A Survey on Data Encryption in Cloud Using KDC

Reenu Lathwal1 and Vinod Kumar Saroha 2*

1 Dept. CSE, BPSM University (Sonipat) HARYANA, India,
2* Dept. CSE & IT, BPSM University (Sonipat) HARYANA, India,

Abstract

Cloud Computing offers services to end-users rather than a product, by sharing resources, software and other information under a pay per usage model, hence economic benefit is the key for Cloud in terms of capital and operational expenditure. It permits hosting of different types of applications such as business, scientific and social networking because it has key characteristics like multi-tenancy, scalability, performance and security etc.

Cloud Computing is currently facing challenges like Data Security, Energy Consumption, Server Consolidation, Virtual Machine Migration to name a few. Existing approaches of secure data transfer use two tier authentications, either based on OTP (One Time Password) which is static in nature and requires additional software/hardware or Digital Signature which leads to the problem of key management. This research work focuses on the study of secure data transfer by using different combination of mechanisms which not only ensure two tier authenticities without involving any above mentioned overheads but also maintain the confidentiality of data and integrity of message using one time key generation. In this thesis, existing secure data transfer techniques have been compared. This technique uses OTP and HMAC with Diffie Hellman Key Exchange to enhance data security in terms of authenticity and integrity in Cloud Computing environment. In this mechanism Optimally Modified HMAC has been used to prevent the man-in-middle-attack. An encryption algorithm has been used to maintain the confidentiality of data in transmits. Flow of the execution stages has been described using Flow Diagram and Sequence Diagram while for simulated environment; MATLAB Toolkit has been used to validate the experimental results of HMAC.

Keywords: - Cloud computing, data privacy, fine-grained access control, attribute-based encryption, ciphertext policy, OTP, HMAC.

1. Introduction

In the Cloud computing services, it can be used from widespread and assorted resources, relatively than remote servers or local machines. There is no usual definition of Cloud computing. Generally it consists gathering of distributed servers known as expert, providing demanded services and resources to dissimilar clients known as clients in a network with steadfastness and consistency of datacenter. The distributed computers provide on-demand services from various resources. Services may be of software possessions e.g. Software as a performance, SaaS e.g. Platform as a Service, PaaS e.g. Hardware as a handler, HaaS or Infrastructure as a Service, IaaS. Amazon EC2 (Amazon Elastic Compute Cloud) is also an example of cloud computing services [2].

1.1 Cloud Components

A Cloud system consists in three components such as datacenter, clients, and scattered servers. Each one element has a decided purpose and plays a specific role in it.

1.1.1 Clients

End users work together with the clients to direct information related to the cloud. Clients mainly fall into three categories as given below [1]:

- Mobile: Smart phones, Windows Mobile Smartphone, like a Blackberry.
- Thin: They don’t do any working out work. They only present the information. Servers do all the installation for them. Thin clients don’t have any internal memory.
- Thick: These apply different browsers like IE or Mozilla Firefox or Google Chrome to attach to the Internet cloud.

Today thin clients are more popular as compared to other because of their low price, low security, low use of power, less noise, easily repairable and easily replaceable etc.

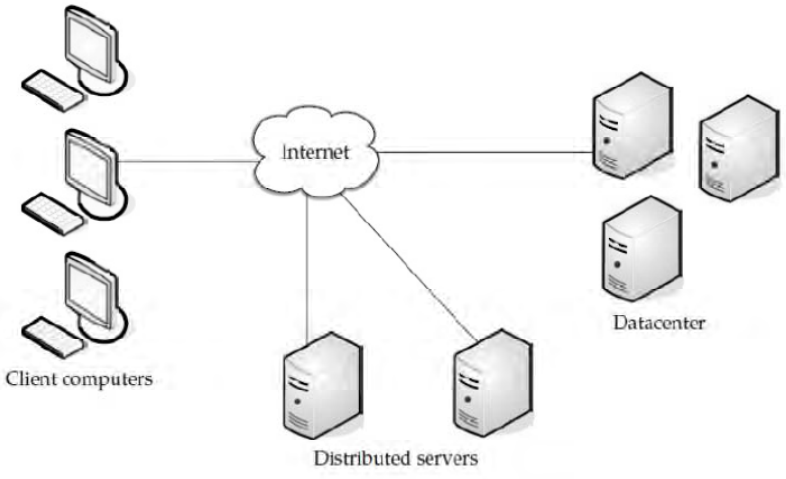

Figure 1.1: Three components make up a cloud computing solution (adopted from [1]).

