Deduplication and Attribute Based Storage in cloud

A Mini Project Report submitted in partial fulfilment of the requirements for the award of the degree of

Bachelor of Technology

in

Computer Science and Engineering

By

Nishi Chaudhary	**Rashi Bansal**	**Pradduman Yadav**	**Tanishka Bhardwaj**	**Pragati Goswami**
171510032	**171510044**	**171510036**	**171510055**	**171510037**

Under the Guidance of
Ms. Ambika Gupta

Department of Computer Engineering & Applications
Institute of Engineering & Technology

GLA University

Mathura – 281004, INDIA

May, 2020

Department of Computer Engineering and Applications
GLA University, Mathura
17 km. Stone NH-2, Mathura-Delhi Road, P.O. – Chaumuha,
Mathura – 281406

Declaration

We hereby declare that the work which is being presented in the B.Tech Project “Attribute Based Storage Supporting Deduplication”, in partial fulfillment of the requirements for the award of the *Bachelor of Technology* in Computer Science and Engineering and submitted to the Department of Computer Science and Applications of GLA University, Mathura. It is an authentic record of our work carried out under the supervision of Ms. Ambika Gupta, Assistant Professor, and GLA University.

The content of this project report, in full or parts, has not been submitted to any other Institute or University for the award of any degree.

Signature:____________
Nishi Chaudhary
171510032

Signature:____________
Pradduman Yadav
171510036

Signature:____________
Pragati Goswami
171510037

Signature:____________
Tanishka Bhardwaj
171510055

Signature:____________
Rashi Bansal
171510044

Certificate

This is to certify that the above statements made by the candidate are correct to the best of my /our knowledge and belief.

Supervisor
Ms. Ambika Gupta
Assistant Professor (Dept. Of CEA)

Project Co-Ordinator
(Mr. Saurabh Anand)

Date:

ACKNOWLEDGEMENT

We would like to express our gratitude to the people who have been instrumental in the successful completion of this project. We are highly indebted to our **Professor Anand Singh Jalal, Head of Department of Computer Science Engineering and Application** for the facilities provide to accomplish this project and for his help and encouragement.

The success of any project depends largely on the encouragement and guidelines of many others. We would like to show our greatest appreciation to **Ms. Ambika Gupta**, our project mentor. We can’t say thank you enough for her tremendous support and help. We feel motivated and encouraged every time we attend her meeting. Without her encouragement and guidance, this project would not have materialized. The guidance and support received from all the members who contributed and who are contributing to this project were vital for the success of the project. We are grateful for their constant support and help.

ABSTRACT

The definition of nowadays is with the data all around, there is a lot of data regarding with each fellow. There are many platforms to handle this data, but when it comes to similar data it is difficult to distinguish between multiple files that which two files are similar or not. When we upload the files or folders on the cloud then there may be some files that are repeated in the storage, to remove the duplicate files and maintain the security of files by encrypting the files we have proposed this paper in which we do the encryption and decryption based on attributes. Attributes are the specific credentials of the users with whom the uploaded files will be shared. The attributes are selected by the provider who will outsource his data on the cloud and want to share with the users matching with the same attributes.

In this paper we have created a website by which the data providers can upload their data on the cloud by selecting their specific credentials and then the attribute based users can then access those files from their portal. The website will be able to find the duplicate files so that the storage and network bandwidth can be optimized.

Table of Contents

List of Figures

Chapter 1
Introduction

Attribute-based encryption (ABE) is regarded as an effective encryption method with fine grained access control in the cloud storage. Attribute-based encryption can be divided into two types of key-policy attribute-based encryption (KP-ABE) and ciphertext-policy attribute-based encryption (CP-ABE). The KP-ABE scheme refers to that the ciphertext is associated with an attribute set, and a user's secret key is associated with an access policy. A user can decrypt the ciphertext if and only if the ciphertext's attribute set satisfy the access policy of user’s secret key. The CP-ABE scheme refers to that the ciphertext is associated with an access policy, and a user's secret key is associated with an attribute set. A user is can decrypt the ciphertext if and only if his attribute set satisfy the access policy of the ciphertext.

Although attribute based encryption technology provides an effective means for data confidentiality, yet it brings another new problem that the users may find it difficult to search for interesting data from a vast number of encrypted data. This problem is called keyword search problem. One of the simplest searching methods is to download all encrypted data locally and then to decrypt it, finally to execute keyword search in plaintext. However, this method will waste huge computational resource and bring a vast cost for user to do the work of decryption.

1.1 USES OF SOME TOOLS-

DriveHQ is a cloud platform providing storage as a service, has offered reliable cloud file storage & sharing service to businesses and consumers

HTML (Hypertext Markup Language) is the most basic building block of the Web. It defines the meaning and structure of web content. Other technologies besides HTML are generally used to describe a web page's appearance/presentation (CSS) or functionality/behaviour (JavaScript)

Bootstrap is an open source toolkit for developing with HTML, CSS, and JS. Quickly prototype your ideas or build your entire app with our Sass variables, responsive grid system, extensive prebuilt components, and powerful plugins built on jQuery.

1.2 Contribution

In this paper, we present an attribute-based storage system which employs ciphertext-policy attribute-based encryption (CP-ABE) and supports secure deduplication. Our main contributions can be summarized as follows.

- Firstly, the system is the first that achieves the standard notion of semantic security for data confidentiality in attribute-based deduplication systems by resorting to the hybrid cloud architecture.

- Secondly, we put forth a methodology to modify a ciphertext over one access policy into ciphertexts of the same plaintext but under any other access policies without revealing the underlying plaintext. This technique might be of independent interest in addition to the application in the proposed storage system.

