International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

Multifactor Authentication System to Enhance Security Issues in Cloud Computing

G. Nivedhitha [1], R. Meenambigai [2], M. Priya Dharshini [2], A. Monisa Shree [2]

[1]Professor Department of Computer Science and Technology Sri Krishna College of Technology, Tamil Nadu, India

[2]UG Scholar Department of Computer Science and Technology Sri Krishna College of Technology, Tamil Nadu, India

ABSTRACT

The rise of big data and data storage in cloud have been peculiar and facilitator to the emergence of big data and cloud computing concepts. In general, cloud computing offers access to data storage, processing and analytics process. The main issue in the cloud storage is the security measure while storing and sharing the data over cloud. To overcome this issue we propose a Multi-factor Authentication Method i.e., automatic rotating password to be generated along with user identification. Along with this we propose a key-aggregate cryptosystem to securely, efficiently and flexible share data with others in cloud storage. This method produce cipher text of constant size such that decryption rights can be assigned to the file. By combining a set of secret key, we can make a compact single key. By considering this compact key, the file has been send to others and will be stored in a restricted secured manner. First, the owner of the data information has been setup for the public system next Key Gen algorithm that generates a public or master/secret key. Making use of this key, user can convert plain text to cipher text. Next user will give input as master secret key by Extract function; it will produce output as aggregate decryption key. This generated key is safely sent to the receiver. Then the user with aggregate key can decrypt the cipher text through the use of Decrypt function.

Keywords: Cloud computing, AES Algorithm, CSP

I. INTRODUCTION

Cloud computing is the on-demand delivery of compute power, that provides many services like storage, software availability, analytics through the Internet with pay-as-you-go pricing and can access as many resources needed by the client, and only pay for what we use. For example, if a business organization wants to build an IT infrastructure, typically it would require the machines to install the servers, software, and networking resources it needed, but nearly all of those services and resources are now accessible by going to third parties that offer them in the cloud. Companies offering these computing services are called cloud providers. There are some security requirements that limits the threats like confidentiality, access controllability, integrity etc. The first form of web-based data storage is the cloud storage. This is a form of networked data storage where data files are stored on multiple virtual servers. The servers used for Cloud storage are typically hosted by third-party companies who operate large data centers. When subscribing to a cloud storage service, you lease storage capacity from the cloud storage service and then have access to the contracted amount of storage space, which can be accessed through Internet.

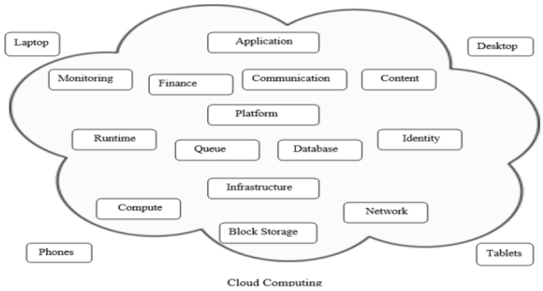

Figure 1. Architecture Diagram

The cloud architecture provides the users with higher bandwidth facility, and allowing authenticated users to have uninterrupted access to file, applications, storage for to quickly and efficiently communicate between servers or between clouds.

The cloud based services are

- ✓ Software as a Service (SaaS) provides software usage as per needed for the application development that can be used and maintained on the cloud. With SaaS, there is no need of installing the software locally.
- ✓ Development as a Service (DaaS) provides web based development tools that can be shared across various communities.

Platform as a Service (PaaS) provides users with application databases and platforms, similar to middleware services.

Infrastructure as a Service (IaaS) provides infrastructure and hardware's like servers, networks, storage devices, etc. running in the cloud, that are available to users against a pay per usage basics.

Cloud storage composes of three categories: Object, File, and Block. In the first category, Object Storage are used for building modern applications from scratch that require scale and flexibility, and also provides to import existing data stores for analytics, backup, or archive. In the second category, File Storage grants the access for many applications to access shared files. File storage are ideal for large content repositories, development environments, media stores, or user home directories. In the third category, Block Storage are provisioned with each virtual server and offer the ultra-low latency required for high performance workloads.

