A New Framework for User Authentication to access Filesstored in Distributed Server Based Cloud Computing

[2]Narayana Galla, [1]Sri M.Gnanavardhan
[1]M.Tech (CSE), [2]Assistant Professor
[1,2]K.I.Ts, Markapuram

Abstract : **The cloud computing platform gives people the opportunity for sharing resources, services and information among the people of the whole world. In private cloud system, information is shared among the persons who are in that cloud. For this, security or personal information hiding process hampers. The development of cloud computing services is speeding up the rate in which the organizations outsource their computational services or sell their idle computational resources. One of the most important aspect refers to security: while some cloud computing security issues are inherited from the solutions adopted to create such services, many new security questions that are particular to these solutions also arise.In this paper we have proposed secure communication system and hiding information from endeavor. In this paper we have shown mainly deals with secure computing framework system on the cloud computing platform.Aiming to give a better understanding of this complex scenario, in this article we identify and classify the main security concerns and solutions in cloud computing, and propose secure computing framework system on the cloud computing platform, giving an overview of the current status of security in thisemerging technology.**

Keywords- Cloud Computing; Security architecture; ECC; onetime password; MD5 Hashing;

I. INTRODUCTION:

Cloud computing as a model is the result of the natural evolution of our everyday approach to using
Technology delivered via the Internet. Cloud computing came into the foreground as a result of advances in distributed computing with server clusters , virtualization and increase in the availability of Internet access. Industry leaders describe cloud computing simply as the delivery of applications or IT services, which are provided by a third party over the Internet. At the present world of networking system, Cloud computing is one the most important and developing concept for both the developers and the users. Persons who are interconnected with the networking environment, cloud computing is a preferable platform for them. Therefore in recent days providing security has become a major challenging issue in cloud computing. At the present world of networking system, Cloud computing is one the most important and developing concept for both the developers and the users. Persons who are interrelated with the networking environment, cloud computing is a preferable platform for them. Therefore in recent days providing security has become a major challenging issue in cloud computing.

In the cloud model, resources are shared among all of the users, individuals and servers in the VM. As a result common shared files\ data stored in the cloud become open to all other server's. Therefore, data or files of an individual can be handled by all other users of the cloud. Thus the data or files become more vulnerable to attack.As a result it is very easy for an intruder to access, misuse and destroy the original form of data. An intruder can also interrupt the communication. The Main problem with the cloud system is that an individual may not have control over the place where the data needed to be stored. Thus, it is also necessary to protect the data or files in the focus of unsecured processing. In order to solve this problem we need to apply security framework in cloud computing platforms. In our proposed security framework model we have tried to take into account the various security breaches as much as possible.

Currently in the area of cloud computing different security models and algorithms are applied. But, these models have failed to solve all most all the security threats.At present, in the area of cloud computing different security models and algorithms are applied. But, these models have failed to solve all most all the security threats. Moreover for E-commerce and M-Commerce different types of online business, we need to imply high capacity security models in cloud computing fields. Security models that are developed and currently used in the cloud computing environments are mainly used for providing security for a file and not for the communication system. Moreover present security models are sometimes uses secured channel for communication. But, this is not cost effective process. Again, it is rare to find a combined work of main server security, transaction between them and so on.

Some models attempt on discussing about all of these, but are completely dependent on user approach. The models usually fail to use machine intelligence for generating key and newer proposed model. Some models have proposed about hardware encryption system for secured communication system . The idea is usually straightforward, but theimplementation is relatively difficult. Besides, hardware encryption is helpful only for the database system, not for other security issues. Authenticated user detection technique is currently very important thing. But, this technique is rarely discussed in the recently used models for ensuring security in cloud computing.In this paper we have proposed new security architecture for cloud computing platform. In this model high security algorithms are used for giving secured communication process. Here files are encrypted with AES algorithm in which keys are generated randomly by the system. In our proposed model distributive server concept is used, thus ensuring higher security. This model also helps to solve main security issues like malicious intruders, hacking, etc. in cloud computing platform. The Elliptic curve cryptography (ECC) algorithm is used for secured communication between the users and the servers.

This paper is formatted in the following way: - section II describes related work of this paper work, section III describes proposed architecture of framework model and its working steps, section IV describes the future aspects related to this paper work.

