Open access Journal International Journal of Emerging Trends in Science and Technology

A Framework for Data Storage Cloud to Provide Security

(By Implementing Encryption through User Private Key)

Authors

Imran Ijaz, Aisha Shahzadi, Komal Riaz, Sehrish Sabir

Fatima Jinnah Women University
Rawalpindi, Pakistan
Email: *imran-ijaz@live.com, aishayounas260@gmail.com, t.tabeer@yahoo.com, seher6500@gmail.com*

Abstract

This research focuses on making the cloud more secure for sharing data. The need of more storage space to hold all your digital property is solved by the cloud storage. But the question arises that all your personal data is safe over the internet? Passwords can be hacked; data can be decrypted by Cloud Server. So for building users' trust in the cloud storage we present a model that provides multi-layer encryption. The cloud has its own certificate store but in our model we present an idea that enables user's data not to be viewed by Cloud servers but only users and the ones whom they allow access. The users' can buy the certificates from a company, any third party that is not involved with the Cloud Storage service. Users encrypt the data through their certificates and then share the data on the cloud. The cloud is considered safe and it is the need of the time to have large storage space for your digital property but we present a way to eliminate the threat in cloud computing.

Keywords – *Certificate, Encryption, Public Key Infrastructure (PKI), Certification Authority (CA), Domain Controller.*

I. Introduction

Our model is to develop a cloud storage environment where users are allowed to share data securely. Cloud storage provides more scalable and efficient way to store data. Cloud storage is cost efficient way to store data and it is the easiest place to explore large collections from computing perspective. Now a days cloud computing is very common but it invites risks along with the advantages it provides. In our model we propose an approach to apply encryption on the data files that are being shared by different users and the encryption is double layer encryption. To provide an increase level of assurance for trading the information over the insecure internet security architecture is being introduced that is known as Public Key Infrastructure? PKI is a combination of methodologies, tools and technologies that together provide a secure infrastructure. It is the use of public and private key for the authentication. Public Key cryptography is a mathematical technique. PKI services can also be used on the information that is being transferred on private networks.

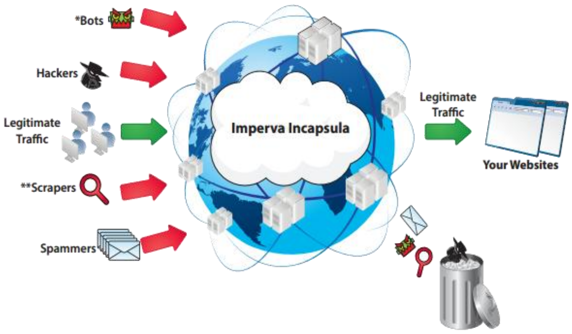


Figure 1: Cloud Security Threats

To avoid the intruder party which happens to be in the way pretends to be the target this kind of scenario is known as man in the middle attack. Two different parties are involved in double encryption. The involvement of two different parties makes the system more secure because if one party leaks the key still data is safe and cannot be used by unauthorized users. Once the encryption is applied on the data, then all the files with the help of certificates that are issued by the public key infrastructure Certificate Authority. The other side can decrypt the data available if it has authority to do so; it will provide the private key first and then through the certificate it will decrypt the data. In case the key is leaked then certificate will maintain integrity of data and keep it confidential and impossible to decrypt for intruders.

This system is being developed for the users of basically unsecure public network such as the Internet to securely and privately exchange data files through the use of a public and a private cryptographic key pair and encryption and another party that issues certificates for secure communication.

II. Literature Review

In this section, a survey is done on the previous work related to our field.

This paper is about Yanching and Youcheng model. They developed a system for sharing over the cloud without the need of key distribution and data re-encryption. [1] In this model, efficient user revocation, Stateless Cloud and Direct Security Guarantee is there.

