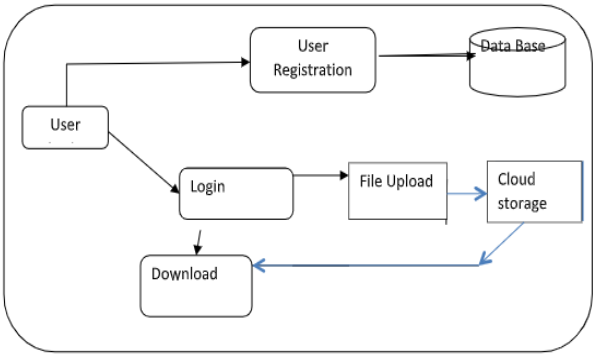
Fig.2 MD5 Round operations

Modules Description

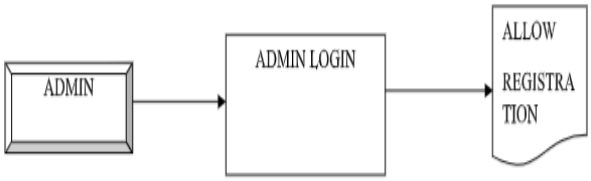
User Interface Design:

The user interface design is the entire knowledge of the user about the project from front view without the knowledge about the process behind .The user is able to view the forms to register , login, upload and download a file.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



Admin Login:



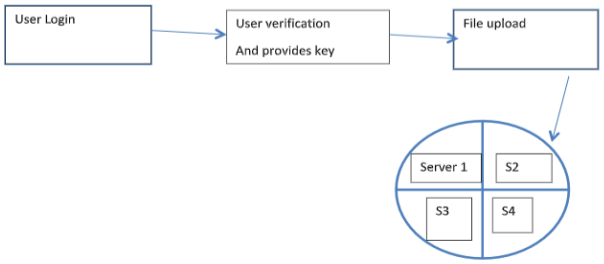
This module allows the admin to login and start the system and maintain users or allow registrations. This module is accessed from the homepage. The details about the admin can be changed in the database only by the admin.

User Registration:

The user has to provide various registration details into the form to enable his account and store his files in the cloud system. The user has to provide a 16 bit key as AES uses 16 bit key to encrypt the file. These details will be stored in the database and is used to verify or decrypt the file in later stages.

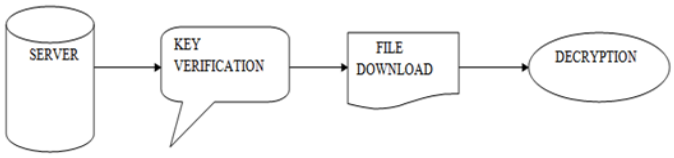
File upload:

The user should login and provide the file location to upload after verification and the file is stored after encryption and splitting into various virtual server storage in the cloud.



File download:

The user should login with his registration details and provide the private key which is used to encrypt the file to decrypt the file from storage servers.



IV. SYSTEM DESIGN

Use-case Diagram:

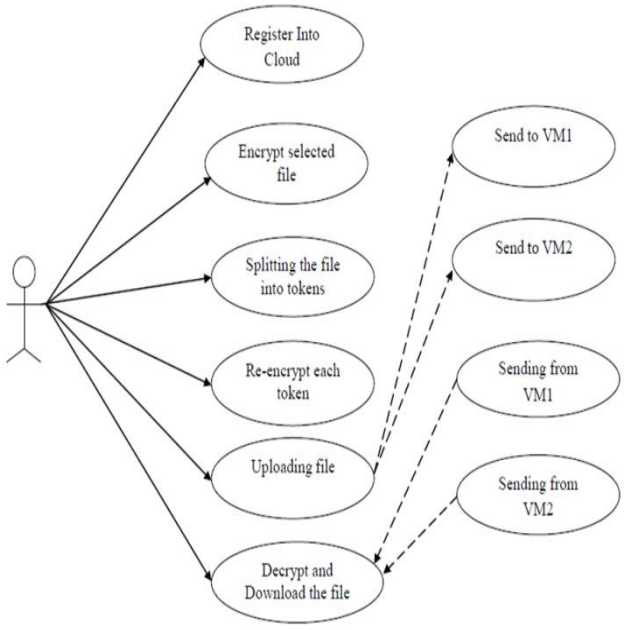


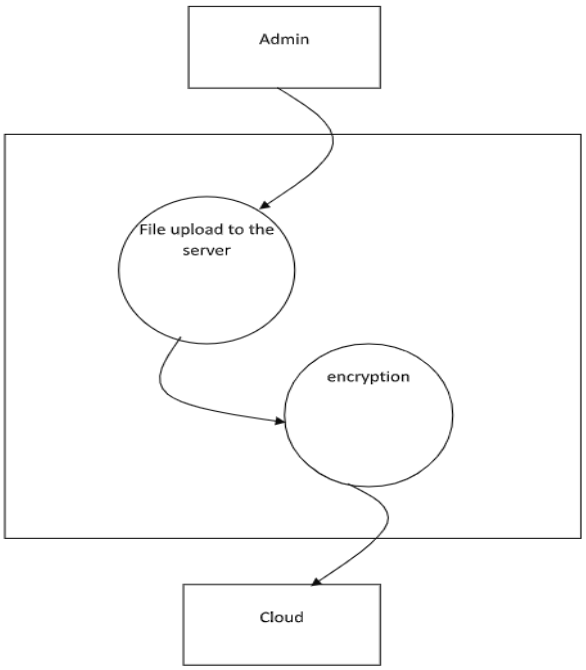
Fig.3: Use-case Diagram

Dataflow Diagram

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Level 0 DFD



Level 1 DFD

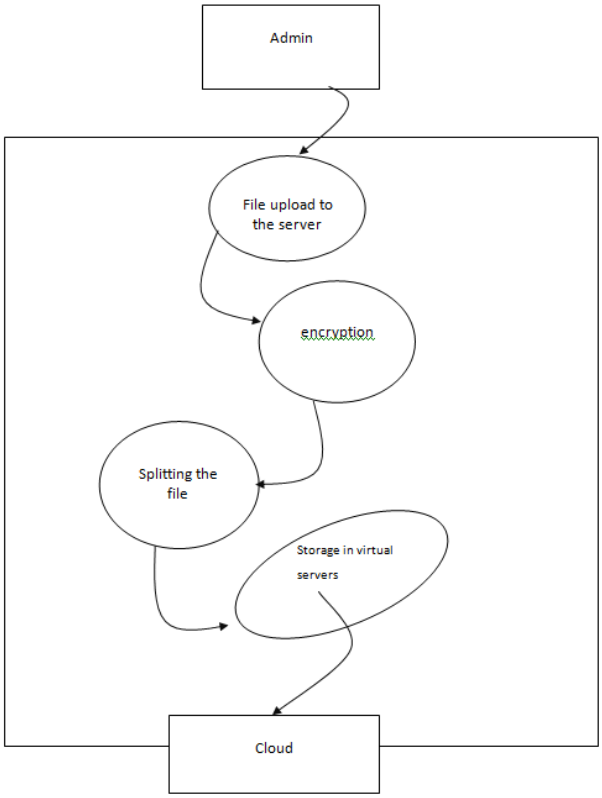
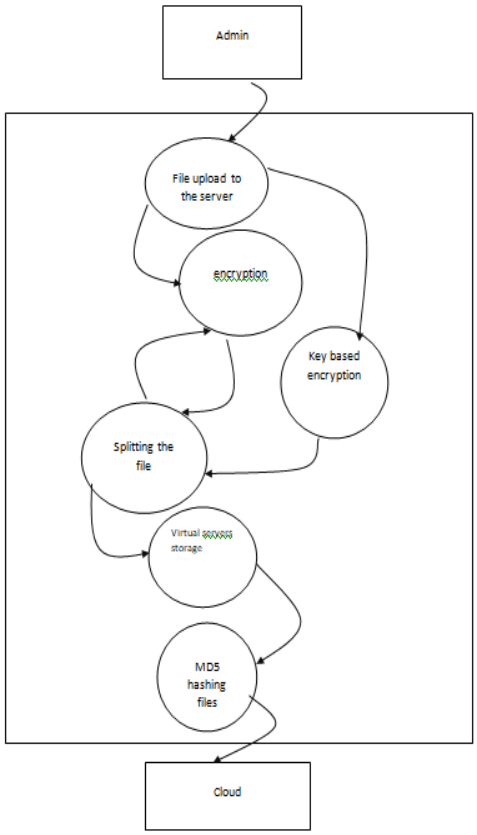