As cloud storage becomes more familiar, securing the file in the cloud has become the tedious process. Many organizations have been increasing their use of services in cloud like Google drive, Dropbox, Amazon Web service, Microsoft One Drive, Pcloud etc.,. The various security issues in cloud computing includes Hijacking of Accounts, Insider Threat, Malware Injection, Abuse of Cloud Services , Denial of Service Attacks, Data Loss.

II. LITERATURE SURVEY

Shen. Jian.et.al.,[1] proposed the Secure Authentication in Cloud Big Data with Hierarchical Attribute Authorization Structure proposed a secure authentication protocol for hierarchical attribute authorization structure in cloud big data. The main contributions of this paper can be listed as follows: a secure authentication protocol for the two-level hierarchical attribute authorization structure in the cloud big data access control system to authenticate authorities or users. In order to meet big data application requirements, we extend the protocol to support multiple levels authentication in the hierarchical attribute authorization structure and with the tree-based secure signature, our protocol can provide security properties of forgery attack resistance, replay attack resistance and privacy preservation.

Ju-Shu Chueh and Min-Te Sun., [2] proposed the Design and Implementation of Security System for Cloud Storage in order to ensure the security through verification and file encryption. Besides, as long as the encrypted files and their keys are stored in the same place, there will be security concerns. For the third party auditor (TPA) verification, it is built to verify the identity of the users instead of having the cloud Service Provider (CSP) to authenticate users. With the help of TPA, the unauthenticated and malicious users can be prevented from accessing the other people's files in the cloud storage. Proper key management and storage structure has been designed for storing the encrypted file and its key at the same place may cause a lot of security problems. This system has the low computational complexity since the keys are stored at a different place, a new key storage data structure is required to handle frequent data insertions and searches. The computational complexity of these functions should be low in order to improve the performance of the system. For the Load-Balancing, instead of having the server do all the computational job, a proper amount of computation load should be allocated to the client's PCs. This can guarantee that the server will not become a bottleneck in system performance. Efficient file encryption/decryption has been assigned a set of encryption and decryption algorithms are required for our system and they should be able to defend any attack within a reasonable amount of time.

Miraj Hossain, Md. Rafiqul Islam.,[3] proposed A Model for Ensuring Data Security to Distributed Financial System in Cloud Storage. In this paper, a multi-level authentication and authorization method. If any user wants to access data in a specific class, then the authentication have to be done first. This process uses id and password of the authenticated user only. If the user wants to get access to confidential and moderate classes he must go through the further authentication and authorization process. In DFS (Distributed Financial System), two data storage has been proposed. One is for storing user information and another is for storing business data (financial data). User Database contains three categories of users. Super user's acts as a data owner. High sensitive, moderate and public data is visible only for this type of user. This type of user remains at top hierarchical level in security suite and no need to provide permission to gain access to the system byte system admin. Data owner can control others users that remains under Super user in hierarchical level. Admin User acts as a system admin in an organization. Public and moderate data is visible only for this type of user except for high sensitive or private data. The Super user can decide what activities are performing by this type of user. Data classification rules are applicable for this type of user. General User acts as a general employee in an organization. If system admin accepts access request of general user, the particular user will gain access for logged in DFS. Only public and moderate data is accessible by these types of users if they are permitted. Also, data classification rules have been applied to this type of user. In a distributed financial system, very strong authentication and authorization method must be applied.

FENG. BIN. et.al., [4] proposed An Efficient Protocol With Bidirectional Verification for Storage Security in Cloud Computing. In addition to the verification of the integrity of the data, most of the current PDP and POR scheme scan support third party verification (public verification). In such schemes, there are three participating parties, i.e., the Data Owner, CSP, and TPA. The characteristic of this structure is that CSP is not sensitive to the identity of the authentication party. Also both the CSP and TPA are only semi-trusted by the Data Owner. Because CSP is semi-trusted, the RDA protocol is been considered. But the conventional three-entity structure cannot solve the problem of the third party's being semi-trusted. Because, in the old structure, the challenge message is very simple so that everyone can send one to the CSP, and the CSP cannot verify the identity of the challenge sender. Under this mechanism, the adversary can either get the related information about the Data Owners file(s) or can gather statistical information about the CSPs service status. But, traditional PDP models meet the security requirements of auditing-as-a service, to support public verifiability. In order to ensure the security and accuracy of verification, most of the existing RDA schemes verification party carries a considerable portion of the computational load. In this field, handling errors has become a difficult problem, and it has attracted the attention of many researchers. Imagine that one user finds that her or his files are corrupted when they are checked. How to deal with these documents has become a serious problem. The user can delete all of the files if they are not important. But what should be done if there is some sensitive (or important) information in these files? Can we try to protect these sensitive data? In addition, situations can occur in which users find errors when they are checking a huge file. Regardless of whether it is an important dataset, deleting the entire document would be a huge loss to the user. In these two cases, the problems become much simpler if we are able to determine the location of the error.