*A*s we know that there are different users who are sharing data in the cloud and they used to share data with some of the consumers but now they may not want to share them with some of the consumers now. So, the revocation from certain consumers is a big issue as the whole data is to be re-encrypted and then a new decryption key will be given to everyone. This will cause a lot of headache and budget overruns. And also, as we know that there are different security threats when the data is stored in the cloud. It can be said that cloud has a huge sea of harmful users. So, we are using “Attribute Based Encryption”. It means that the accesses are given on the bases of the attributes. It is a form of more finely grained access control.

As we know in the traditional encryption mechanism, a user would encrypt her data using his public key and all other can decrypt the data which have the user’s private key. But ABE (Attribute Based Encryption is a bit different). In this, during encryption there is a very complex access control policy and during decryption, there are two types of ABE. One is Key Policy ABE and other is Cipher Text ABE. In key policy ABE, we associate the cipher text with some attributes and then we issue a private key according to our access controls. In cipher text ABE, we create the cipher text with the preconditions having the access control policies and issue the private keys with association with attributes. In this scheme, input is the “security parameter” and the outputs are a public key and a master key. Proxy Re-Encryption (PRE) has inputs the “security parameter” and output is the “Param” in which detail about the plain text space is given.

*N*ext there is stateless cloud which means that the history of the cloud will not be saved about what users are not having permission to access the cloud will not be saved in the cloud. As there are hundreds of users who have been revoked, hence no information will be retained.

*T*he security of those algorithms which are ABE, proxy encryption scheme and symmetric key encryption scheme is retained so this model has a retained all those security features. In ABE, there are different access rights for each set of users and thus flexibility in the rights granted to user is achieved. The user will be able to access the data only if the values of cipher text and user’s key are same.

*T*his model still has some drawbacks, one of which is that at the time of access to the data by the user, the user’s privacy is not maintained and its attributes can be compromised. As the information of attributes is also the user's identity information so it may be the case that the cloud servers access all the information of a user's identity.

The second paper discusses that as we know that if sensitive data is being shared on the cloud then it may be very harmful for the user so Zhousong Liu has presented a technique of "identity based group signature" and then it is applied for "anonymous" user authentication. [2]The occurrences of user grant and user revocation will also be done by the group techniques. Group signature will be used in this model

A. Group Signature:

*I*n this model, any one group member does signature on behalf of the whole group. The power is with all the group members to do signature but his/her identity is hidden and only the "group manager" will know about the signer.

*I*n this model, and "efficient-identity based group signature" will be constructed. It is a combination of "group signature" and "identity based scheme". Now it means that it will be a group signature and the verifying public key which is to be used will be the identity of the group. So in this way, two schemes are joined and both of their characteristics are added in this model.

This will have 6 steps which are:

- Setup
- Extract
- Join
- Sign
- Verify
- Open

There are four entities. It consists of data owner, data user, Cloud servers and Third Party Auditor. Third party Auditor issues unnamed credentials are issued to the users. The user has to perform anonymous authentication to access the files of the remote stored data. An immense ability of storage and a large power of computation are there. Cloud Service Benefactor operates the cloud servers and always online. Every file access event is audited by the third party auditor and it is also online. Storing data files and running the code of cloud servers are done by the data owner. The cloud servers will not be able to know the identity of any users.

III. System Architecture

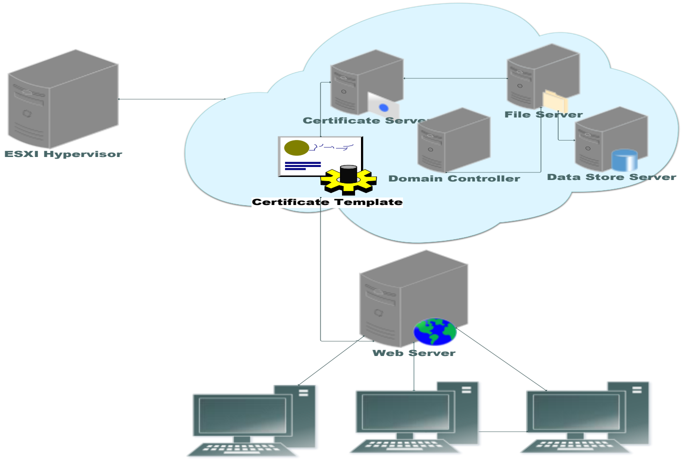


Figure System Architecture

A. System Components

a) Certificate Authority:

