International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 7, July - 2014

An Approach For Securing Cloud Storage And Transmission

Devaang Soni
M.Tech Scholar
JECRC University

Vijay Prakash Sharma
Assistant Professor
JECRC University

Abstract: In recent years, various Cloud Computing technologies have gained rapid popularity and Cloud can be cited as most prominent or proficient technology today. While the economic case for cloud computing is compelling, the security challenges it poses are equally striking .If we are talking about the storage and transmission in cloud technology today we need to secure our credential data that stored in a distributed environment in cloud. For securing a cloud storage I present a work in cryptography with AES algorithm to encrypt the text and then store it in the cloud storage. After achieving the secure data storage and authentication, the communication security will also be achieved, by integrated the session based communication. The main objective of the work is to define an intermediate security layer between cloud clients and servers to integrate multiple clients and servers. The significance of work is to provide three level security with authentication, storage and communication. This is just an up-dation of security features based on the present requirement.

Keywords: Cloud, AES, Distributed , Cloud Security, Elasticity, Session based Communication.

I. INTRODUCTION

Cloud computing is a big development in this era of technology. Cloud computing, a new kind of computing model, is coming. This word is a new word that appears at the fourth season, 2007. It is an extend of changing with the need, that is to say the manufacturer provide relevant hardware, software and service according to the need that users put forward. With the rapid development of the Internet, user's requirement is realized through the Internet, different from changing with the need. In fact cloud computing is an extend of grid computing, distributed computing, and parallel computing. Its foreground is to provide secure, quick, convenient data storage and net computing service centered by internet.

The character of cloud computing is in the virtualization, distribution and dynamically extendibility. Virtualization is the main character. Most software and hardware have provided support to virtualization. We can virtualized many factors such as IT resource, software, hardware, operating system and net storage, and manage them in the cloud computing platform; every environment has nothing to do with the physical platform. Carries on the management, the expansion, the migration, the backup through the hypothesized platform, all sorts of operations will be completed through the virtualization level. Distributional refers to the physical node which the computation uses is distributed. Dynamic expandability is refers to through the dynamic extension virtualization level, then achieves to above applies carries on the expansion the goal. Has broken between the physical structure barrier, represents is transforming the physical resources for logic may manage the resources the inevitable trend. In the future, all resources transparently will move in each physical platform, the resources management will carry on according to the logical way, will realize the resources automated assignment completely, but the virtualization technology realizes this ideal only tool. In view of the cloud computation, the virtualization technology's fusion and the application should face the high-quality hypothesized main engine, the application and the resources, as well as aspects and so on.

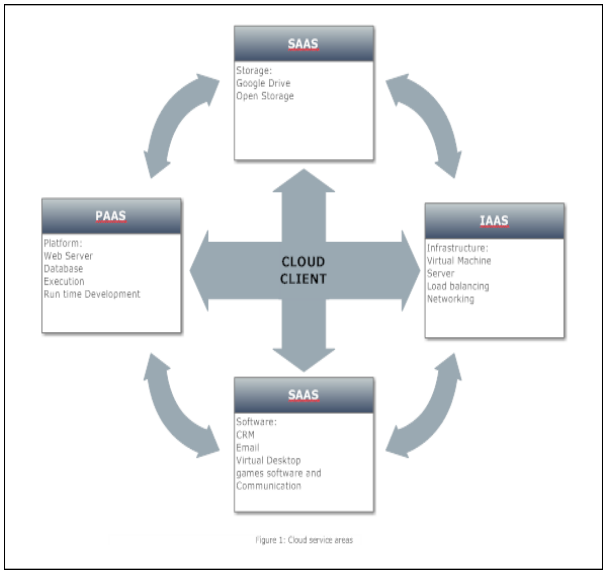

Figure 1: Cloud service areas

II. DEPLOYMENT MODELS IN CLOUD COMPUTING

The cloud can be deployed in three models. They all are described in many ways but in general it is described as below:

A. *Private Cloud*

A private cloud is one in which the services are maintained on a private network, a company or a individuals. The whole infrastructure is also purchased by a company. In this cloud the highest security is provide by the cloud provider but it reduces the cost savings for a company because the company required to purchase and maintain all the software and infrastructure for this type of cloud. The figure:2 explain its structure [2].