- Thirdly, we propose an approach based on two cryptographic primitives, including a zero-knowledge proof of knowledge and a commitment scheme, to achieve data consistency in the system.

1.3 Motivation

The cloud is a very popular in today's world. The industries from every field are moving to the cloud. To access the services of cloud one must need a proper network to the public network and also there is excess of storage though but it is more time taking to fetch data, when we have multiple same files on the cloud server. These problems are occurring in the cloud and we are motivated as this is a current problem and if this problem will be eliminated then the security of attribute based encryption will give a next level in the access controls and authentication of the cloud. Also the network bandwidth, which is main problem in our country, will be optimised, as a file already uploaded will not consume network again and again.

Chapter 2
Literature Review

Hui CUI, Robert H. DENG et al. [3] proposes a secure system which can remove the deduplication in the hybrid environment. They discuss the outsourcing of the data by the provider and the removing the duplication of files in the cloud.

Naga Malleswari TYJ and Vadivu G [4], they discuss the existing techniques of deduplication like fixed length of data, variable length of data, and block deduplication of data. Their implementation in the *public cloud* and comparison with the existing techniques of deduplication.

R. SHOBANA, K. SHANTHA SHALINI et al. [5] describe in their paper about the removing duplicate and identical data which is heavily used in *public cloud* storage so as to minimize the storage and save network bandwidth. To maintain the confidentiality of data which is sensitive during removing of the duplication, one encryption method is used to encrypt the data.

According to **Peter Schoo, Volker Fusenig** et al. [2] there are some challenges in the cloud security network which are discussed in their paper. The challenges are grouped in various categories like content protection in *public cloud*, distribution transparency control, security in virtual technology, and secure the private operations.

B. Tirapathi Reddy, U.Ramya, Dr.M.V.P Chandra Sekhar et al. [1] discuss about the deduplication in cloud as according to them in future cloud storage will be playing an essential role for all remote users, as it helps in reducing the overhead of data management and minimization of storage cost. They introduced the concept of *tokens* for the duplicate files which are generated by the *cloud* server having secret keys, and also they discussed about the duplication check in the hybrid environment.

Arvind Kumar Maurya, Avinash Singh, Unnati Dubey2 Shivansh Pandey and Upendra Nath Tripathi et al. [16] proposed a method to encrypt a transparent data and files to prevent

Unauthorized access to data by restoring the files from anther server. Increasing level of security by encrypting and decrypting data files, log files, backup files without dissolving transparent properties for its users. Applied distributed and encrypted techniques to protect from data loss.

According to **K. V. Pradeep, V. Vijayakumar, and V. Subramaniyaswamy** et al. [17] the data accessed or shared through any device from cloud environment has security concerns like Identity Access Management, hijacking an account or services by internal or external intruder are challenges in cloud environment. Provider has full access to data and key, client cannot trust data provider completely. Author proposed framework to share file in secure public key infrastructure. File shared among users is protected using CKMS ensure authenticity from internal and external users. Key is distributed among users using key transfer protocol.

Yeshwanth Rao Bhandayker et al. [18] describes the challenges and trends in the cloud computing as lots of new brand technologies like mobile technology and emerging to mobile cloud computing, cloud containers are emerging at a quick pace so one need to be highly cautious to recognise security threats and challenges in making use of new technologies. Cloud provider should educate client about the degree of security used.

Chapter 3
Proposed Work

The project Deduplication and Attribute Based Encryption in the cloud is comprised of two aspects which are very important and main portion for every cloud, these are deduplication and Attribute based Encryption. We will first be introducing with both the parts individually in the cloud and then we will be taking our project into consideration in which we have implemented both the phases.

2.1 Deduplication

Deduplication refers to the eliminating of duplicate or redundant data. Data Deduplication storage is a process that eliminates redundant copies of data to reduce storage overhead. Data deduplication aligns with the incremental backup, which copies only the changed data.

In cloud the deduplication is very normal as all the cloud platforms has a good number of users and using storage as a service in the cloud is frequent nowadays. Over millions of data is uploaded on the cloud every day. The data on the cloud can be of various kind, most of the data uploaded is the replication of one another. There are two major problems of having unwanted replicate data, first is that it occupies the extra storage, we know that cloud is said to be a large pool of the resources and storage is the major service available on the cloud, but all the storage is actually a physical storage somewhere, so to optimise the storage we should work on eliminating multiple replicates of a file. Now, secondly when the duplicate files present on the cloud already are again being uploaded by other users, it consumes a lot of network bandwidth to upload them, if we can the existence of the data before uploading it then the time and cost of uploading data can also be eliminated.

As we know there is no proper standard of the services provided by cloud computing vendors so far, and we also do not know that how the public cloud providers store and arrange their data on their servers. So to apply the deduplication on the cloud depends on the cloud vendor and also it could be a tedious task to do so.

We are working on this problem and has created a simulation by using public cloud and private cloud together. We have created a website which will be having various kind of users with different access policies.