*T*he certificate authority (CA) issues the digital certificates.

b) Domain Controller:

*W*ithin a Window Server Domain responding to security authentication requests such as logging in, checking permissions, granting access is the main function of domain controller (DC) server. It allows host to access domain resources. The domain controller enforces a security policy it's responsible for storing user account information and authenticate user.

c) Hypervisor (ESXI)

Virtual Machine manager is called a hypervisor. Multiple operating systems are allowed to share a single hardware host through this program. Host's processor, memory and other resources are held by the operating systems to themselves. Hypervisor is responsible for controlling the processor and resources of the host, the need of each operating system is fulfilled by allocating the specified resource and making sure that the virtual machines do not interrupt each other.

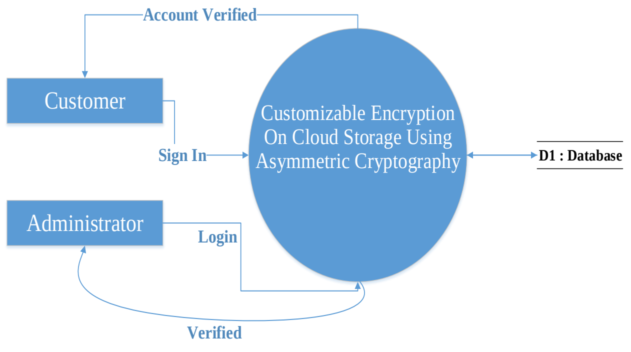
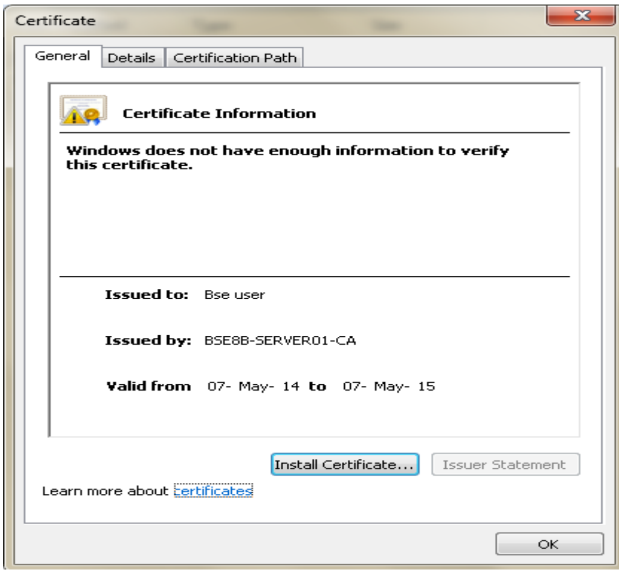

Account Verified
Customer
Sign In
Customizable Encryption On Cloud Storage Using Asymmetric Cryptography
D1 : Database
Administrator
Login
Verified

Figure3: *Context Level Systems DFD*

B. Certificate Template:



Certificate Information

Windows does not have enough information to verify this certificate.

Issued to: Bse user

Issued by: BSE8B-SERVER01-CA

Valid from 07- May- 14 to 07- May- 15

Learn more about certificates

Figure 4: Certificate Template

IV. PROBLEM STATEMENT

As normal techniques are used to provide network security, can those techniques also be implemented on cloud security? If yes, can this secure the data during transit or at rest?

Deploying Double Encryption through Secure Socket Layer (SSL) certificates and private key of the user will enable users to share data by maintaining integrity of data and retaining its confidentiality making incredible for attackers to decrypt data files.

V. IMPLEMENTATION

An IaaS (Infrastructure as a Service) developed which one of the service models of cloud is computing. Cloud computing enables a person to use computing as a service and this service is given to users over a network which is mostly internet. In IaaS, a virtual machine is offered to the user by the cloud. Virtual machine provides storage, certain software and disk image library etc. This virtual machine will be run on a hypervisor which could be VM Ware ESXi, ESX, KVM, Oracle Virtual Box etc. In our model we are using ESXi which is an extended version of ESX. VMware ESX and VMware ESXi are both Type 1 hypervisors. The virtual machine developed will be run as guest on the ESXi.