B. *Public Cloud*

The public cloud is a general cloud which is available over the internet. A third party who is provider of that service via web applications or web services and take charges on utility basis. In this type of cloud the security is general no extra high security needed in public cloud. Many web application based on the public cloud like google drive, dropbox, where the user have to pay only the internet charges.

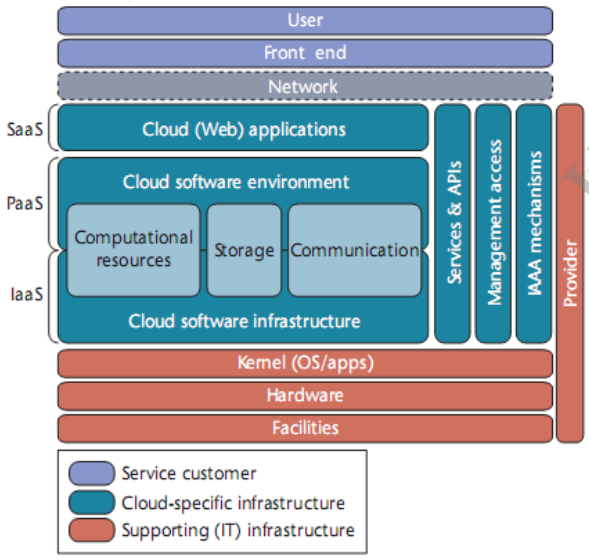

Figure 2: Cloud Architecture

C. *Hybrid Cloud*

The Hybrid cloud is a combination of a private cloud with the use of public cloud services. The main goal of hybrid cloud is to combine the service and data from various cloud models to make a automated environment. So the environment consists of various internal and external providers.

III. CLOUD SERVICES

Three types of services is provided by the cloud are as

A. *Software as a Service*

Consumer software is traditionally purchased with a fixed upfront payment for a license and a copy of the software on appropriate media. This software license typically only permits the user to install the software on one computer. When a major update is applied to the software and a new version is released, users are required to make a further payment to use the new version of the software. Users can continue to use an older version, but once a new version of software has been released, support for older versions is often significantly reduced and updates are infrequent. When a user exclusively uses network or Internet-based software services, the concept is similar to a thin client model, where each user's client computer functions primarily as a network terminal, performing input, output, and display tasks, while data are stored and processed on a central server. Thin clients were popular in office environments prior to the widespread use of PCs [2].

B. *Storage as a Service*

Instead of purchase servers, network equipment, a user can buy a fully service as a whole infrastructure as pay per use [1]. Through storage as a service, users can outsource their data storage requirements to the cloud. All processing is performed on the user's PC, which may have only a solid state drive (e.g., flash-based solid-state storage), and the user's primary data storage is in the cloud. Data files may include documents, photographs, or videos. Files stored in the cloud can be accessed from any computer with an Internet connection at any time. How-

ever, to make a modification to a file, it must first be downloaded, edited using the user's PC and then the modified file uploaded back to the cloud. The cloud service provider ensures there is sufficient free space in the cloud and also manages the backup of data. In addition, after a user uploads a file to the cloud, the user can grant read and/or modification privileges to other users [2].

C. *Processing as a Service*

Processing as a service provides users with the resources of a powerful server for specific large computational task. The majority of tasks, which are not computationally demanding, are carried out on the user's PC. More demanding computing tasks are uploaded to the cloud, processed in the cloud, and the results are returned to the user. Similar to the storage service, the processing service can be accessed from any computer connected to the Internet. One example of processing as a service is the Amazon Elastic Compute Cloud service

IV. REVIEW OF LITERATURE

This review basically discuss, the work performed on information security in distributed system. The security is here been defined for grid and cloud computing system under the cryptographic approach.