II. RELATED WORK

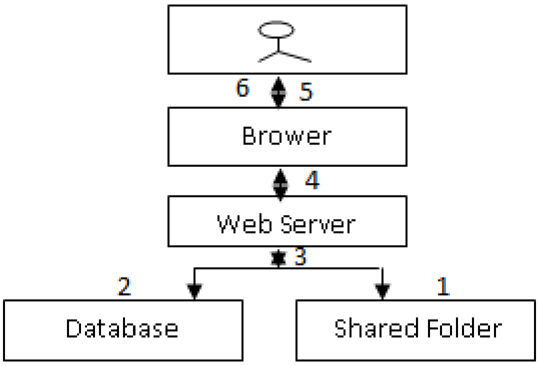
Many research on security in cloud computing has already been proposed and done in recent times. Identification based cloud computing security model have been worked out by different researchers [12]. But only identifying the actual user does not all the time prevent data hacking or data intruding in the database of cloud environment. The flaw in this system is that it does not ensure security in whole cloud computing platform. Research related to ensuring security in whole cloud computing environments was already worked out in different structures and shaped. AES based file encryption system is used in some of these models. But these models keep both the encryption key and encrypted file in one database server. Only one successful malicious attack in the server may open the whole information files to the hacker, which is not desirable. Some other models and secured architectures are proposed for ensuring security in cloud computing environment. Although these models ensures secured communication between users and servers, but they do not encrypt the loaded information. For best security ensuring process, the uploaded information needs to be encrypted so that none can know about the information and its location. But, these models also fail to ensure all criteria of cloud computing security issues .

III. PROPOSED FRAMEWORK MODEL

In our proposed framework model we have worked with the following security algorithms:-

1. ECC algorithm for secured communication.
2. AES for Secured file encryption
3. MD5 hashing for cover the tables from user
4. One time password for authentication.

At present ensuring security in cloud computing platform has become one of the most significant concerns for the researchers. We have started these problems in our research, to provide some solution correlated with security. We have proposed the following security model for cloud computing data storage shown in Figure 1.



In this model, all the users irrespective of new or existing member, needs to pass through a secured channel which is connected to the main system computer. System server computer has relation with other data storage system. The data storage system can be servers or only storage devices. Here, each of the data storage devices can be thought as one or more servers in number. This means, there are no dedicated servers in cloud computing, rather all are independent servers and can be scaled as necessary.

In the proposed model ECC encryption algorithm is used for making the communication safe. Usually the users' requests are encrypted while sending to the cloud service provider system. ECC algorithm using the system's public key is used for the encryption. Whenever the user requests for a file the system sends it by encrypting it via ECC encryption algorithm using the user's public key. Same process is also applied about the user password requests, while logging in the system later. After receiving an encrypted file from the system the user's browser will decrypt it with ECC algorithm using the user's private key. Similarly when the system receives an encrypted file from the user it will immediately decrypt it using its private key. As a result the communication becomes secured between the user and the system.

In the proposed security model one time password has been used for authenticating the user. The password is used to keep the user account secure and secret from the unauthorized user. But the user defined password can be compromised. To overcome this difficulty one time password is used in the proposed security model. Thus whenever a user login in the system, he/she will be provided with a new password for using it in the subsequent login. This is usually provided by the system itself. This password will be generated randomly. Each time a new password is created for a user, the previous password for that user will be erased from the system. New password will be updated for that particular user. A single password will be used for login only once. The password will be sent to the users authorized mail account or authorized mobile or both. Therefore at a same time a check to determine the validity of the user is also performed. As a result only authorized user with a valid mail account/phone will be able to connect to the cloud system. By this system, existence of unauthorized user or a user with an invalid mail account will be pointed out. The newly generated password is restored in the system after md5 hashing. The main purpose of MD5 hashing is that this method is a one way system and unbreakable. Therefore it will be difficult for an unauthorized or unknown party for retrieving the password for a selected user even if gained access to the system database.

After connecting with the system a user can upload or download the file(s). For the first time when connected with the system the user can only upload file(s). After that users can both upload and download their files. When a file is uploaded by an user the system server encrypts the file using AES encryption algorithm. In the proposed security model 128 bit key is used for AES encryption. 192 bit or 256 bit can also be used for this purpose. Here the 128 bit key is generated randomly by the system server. Key , File Name and File checksum is used only once. That particular key is used for encrypting and decrypting a file of a user for that instance. This key (Key+FN+FCS) is not further used in any instance later. The key is kept in the database table of the system server along with the user account name. Before inserting the user account it is also hashed using md5 hashing. This insures that unauthorized person cannot retrieve the key to decrypt a particular file for a particular user by simply gaining access and observing the database table of the system server. As a result the key for a particular file becomes hidden and safe. It's very difficult to know the hackers, Again when the encrypted file is uploaded for storing to the storage server; the path of the encrypted file along with the user account is kept and maintained in the database table on the storage server. Here user id, file name is used for synchronization between the database tables of main system server and the storage server. We have developed normal table which will holds the hash value of particular file details into the table.

User Login into the proposed frame work system is compulsory when a user wants to download aexisting stored file. When the user selects a file to download, the system automatically retrieves the key for the requested file from the proposed framework system server. The system matches user account Id ,file id, file checksum saved in its database tablewith that saved in the storage server after hashing it using md5 hashing. The path of the encrypted file from the storage server is found by using the user account name and the hash table input for the requested file.