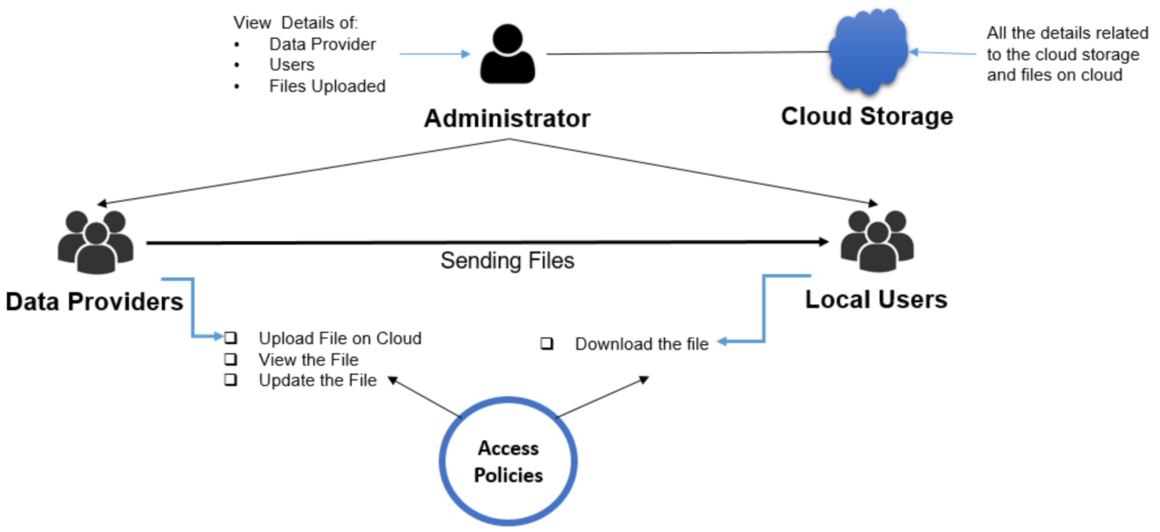


Fig 2.1: Access Policies provided to roles

The above figure give a complete description of the policies and rights given to each individual based on their roles in the website or the portal.

2.2 Attribute Based Encryption

Attributes are the piece of information which determines the properties of some data. Attribute based encryption is a type of public key encryption in which the secret key of the user and the ciphertext are dependent upon attributes, the attributes can be the country in which they live or the subscription they have. In AES, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. There are mainly two types of attribute-based encryption schemes: Key-policy attribute-based encryption (KP-ABE) and ciphertext-policy attribute-based encryption (CP-ABE).

In KP-ABE, users' secret keys are generated based on an access tree that defines the privileges scope of the concerned user, and data are encrypted over a set of attributes. However, CP-ABE uses access trees to encrypt data and users' secret keys are generated over a set of attributes.

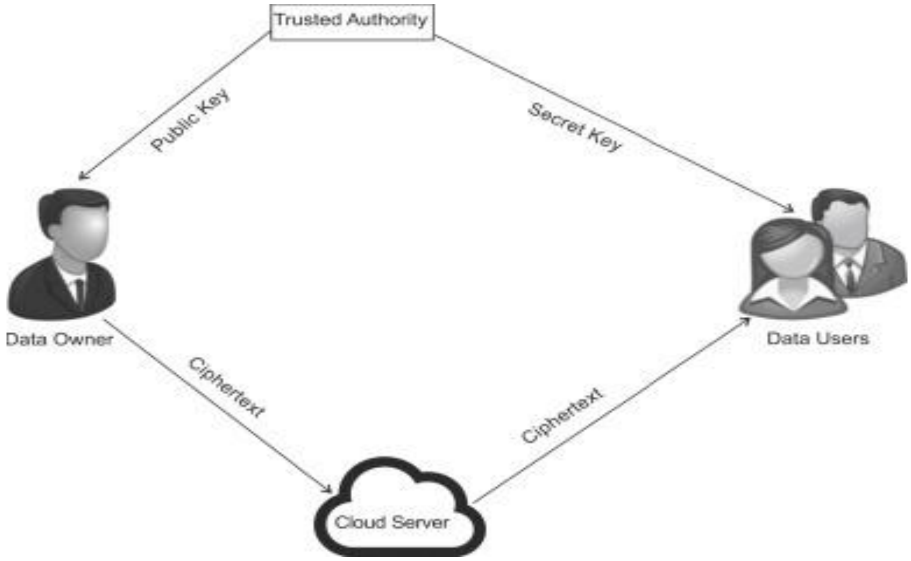


Fig 2.2: Attribute Based Encryption in the cloud

The above picture can give a view of how actually attributes are related with the data owner and how the encryption and decryption of the data, in cloud having ABE, takes place.

If we go to our project then we can distinguish our roles based on the figure. The data owner is termed as Data Provider in our project who will upload the files and can view them and update them. The files uploaded by the data provider will be encrypted files. Then there are the users who will be receiving those encrypted files. The trusted authority here is the administrator who will be having all the access rights and the secret key for decryption will be shared with him only. The secret key will then be send to authorize and authenticated users by the admin.

The cloud server will be a public cloud server where all the files uploaded will be stored and the user will be given the redirected links to download the file from the server.

If we talk about a rough idea then, in ABE, the data is shared by the owner only with specified attributes. All the users those are the part of that attributes will be receiving the file and only they should be getting the secret key which will be helping them to decrypt the files and view them.

Chapter 4

Implementation of the Project

We are very well known what deduplication and attribute based encryption individually means in the cloud. Now, we will be proposing the solution including both the parts in our project.

3.1 About the website

We have used basic HTML, CSS, Bootstrap, JavaScript and PHP as the main languages for the creation of the website. We have discussed these languages in the introduction section, so we will continue with the development part.

The website is a access based website, in which there are different logins for different type of users, and we have added the sessions for every user. No unauthenticated user can access the data of other users. Proper credentials of everyone is being maintained using MySQL.

