International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 2 17 – 20

Securing User's Data on Cloud Using AES

Miss. Gauri Wagh
Dept: Information Technology,
Shah And Anchor Kutchhi
Engineering Collegr Chembur.
Mumbai ,India .
Email-gauri1995wagh@gmail.com

Miss. Shruti Gurav
Dept:Information Technology,
Shah And Anchor Kutchhi
Engineering College,Chembur.
Mumbai ,India.
Email-guravshruti2712@gmail.com

Mr. Sagar Vira
Dept:Information Technology,
Shah And Anchor Kutchhi
Engineering College,Chembur .
Mumbai ,India
Email-virasagar@gmail.com

Mr. Mitesh Dung
Dept:Information Technology
Shah And Anchor Kutchhi Engineering College,Chembur
Mumbai ,India
Email-miteshdung494@gmail.com

Prof. Archana Chaugule
Dept:Information Technology,
Shah And Anchor Kutchhi Engineering College,Chembur
Mumbai ,India
Email-sakec.archanac@gmail.com

Abstract: Data security is a major issue in our day to day life in IT field, but in cloud it is particularly of serious concern since data is scattered at different places all over the globe. To this trustworthy environment there is lot usage of cloud done for scattered environment. Cloud computing security or, more simply, cloud security is an evolving around sub-domain of environment in cloud computing paradigm, Rajkumar Buyya Wiley publications in, more broadly way, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

Keywords: *Cloud Computing, Cryptographic algorithm, Computing Services, IaaS, PaaS, SaaS.*

*****

I. INTRODUCTION

Cloud computing is a resource model for providing convenient way and, on-demand analysis of network access to a shared(network) pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimum use of management effort with specified criteria or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics such as mobility, feasibility three service models such as Iaas, Paas, SaaS and four deployment model such as private cloud, public cloud, hybrid cloud, community cloud.

2.Literature Survey

The analysis behind this work of security could be subdivided into this 3 different sub- fields:

1. Study of cloud computing and various cloud computing models IaaS, PaaS, SaaS etc. Study of different business models and study of service level agreements.
2. Study of security issues in cloud.
3. Study of Cryptography.

2.1 Overview of cloud computing

This topic describes the combination of logical entities like data, software ,cloud computing analysis, enhancement of work to the deployment model i.e private cloud which are accessible via internet. Client(user) data is generally stored in restricted area of servers spread across the globe. Historically, each software like a phrase processor requires a license software to be installed on client's(user's) machine. However with this workgroup becoming more highlighting, the client-server model arrived to real world existence, which provided large storing capabilities allowing users to host applications with data for work area. The client machine would demand for a browser to get into these server functionality for access of data with it's privacy, and would use CPU and memory for processing. Cloud computing will vary from traditional client-server model by providing applications from the server which are processed and well managed by a client's internetworking browser, with no installed client version of a credit card application require. Cloud providers helps the client from software from one peak point to another of authenticated license management etc. since the services are accessible via internet, gprs . Software as a Service

(SaaS), given by cloud company, for proper and beneficial software.

• PaaS

Platform as a Service (PaaS) as the name justifies, cloud platform for deployment of user application for security, confidentiality, integrity but doesn't give control of underlying hardware of usage of system or infrastructure (storage, network).

• IaaS

Infrastructure as a Service (IaaS) wherein limited accessibility of infrastructure is provided to the client for storage, network, execution etc. The client can deploy and execute is application using their own infrastructure, the advantage of infrastructure cloud pays an attention for the user to buy from both the top down servers, software's, data-center space, network infrastructure etc. Hence the clients are charged on per-use basis wherein he/she uses the data software.

