Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 2, February 2015, pg.331 – 340

RESEARCH ARTICLE

IMPROVE SECURITY OF DATA ACCESS IN CLOUD COMPUTING USING LOCATION

Goikar Vandana T., Jagdale Supriya K., Parade Priya B., Pawar Sumedha D.
Guide: Prof. Nalawade V.S.
Dept. Of Computer Engg., SBPCOE, Indapur

Abstract—

Cloud computing is a new approach in the field of information technology based on the World Wide Web. It is new approach in the field information technology and also it satisfies a end users requirement for computing resources like services and applications etc. Security is one of the most challenging issue in the cloud computing. In cloud computing, services need to address the security during the transmission of sensitive information. Many organization, companies or banks have confidential information, this information is very essential. The cloud does not provide a fully guaranteed of data and it is compromised by the attackers. In this paper by providing a new method, we improve the security of data access in the cloud computing for a bank or any other particular location by using location-based encryption.

Keywords-- Cloud Computing, Services, Security, Geo-Encryption, Location-based Encryption

© 2015, IJCSMC All Rights Reserved

I. INTRODUCTION

Nowadays with the advancement of technology, information security and data security are needed more than any other types of the security. Some types of information and data are confidential such as companies' confidential information, bank's information, even the military intelligence and the like. On the other hand with the increasing users need powerful tools to process and store their data. In recent years a new technology for this purpose has been proposed which is called cloud computing. Cloud computing is a pay-per-use model for enabling available, on-demand network access to a shared group of computing resources. Cloud computing through of as a "Time-Sharing", or the ability to share computing resources among many users. In nowadays many companies actually shared a single computer that was located in a remote data center. To store their data and information on the cloud and they can access their own data at any time, from any place and using any computer through the internet.

This technology is certainly a big advantage and always beside the advantages and also their disadvantages. The biggest challenge related about cloud computing is to provide a security. In cloud computing the data or information are compromised by the attacker so, the cloud computing does not provide a extra security for the confidential data or information. So in this paper we have introduced two technologies "Location-based-cryptography" and another is "Geo-Encryption algorithm". By using this technology we can improve the security in cloud for data access.

A. Cloud Computing

According to author Soheil Nazem definition of cloud computing is "Cloud Computing is a paradigm that focuses on sharing data and computations over a scalable network of nodes"[2]. And according to author Mahdi definition of cloud computing is "Cloud Computing is model to access information and services using existing technology and internet infrastructures that allows establishing communication between clients and the server"[5]. Users do not have the actual physical infrastructure and they just pay a fee to cloud provider and gain access to resources. Cloud computing is a model for enabling convenient, on-demand network access to a shared computing resources like applications and services[6].

B. Architecture of service Models

The architecture of service models includes three types of service(figure.1):

- **Software as a Service:** SaaS is a complete operating environment for user interface, applications and program management. In the SaaS model, the application is provided to the client through a browser and the customer's responsibility begins with data entry and ends with data management and user interactions.[6,7].
  Eg. GoogleApps, virtual desktop.

- **Platform as a Service (PaaS):** This service provides a platform that enables software developers to for developing Websites without installing any software on the system. It

© 2015, IJCSMC All Rights Reserved

provides virtual machines, operating systems, applications, services, development frameworks, transactions, and control structures[1,6,7].
Eg. IBM, GoogleAppEngine, Force.com.

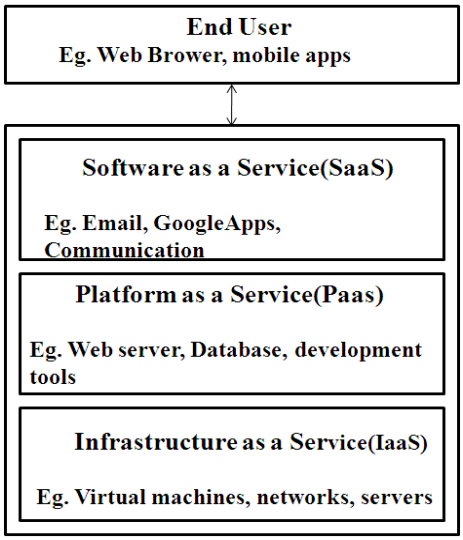

Figure 1.Architecture of service models

- **Infrastructure as a Service (IaaS):** This service provider manages all infrastructures and also that support various operations like Virtual storage,virtual machine, hardware, servers and networking.[6,7]. It include the operating system, applications, and user interactions with the system.
  Eg. Servers, network devices.