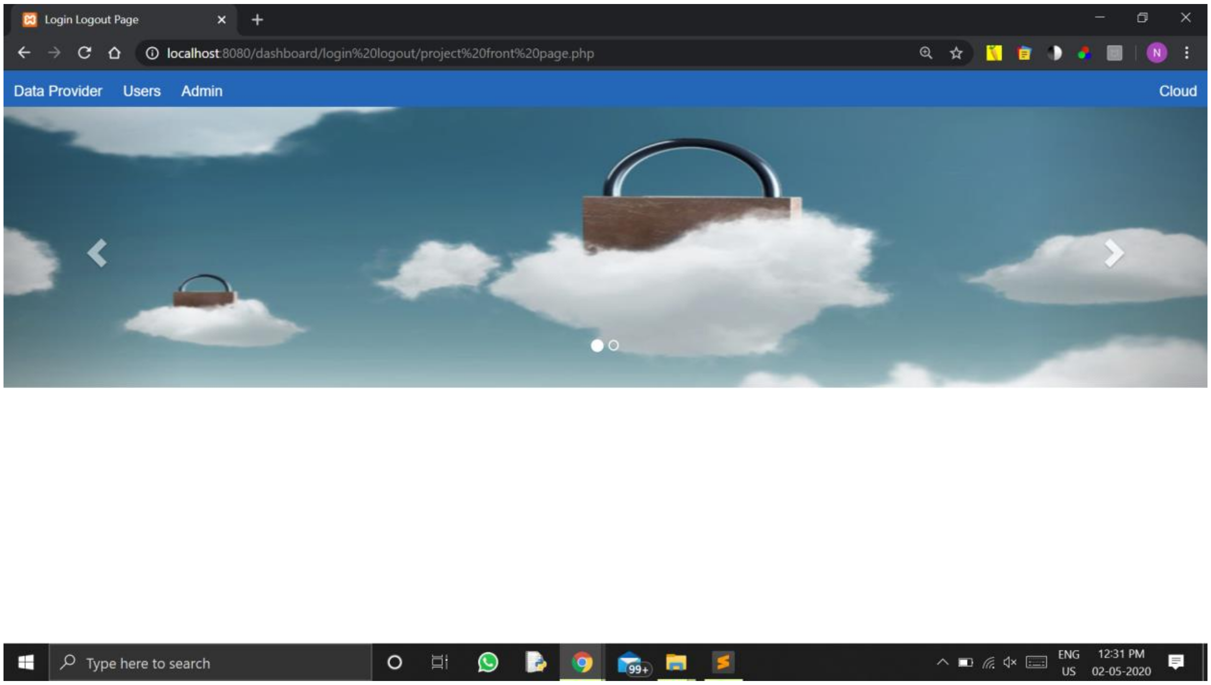


Fig 3.1: Main page of the website

3.2 Structure of the project

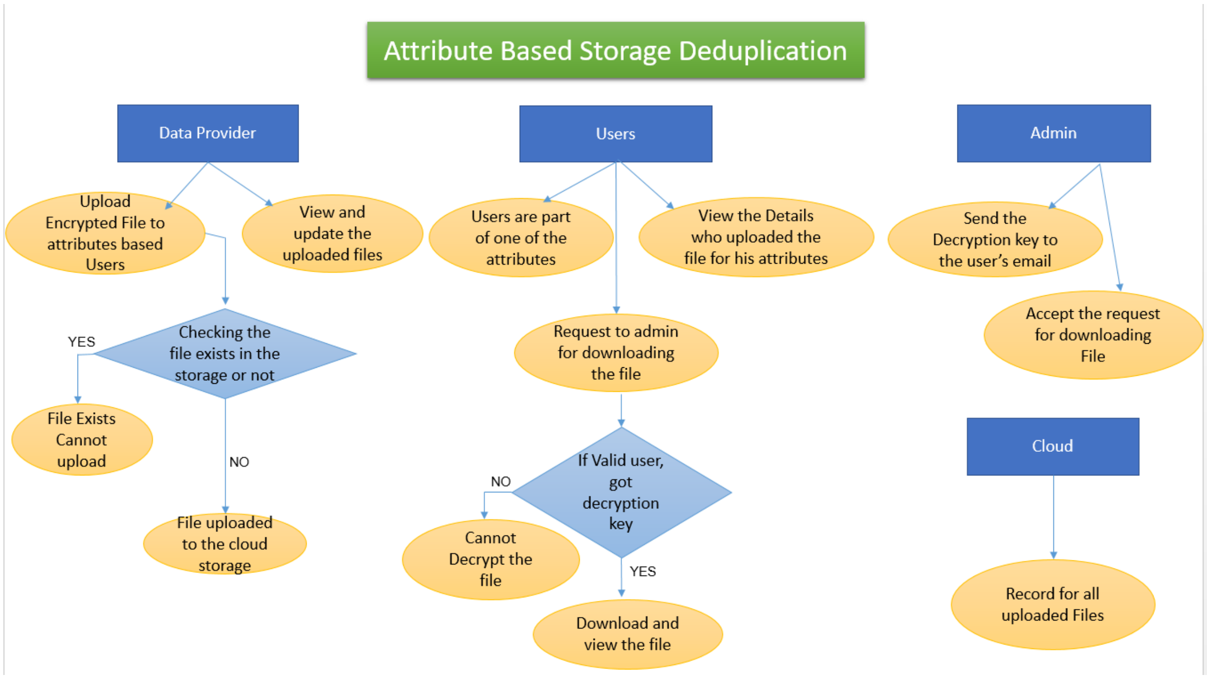
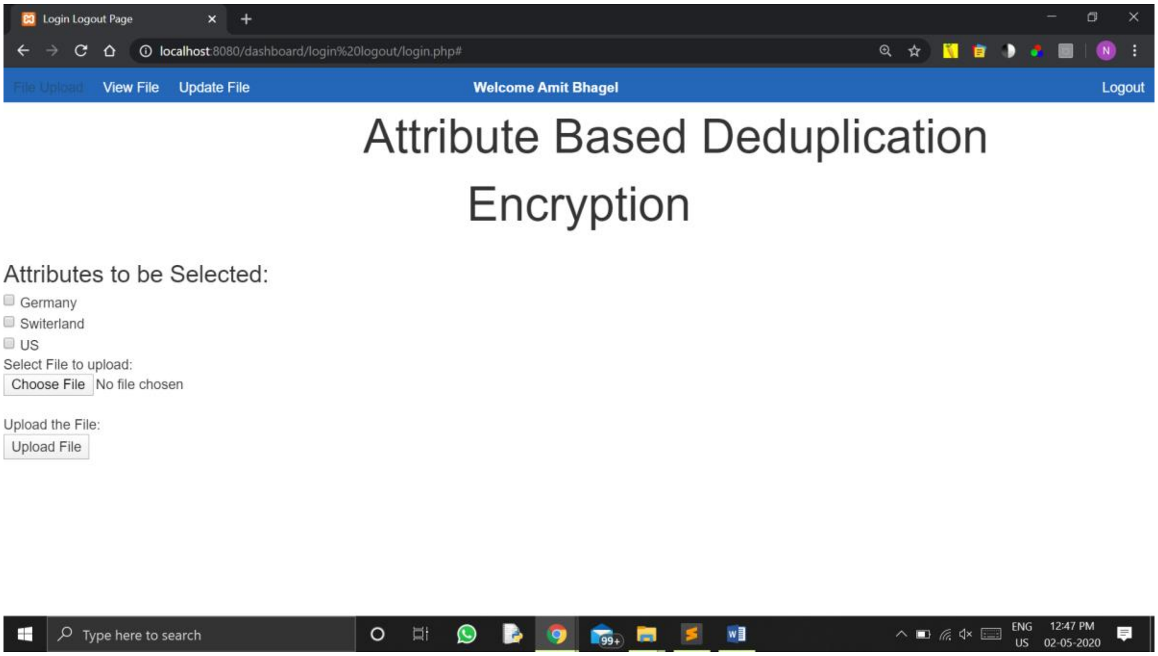