2.2 Security issues in cloud

Every coin has 2 side, and hence within the same in cloud computing which has no exception. There is criticism about privacy in cloud model, because of the tackle fact that administrator authorization is been done to the system's access to data stored in the cloud. They can unintentionally or intentionally access the client data. Traditional security or protection techniques need reconsideration for cloud. Except for private cloud where the system maintains it's own organization does not have control over the equipment, the progress of cloud is seems little slow, because organizations think instead of compromising on the security of the data, they are still willing to invest in buying private equipment to setup their own infrastructure. Security issues which are of concern to the client can be classified into sensitive data access, data segregation, bug exploitation, recovery, accountability, malicious insiders, and account control issues. Like different disease have different medicines, different cloud security issues have different solutions, like cryptography, use of more than one cloud provider, strong service level agreement between client and cloud service provider. Heavy investment is needed to secure the compromising data in cloud. Cloud can grow only if it is possible to build a trust in client, and which can be built only if security concerns are being addressed. Following are some of the concerns:

1. System Complexity

Compared to traditional data center the cloud architecture is much more complex. Therefore while considering security, security of all these components and interaction of these components with each other needs to be addressed.

2. Shared Multitenant Environment

Since the clouds need to provide service to millions of client, a logical separation of data is done at different level of the application stack. Because of which a 8 attacker in the face off client can exploit the bugs gaining access to data from other organizations.

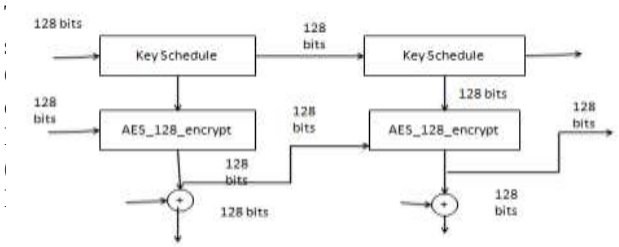
3. Internet-facing Services

The cloud service which is accessed over the internet via browser, the quality of service delivered on the network is another concern.

4. Loss of control

As the data of client is stored anywhere across the world control loss over physical, logical of system, and alternative control to client's assets, mismanagement of assets are some additional concerns.

5. Advanced Encryption Standard (AES)



.

The AES supplanted the DES with new and upgraded gimmicks:

•block encryption usage

•128-bit bunch encryption with 128, 192 and 256-bit key lengths.

• 20-30 years for data security.

II. SYSTEM DESIGN

In the proposed design, a hash service data integrity verification, encryption/decryption service, and provision for defining list of people which can access data securely, is provided by a trusted 3rd party which is separate from the storage cloud provider.

3.1 Business Model with separate encryption/decryption and hashing service.

3. Services provided

- **SaaS**

The system provides hash, access list, encryption/decryption by a trusted 3rd party over the network in the form of "Software as a Service" (SaaS). The system has a separate storage service which is also provided as a SaaS. The data storage for each client is done in database in the form of "BLOB". The trusted 3rd party which provides these security services does not store any data at its ends, and stores only master key for each client for data encryption and decryption, and hash of the data which is calculated on client side. To enhance the security, the communication between client and security server is secured using Diffie Hellman key, which is used as a input for AES. This division of responsibility has big effect, as no single provider has access to other data and security key, hash at the same time.

Diagram

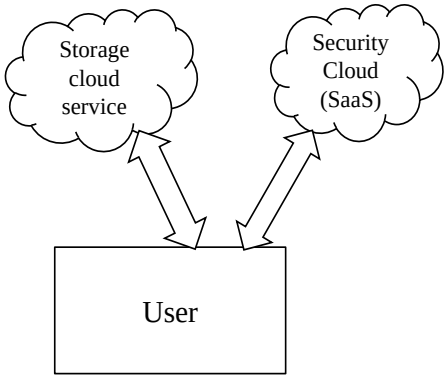


Figure 3.1: System Architecture

Figure Is an overview of the architecture where storage and encryption/decryption/hash services (security services) are separated. For example (as described in chapter 1, Motivation) a small or medium scale business who wish to store all its account related data in cloud storage, will first calculate the hash of the data, encrypt the data using encryption
Figure 3.1: System Architecture service and then store the data in storage provided by separate provider. The system also provides functionality where other users from small scale business Company will be able to access data which is stored in cloud storage. The sessions between client and security server is secured using DiffieHellmen Key and AES as the encryption algorithm. SHA-1 is used for calculating the hash of the data, and AES is used a encryption/decryption algorithm for computing cipher at security server end.