1) **Ching-Nung Yang** (2013) has defined a work on data security and integrity in cloud environment to perform reliable service distribution in cloud networks. Author defined a data or storage oriented secure service distribution mechanism so that the service distribution benefit will be taken by the cloud users. Author defined a work on key based authentication for cloud security analysis. Author used a combined secure approach for information sharing using ECC and Diffie Hellman approach. Author used the symmetric bivariant polynomial information sharing system for cloud environment. Author defined a trusted third party system where multi-server system is extended to get fit to the environment. Author defined a multi server system so that effective secure service provider is established. Author proposed an effective secure service mechanism in cloud environment.

2) **J.Mc Dermott** (2013) defined a virtualization process for the military cloud. Author defined the secure communication using cryptography for the military based system. Author provided the secure sharing over the cloud environment under the hardware based data communication with cryptographic security. Author defined an approach called infrastructure virtualization to achieve the secure communication over cloud. Author also performed a secure verification of the system in cloud environment. Author defined the secure kernel system to achieve the systematic secure transmission in cloud system.

3) **Piotr K. Tysowski** (2013) presented a key based secure and scalable cloud environment for the application based security. Author provided a trustful cloud environment to provide the secure communication based on secure key management scheme. Author provide provided the secure application mechanism to achieve the coordination between the owner and multiple users.

4) **Chang-Ji WANG** (2012) provided the attributed oriented encryption analysis with constant size with cipher text. Author provided a new cryptographic algorithm to provide the fine grained data sharing with decentralized access control system. Author defined the secure key policy system with cipher text and to achieve the attribute and private key association over the system. Author provided the trustful cloud storage over the cloud system under the KP-ABE scheme. Author defined an application level secure system to embed the security under the cloud storage environment. Author defined the monotonic structural access over the cloud system and also provided the secure key exchange mechanism using Diffie Hellman algorithm.

5) **Dexian Chang** (2012) defined a trust analysis on cloud environment. Author defined the trusted relationship over the cloud environment under the flexibility and scalability parameters. Author defined the cloud virtualization under the different user domains. Author defined a trusted service domain for multiple user domains to achieve the cloud virtualization platform. Author also provided the inter domain communication and migration facility to provide the reliable communication over the system.

6) **M.Venkatesh** (2012) defined a work over the secure data storage in cloud system with public audit ability. Author uses the internet feature and software support to improve the communication capability in the cloud system. Author defined the secure remote communication to utilize the cloud resources. Author used the AES based secure storage system with public auditing to improve the cloud system. The public key cryptography is here implemented to improve the security support along with reduction of the computation time on cloud system. Obtained results shows that the work has improved the security over the existing method.

7) **Sahil Madaan** (2012) also defined the identity based secure system in cloud environment. Author defined the key based clod communication to provide the deep rooted secure communication. Author provided the secure transmission and resource sharing in cloud environment. The provided technology satisfy the security challenges in cloud system with inclusion of secure computing services. Author presented the implementation on identity based distributed secure system for the data storage in cloud. Author provided the third party based security over the cloud environment so that effective communication will be done in same environment.

8) **Tamal Kanti Chakraborty** (2012) defined a secure cloud based system in the computing environment to resolve the security issues over the cloud based system. Author proposed the homomorphism encryption scheme using ECC. Author provided the secure data processing under different cloud. Cryptography has been around for centuries; as long as there has been communication, there has been the need for privacy and safe, secure methods of transmission. Although many types of difficult problems can be classified as cryptography problems, what we are mostly concerned with today is the ability to keep transmissions private through the use of data encryption techniques. This has become an even greater issue due to the changing nature of communications since the information revolution. More and more people rely on electronic communications for the transmission of sensitive or personal data; e-mail, e-commerce, FTP, and HTML are all examples of technology that have already filtered

into the social consciousness as primary ways for disseminating and gathering information and for exchanging goods and services. While this technological shift has made communication faster, easier, and better in many ways, it has also brought along with it a whole host of difficult problems and social policy issues.