C. Cloud Types

Cloud is a scalable network of servers or even individual PCs interconnected in a grid. In fact, cloud is a metaphor for the internet. So in cloud the important element is that human management there is no needed for allocating processes to resources. And also cloud is a set of hardware and software which are work together to deliver services to customers over a network. There are four types of cloud. The first type of cloud is **Public cloud**. In this, cloud infrastructure are made available to the general public. It use for a large industry group over the online service. Like "Amazon" and "GoogleApps". The second type of cloud is **private cloud**. In which the computing environment is operated for an single organization. It is managed either by the organization or third party. A private cloud gives the organization larger control over the infrastructure than does a public cloud. eg. Business. The third type of cloud is **Hybrid Cloud**. A hybrid cloud is a combination of two or more clouds i.e. private, community, or public cloud. Basically it is an environment in which multiple internal or external suppliers of cloud services are used. And also it may allows standardized access to information and application. It is being used by most of the organizations such as "IBM".

© 2015, IJCSMC All Rights Reserved

And the fourth type of cloud is **Community Cloud**. It is combination of one or more public, private and hybrid cloud. In which the infrastructure and resources are shared by many organizations that have common privacy and security, rather than for the use of a single organization. And it is managed either by third party or internally.

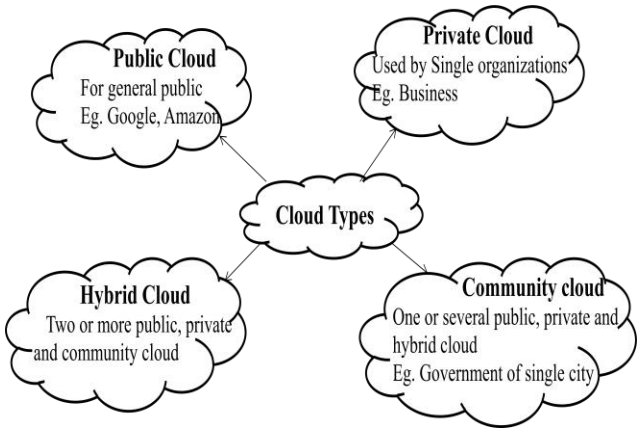

Figure 2.Cloud Computing Types.

II. RELATED WORK IN CLOUD COMPUTING FOR SECURITY AND CHALLENGES

Security is one of the concerns in cloud computing which delaying its confirmation. When we move the information into the cloud but we lose control of it. So, we provide biggest security to cloud. The cloud gives we access to our data, but we have not ensure to someone else does not access the data. In cloud based software environment, physical security stronger because loss of client system does not adjust the data or software. Cloud computing seems offer great advantage for communication. The availability of improbable set of software application access to lightning-quick processing power, unlimited storage and the ability to easily[1,7].

1**. Privacy:**

Privacy is the one of the security issue in online world. In cloud personal information move across the world. When information stored the outside of country then they have number of restrictions. End user access the cloud services without the need for any knowledge of the technology and also every end user lawful to control the his or her own data whether it is public or private[6,7].

2. Identity and access management:

In cloud computing technology, their aims to provide the scalable access of resources or services over a online service. Identity management system contain the management of the multiple identities and also their authentication, authorization. In identity management system, it is useful

© 2015, IJCSMC All Rights Reserved

for the password administrator including single sign-on. In identity management system has various feature such as access management, identity authentication and authorization[6,7].

Following are some of challenges facing cloud computing:

1. Cloud computing database:
Database environment used in cloud can be different and they run on cloud computing platform. For example, some database environments support multiparadigm model and some others support multi-tenancy model. In cloud computing cloud database use for achieving optimized scaling, multi-tenancy[7,9].

2. Data protection:

Data stored in the cloud which is resides in a shared environment and arranged alongside data from other to enable access data and the data kept safe[9].

3. Identity management:

In cloud computing one of the main issue is identity management and authentication. In organization main thing is that unauthorized access to resources in cloud. One of the main reasons is that organization identity issue and authentication[9].

III. ALGORITHM USESD FOR PROPOSED SYSTEM

1. LOCATION-BASED ENCRYPTION

Location-based encryption technique is used for encryption wherein the cipher text can be decrypted at a specified location. If someone try to decrypt the data at another location the decryption process fails and no information about the plain text. The device performing the decryption and determine its location by using location sensor i.e. GPS receiver. In cryptography "identity" is very important component and in our paper we are using "Location" as identity. In this principle, location and time specification is attached to cipher text file. So that data is decrypt only within specific location and time constraints. Location is coded as latitude and longitude pair at precision of 1 centimeter or 1 kilometer. Then there are only 100,000 possible values for each of latitude and longitude or 10 billion possible keys. Testing of this is easy.

2. GEO-ENCRYPTION ALGORITHM

"Logan scott" and "Doronthy E Denning" has firstly proposed and developed the idea of geo-encryption. Geo-Encryption is based on cryptographic algorithm and also based on adding a new security layer on the available encryption protocol structure using the receipients location information. In this, data is encrypted for a specific place or broad geographic area.