Algorithm steps

1. Generated Key using User ID , File Id , File Checksum and Random number of the File first time.
2. Key is hashed with algorithm MD5
3. Generated Key hash value is stored in the proposed DB table with User Id and FileId
4. While reading the file the user first should access the proposed framework using the OTP
5. Once the OTP is authorized successfully then framework allows the user to access the DB details
6. If OTP is not authorized successfully then framework declines the user to access the file details in the DB

In the above proposed framework model, the encryption key for a particular file of a particular user is only known to the main system server. The path of the encrypted file is only known to the storage server which is only known to the main server. For this, the key as well as the encrypted file is hidden from the unauthorized persons. In this communication system when a file is sent from the main system server to the storage server it is already in its fully encrypted form. That's why there is no need to provide security in this communication channel. At last, we propose hardware encryption for making the databases fully secured from the attackers and other unauthorized persons.

Figure 2 is the Pictorial representation of the proposed cloud security architecture. Here, single user and server represent n users and n servers.

An algorithm is developed, which is used for inserting the file in the main server (System), and in the database table where the encrypted file is kept. This is saturated from the system server for the cloud computing platform. In the system server, the file is inserted by maintaining the sequence. In file saving server, the file is inserted in a random order which becomes the output of the algorithm.

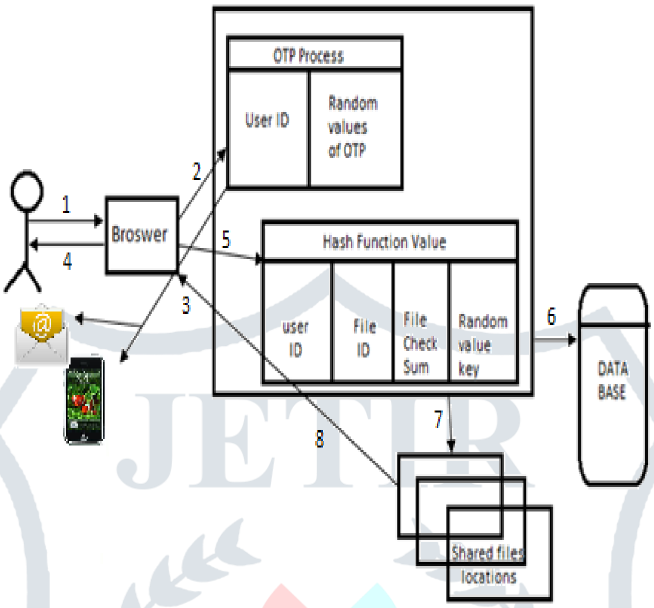


Figure 2 : Pictorial Representation of the proposed cloud security architecture

IV. CONCLUSION

In this paper we have proposed a new framework security for cloud computing environment which includes AES file encryption system, ECC system for secure communication, Onetime password to authenticate users to access the framework and MD5 hashing for hiding information of file details and access. This proposed framework ensures security for whole cloud computing structure. In our proposed framework ahacker cannot easily get information and upload the files because he needs to take control over all the servers, which is quite difficult. This model, though it is developed in a cloud environment, individual servers' operation has got priority here. So, decision taking is easy for each server, like authenticate user, give access to a file etc. In our proposed model we have used ECC encryption system which is deterministic. In this future we also want to work with encryption algorithms to find out more light and secure encryption system for secured file information stabilizingframework.

REFERENCES:

[1] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano.The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In Proceedings of the 2012 IEEE Symposium on Security and Privacy, pages 553–567, May 2012.

[2] M. Brian. Gawker media is compromised. the responsible parties reach out to tnw [updated], 2010.

[3] http://goo.gl/0SvCj.

[4] D. Chappell. Introducing windows cardspace. http://msdn.microsoft.com/en-s/library/aa480189.aspx, April 2006.

[5] Naresh Kumar N (M.Tech), 2 Prof. Mohan K , ―GCM Service Driven Communication With An Android Application In Cloud Computing‖ , ISSN: 2278-0181, May 2013.

[6] M.satyanarayanan, V. Bahl , R.Caceres, and N. Devise, ―The case for VM-based Cloudlets in Mobile

[7] Computing‖ , IEEE persive Computing, Carnegie Mellon University, Microsoft Research, AT&T Research, Lancaster University , 2009.

[8] G. H-Canepa and D.Lee, ―A Virtual Cloud Computing Provider for Mobile Devices‖ . San Francisco : MCS'10, 2010.

[9] B. G. Chun and P. Maniatias. ―Augmented Smartphone Application through Clone Cloud Execution‖, ACM, Intel, Berkeley, Princeton, 2011