Rushikesh Nikam and Manish Potey [5] proposed the Cloud Storage Security Using Multi-Factor Authentication Technique for developing a private cloud and providing secure storage service using MFA (for authentication) and CP-ABE (for data Confidentiality). The private cloud is developed using open source technologies like Apache Ambari [8], Oracle VM Virtual box [9], Vagrant [10], Putty. For the cloud system, Centos operating system - a Linux distribution is used. The user registers and logs in with its credentials, enters One Time Password (OTP), this OTP is in a token form which is provided by Google Authenticator application in Mobile devices. To enter into the cloud environment, user's personal credentials as well as Token (using TOTP algorithm) provided by the Service provider is needed. For uploading a file, User provides the file as input and the cloud service encrypts it using CP-ABE algorithm. The encrypted file is stored on cloud. The cloud contains the clusters for storage. To download file from the cloud, user again has to login with its credentials and OTP generated by Cloud Service. Then it selects the file from cloud which he wants to download. Cloud service based on user's demand to retrieve the encrypted file or the decrypted file does the processing. If decrypted file is to be fetched, the Cloud service using CPABE decrypts the file and sends it to user, otherwise the file is downloaded in encrypted format and is sent to the user. An additional layer of security is available for files that need to be decrypted and downloaded, i.e. attributes are to be filled by the users (as provided in the registration phase) into the verification page. If verification is successful, file is downloaded in a plain-text format, else download fails). Authentication levels are as follows: 1. Static user name and password. 2. OTP using new tokens or default tokens. The CP-ABE encryption technique is used to provide confidentiality and access control. It has four algorithms such as setup, encryption, key generation, & decryption. In CP-ABE, it is not the set of attributes that do the working but the policies defined over a set of attributes carry the encryption process. In CP-ABE there is no separate access control or authorization mechanism. It is incorporated in the encryption mechanism itself. Users can even obtain their secret keys after data encryption using the access structure is an important add-on. Future users are given a key based on the attributes and the policy satisfies, such users are only genuine decrypts of the system.