1.1.2 Datacenter

Datacenter is a group of servers hosting diverse applications. A user connects to the datacenter to promise different applications. A datacenter may subsist at a large distance from the user.

Now a thought called virtualization is used to mount software that allows various instances of virtual attendant applications.

1.1.3 Distributed Servers

Distributed servers are the parts of cloud servers which are present during the Internet hosting dissimilar applications. But while using the request from the cloud, the client will feel that he is via this application from its personal machine.

1.2 Type of Clouds

Based on the province or environment in which clouds are second-hand, clouds can be divided into three categories:

- Public Clouds
- Private Clouds
- Hybrid Clouds

1.3 Virtualization

It is an especially use full concept in framework of cloud systems. Virtualization means “somewhat which isn’t valid”, but gives all the facilities of an actual. It is the software performance of a computer which will execute dissimilar programs like an actual machine.

Virtualization is associated to cloud, because using virtualization client can use different services of a cloud. The isolated datacenter will provide dissimilar services in a full or incomplete virtualized manner.

Two types of virtualization are established in case of clouds as given in [1]:

- Full virtualization
- Para-virtualization

1.3.1 Full Virtualization

In case of full virtualization an absolute installation of one apparatus is done on than other apparatus. It wills outcome in a virtual apparatus which will have all the software’s that are nearby in the actual server.

Figure 1.2: Full Virtualization (adopted from [1]).

Here the isolated datacenter delivers the services in an abundant virtualized way. Full-virtualization has been doing well for several purposes as meaningful out in [1]:

- Sharing a computer system between multiple user
- dividing users from each other and from the organize program
- Emulating hardware on an added machine

1.3.2 Para virtualization

In Para-virtualization, the hardware allows various operating systems to run on single machine by efficient use of system resources such as memory and processor. E.g. VMware software. Here all the services are not fully obtainable, rather the services are provided partially.

Para virtualization has the subsequent advantages as given in [1]:

- Disaster recovery: In the event of a system collapse, visitor instances are moved to hardware until the instrument is repaired or replaced.
- Migration: As the hardware can be replaced easily, hence migrating or affecting the different parts of a new machine is sooner and easier.
- Capacity management: In a virtualized atmosphere, it is easier and sooner to add more hard drive capability and processing influence. As the system parts or hardware examine be moved or replaced or repaired without problems, capacity management is straightforward and easier.

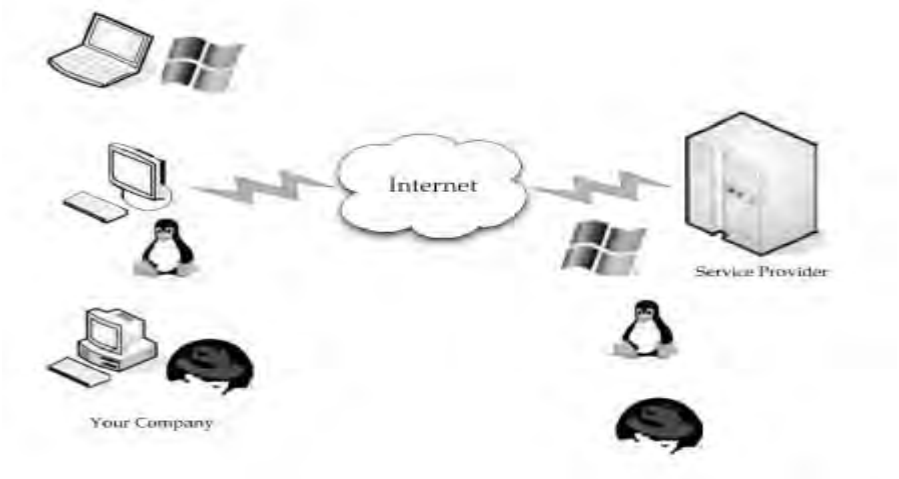

Figure 1.3: Para virtualization (adopted from [1]).

