IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 04, Issue 12 (December 2014), ||V1|| PP 22-24

An encrypted mechanism for securing cloud data from data mining attacks

Priyadarshini Adyasha Pattanaik
Department Of Computer Science and Informational Security KIIT University,Bhubaneswar,Odisha,India.

Abstract: - Cloud Computing is a vast infrastructural and rising pool which provides huge storage of data in one sphere. Organizations nowadays are in the marathon of equipping the whole system in a cloud form. In this paper we are concern for providing a greater security to the cloud data from data mining attacks. Time complexity and security issue is taken into consideration. Data security and privacy protection issues are associated with cloud computing have been enhanced and modernised in this paper. We have proposed an architecture comprising of various components and network designs which provides a high level of security to the data. The rate of growth of cloud computing is so fast that it has already put its head in the mortar and is spread as the most durable untiring technology now. As cloud computing is a store house of data which might get affected by data mining attacks so we have launched this architecture.

I. INTRODUCTION

Cloud Computing seems as a most complicated and much simple concept. In simple way to define, Cloud computing is a library of high storage data. Cloud Computing is a design philosophy separating the Operating System and Applications from the Hardware. Otherwise it can be explained as the process of disconnecting the application, Operating System and the hardware between themselves. Cloud Computing is a latest and greatest thing that companies are busy in using in their marketing campaign. Cloud Computing is a store house of various components such as virtual computing, Web Applications, clusters, application servers, etc. Virtualization is a component of cloud computing which states as follows:

For example: Let's consider a server (CPU, Power supply, RAM, Hardware) present, in which a server OS is installed (Windows nt4), and in the server OS a Microsoft extended server OS is installed(Email).If by chance the CPU fails or due to failing of power supply the entire extended server fails and as the email server depends on the server OS and the server OS depends on the main server or hardware then any one failure would lead to the whole failure or damage. In an organization, if this situation arises, the whole organization work breaks down, and this leads to many losses in every sphere. In order to overcome this failure a revolutionized concept came into account that is cloud computing. In the concept of virtualization, if the hardware fails then we can move the existing OS (whole OS including server + application) to the nearby server (hardware).Then by this process we can again start up the work. Another issue arises, that exchanging of OS to other hardware or server who takes a lot of time. So, in order to overcome this issue, we can copy the application server to the other hardware which could for sure save the time and start up the process from the left stage.

II. ARCHITECTURE

Here we discuss our proposed system architecture that prevents data mining based privacy attacks on the cloud. Our system consists of two major components: Cloud Data Overlay network Distributor and Location Based Cloud Providers. The Cloud Data Overlay network Distributor is a layer of virtual network layer topology consisting of many clusters of cloud data distributors connected to each other with virtual or logical links which directly interfaces to users. The Cloud Data Overlay network Distributor is open to all kinds of internet users and the data routing in overlay networks is very flexible. The Cloud Data Overlay network Distributor consists of clusters of Cloud Data Distributors and each Cloud data distributor receives data from the clients in the form of files, splits each file into chunks and distributes these chunks among Location based cloud providers.

Again important concept is the network through which the outside user get connected to the cloud data overlay network distributor is a VPN network(Virtual Private Network).VPN network is a secured network which lies of the public network such as Internet.VPN network provides an encryption, authentication and message integrity network flow data . Encryption algorithm enables the attracter by only viewing the encrypted data that cannot decrypt the traffic. So as the Encryption provides confidentiality so as the authentication lights up the access of only authenticated users and the message integrity detects the tampering with transmitted messages.

A. Cloud Data Overlay Network Distributor:

The Cloud Data Overlay network Distributor is a layer of virtual network layer topology consisting of many clusters of cloud data distributors connected to each other with virtual or logical links which directly interfaces to users. The Cluster Cloud Data Distributors in overlay networks are highly connected to each other and easily communicate to another end-one via overlay networks. The whole Cloud Data Overlay Network Distributor consists of much number of clusters in which each cluster comprises of many number of Cloud Data Distributors. In the whole overlay network the multiple clusters present are always talking to each other. Information or data send to the clusters are always in a replicating stage with each other. When the user or client hits to the clusters, then the user only gets connected to cloud data distributor which is less loaded or busy. If one of the distributor fails or crashes off then the user automatically moves to the other distributor through the cluster veins. The cloud data distributors are placed in different levels.