Attribute Based Storage Deduplication
Data Provider
Users
Admin
Upload Encrypted File to attributes based Users
View and update the uploaded files
Users are part of one of the attributes
View the Details who uploaded the file for his attributes
Send the Decryption key to the user's email
Accept the request for downloading File
YES
Checking the file exists in the storage or not
File Exists Cannot upload
NO
File uploaded to the cloud storage
Request to admin for downloading the file
NO
If Valid user, got decryption key
Cannot Decrypt the file
YES
Download and view the file
Cloud
Record for all uploaded Files

Fig 3.2: Structure of the website

The clear structure of the project is shown above. The data provider is able to upload the files to the attributes and he can view and upload the files. The data provider's page of uploading the file.



Attribute Based Deduplication Encryption

Attributes to be Selected:

□ Germany
□ Switerland
□ US

Select File to upload:

Choose File No file chosen

Upload the File:

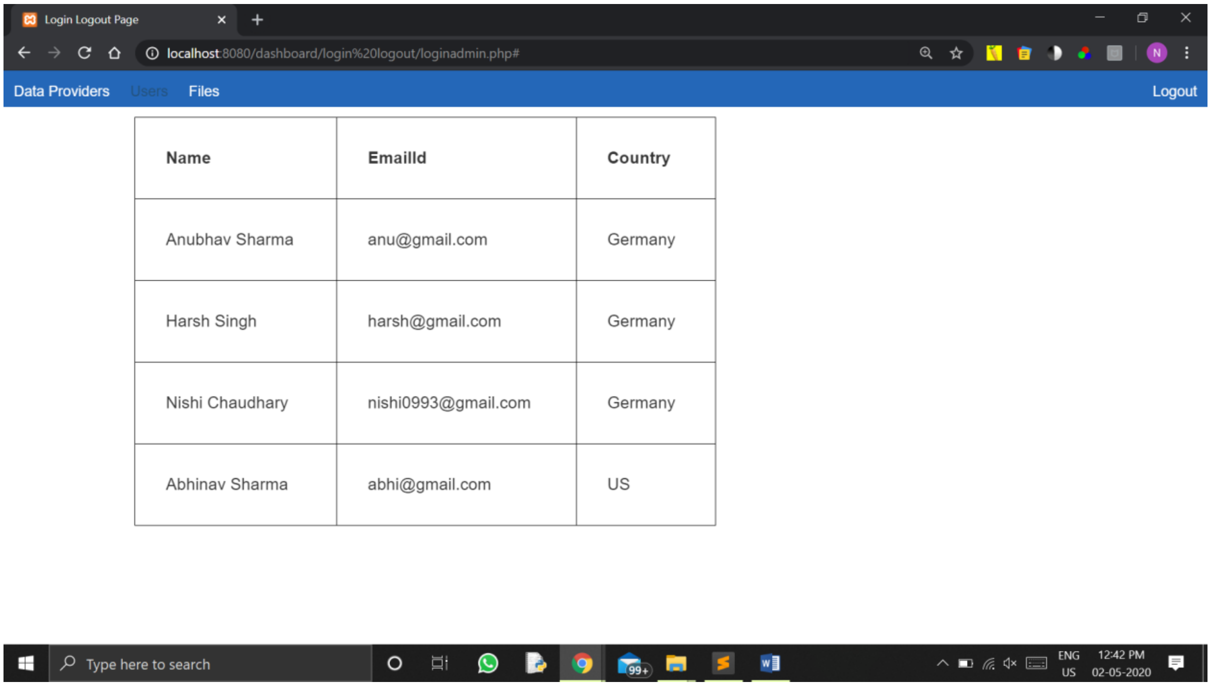
Upload File

Fig 3.3: Data Provider portal, File uploading based on attributes

The data provider will upload the file and a PHP code in the backend will run to check whether the file the data provider wants to upload is present on the server already or not. If the code finds the file with same name then it would show that ‘the file already exists and it do not upload it again’. And if the file do not exist then it will upload the file to the server. We have already discussed that the file uploaded will be an encrypted file, encrypted with a secret key. He can also view the file and update the same.