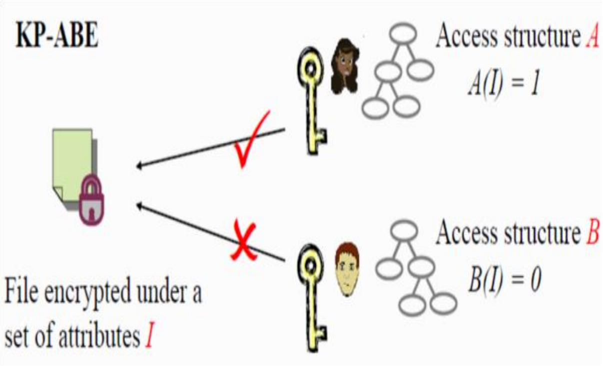

Figure 2. KP-ABE Scheme

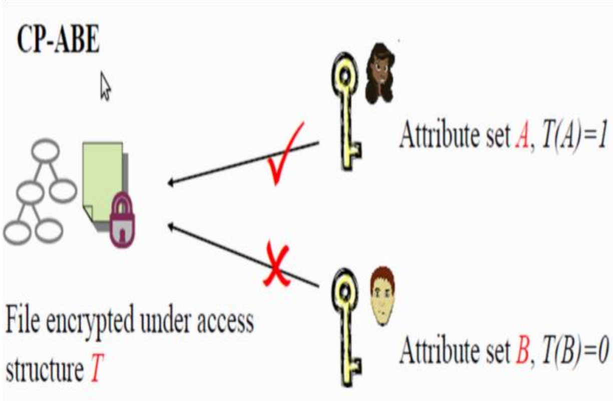

Figure 3. CP-ABE Scheme

III. PROPOSED SYSTEM

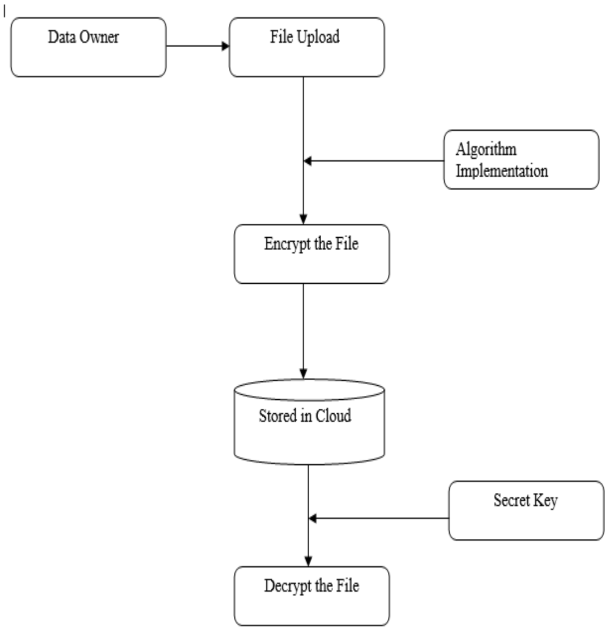

Figure 4

In the data flow diagram, the data owner registration form is created for registering the details in the cloud. The data owner uploads a file using the registered user name and password. The client registers the necessary details such as Username, Password, Email and mobile number for the authentication process. The AES algorithm has been implemented to encrypt and store the file. The encrypted file will be stored in the cloud.

The secret key will be used to decrypt and download the file from the cloud.

ADVANCED ENCRYPTION STANDARD (AES):

Advanced Encryption Standards, is a cryptographic cipher text function that is applied for the information security. AES comprises of three block ciphers: AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256-bits respectively.

Symmetric (also known as secret-key) ciphers use the same key for both the encrypting and the decrypting. The sender and the receiver must both know and use the same secret key. All key lengths are either 192 or 256 bit key lengths. For 128 bit, 192 bit, 256 bit key length 10 rounds, 12 rounds and 14 rounds are carried out respectively. Each round includes several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of cipher text.

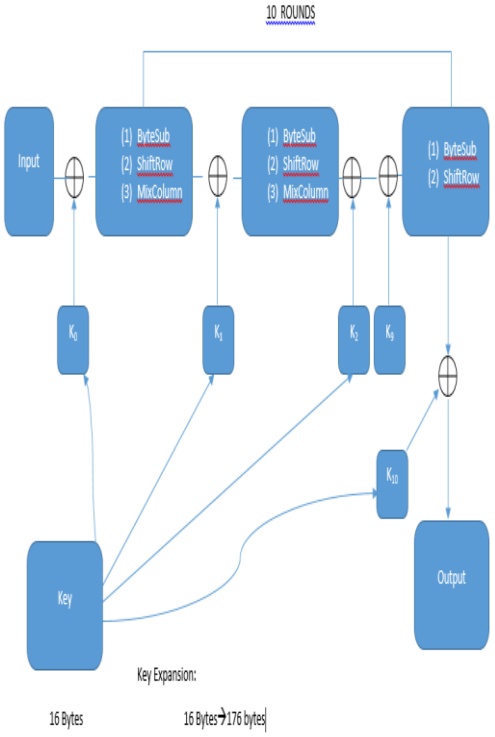

Figure5. AES Algorithm

The first processing step in the AES encryption cipher text is substituting the data in the substitution Table . The second processing transforms by shifting data rows, then the third processing mixes the columns. The last processing is the exclusive or XOR operation performed on each column using a different part of the encryption key. For longer keys, the processing needs more rounds to complete.

1) PROCEDURE OF THE ALGORITHM:

1. Sub Bytes: Key expansion processes the corresponding cipher key and the number of round keys has been assigned.
2. Shift Rows: Rows of the block are cylindrically shifted in left direction. Initially the first row is untouched, the second by one shift, third by two shift and fourth by 3.