2. Related work

The scheme uses a symmetric [1] key approach and does not support authentication. Symmetric key algorithm uses same key for both encryption and decryption. The authors take a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users. A new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. The validity of the user who stores the data is also verified. The proposed scheme is resilient to replay attacks. In this scheme using Secure

Hash algorithm for authentication purpose, SHA is the one of several cryptographic hash functions, most often used to verify that a file has been unaltered. Paillier algorithm use for Creation of access policy, file accessing and file restoring process. Once user passes the two tiers of authentication then he replies back to the server with the operation (e.g. uploading/ downloading) what he wants to perform using HMAC. This communication is decrypted by the server after that secure network connection has been opened in between client and Cloud storage so client can upload or download case from Cloud storage in encrypted outline during transmission which ensures discretion as well. This paper [3] presents an anonymous privilege control scheme Anony Control to address not only the data privacy problem in cloud storage, but also the user identity privacy issues in existing access control schemes. By using multiple authorities in cloud computing system, our proposed scheme achieves anonymous cloud data access and fine-grained privilege control. Our security proof and performance analysis shows that Anony Control is both secure and efficient for cloud computing environment. In the proposed [4] scheme, the cloud verifies the authenticity of the user without knowing the user's identity before storing data. Decentralized scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. A secure data relocate technique has been designed and the design of this technique has been depicted through its architecture, Data Flow Diagram and Sequence Diagram. If multiple authorities [5] are corrupted, they cannot collect the user's attributes by tracing his GID. Notably, our scheme only requires standard complexity assumptions (e.g., decisional bilinear Diffie-Hellman) and does not require any cooperation between the multiple authorities, in contrast to the previous comparable scheme that requires non-standard complexity assumptions (e.g., q-decisional Diffie-Hellman inversion) and interactions among multiple authorities. As cloud has become [6] alternative solution for storing huge amount of data and processing, the research on data sharing and security has assumed importance. Recently Liu et al. have provided a comprehensive solution for member and data dynamics in cloud computing environment where members belong to a group and group manager can have provision to revoke users. Users can dynamically add and get revoked from the group making it a dynamic group. The designed has been proposed while

encryption/decryption working and parallel algorithm for Modified HMAC has been coded on MATLAB tool which shows improvement over existing Modified HMAC.

3. Problem formulation

There are some problem come under this technique:-

- The problem with KP-ABE scheme is the encryption cannot decide who can decrypt the encrypted data. So main problem in this to find user who decrypt the encrypted data.
- The problem with attribute based encryption (ABE) scheme is that data owner needs to use every authorized user's public key to encrypt data.
- The application of this scheme is restricted in the real environment because it use the access of monotonic attributes to control user's access in the system.

4. Proposed work

This paper deals with the security in cloud computing. For this purpose cloud environment is situate up in MATLAB and two tier security algorithms is executed over that. In first tier security username and password protection is kept. Every new user will be assigned an original password and that will be saved in the database. The structural design of proposed work is discussed under.

4.1 Architecture of Proposed Technique

In the proposed architecture as shown in fig Figure 4.1, Multi factor authentication through OTP (One Time Password) and message integrity through HMAC (Hashed Message Authentication Code) have been ensured using Diffie Hellman key exchange algorithm. Once shared secret key is generated in between Cloud Storage Server and Cloud user, it is used throughout the session for reducing the total time. OTP may be generated habitually by authentication server after adding current login number to shared secret key. This technique requires no added software/ hardware for substantiation, no need to be anxious about the key supervision because each time new key is generated for each procedure which results in more protection with less space mandatory and fast in completing because single key is used during the session.