Now comes the user who will be the part of one of the attributes. In our scenario we have taken three countries: Germany, Switzerland and USA. The user must be an authenticated user, by their credentials he will be able to login and would be receiving the files based on their attributes. The files are decrypted by the secret key so they first have to request to the admin for granting him the secret key. When they got the key they will be able to download the file and decrypt the same.

The administrator is the complete controller of the website. He will be accessing all the data related to the users and data providers. His job is to send the secret key to the users.



Name	EmailId	Country
Anubhav Sharma	anu@gmail.com	Germany
Harsh Singh	harsh@gmail.com	Germany
Nishi Chaudhary	nishi0993@gmail.com	Germany
Abhinav Sharma	abhi@gmail.com	US

Fig 3.4: Users details in Admin Portal

3.3 Encryption and Decryption

Encrypting a data refers to hiding the actual data with an unreadable data. We will be converting the plain text into a ciphertext and sending it to the appropriate receiver. There is a channel between the sender and the receiver by which they communicate with each other. Encryption provides confidentiality of the data.

Decryption is the reverse process of encryption, in this we convert the ciphertext into the same plane text. It is done by the receiver when he gets the encrypted data then to make it in a readable form he decrypt it and then can view the actual data. In this way the data shared between two remain secret and not be read by any intruder or third party.

There is mainly two type of encryption: Symmetric Encryption and Asymmetric Encryption.

Symmetric encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic information. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process. This encryption method differs from asymmetric encryption where a pair of keys, one public and one private, is used to encrypt and decrypt messages.

By using symmetric encryption algorithms, data is converted to a form that cannot be understood by anyone who does not possess the secret key to decrypt it.

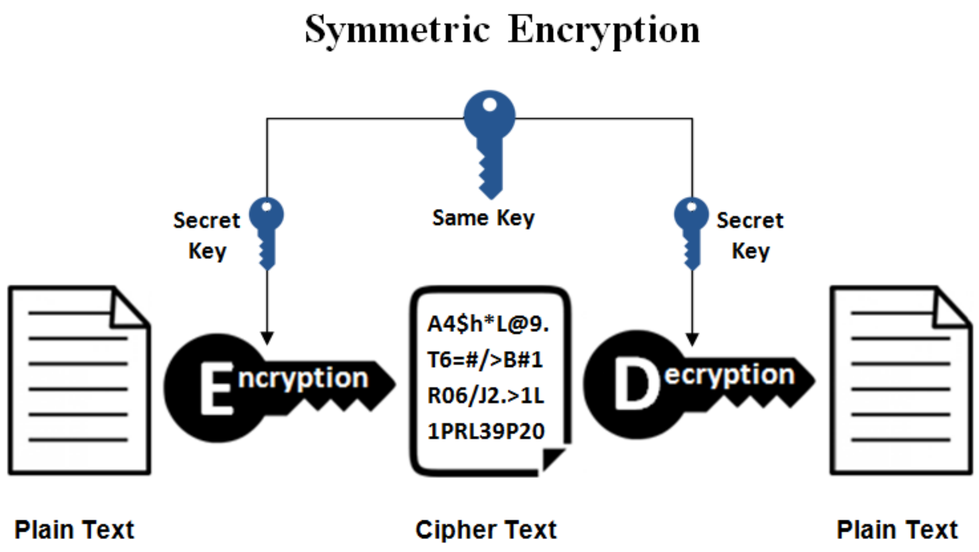


Fig 3.5: Symmetric key encryption

Example for the symmetric key encryption are: AES (Advanced Encryption Standard), DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), Blowfish (Drop-in replacement for DES or IDEA), RC4 (Rivest Cipher 4), RC5 (Rivest Cipher 5), RC6 (Rivest Cipher 6).

Asymmetric Encryption encrypts and decrypts the data using two separate yet mathematically connected cryptographic keys. These keys are known as a '**Public Key**' and a '**Private Key**.' Together, they're called a 'Public and Private Key Pair.'

Asymmetric Encryption uses two distinct, yet related keys. One key, the Public Key, is used for encryption and the other, the Private Key, is for decryption. As implied in the name, the Private Key is intended to be private so that only the authenticated recipient can decrypt the message. Let's understand this with a simple asymmetric encryption example.

Pretend you're a spy agency and you need to devise a mechanism for your agents to report in securely. You don't need two-way communication, they have their orders, you just need regular detailed reports coming in from them. Asymmetric encryption would allow you to create public keys for the agents to encrypt their information and a private key back at headquarters that is the only way to decrypt it all. This provides an impenetrable form of one-way communication.