The main problem that comes with electronic communications is the ease with which transmissions can be eavesdropped or impersonated. Paper communications obviously have security problems as well as documents can be stolen, steamed open, have forged signatures or changed contents. However, if someone is trying to catch a specific transmission (or type of communication), it is much easier when dealing with an electronic medium. It is a trivial matter for people to set up programs that systematically scan e-mail for keywords, or that sniff packets in a Telnet session for passwords, whereas randomly steaming open mass quantities of paper mail looking for a certain document is clearly infeasible. Also, since there can be (and often are) multiple copies of any given electronic transmission, it is difficult to know if someone has stolen a copy or somehow altered the original.

Secondly, there is an access control problem. Many electronic transmissions are made in a broadcast manner, as seen with cable or satellite television and wireless phones. People can install devices to intercept these transmissions, and senders usually have no way to either monitor or stop this. In order to prevent unwanted people from making free use of their services, senders must encrypt their outgoing transmissions. To their paying customers, they can give special devices to decrypt the information.

Finally, there is the problem of authentication: electronic communications are impersonal, and can be easily forged by impersonating IP addresses, changing "sender fields" in e-mail, "cloning" cellular phone numbers, and so forth. In order for people to want to - and, indeed, be able to - use electronic communication in the coming years, it is essential that these problems be resolved. Right now, advances in cryptography are the best way to address these issues. Data encryption not only provides privacy and access control by rendering communications illegible to unauthorized parties; it can provide effective authentication as well through the use of digital signatures and timestamps.

9) **Vasyl Ustimenko** (2012) defined a mathematical security aspect for the cloud based system. Author defined the holomorphic encryption with multi variant key cryptography. Author observed the recent analysis on the cloud security using the quantum cryptography. Author provided a key based cryptography under different classes of security. New algorithm was proposed by the author based on the holomorphic encryption and the key formation was done using multivariate dependent key algorithm.

10) **Yingjie Xia** (2010) defined a ECC model over the cloud system to improve the security on cloud system. Author defined a hybrid ECC system for cloud data. It provided a platform to provide secure file communication, backup system and the resource sharing on distributed cloud. Author provided different security levels for different kind of cloud and avail different secure services with confidential protocol and privacy. Author combined the hash key based cryptography and enhance it using ECC to provide secure user control system.

11) **V. D.Cunsolo** (2009) performed a work to achieve the information security in distributed system. To resolve the security problem in network based distributed system, author suggested a light weighted cryptographic approach. The objective of work was to provide a secure asymmetric approach to provide secure communication of data as well as file system. Author proposed a secure distributed file system with asymmetric or symmetric structure. Author defined the secure interfacing with cloud and grid based systems.

V. PROPOSED WORK

1) Problem Statement

Today instead of maintaining the data on individual system, whole data and information is generally placed on some centralized system with distributed environment. Such distributed system can have multiple service providers as well as multiple users. This kind of environment is provided by Cloud environment.

In this work, a secure middle layer is suggested for multiple clouds as the common integrated layer. At the time of registration, user can use single account to access multiple cloud services. According to the type of user, user can also opt the required security features as well as the required cloud services. The security selection will be service based. After the registration process, user can update the security features for selected service or can select more integrated services. Now after the registration, as the user will access the particular service, the security option will get integrate to it. The security options considered here includes the storage related services as well as communication security. To achieve these kind of security, symmetric key cryptography will be used that will be applicable on textual data. In this work AES will be considered as the cryptographic approach. After achieving the secure data storage and authentication, the communication security will also be achieved, by integrated the session based communication.

2) Objective

The presented work will cover the following research objectives

a) The main objective of this work is to define an intermediate security layer between cloud client and servers to integrate multiple clients and server.

b) To provide the secure authentication, Storage and Communication over cloud environment.

3) Scope Of the Work

The presented will provide the secure cloud access with following significance.

a) The significance of work is to provide three level security with authentication, storage and communication.

b) The significance of work is the single authentication for multiple clouds.

c) The significance of work is the updation of security features based on requirements.