3.2 Typical Scenarios In Design

Typical 3 basic scenarios are, user data upload, user data download, group user access. In this section we discuss the each of these scenarios.

3.2.1 Data Upload Scenario

1. The end user login to the system with his/her username & password.
2. Once the user is authenticated, the Diffie Hellman key is exchanged for the session.
3. Now a user can select the files which he/she wants to upload it to storage cloud.
4. The user can also select is he/she wants to share the file with specific users.
5. The hash of the data in file is calculated, using SHA-1 (originalhash).
6. The data in file is now encrypted using DH keys.
7. The complete encrypted file and original hash of file data, are now transferred to Security Cloud.
8. At Security Cloud, encrypted files is decrypted back using DH key, while the hash is sorted in security cloud database.
9. The decrypted file is now encrypted with Symmetric Algorithm namely AES, using the Master Key generated for each user during user creation.
10. File ID, original hash (file/data hash), master key for each user are stored in Security Cloud database.
11. The Security Cloud now discards any contents of the files from its system, and does not store any file contents in its system.
12. The Encrypted file is sent back to user, to be uploaded to Storage Cloud.
13. The user now can upload the encrypted file to Storage Cloud.

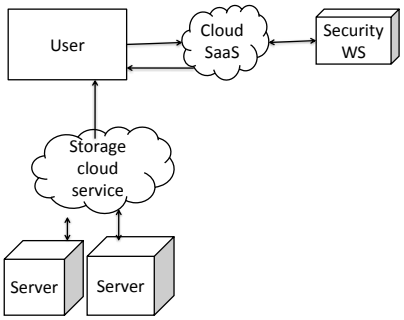


Figure 3.3: User Data Upload Scenario

3.2.2 User Data Download Scenario

1. The end user login to the system with his/her username & password.
2. Once the user is authenticated, the Diffie Hellman key is exchanged for the session.
3. Now a user can select the files which he/she wants to download it from storage cloud.
4. The encrypted file is now downloaded from storage cloud to user's machine.
5. The complete encrypted file is now transferred to Security Cloud.
6. The data in file is now encrypted using DH keys.
7. The complete encrypted file and original hash of file data, are now transferred to Security Cloud.
8. At Security Cloud, decrypted files with Symmetric Algorithm namely AES using Master Key stored in security cloud database for each user.
9. The decrypted file is now encrypted with DH key.
10. The DH encrypted file and hash of the corresponding file is now passed to the users.
11. At user end, on receiving the encrypted file, it is decrypted with DH keys.
12. The hash of decrypted file is calculated using SHA-1 and original hash are now compared to see if they match, and accordingly appropriate message like, File tampered or File is intact are flashed on user screen. Thus the integrity of the data is verified.

3.2.3 Group User Data Download Scenario

1. The end user login to the system with his/her username & password.
2. Once the user is authenticated, the Diffie Hellman key is exchanged for the session.
3. Now a user can select the files which are shared by other user.
4. The encrypted file is now downloaded from storage cloud to user's machine.

5. The complete encrypted file is now transferred to Security Cloud.
6. At Security Cloud, decrypted files with Symmetric Algorithm namely AES using Master Key stored in security cloud database for each user.
7. The decrypted file is now encrypted with DH key.
8. The DH encrypted file is now passed to the group users.
9. At user end, on receiving the encrypted file, it is decrypted with DH key.