In this model, there are 4 parties involved.

1. Cloud PKI Provider
2. User
3. Company to generate certificate for 2nd Cloud Server
4. Encrypting software

A. The work of this model is as follows:

1. A certificate is to be generated as per company and user requirements.
2. For generating this certificate, a setup of PKI is generated.
3. Firstly a DC (Domain Controller) is made and then policies are made for the certificates.
4. Then a setup of PKI is applied. User will issue certificates and here first level of encryption will be done.

a) Phase 1:

DC (Domain Controller) is made.

b) Phase 2:

PKI Setup is made.

c) ***Phase 3:***

Certificates are exported.

d) ***Phase 4:***

Encryption of data which is transferred.

B. Overall Working:

*F*irst encryption of the file is done by the user before sending the data to the cloud. This encryption will be done by the user generated certificates which are made by the user. Then we will use encryption software to encrypt the file with self-generated certificate. The software used can be secure zip or PKI zip. (The certificate can also be taken from another company which acts as 4th party in our model).The advantage of this user encryption would be that if the data stored on the cloud is compromised then the person cannot know the contents of the data. Only he will get the encrypted data and the decrypt password will only be *with* owner of the data who is sharing data on the cloud.

*A*nd for doing decryption, the opposite sequence of encryption will be done. In our model we are using hash function for encryption and the certificates made are having this hash function which is SHA1 algorithm.

The main properties of the hash function are:[4]

a. Hash value can easily be calculated from the input message

b. It is impossible to recreate the message from the hash value

c. It is impossible to change the message unless the hash is also changed

d. Two different inputs can never have the same hash

e. A small difference in input can create a lot difference in the output

C. Customizable Encryption:

We will do customizable encryption as per the requirements of the user. If a very high data is to be encrypted, then we use 2048 bits of data for encryption purpose, so more security will be given.

D. Dual Encryption:

We will perform double encryption on data so that if the encryption done by the cloud is somehow insecure then our own encryption will enable securing the data.

Algorithm of the model:

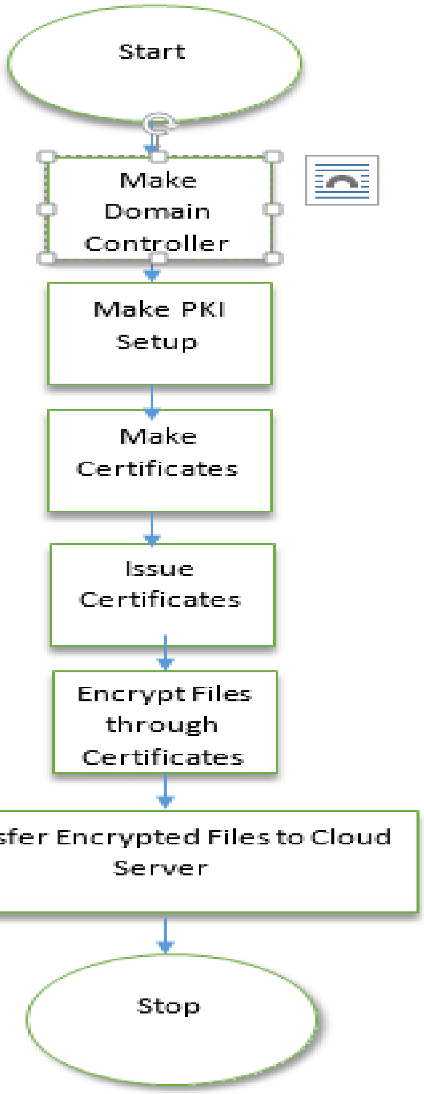


Figure 4: Algorithm of Model

Some hardware and software requirements of the system are :

Software Requirements:

- System: 64 or 32 bit operating system

- Windows Server 2008 for Domain Controller
- Windows Server 2008 for development of Public Key Infrastructure
- Windows 7/ Windows Vista for Client PC

Hardware Requirements:

- 8 GB RAM
- Dual Core or higher speed processor

VI. Testing/Performance Analysis

*T*esting through URL and SSL URL is done by uploading 697MB files of encryption (compression) and without encryption.