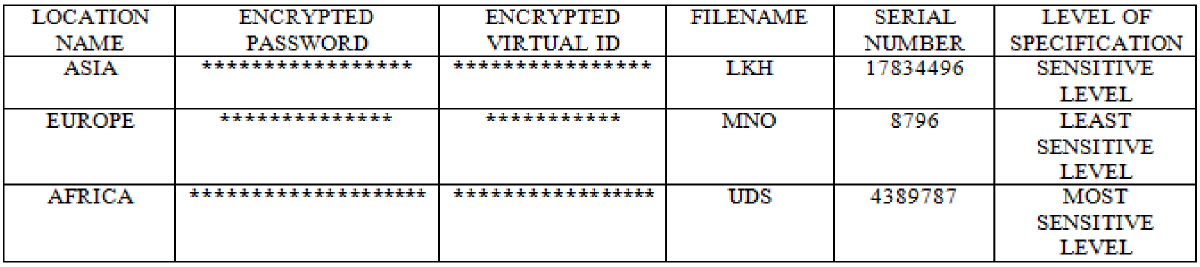
The cloud data distributor carries a table comprises of user name, encrypted password, filename, serial number, distributor level number. Only the authenticated and encrypted users can access and enter the password. The procedure of entering password carries some terms and conditions. If a user fails the maximum number of attempts that is 3 then the server automatically blocks the user access. Then the particular user can’t enter the password as the server has already blocked. So, the user has to undergo a procedure of terms and conditions where it has to provide it whole details to the server. The password which the cloud data distributor is carrying is in a encrypted form. This processing is done in order to increase the security of accessing and making the cloud data more secure and reliable.

TABLE I CLOUD DATA DISTRIBUTOR TABLE

USER NAME	ENCRYPTED PASSWORD	FILENAME	SERIAL NUMBER	DISTRIBUTOR LEVEL NO.
UN1	*************	XYZ	2	0
UN2	*********	ABC	7	1

The Cloud Data Distributors in each cluster even carries the information of the Providers, and chunks because during the retrieval of data this information is required. The user or client who want the stored data have to check through the following section in the table provided. The table consists of various entities described below:

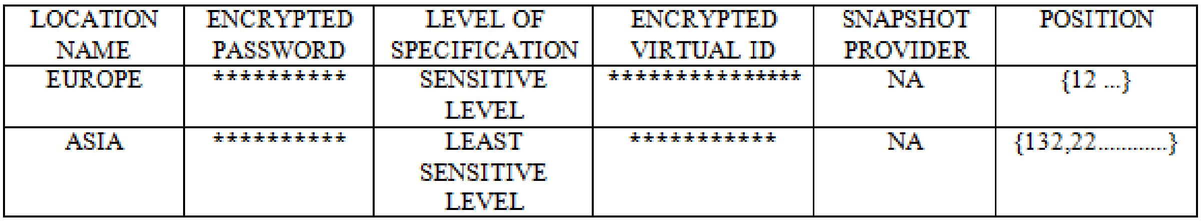
TABLE II LOCATION BASED CLOUD PROVIDER TABLE



LOCATION NAME	ENCRYPTED PASSWORD	ENCRYPTED VIRTUAL ID	FILENAME	SERIAL NUMBER	LEVEL OF SPECIFICATION
ASIA	******************	*****************	LKH	17834496	SENSITIVE LEVEL
EUROPE	***************	************	MNO	8796	LEAST SENSITIVE LEVEL
AFRICA	*********************	******************	UDS	4389787	MOST SENSITIVE LEVEL

The data received from the cloud data distributor from the user is fragmented and distributed to the cloud providers present below. The cloud providers are distributed between each other in the basis of particular location and the data are stored or saved in a respective cluster in a location based cloud provider. A particular location based cloud provider consists of a number of chunks of data. The table carries encrypted virtual id, filename, serial number and level of specification. The level is based on the privacy of data that is most sensitive level carries (private information of a company, personal information, legal docs),Sensitive level carries moderate sensitive data like(health information of an individual) and the least sensitive level data include (data that do not reveal any protected or private information). The location based cloud provider provides an advantage by reducing the time complexity so that the user can easily get the information as per its requirement.

TABLE III CHUNK TABLE



LOCATION NAME	ENCRYPTED PASSWORD	LEVEL OF SPECIFICATION	ENCRYPTED VIRTUAL ID	SNAPSHOT PROVIDER	POSITION
EUROPE	***********	SENSITIVE LEVEL	***************	NA	{12 ...}
ASIA	***********	LEAST SENSITIVE LEVEL	************	NA	{132,22...........}

Chunk table comprises of the location based name entity with its respective encrypted password, level of specification, encrypted virtual id, snapshot provider which stores the snapshot of the before and after modified chunks, position states the the set of positions of misleading data bytes for all chunks.

