DATA PROTECTION OVER -THE CLOUD TRANSMISSION

[1]Ms.Kritika, [2]Kuldeep Kumar, [3]Lakshay Mangu, [4]Kulbhusan, [5]Kunal Gupta

[1]Assistant Professor, [2,3,4,5]Student(CSE)

[1]BPIT, GGSIPU, [2,3,4,5]BPIT, GGSIPU

[1,2,3,4,5]Delhi, INDIA

Abstract*— Cloud Computing has been imagined as the next generation architecture of Computer and IT Enterprise. In contrast to classical solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to large data centers, where the management of the data and resource may not be fully reliable. This unique attribution, however, poses many new security challenges which have not been well understood. In this, we concentrate on cloud data storage security which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By putting in use the prejudiced token with distributed verification of erasure-coded data, our idea achieves the desegregation of storage correctness insurance and data error determination, i.e., the recognition of misbehaving server. Unlike most preliminary works, the new idea support feature to secure and efficient dynamic operations on data blocks, that includes data alteration, delete, append and update. Extensive security and performance analysis shows that the proposed scheme is highly valuable and resilient against Byzantine failure, malicious data moderation attack, and even server colluding attacks.

***Keywords*—Cloud Computing, Erasure-coded data, Data protection, Malicious data moderation, SaaS, DES,Security.**

I. INTRODUCTION

In Modern world, Secure Transmission refers to the transfer of data such as confidential or proprietary information over a secure channel. Many secure transmission methods require a type of encryption so the data can be sent over the net without any disturbance by third party.

Secure transmissions are put in place to prevent attacks such as ARP spoofing and general data loss. Software and hardware implementations attempts to prevent the unauthorized transmission of information from the computer systems to an organization on the outside.[1]

Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the software as a service (SaaS) computing architecture, are transforming data centre into pools of computing service on a huge scale. The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centre. Moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct hardware management. The pioneer of Cloud Computing vendors, Amazon Simple Storage Service and Amazon Elastic Compute Cloud are both well-known examples.

II. LITERATURE

It has been a time since number of computer users has increased in the world, and it also created a need for transferring the data in faster way and we choose internet for it. It's a simple and faster way to transmit the data with the help of Cloud storage device and servers, many companies has started providing these features to the user. A user can upload a file on to the cloud and download it as if it's required.

When something stored in the cloud, it means it is stored on the internet servers instead of on your computer. It's like having an extra hard drive-one that you can access anywhere and anytime while you're connected to the internet. In the past there were only a home computer with a software installed on it. Now we can take our files anywhere. Thanks to cloud based application called web apps, which run inside our internet browsers. A web app that is generally used by people is Google Docs. It is free and doesn't require anything to install to use it. It allows to create several different types of projects. One can access everything created on Google Docs from any computer or device with an internet connection. Since only an internet connected device is required to access the cloud, one can take all his music, photos, and videos with him wherever he goes. For instance if someone takes a photo on his mobile phone and uploads it to the cloud-based photo storage service like Flicker or Picasa , one can access the photo on any other devices or computer or a TV. Storing the data in the cloud is a great way to protect data from accidents or viruses and more. One can use cloud-based storage services to back up the content of computer. These services run continuously and automatically, so one has the most recent version of his files stored in online servers. If something bad happens to the computer, the backup files can be easily transferred from storage service to another device. It's a faster way to transfer the file, rate of users has increased exponentially in last few years. Its advantages attracts a lot of users but it also attracts the hacker. The basic problem of transferring the data is security, security is the primary concern for user.

Cloud computing needs storing of data in the servers. These servers may be accessed by any unauthorized person or a person with malicious intent. This may lead to unauthorized access of person's private data to a hacker or completely losing it. Security of the data from these person is one of the biggest concern in cloud computing. The cloud is not a personal private space anymore. Enterprises have accepted that this future service is not a tool anymore. The cloud has evolved in the last five years ranging from private storage to being a computing centre for a company. Executives are finding new easy ways to use cloud services to achieve their desired goals. Comparing Statistics, around 1.6 ZB of traditional data centre traffic was reported in 2013 which rose to 6.5 ZB as cloud data traffic in 2018[3].