4) *Methodology*

In this work, a secure session establishment is been defined for the registered users. The model of the presented system is shown in figure 3.

As shown in the figure, the cloud server is having the raw data or the file as the available data resources. System can have single or multiple cloud system. This cloud server is the top layer that will provide the resources to all users publicly. The users that will perform the data request can be registered user or the free visiting users. The security is here mainly incorporated for the registered users. To provide the security over the system, security is here implemented on the middle layer called the security layer. The work of this security layer is divided in three parts.

The three activities associated with the proposed model are

a. Authentication

The authentication is here provided at two levels. For the free users, the authentication is provided using AES cryptography approach where as for the registered users, the authentication will be achieved using hash key based AES algorithm. As the user will enter to the system, the authentication check will be performed using the cryptographic approach. A free user is a visiting user that can visit the public pages of the cloud but cannot perform any data oriented operation over the cloud. But the registered user is allowed to perform the data downloading on cloud.

b. Secure Session Communication

If the authenticated register user want to download some data from the cloud server, the hash key based session key will be generated. This hash key code will be activated for the specific period. As the session will be established, the next work is perform the secure data transfer on client end from the server. To perform this secure transmission SSL enabled secure tunnel will be generated between the client and the server with specific bandwidth. The communication will be performed using this tunnel. As the communication will end, the session key will be deactivated.

c. Data Management

Data over the cloud will be managed in the cryptographic form. To perform the data encryption over the cloud the AES based cryptography approach will be implemented.

5) *Research Design*

between the cloud and the server. The presented work is the combination of hash key encoding, AES encoding and SSL based tunnel approach to perform the reliable communication over the network. The work will provide the secure authentication, reliable data communication and secure data management over the cloud.

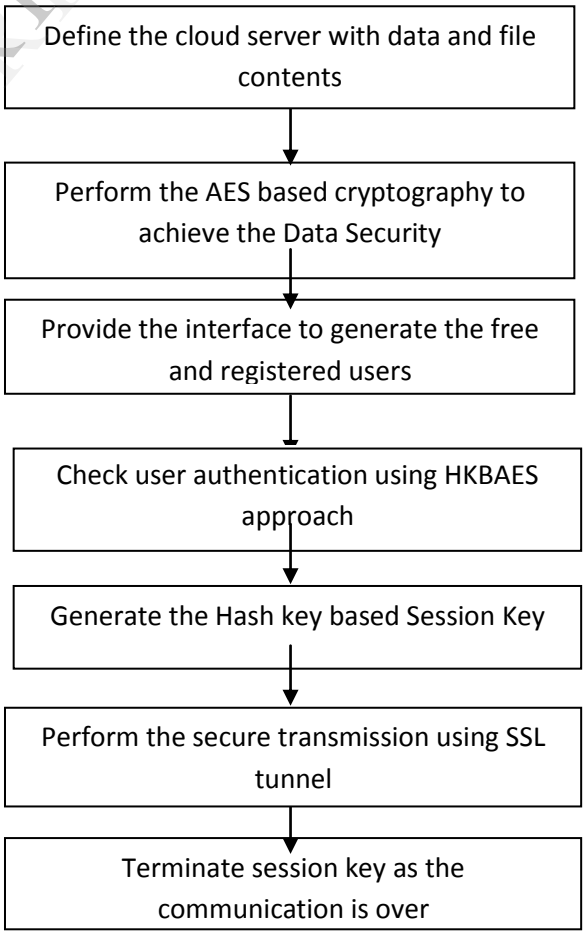

Figure 3: Flow of Work

a) SSL Tunneling

The SSL layer connection is defined for the cloud system to perform the document level or file level transmission. This kind of transmission is controlled by HTTPS, SNEWS or by using some another protocol. It provides the cryptographic transmission over the network. The steps are as follow:

1) As the primary step, the request is performed by the client to access the particular document or the service over the cloud. The request is performed under the secure requirement.