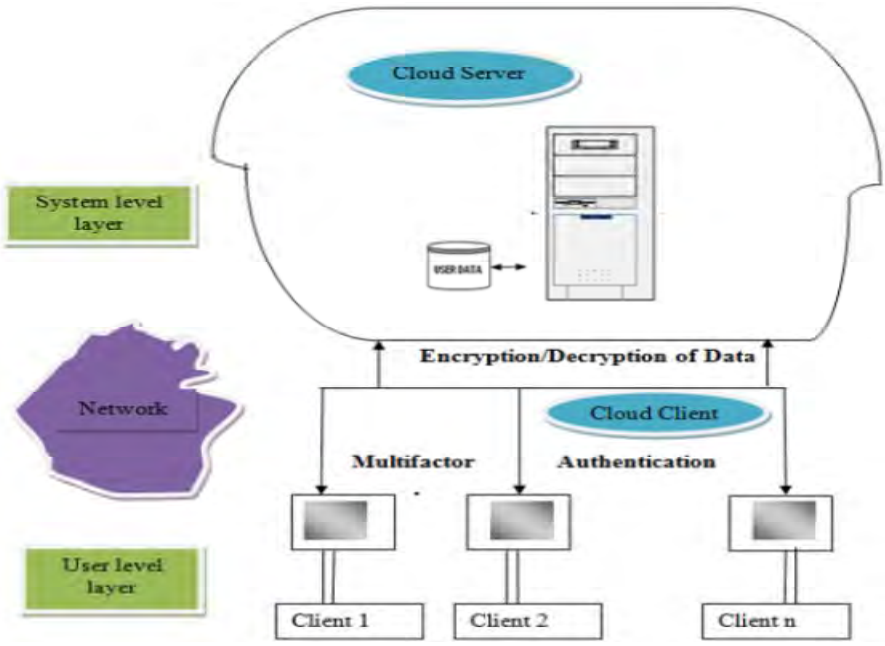

Figure 4.1: Proposed Architecture

Below are the different execution steps of proposed technique that enhance the security of information in Cloud by combining different mechanisms.

4.2 Execution Stages

Assumptions:

(i) Users are already registered to the Cloud.

(ii) Server is intelligent sufficient to decrypt the HMAC using the similar client side coding and maintain the login number of each user.

1. Login
    1.1 Credential authentication using username/password
    1.2 Diffie Hellman key exchange
2. Double authentication using OTP (Shared Secret Key+ Current Login Number) generation
3. HMAC (Shared Secret Key || Operation || Method)
4. Downloading/ Uploading Data Encryption
5. Data is retrieved and stored to Cloud Storage
6. Logout

4.3 Sequence Diagram

Figure 4.2 shows the sequence diagram for secure data transfer on Cloud via two way authentication between Cloud User and Cloud Server. It shows the interaction between Cloud user and Servers that how user passes two tier authentications then download/upload data from Cloud storage.