Abbreviations and Acronyms--
SaaS - *Software as a service,* ***ZB*** *- Zetta byte,* ***Admin*** *- Administrator,* ***IDEA -*** *International Data Encryption Algorithm,* ***DES*** *- Data Encryption Standard,* ***OTP*** *- One Time Password,* ***ARP*** *- Address Resolution Protocol*

Proposed Work ---

The Cloud Computing System is meant to keep the security of the cloud send between the users in Internet. We are using the Algorithm Blow-Fish encryption for encrypt the file data (cipher text). User can encryption & decrypted the data. But without secret key (which is generated by the user at the uploading) or wrong key software provide fake data to the claimer. Admin is authorized for view the user's record data. But admin can't see the user data. The main concern of this project is to improve the efficiency and effectiveness of the whole system. Its increase the security by two way.

III. METHODOLOGY

First of all when the project run its open a local-host sever which is built with the help of Wamp Server (It provides a platform to open a host browser). There are 2 modules in the project. First module is the ADMIN Module and the second module is the USER Module.

DATAFLOW DIAGRAM

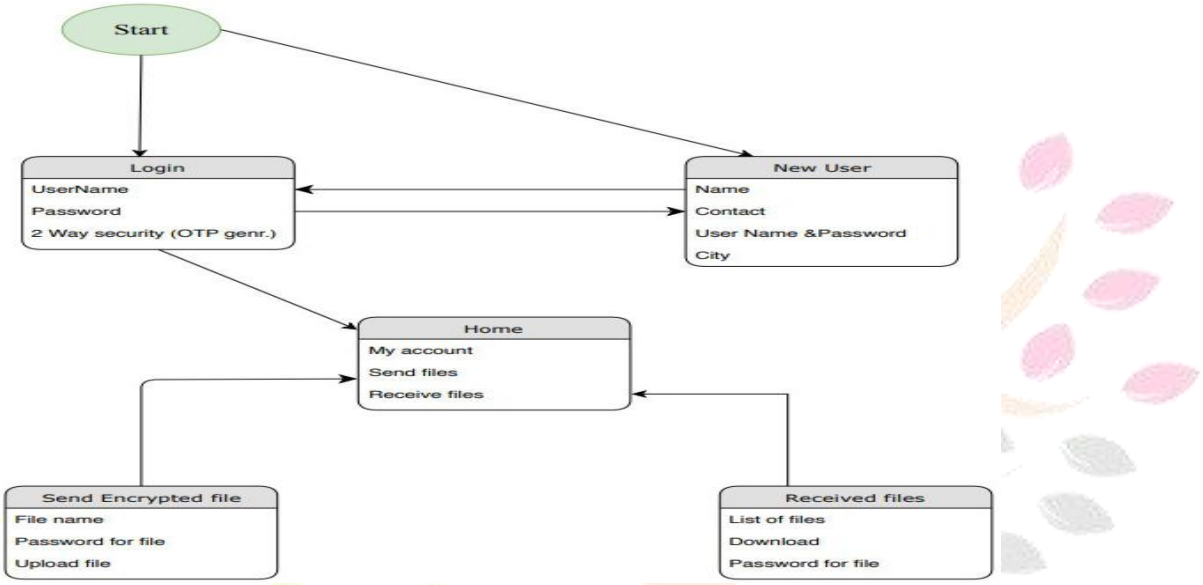

Figure 1(Above figure represent the data flow of our methodology)

ADMIN Module:

In Admin Module the Admin can login using his valid credentials. After a successful login admin can view all the authentic user in a listed view.

USER Module:

After successful build up and running, User get a tab in the specific browser in which he/she can enter the respective username and Password. If the user is already registered and if not registered, then user can click the button to sign up and get registered by entering the required details like Email id, password, Username, Contact number etc. After successful registration the user can now login. At login page there is a two way security system that occurs. If the login credentials entered by the registered user is correct, the page will generate an OTP which will be sent to the registered email address of the user. If the login credentials entered by the user is incorrect, a dialogue box appears with a message written as "unregistered user". Once the OTP is received by the user through email address, the user has to enter the same OTP in required field present on the second page. If the OTP entered by the user is correct the user is directed to his home page and if the OTP is incorrect, a dialogue box appears with a message written as "Invalid OTP".

