International Journal of Advanced Research in

Computer Science Engineering and Information Technology

Volume: 4 Issue: 3 11-Apr-2015,ISSN_NO: 2321-3337

USE LOCATION TO IMPROVE SECURITY IN CLOUD COMPUTING

Pawar Sumedha D., Parade Priya B., Jagdale Supriya K., Goikar Vandana T.

Guide: Prof. Nalawade V.S.

Dept. Of Computer Engg.

SBPCOE, Indapur.

Abstract---*Cloud computing is based on world wide web. And nowadays it is used in field like information technology and development of computer technology. Its services provides more benefits to the user in terms of cost. Cloud environment is used for data processing and storage in large scalable network. It satisfy user requirements for computing resources without physically acquiring them. Cloud computing security is one of the most challenge. Security to data which is stored in banks, institutions, companies, military etc. is very essential. In this paper we use location based encryption to improve the security of data access in cloud computing for bank.*

Keywords--- Cloud computing, security, services, geo-encryption, cryptography, location-based encryption.

I. INTRODUCTION

Cloud computing is dynamic scalable network that provide services which work together over network[1,2]. It is the use of hardware and software that deliver data and information over internet. Security is very important part in human life. People always look for physical and financial security. In information technology, information security and data security are very important.Bank data is very vast and it is scattered. So, to store that data we use cloud computing. In cloud computing, we store the data on the cloud instead of keeping data on our hard drive. We use service over internet and store data and information at another location doing ,we give some privacy[4].Cloud computing allow indivisual or organization to use software and hardware that manage by remote server and provide the independence access them through network[3,4]. It is basically meant to give maximum with the minimum resources .i.e. The user end required the minimum hardware requirement but it is using the maximum capability of computing.[3]. In this paper, we have discussed about cloud and also explained location based cryptography and geo-encryption algorithm.

1.1. Definition of Cloud

Cloud is set of different type of hardware and software which work together to deliver many aspect of computing to end user as an online service. Cloud is scalable network of server that connected together through grid.

1.2. Cloud Computing

According to author Mehrdad definition of cloud computing is “A paradigm that focuses on sharing data and computation over a scalable network of nodes”. And according to author Choubey definition of cloud computing is “A pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resource like networks, servers, storage, applications, services, etc. that can be rapidly provisioned and released with minimal management effort or service provider interaction ”.

1.3. Architecture Of Service Models

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

- **Software as a Service(SaaS)** [6,7]**:** It is fully operational environment for user interface. It also provides application to end user. It is available to user through internet. SaaS involves infrastructure and platform. It is mostly used in small business. InSaas programmers and admimistrator are not required.
  eg. android, GoogleApps, oracle on demand, etc.

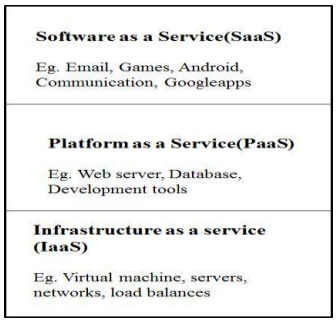

Figure 1. Architecture of service models

- **Platform as a Service(PaaS)** [7]**:** It provides infrastructure and platform to the software developer to create application.Client can deploy its application on cloud infrastructure if PaaS service provider support the language and tools which are used to program that application. Application deployed on cloud are installed and managed by client.
  eg.:force.com, GoogleAppEngine, etc.

- **Infrastructure as a Service(IaaS)**[7]**:**It provides virtual machines, virtual storage, virtual infrastructure and other hardware as resources for customers. Operating system, application and user interaction with the system are included in IaaS. It requires administrator to manage infrastructure. And also programmers are required.
  eg. Amazon, IBM. HP, etc.

1.4 Cloud Types:

There are four types of cloud. The first type of cloud is **Private Cloud.** In this, cloud infrastructure is dedicated to single organization. Private cloud infrastructure and corporate are completely managed by the organization itself. It can be managed externally and internally. Its eg. is Business. The second type of cloud is **Public Cloud.** In this, cloud infrastructure is dedicated to large organization like google, amazon. The third type of cloud is **Hybrid Cloud.** It is the combination of two or more cloud such as public and private cloud. And the fourth type of cloud is **Community Cloud.** It contain several organization. It is combination of one or more public, private and hybrid cloud.

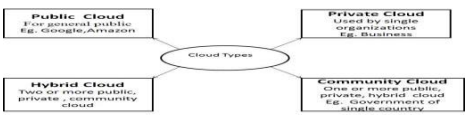

Figure 2. Cloud Computing Typ

2. 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]

2.1 . 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].

2.2. Identity and access management:

In cloud computing technology, their aims to provide the scalable access of resouces or services over a online service. Identity management system contain the management of the multiple identities and also their authentication, autherization. In identity management system, it is useful for the password administrator including single sign-on. In identity management system has various feature such as access management, identity authentication and autherization[6,7].

3. Following are some of challenges facing colud computing:

3.1. 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].

3.2. 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].