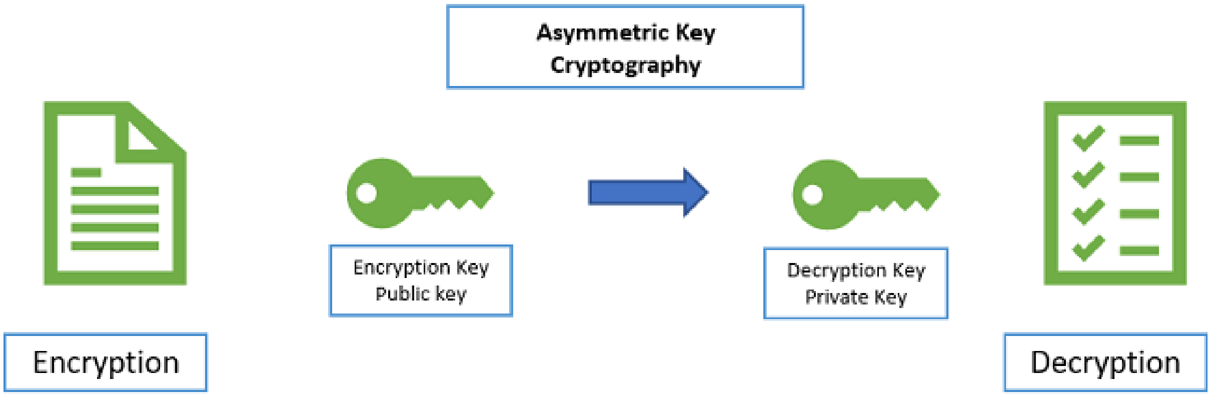

Asymmetric Key Cryptography
Encryption Key Public key
Decryption Key Private Key
Encryption
Decryption

Fig 3.6: Asymmetric Key Encryption

Example of asymmetric encryption are: RSA, Diffie Hellman, ECC, EL Gamal, and DSA.

There are many algorithms which we can use for the encryption but we have used AES in our project because there are following benefits of using AES algorithm:

- As it is implemented in both hardware and software, it is most robust security protocol.
- It uses higher length key sizes such as 128, 192 and 256 bits for encryption. Hence it makes AES algorithm more robust against hacking.
- It is most common security protocol used for wide several of applications such as wireless communication, financial transactions, e-business, encrypted data storage etc.
- It is one of the most spread commercial and open source solutions used all over the world. No one can hack your personal information.
- For 128 bit, about 2^{128} attempts are needed to break. This makes it very difficult to hack it as a result it is very safe protocol.

3.4 AES

The most commonly used symmetric algorithm is the Advanced Encryption Standard (AES), which was originally known as Rijndael. This is the standard set by the U.S. National Institute of Standards and Technology in 2001 for the encryption of electronic data announced in U.S. FIPS PUB 197. This standard supersedes DES, which had been in use since 1977. Under NIST, the AES cipher has a block size of 128 bits, but can have three different key lengths as shown with AES-128, AES-192 and AES-256.

- AES is the short form of Advanced Encryption Standard.

- It is FIPS approved cryptographic algorithm used to protect electronic data.

- It is symmetric block cipher which can encrypt and decrypt information.

- Encryption part converts data into cipher text form while decryption part converts cipher text into text form of data.

- AES algorithm used different keys 128/192/256 bits in order to encrypt and decrypt data in blocks of 128 bits.

- AES is implemented in both hardware and software to protect digital information in various forms data, voice, video etc. from attacks or eavesdropping.

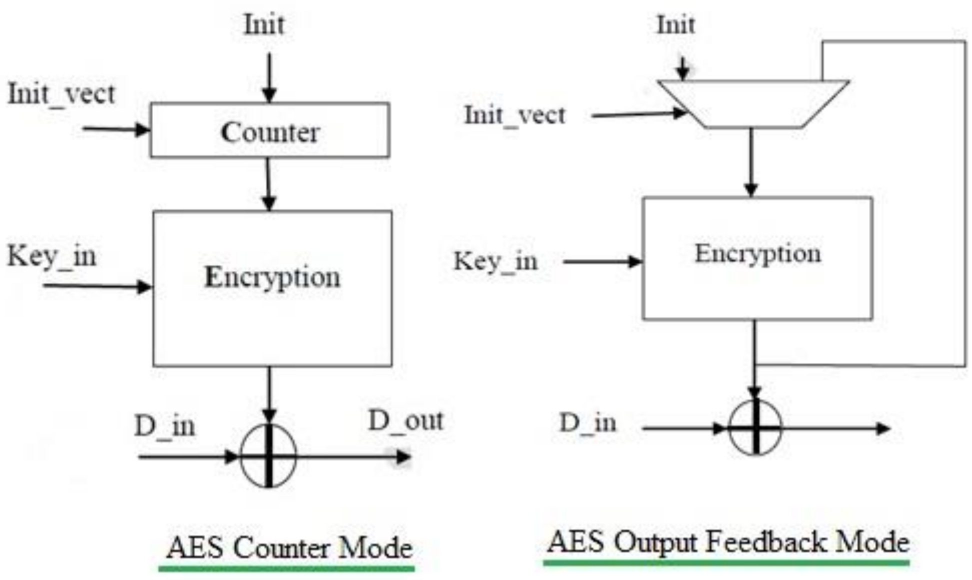


Fig 3.7: Attribute Based Encryption

The figure-3.7 depicts two modes of AES algorithm viz. CTR (counter) mode and OFB (Output Feed Back) mode.

In CTR (counter) mode, the output of the Counter is the input for the Encryption core and an initialization vector is used to initialize the counter. Input data is encrypted by XOR'ing it with the output of the Encryption module. The data coming out after this operation is called cyphertext. Decryption reverses the encryption operation.

In OFB mode, the output of the Encryption operation is fed back to the input of the Encryption Core. An initialization vector is used for the first iteration. Input data is Encrypted by XOR'ing it with the output of the Encryption module.