*U*ploading file in cloud storage (URL) with encryption will take 50 seconds.*In https, u*ploading file in cloud storage (URL) without encryption will take 3 minutes. *U*ploading file in cloud storage (URL) with encryption will take 2 minutes.

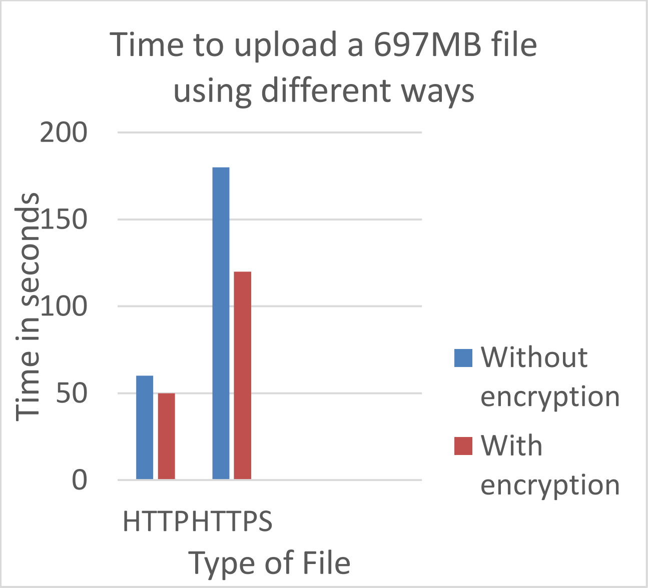


Figure 3: Time for uploading files

VII. Results

*S*o, the testing results tables shows that in http, the encrypted file is uploaded fast and there is a 1 minute advantage of a file of size 697MB. The uploading of files in http is faster but the secure one is https.

VIII. Conclusion

*T*he main conclusion of the project is that the cloud storage provides excellent way of sharing data among users but the foremost fact is that it is not very secure but our model has made a little development in this area. The implementation of Public Key Infrastructure on cloud is effective. We have secured the data and it cannot be decrypted by the cloud server himself unless user does not give permission. It is secure from intruders and hackers. As with the increase in IT the risks are also increased by Multi layered encryption this model is able to reduce risk in cloud storage has amplified security and can be used to revive user's trust in data storage on the internet.

References

1. Yanjiang Yang and Youcheng Zang, "A generic scheme for secure data sharing in cloud", International Conference on parallel processing workshops, 2011:5
2. Zhusong Liu, "A secure anonymous Identity based access control over cloud data", School of Computers, Guangdong University of Technology, China, Fourth International Conference on Emerging Intelligent Data and Web Technologies, 2013:7
3. Preeti Garg, M.Tech CSE Scholar, Dr. Vineet Shanna ,Professor Dept. of CSE , "An Efficient and Secure Data Storage in Mobile Cloud Computing. Through RSA and Hash Function" , KIET Ghaziabad, International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 :8
4. "Cryptographic Hash Function" , 5th August 2014, http://en.wikipedia.org/wiki/Cryptographic_hash_function
5. Imran Ijaz, "Design and Implementation of PKI (For Multi Domain Environment)," International Journal of Computer Theory and Engineering vol. 4, no. 4, pp. 505-509, 2012.

6. Z. Javaid and I. Ijaz, "Secure user authentication in cloud computing " in Information & Communication Technologies (ICICT), 2013 5th International Conference, Karachi Pakistan, 2013, pp. 1 – 5.

7. Imran Ijaz, "Securing user Authentication through Customized X.509 in Cloud Computing", International Journal of Soft Computing and Engineering (IJSCE), Volume-4, Issue-3, July 2014, pp. 90-94.