© 2015, IJCSMC All Rights Reserved

And it also supports constraints in time as well as space. It can be used in fixed and mobile application and also supports a range of data sharing and distribution policies. It also provides strong protection to location spoofing[5].Symmetric encryption(private key) in terms of computational and implementation is very fast .Asymmetric encryption(public key) method uses both public and private keys and it provide very high security. The difficulty in computing its performing rate is low. In Geo-Encryption algorithm, combination symmetric and asymmetric encryption is used. Symmetric key algorithm is used to encrypt the information and the public key algorithm is used to provide security and also distribute the session key(figure 3).To encrypt the desired data sender uses session key and AES which is symmetric algorithm.

Following are the steps for Geo-Encryption Algorithm:

1. Compute geolock by using receipients PVT information.
2. GeoLock is then XOR with the session key (Key_S) to form a GeoLocked session key.
3. Encrypt result by using asymmetric algorithm and send to receiver.
4. GeoLocks are computed using an AntiSpoof GPS receiver.
5. Compute PVT → GeoLock mapping function.
6. Check for PVT. If PVT values are correct then resultant geolock will XOR with geolocked key and we get session key.
7. Compute decryption by using resultant session key.

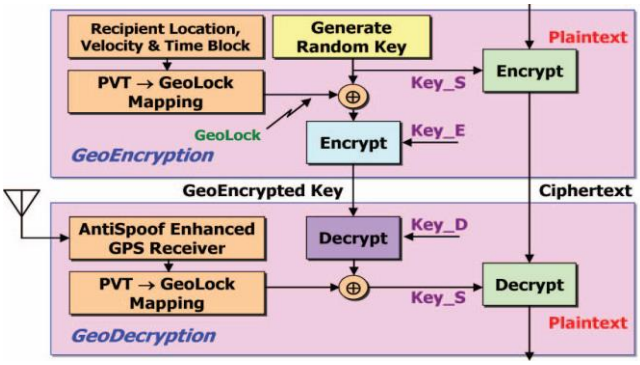

Figure 3.GeoCodexGeoEncryption algorithm.

© 2015, IJCSMC All Rights Reserved

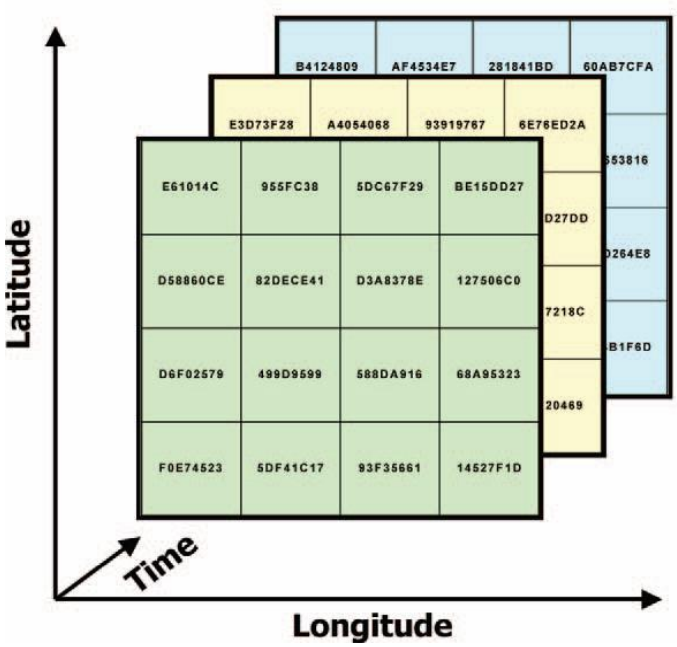

Figure 4. PVT->GeoLock mapping function.

PVT ->Geolock mapping function have eight inputs:

- Position (East, North, Up)
- Velocity (East, North, Up)
- Time
- Co-ordinate system parameters

IV. PROPOSED SYSTEM

As we have already mentioned in previous section, data security in the cloud is very important. In this paper we are implementing the bank application, as we know the bank data is very confidential data. This bank data stored on cloud. But we know the data on the cloud can be access anyone so, the cloud does not provide a security to the confidential data. This type of data were compromised by the attackers. So, we need to provide extra security for the bank data on cloud. In this paper we are implementing the encryption and decryption technique for provide security to that data. Also provide a extra security layer we use the user location and geographical position. To provide this, we need Anti-spoof GPS which is gives very accurate location of the user for accessing data and it can give us the latitude, longitude and altitude accurately. Label can be given to data which is stored on cloud. Index table contains these label and refers to users geographic location and timeframe. Label and data stored on cloud can be added manually or automatically.