B) Location Based Cloud Provider:

Cloud providers are divided into different providers depending on their specific locations. The chunks of data are stored in the cloud providers and can be retrieved through identifying their respective virtual id or matching by the entities present in chunk table. The basic need of placing the cloud providers as per location is that it will reduce the access time of the client and can easily retrieve the data by even delivering the data to the client as per requirement. Each cloud provider is considered as a separate storage house for client's data. Individual cloud provider carries individual character tics such as some cloud providers are more trustworthy while some provide cheap services. Likewise sensitive dates are stored in secured providers and regular data in cheap providers considering the level of specification infront. Basically Cloud Providers are the store house of storing chunks of data and removing chunks as per requirement or demand of the client.

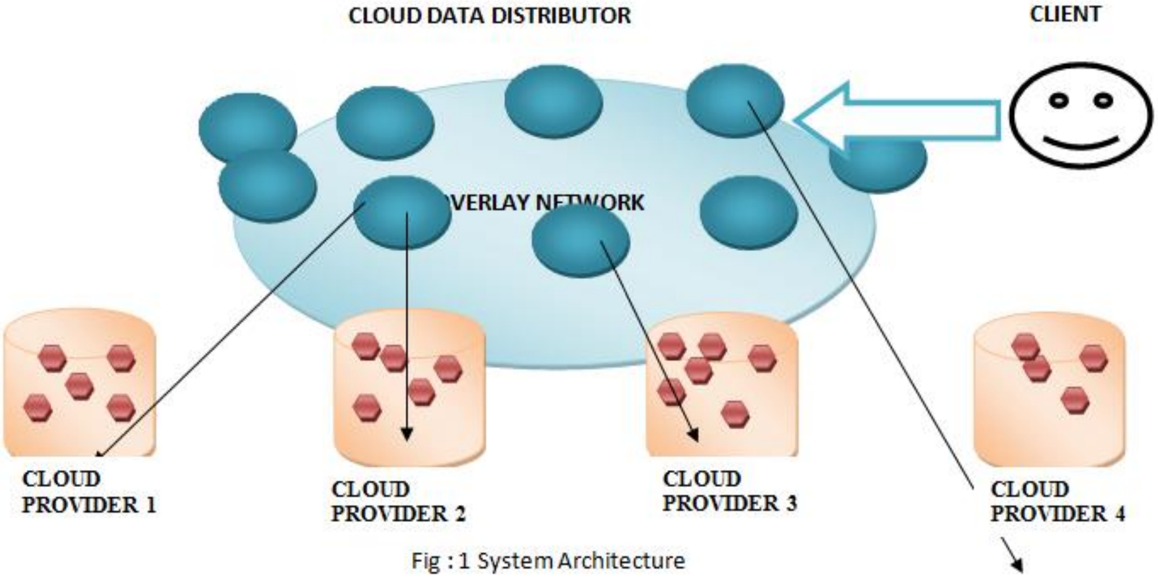


Fig : 1 System Architecture

III. ARCHITECTURAL ISSUES

Critical issue in this architecture is that the Cloud Data Overlay Network Distributor is open to all types of internet users, security and privacy issues which can be a major issue. Continuous access of the data distributor can lead to failure at some certain time. Location Based Cloud Providers can also be an issue, if the hacker traces the location then it can get the secured data of all the cloud providers placed in that particular location. For example: The cloud providers have gained some data of the location London which is placed in a particular provider(Location London),if the hacker gets through the particular provider then it could easily hack or gain the data of the entire London city. Lastly, the architectural structure is sub divided into many entities or parts so that the data is totally secured but as per the demand of the client in order to retrieval of data it undergoes various steps which increases the access time.

IV. CONCLUSION

In this paper, we have enhanced the security and extended the data privacy in order to protect the data from data mining attacks. Our approach combines the mechanism for providing more security in each step of the system architecture. Encrypted and authenticated users or clients can only enter to the architectural premises. It even provides quick performance when the client wants to access the data.

REFERENCES

[1] Secure and Efficient Data Storage in Multi-clouds, Veena Khandelwal -2013
[2] Database system concept, Abraham Silbersschtz, Henry F. Korth.