3. Mix Columns: the block is multiplied with a fixed matrix combining the four bytes in each column.
4. Add round key: In this step each byte is XOR-ed with the corresponding element of key's matrix
5. Final Round (no Mix Columns)
    1. Sub Bytes
    2. Shift Rows
    3. Mix Columns

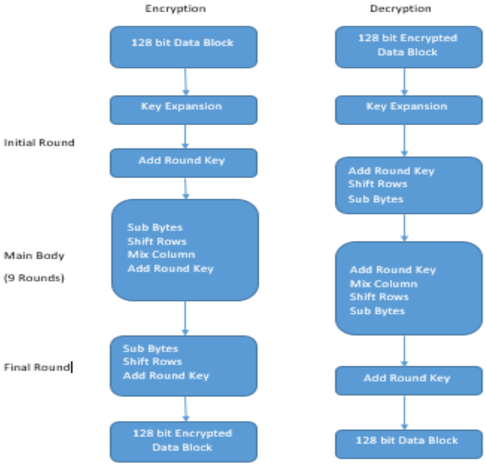

Figure 4. AES Encryption and Decryption

MODULE DESCRIPTION:

REGISTRATION

The registration module includes client and data owner registration. During registration a random key will be generated which will be used later for downloading the file.

Client Registration

The client registration includes entering the client user name, password and mail id. The client will receive the key generated from the data owner through mail.

Data-Owner Registration

The data owner must register before uploading any file in the cloud. To register he enters the user name and password.

UPLOADING THE FILE IN THE CLOUD

The data owner enters the registered user name and password to get logged in. Once the user name and password is verified it gets directed to another page where the file which is to be uploaded must be chosen.

AES ENCRYPTION

AES Encryption takes place in block of ciphers. A block cipher is an algorithm that encrypts data on a per-block basis. The size of each block is usually measured in bits. In general, AES 128 bit encryption is the least strong, while AES 256 encryption is the strongest. 128 bit AES encryption is faster than AES 256 bit encryption. The generated key will be used for file encryption.

DOWNLOADING THE ENCRYPTED FILE FROM CLOUD

To download the file from the cloud, the corresponding user enters the particular registered user name and password along with the data owner from whom the client wants to download the file. After the authentication detail has been verified, the page will be directed to next page for downloading. There the client selects the particular file that is required and downloads from the data owner by entering the corresponding key generated through the mail. After verifying the key that the data owner provided the file will be downloaded.

AES DECRYPTION

The key generated through mail is used for the AES decryption, where the cipher text with the help of key will be used to convert the encrypted file to a decrypted format.

IV. CONCLUSION

Cloud computing is the technology used to Store and process the data in the cloud. The cloud storage is maintained by third party authentication. To provide the security to the file that is stored in cloud, multifactor authentication technique is developed with AES Encryption algorithm. Our System provides security with the customized access to the data. In future, our algorithm can be improved to store the all kind of file systems since our system works only for multiple files

V. REFERENCES

[1]. Jian Shen, Member, IEEE, Dengzhi Liu, Qi Liu, Xingming Sun, Senior Member, IEEE, Yan Zhang, Senior Member, IEEE "Secure Authentication in cloud big data with hierarchial attribute authorization structure.",2332-7790 (c) 2016 IEEE.

[2]. Ju-Shu Chueh and Min-Te Sun," Design and Implementation of Security System for Cloud Storage", 978-1-5386-1101-2/17/$31.00 2017 IEEE.

[3]. Miraj Hossain, Md. Rafiqul Islam," A Model for Ensuring Data Security to Distributed Financial System in Cloud Storage", 2017 3rd International Conference on Electrical Information and Communication Technology (EICT), 7-9 December 2017, Khulna, Bangladesh

[4]. BIN FENG, XINZHU MA, CHENG GUO, HUI SHI, ZHANGJIE FU, AND TIE QIU, "An Efficient Protocol With Bidirectional Verification for Storage Security in Cloud Computing", 2169-3536, 2016.

[5]. Rushikesh Nikam, Manish Potey, "CLOUD STORAGE SECURITY USING MULTI-FACTOR AUTHENTICATION" IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2016), December 23-25, 2016, Jaipur, India