3.3. Identity management:

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

3.ALGORITHM USESD FOR PROPOSED SYSTEM

3.1.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

3.2. 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. 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.

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.

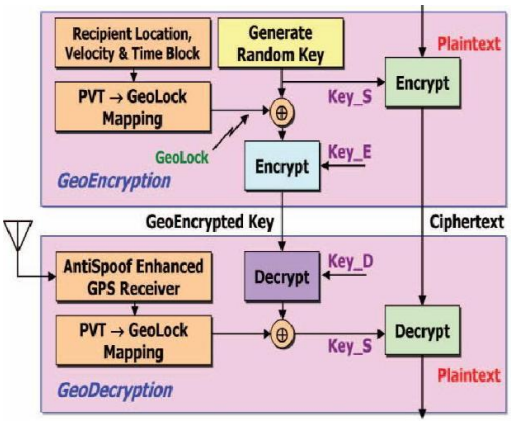

Figure 3. GeoCodex GeoEncryption algorithm.

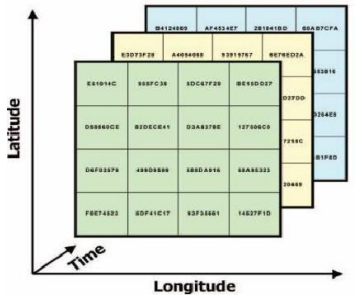

Figure 4. PVT->GeoLock mapping function.

PVT -> Geolock mapping function have eight inputs:

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

4. PROPOSED SYSTEM

As we have already mentioned in previous section, data security in the cloud is very important. As we are implementing the bank application, bank data is stored on cloud. This data is critical and confidential. So the access control to such information in cloud is very important part of data security in cloud. As we know that encryption, decryption etc. are used to secure the data access in cloud. But it is not sufficient to secure the data in cloud. So to provide extra security layer we use user location and geographical position. To provide this, we need Anti-spoof GPS which is very accurate 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.

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.

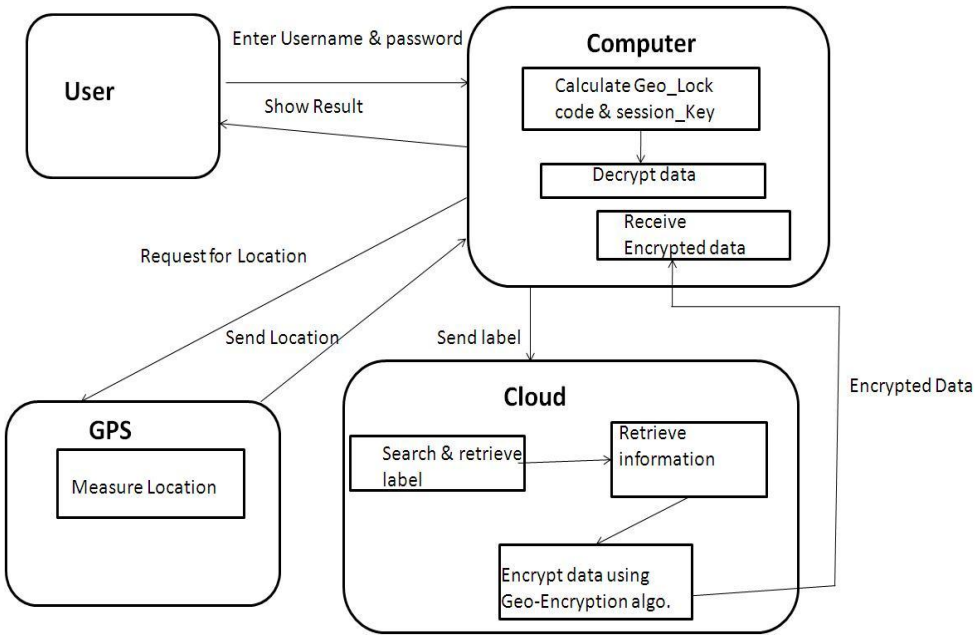

Figure 5. Block diagram of proposed system

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

PVT -> Geolock mapping function have eight inputs:

1. First, user enter username and passwords. This username and password collectively called label. This clients label is sent to cloud.
3. Searching for the similar label and retrieving it is done on cloud. 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 geoencryption algorithm encryption of data takes place. And this encrypted data is send to the user.
5. Users computer receives that encrypted data.
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.

5. CONCLUSION

Data access control is one of the most challenging issue in cloud computing. Also there are some advantage of cloud computing. So many people and company uses cloud computing. But there are some challenges in using cloud computing. So, to provide extra security layer to cloud we are using location based encryption technique. This method can be used 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] GurudattKulkarni 1 et al, “Cloud Security Challenges’’, 7th International Conference on telecommunication systems, Srevices and Applications(TSSA),IEEE,2012.

[7] Meer SoheilAbolghasemi, Mahdi sefidab, Reza EbrahimiAtani, “Using Location Based Encryption to Improve the Security of Data Access in Cloud Computing’’, international conference on advances in computing2013.