© 2015, IJCSMC All Rights Reserved

Nowadays we use username and password to provide security to data access stored on cloud in many applications such as banks, big companies, institutions etc. But this security is not sufficient to cloud data access. Because any unauthorized user can access data on cloud easily from any location. So to provide extra security to cloud data access we use location based encryption. By using this method, we can avoid any unauthorized access of data in cloud.

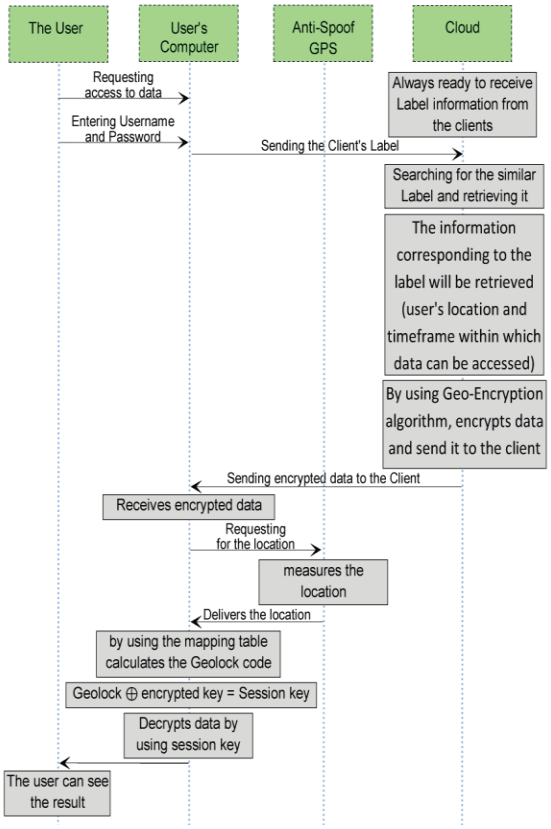

Figure 5. Block diagram of proposed system

Following are the steps which are taken to get access the data on cloud:

1. First, user enter username and passwords. This username and password collectively called label. This clients label is sent to cloud.
2. Searching for the similar label and retrieving it is done on cloud.
3. After that the information corresponding to the label will be retrieved(that information contain user location and timeframe within which data can be access.)
4. By using this information and geo-encryption algorithm encryption of data takes place. And this encrypted data is send to the user.
5. Users computer receives that encrypted data.

© 2015, IJCSMC All Rights Reserved

6. Anti-spoof GPS is used to measure the users location and delivers the location to the users computer.
7. Then calculate the geolock code by using the mapping table.
8. Geolock XOR Encrypted key=Session key.
9. And finally decryptes the data by using this session key.

V. CONCLUSION

Data access control is one of the most challenging issue in cloud computing. Security of customer information is a major requirement for any services offered by any cloud computing. There are some advantage of cloud computing, so many people and company uses cloud computing. But there are some challenges in using cloud computing for data access. In this paper we are provide extra security layer to cloud using location based encryption technique. This method can be useful for many applications such as banks, big companies, institutions, etc.

REFERENCES

[1] V. Krishna Reddy, Dr. L.S.S. Reddy, "Security Architecture of Cloud Computing'', Department of Computer Science and Engineering2011.

[2] Mehrdad Mahadavi Boroujerdi Soheil Nazem, "Cloud Computing: Changing Cogitation about Computing'', World Academy of Science, Engineering and Technology 2009.

[3] CloudHooks: "Security and Privacy Issue in Cloud Computing'', Proceesing of the 44thHawai International conference on System Sciences-2011.

[4] Weiss,A.(2007) "Computing in the Clouds'', Networker, Vol 11, No. 4, pp:16-25, December 2007.

[5] Loganscott& Dorothy E. Denning, "Location Based Encryption & Its Role in Digital Cinema distribution'', Proccedings of ION GPS/GNSS 2003, pp 288-297.

[6] Gurudatt Kulkarni 1 et al, "Cloud Security Challenges'', 7th International Conference on telecommunication systems, Srevices and Applications(TSSA),IEEE,2012.

[7] Meer Sohei l Abolghasemi, Mahdi sefidab, Reza Ebrahimi Atani, "Using Location Based Encryption to Improve the Security of Data Access in Cloud Computing'', international conference on advances in computing2013.

© 2015, IJCSMC All Rights Reserved

[8] Rajnish Choubey et al., "A Survey on Cloud Computing Security, Challenges, Threats'', International Journal on computer Science and Engineering(IJCSE)2011.

[9] Wayne Jansen, Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing'', Computer Science Division Information Technology Laboratory National Institude of Standards and Technology Faithersburg,MD 20899-8930 January 2011.

© 2015, IJCSMC All Rights Reserved