AES type	Key Length (Nk words)	Block Size (Nb words)	Number of rounds (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

The table above mentions three types of AES based on key lengths used in the algorithm.

3.5 Procedure of the project

The project is a website created to implement the above scenario.

- Creation of the website using PHP
- Encryption of files by data provider
- Data Owner uploading the files on the cloud server based on the attributes
- Deduplication checking at the data owner side
- The admin get the secret key for decryption
- The user will get the notification of the file uploaded
- User will request to admin to download the file
- Admin will then grant permission and accept the user to download
- Admin will provide the secret key to the authenticated user
- The secret key will be send on the email ID of the user
- The user will copy the secret key and paste it in the portal
- Then the user will download the file
- The file will then be decrypted by the secret key
- The user can now view the file
- Admin will be monitoring the whole process manually
- Admin will be having the details of all the members on the same portal
- Cloud are having all the encrypted files

Chapter 5
Conclusion and Future Work

In this project we have simulated the deduplication in the cloud applying attribute based encryption. The consumption of network bandwidth and storage is being optimised by this implementation. We discuss the importance of deduplication in the cloud and its need. Also we discuss what attribute based encryption means and how do it works in the cloud computing. We learn about the symmetric and asymmetric encryption. We use AES algorithm for the encryption and decryption of the files shared between the sender and receiver.

We try to implement it using the public cloud and doing all the operations on the private end.

4.1 Future Work

The purpose of this project is to have a better understanding of the deduplication and ABE. How they can be used in the cloud to optimise the cloud resources. The website is now a static website. In future we will be using it as a dynamic website and it can be used by the users to share the files among them.

Also we will be adding some security features in future for securing our website from following cyber-attacks like: SQL injections, Cross-site scripting, Credentials Brute Force Attacks, Website malware infections and attacks, etc. We are also looking for creating its application for the public use.

Chapter 6
References

[1]. **B. Tirapathi Reddy, U.Ramya and Dr.M.V.P Chandra Sekhar (2016). "**A comparative study of data deduplication techniques in cloud storage**"** *International Journal of Pharmacy & Technology,* ISSN: 0975-766X.

[2]. **Peter Schoo, Volker Fusenig, Victor Souza, Márcio Melo, Paul Murray, Hervé Debar, Houssem Medhioub, Djamal Zeghlache (2010).** "Challenges for Cloud Networking Security" *International ICST Conference on Mobile Networks and Management,* HP Laboratories HPL: 2010-137.

[3]. **Hui CUI, Robert H. DENG, Yingjiu LI, Guowei (2017**). "Attribute-based storage supporting secure deduplication of encrypted data in cloud" *Published in IEEE Transactions on Big Data, 2017 January,* 10.1109/TBDATA.2017.2656120.

[4]. **Naga Malleswari TYJ and Vadivu G (2019**). "Adaptive deduplication of virtual machine images using AKKA stream to accelerate live migration process in cloud environment" *Journal of Cloud Computing: Advances, Systems and Applications*, 8:3.

[5]. **R. SHOBANA, K. SHANTHA SHALINI, S. LEELAVATHY and V. SRIDEVI (2016).** "DE-DUPLICATION OF DATA IN CLOUD" *Department of Computer Applications, Aarupadai Veedu Institute of Technology, Vinayaka Missions University, CHENNAI (T.N.) INDIA*, 6, 2933-2938 ISSN 0972-768X.

[6]. AES, URL:" https://proprivacy.com/guides/aes-encryption".

[7]. Advanced Encryption Standard, URL:"https://en.wikipedia.org/wiki/Advanced_Encryption_Standa rd".

[8]. PHP Symmetric encryption and decryption of large files, URL: "https://riptutorial.com/php/example/25499/symmetric-encryption-and-decryption-of-large-files-with-openssl".

[9]. Uploading file on DriveHQ, URL: "https://www.drivehq.com/bbs/getmsg.aspx/bbsID110/msg_id5988980/page28#5988980".

[10]. Download file, URL: "https://www.phptpoint.com/how-to-download-file-in-php/".

[11]. **Cipher text-Policy ABE, URL: "**https://crypto.stackexchange.com/questions/17893/what-is-attribute-based-encryption**".**

[12]. Changji Wang and Jianfa Luo (2013). "An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Cipher text Length" *International Conference on Computational Intelligence and Security (CIS2012)*, Article ID 810969.

[13]. Cipher test-policy, URL: "https://www.cs.utexas.edu/~bwaters/publications/papers/cp-abe.pdf".

[14]. Duplication in Cloud, URL: "https://nektony.com/duplicate-finder-free/remove-duplicate-photos-in-icloud".

[15]. AES encryption, public and private keys, URL: "https://stackoverflow.com/questions/273396/aes-encryption-what-are-public-and-private-keys".

[16]. http://compmath-journal.org/dnload/Arvind-Kumar-Maurya-Avinash-Singh-Unnati-Dubey-Shivansh-Pandey-and-Upendra-Nath-Tripathi/CMJV10I01P0190.pdf

[17]. https://www.hindawi.com/journals/jcnc/2019/9852472/

[18]. N Subramanian, A Jeyaraj - Computers & Electrical Engineering, 2018 – Elsevier

[19].https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=2ahUKEwjO3L3BzpDpAhUZzTgGHXfGCewQFjACegQIDRAD&url=https%3A%2F%2Fwww.ijcsmc.com%2Fdocs%2Fpapers%2FMay2017%2FV6I5201741.pdf&usg=AOvVaw0YEP9yAcfJbg9jwM1DVAf3