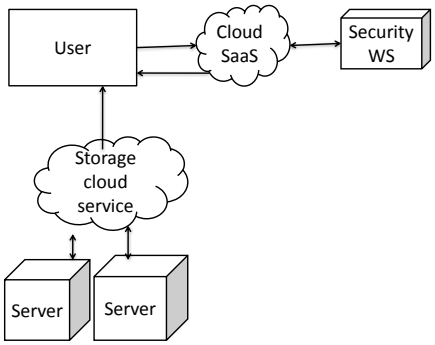


Figure 3.4: User Data Download Scenario.

10. The group user can now view the file; & the data integrity is also verified at group user's end.

Since the responsibility is divided between 2 providers, Storage Cloud provider and Security Cloud provider are different, the Storage Cloud provider although has access to file/data, it is in encrypted format, and it has no access to any kind of encryption/decryption keys. Second, as the Security Cloud only stores user's master key and encrypted data hash, and does not store any data/file, therefore it has no use of the keys. In case the data/file is tampered anywhere it will be caught during the integrity verification. Third, while the session keys are established during the user login, all the cascading data transfer is secured. This allows the user to access its data from any machine, which is one of the definite of cloud services. Thu s the user data transferred and stored in secured manner in storage cloud. Fourth it is possible to share data with preferred band of people securely.

3.3 Algorithm selection

In this section we discuss some of the advantages of selection of particular algorithms over the other. We begin with discussion of AES.

3.3.1 Selection Of AES

Broadly speaking the encryption/decryption can be done via symmetric key or asymmetric key. In symmetric algorithms, both parties share the secret key for both encryption/decryption, and from privacy perceptive it is important that this key is not compromised, because cascading data will then be compromised. Symmetric encryption/decryption requires less power for computation. On the other hand asymmetric algorithms use pairs of keys, of which one key is used for encryption while other key is used for decryption. Generally the private key is kept secret and generally held with the owner of data or trusted 3rd party for the data, while the public key can be distributed to others for encryption. The secret key can't be obtained from the public key. In our case since the encryption/decryption is performed on trusted 3rd party server, symmetric key is used, and it delegates the burden of key management to the trusted 3rd party.

If key management where to be done at clients end it would mean,
1. Either they have to remember the big key.
2. Store the key in all devices/machine which will be used to access the cloud services, which make user device a bottleneck.
3. Individual owner has to take the responsibility of sharing the key with specific authorized group of user which he/she define.

While on the other hand using symmetric key encryption the master key or private key usage which would be stored in security cloud provider per user gives the client the advantage like,
1. Freedom from remembering any key.
2. Client can use any device/machine to access the data stored in cloud.
3. The client need not worry as to how the data will be shared securely, the client just need to define the individual whom he/she wants to share the data with.

3.4 Technologies Used

In order to implement a cloud architecture or a Software As A Service (SaaS architecture) we need
1. Web Service – Need to implement a web service.
2. Glass-fish Server – to host web service
3. SOAP API – to be able to call web service at client side we need to use SOAP API or even XML. Version
3.2. 4. Java 1.6.18 5. Operating System Windows 7. 6. MySQL 5.2. 19

Access control policies are to be established and client identities are to be checked. Datacenter platforms, infrastructure and client devices are to be secured by trusted computer policies.

III. CONCLUSION

To have physical and virtual controls in the cloud environment one must protect data by implementing strong encrypting techniques using secure connections and applying data loss prevention policies .

Access control policies are to be established and client identities are to be checked. Datacenter platforms, infrastructure and client devices are to be secured by trusted computer policies.

REFERENCES

[1] "Secure virtualization for cloud computing "Flavio Lombardi, Roberto Di Pietro, June 2010
[2] IDC (2009) Cloud Computing 2010 – An IDC Update.slideshare.net/JorFigOr/cloud-computing-2010-an-idc-update
[3] K. S. Suresh, Prof K. V. Prasad, Security Issues and Security Algorithms in Cloud Computing ,International Journal of Advanced Research in Computer Science and Software Engineering, Hyderabad, 10, October 2012 .