After login successfully user can upload files of different formats like image, doc files, pdf etc and can download these files when required. While uploading the file from a local drive to the cloud, the user has to create a pin. Now this pin created by the user is also required at the time when the same file is downloaded from the cloud to local drive. The file user wants to upload is uploaded in encrypted form. This file is encrypted using Blow-fish Algorithm (It is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits). The file is encrypted at the time of uploading and decrypted at the time of downloading the file. For encryption and decryption the key used is the same pin created by the user.

Main feature consists of sharing files among the registered users. One user can send files of different format to other registered user. Sender user has to upload the file and the same file can be downloaded by the receiver. While uploading the file from a local drive to the cloud, the sender user has to create a pin. Now this pin created by the sender user is also required at the time when the same file is downloaded by the receiver. The file sender user uploads is uploaded in encrypted form. This file is encrypted using Blow-fish Algorithm (It is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits). The file is encrypted at the time of uploading and decrypted at the time of downloading by the receiver. For encryption and decryption the key used is the same pin created by the user. If the shared pin is incorrectly entered by the receiver, the data of original file is manipulated and shows fake data inside it.

IV. BLOWFISH ALGORITHM

Blow-fish is also an encryption method that is a very strong weapon against hackers and cyber-criminals. It is used in a wide array of products, including some secure E-mail encryption tools, backup software, password management tools. Blow-fish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt messages. Blow-fish is also a block cipher, meaning that it divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded. Blowfish is public domain, and was designed by Bruce Schneier expressly for use in performance-constrained environments such as embedded systems. It has been extensively analyzed and deemed "reasonably secure" by the cryptography community. A block cipher is basically a computer routine that takes any amount of plain text and converts it into coded text, or cipher-text. It performs this routine on chunks of text called blocks. And in order for the text to be decoded on the other side of transmission, the function must also generate a key to unlock the cipher-text.

PROCESS OF BLOWFISH

It mainly has two parts first is sub key generation an second is data encryption.

1 Sub key generation

1.1 sub key are kept in array k1, k2,...,kn(1<n<14) each k is of 32 bits, so the maximum bits (32x14) 448bits.

1.2 P-array is initialized p1,p2,p3....p18 (32 bits).

1.3 4-S boxes is initialized substitution box. Each contains 256 32 bits entries.

1.4 P-array & S-boxes values are initialized in hexadecimal form of Pi.

1.5 XOR operation performed between P and K.

1.6 64 bits plain text is taken. All bits are 0 in beginning

V. STATISTICS OF CLOUD COMPUTING USERS

YEAR	No. of users(in millions)	Data Security breach over cloud(approx)
2014	1136	800
2015	1329	1100
2016	1561	1350
2017	1754	1500
2018	1926	1700
2019	2111	300+

Table 1. (Above statistic compares the number of cloud computing users (in millions) in different years from 2014-2019. In 2020, an estimated 2.3 billion people worldwide will be using personal cloud storage.)[4]

VI. OUTCOME AND CONCULSION

This Desktop Application provides facility to transfer sensitive file from one user to another user through security system. This project work on client server architecture that means if server is started then server receive client file. For the encryption process blowfish algorithm is used. The sensitive data which needs to be uploaded by the user is encrypted and decrypted while downloading the encrypted data by the user. Ultimately providing security in cloud computing.

REFERENCES

[1] https://www.embedded.com/design/configurable-systems/4024599/Encrypting-data-with-the-Blowfish-algorithm
[2] https://study.com/academy/lesson/blowfish-encryption-strength-example.html
[3]https://en.wikipedia.org/wiki/Cloud_computing_security
[4] www.marketwatch.com/story/how-the-number-of-data-breaches-is-soaring-in-one-chart-2018-02-26.
[5]Cloud Computing Security issues
http://uru.ac.in/uruonlinelibrary/Cloud_Computing/Cloud%20Computing%20Security%20Issues.pdf
[6]Counter measures for data breach in cloud computing
https://www.ijrcar.com/Volume_2_Issue_11/v2i1130.pdf.
[7]Data breach as top security concern in cloud computing
https://acadpubl.eu/hub/2018-119-14/articles/1/3.pdf
[8]https://www.engpaper.com/cloud-computing-2018.htm