2) As server get the request, it sends the certificate to the client to perform the certificate level handshaking.

3) As client receive the certificate, a check is performed at client end to identify the server entity and to get the trust level. As the trust is verified, the connection can be processed by the server. Netscape navigator and communicator enables the warning messages over the server so that the certificate trust will be verified. It also provides the choice to enable the system.

4) As the client get the certificate, the next work is to provide the information distribution over the web to provide the domain level security. This security information is compared to provide the secure trust level matching so that the security get enable to the system.

5) The client will inform the server about the key and the cipher type so that secure communication will be performed.

6) Server basically enable the cipher type based on the security level required.

7) Now this cipher is used by the client to generate a session key. It uses the symmetric encryption so that secure transmission will be performed.

8) Client perform the session key encryption and send it to server side and enable the secure session.

9) As the server get the secure encoded key, the decryption is performed by its own private key.

10) Now this key pair enable both client and server to perform secure transmission between client and the server.

6.) *Algorithm*

HKBAES(Text)

/*Text is the information that we have to encrypt*/

{

1. Divide the Text in N message Blocks of Equal Size (512) bits called m1,m2,m3…….mN.
2. For i=1 to N

   {
3. Divide the Message in M sequence words called W1,W2….WM
4. WT = W1 Xor W2 Xor W3…..Xor WM

   [Ex-Or all Sequence Word Blocks to generate the aggregative word]
5. Define two hexa blocks H1 and H2 to represent the sub register values for Hash Processing.
6. Set H1=WT
7. Perform WT Cyclic Shit for 1 bit
8. Set H2=WT
9. AggH1=AggH1 U H1
10. AggH2=AggH2 U H2

}

}

VI . CONCLUSION

The present work is to avail a secure service cloud publicly. Here the service cloud is providing the services like uploading, downloading etc. This cloud is available to all users in an authenticated way. The authentication is performed on each file on service cloud. A file can be uploaded by the admin only. As the uploading process is performed the file is first encrypted by using the private key cryptography. Admin encode the file by using his private key and upload it on specific servers. As the client enter to the system, he can download the file by selecting the appropriate server and by providing the authentication key to the system. The uploading and downloading is performed using secure SSL tunnel. So the proposed work can be beneficial to all the business association that works with the cloud or the distributed environment.

VII . FUTURE WORK

In this presented work, the files are uploaded to different service cloud and security is being achieved by using the public key cryptography and SSL layer. But here we have encoded the complete file contents, if the file size is large it will take much time in encryption and decryption. In future we can use the concept of message digest to encode a file partially or the header of the file only. We can also implement some other cryptographic techniques to perform the data security over cloud.

REFERENCES

[1] Vijay Prakash Sharma, Devaang Soni "Cloud Computing and Emerging Security challenges", International journal of Engineering research and technology, 2014.
[2] Schridde, "An Identity-Based Security Infrastructure for Cloud Environments", 2010
[3] Akhil Behl, "Emerging Security Challenges in Cloud Computing", Center of Excellence, Advance Services, Cisco Systems.
[4] Young-Gi Min, Hyo-Jin Shin,Young-Hawn Bang, "Cloud Computing Security Issues and Access Control Solutions", Journal of Security Engineering, February 2012.
[5] Huaglory Tianfield, "Security Issues In Cloud Computing", IEEE International Conference on System, Man, and Cybernetics, October 2012
[6] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, 2011.
[7] Shucheng Yu, Cong Wang, Kui Ren, Wenjinng Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", IEEE Infocom, 2010.
[8] Anas Bouayad, Asmae Blilat, Nour el houda, Mohammmed El Ghazi, "Cloud Computing: Security Challenges", LTTI laboratory, 2012
[9] Balachandra Reddy, Ramakrishna Paturi, Dr. Atanu Rakshit, "Cloud Security Issues", IEEE International Conference on Service Computing, 2009.
[10] Wentao Lio, "Research on Cloud Computing Security Problems and Strategy", IEEE, 2012.