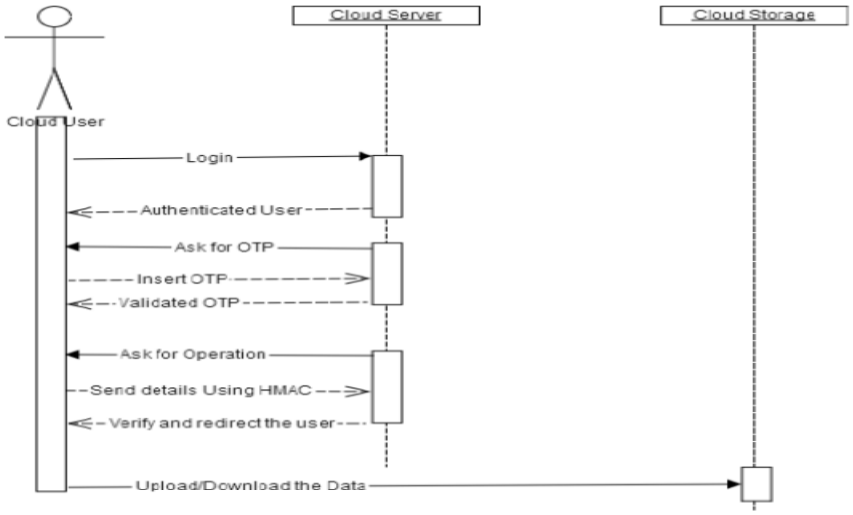

Figure 4.2`: Sequence Diagram of Proposed Method

5. Conclusion and future work

This paper gives a preamble to Cloud computing and background of various secure data transfer mechanisms to manage the authenticity, confidentiality and integrity of messages. In this work a secure data transfer mechanism has been proposed which uses Diffie Hellman key exchange algorithm for 3 way protection. Execution stages have been presented using flow and sequence diagram while encryption/decryption working and experimental result of HMAC has been

collected using MATLAB R2011b tool which shows proposed parallel execution of Modified HMAC takes less time 1.2seconds as compared to existing one 1.9seconds.

This work shows the secure data transfer via two tier authentication using OTP and HMAC which protect data against different attacks like On-Line guessing, Eavesdropper, Verifier impersonation and Man-in-the-middle. In the future, Replay attack can also be considered and prevented using Time Stamp in HMAC. It is also foreseen to perform real test with distributed computing on Amazon cloud along with MATLAB tool.

6. Reference

[1] "Cloud Computing Evolution," [online] Available: www. computerweekly.com/feature/A-history-of-Cloud-computing. [Feb. 20, 2014].
[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica and M. Zaharia, "A view of cloud computing", Communications of the ACM, vol.53, no.4, pp. 50-58, 2010.
[3] M. Creeger, "Cloud computing: an overview," ACM Queue, vol.7, no.5, pp. 2, 2009.
[4] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation computer systems, vol. 25, no. 6, pp. 599- 616, 2009.
[5] I. Foster and C. Kesselman, "The grid 2: blueprint for a future computing infrastructure," Waltham: Morgan Kaufmann Publishers, 2004.
[6] M. A. Rappa, "The utility business model and the future of computing services," IBM Systems Journal, vol. 43, no. 1, pp. 32-42, 2004.
[7] L. Kleinrock, "A vision for the internet," ST Journal of Research, vol. 2, no. 1, pp. 4-5, 2005.
[8] M. Turner, D. Budgen and P. Brereton, "Turning software into a service," Computer, IEEE, vol. 36, no.10, pp. 38-44, 2003.
[9] "Evolution of Cloud computing," [online] Available: www.tech.gaeatimes.com/index.php/archive/top-10-Cloud-computing-serviceproviders- \in-2010. [Feb. 20, 2014]
[10] "Cloud Watch Hub," [online] Available at: http://www.cloudwatchhub.eu/glossary. [Oct. 4, 2013].
[11] "Seeding the Clouds: Key Infrastructure Elements for Cloud Computing," [online] Available: http://www.935.ibm.com/services/in/cio/pdf/oiw03022usen.pdf. [Feb. 20, 2014]
[12] Vaquero, M. Louis, R. Merino, Luis and Maik, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50-55, 2008.
[13] "Gartner says contrasting views on Cloud computing are creating confusion," [online] Available: www. gartner.com/newsroom/id/766215. [Feb. 20, 2014]
[14] M. Brown, "White paper: Cloud computing," Maximum PC, Jan. 12, 2009.
[15] R. Buyya, C. Yeo, and S. Venugopal, "Market-oriented cloud computing: vision, hype and reality for delivering it services as computing utilities", Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications, HPCC-OB, IEEE CS Press, Los Alamitos, CA, USA,pp. 5-13, 2008.