Fig.4: Dataflow Diagram

Level 2 DFD



Sequence Diagram:

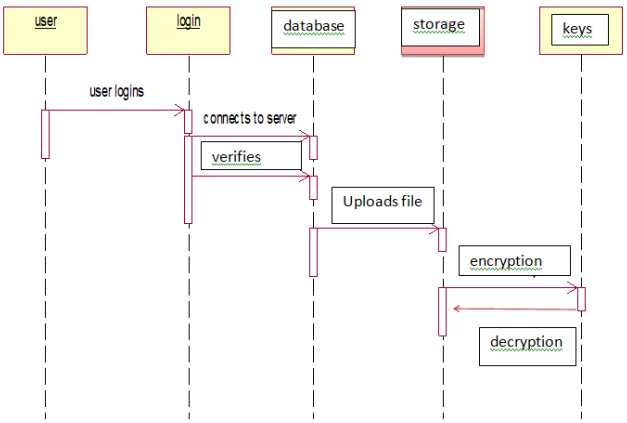


Fig.5: Sequence Diagram

The sequence diagram represents the various processes operating with one another and in which order the uploaded data will be encrypted and it will be stored in the cloud server. After uploading the encrypted file, keywill later be used by the users to access the files

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

during the retrieval phase. Now if any user wants to access a particular file, they need first to provide the necessary authentication keys assigned to the requested files. Once the user provides the key, it is first verified, and the file will then be decrypted, and the user is allowed to access the file and download it.

Collaboration Diagram:

The collaboration diagrams are used to describe interactions among objects regarding sequenced messages. Collaboration diagrams represent a combination of data taken from class, sequence, and use case diagrams to describe both the static structure and dynamic behavior of the system and how the operations are performed.

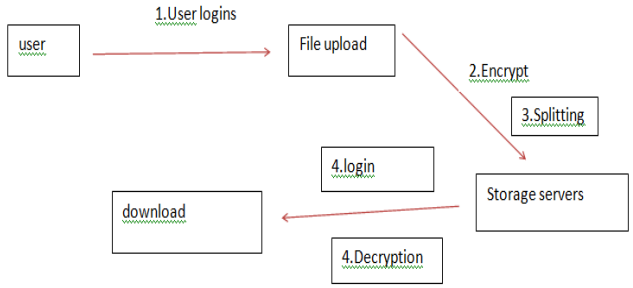


Fig.6: Sequence Diagram

Object Diagram:

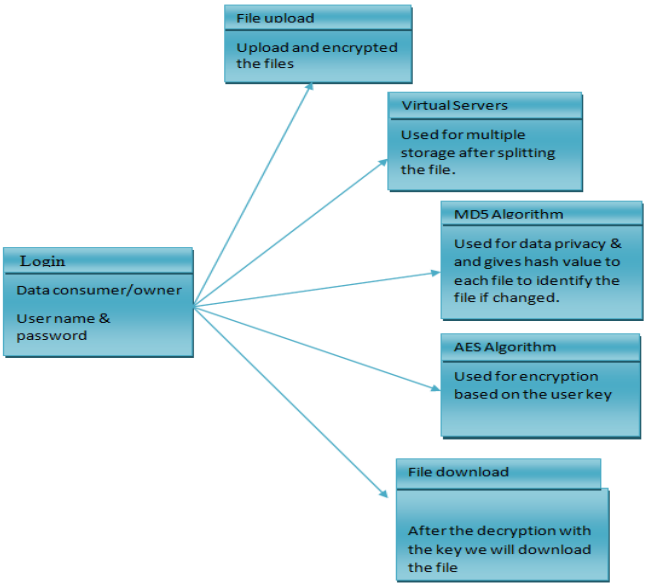


Fig.7: Object Diagram

V. SNAPSHOTS

GENERAL

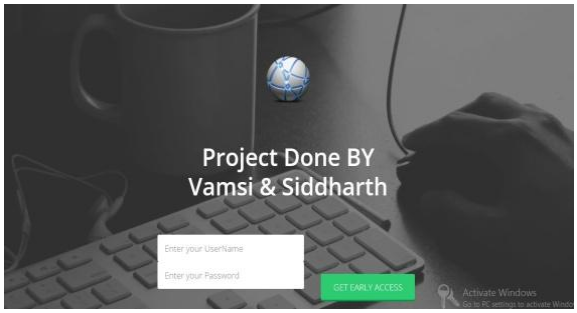
Snapshot is nothing but every moment of the application while running. It gives the clear elaborated of application. It will be useful for the new user to understand for the future steps.

VARIOUS SNAPSHOTS

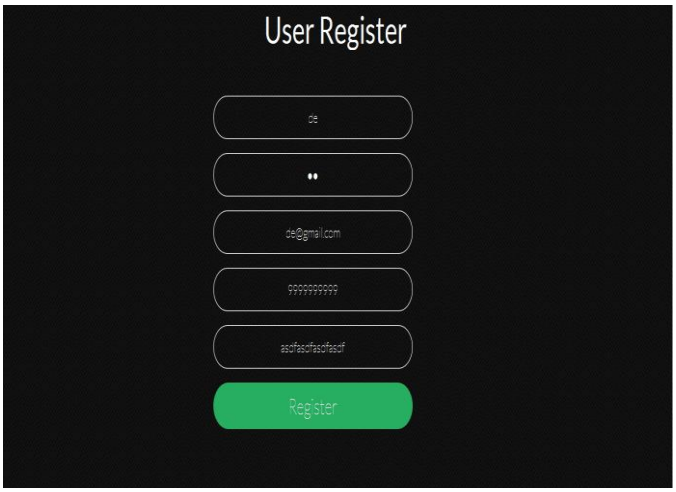
HOMEPAGE:

The homepage consists of the features like admin, upload, download and contact details tabs.

ADMIN PAGE:



USER REGISTRATION:



ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

UPLOAD:

DOWNLOAD:

YOUR SERVER WAS TRIED BY HACKERS

VI. CONCLUSION

This project focused on imparting security to cloud operations where data sharing is involved among various users. Mere encrypted storage of file has become vulnerable to external attacks. So what needs to be done is to enhance the security by distributing the file to various storage locations that not only encrypts the files but also generates different chunks of file with different locations of storage thereby strengthening the security measures. The project provided an enhanced methodology for secure data sharing in clouds.

REFERENCES

[1] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Iacono, and Ninja Marnau, "Security and Privacy Enhancing Multi-Cloud Architectures", IEEE Transaction on Dependable and Secure Computing, Jan 2013.

[2] "An Effective Integrity Check Scheme for SecureErasure Code-Based Storage Systems ,"Shiuan-Tzuo Shen, Student Member, IEEE, Hsiao-Ying Lin, and Wen-GueyTzeng, Member, IEEE

[3] Cong Wang, Qian Wang and Kui Ren, "Ensuring Data Storage Security in Cloud Computing", Department of ECE, Illinois Institute of Technology.

[4] Zhifeng Xiao and Yang Xiao, "Security and Privacy in Cloud Computing", IEEE Communication Survey & Tutorials, Accepted for Publication, March 2012.

[5] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom' "Cloud Computing Security: From Single to Multi-Clouds", International Conference on System Sciences, 2012.

[6] Jing-Jang Hwang and Hung-Kai Chuang, " A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service," National Science Council of Taiwan Government, IEEE ,2012

[7] M. A. AlZain, B. Soh and E. Pardede," MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing," in Proceeding of 2011 Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing, IEEE,2011

[8] Kan Yang, XiaohuaJia, " Attributed-based Access Control for Multi-Authority Systems in Cloud Storage," in Proceeding of 2012 32nd IEEE International Conference on Distributed Computing Systems , IEEE ,2012.