Location based Encryption and Authentication of Cloud Data

Atul Kamble, Student, Department of Computer Engineering, Government College of Engineering and Research, Awsari (KD), Pune, India

Poonam Mantri, Student, Department of Computer Engineering, Government College of Engineering and Research, Awsari (KD), Pune, India

Parmeshwar Shinde, Student, Department of Computer Engineering, Government College of Engineering and Research, Awsari (KD), Pune, India

S. B. Nemade, Assistant Professor, Department of Computer Engineering, Government College of Engineering and Research, Awsari (KD), Pune, India

***Abstract*— Cloud Computing is an approach in the field of information technology which satisfies end user requirements for computing resources like services and applications. Security of access to critical and confidential information in banks, institutions etc. are extremely essential. We can improve security of data access in cloud computing using location based encryption and authentication.**

***Key Words*— Cloud Computing, Geo-Encryption, Security, Services**

I. INTRODUCTION

With the advancement of technology, threat to information security and data security also get increases. Many times information and data are confidential in case of corporate field, bank and military intelligence. On the other hand with the increasing number of users more powerful tools are needed to process and store their data. In recent years a new technology for this purpose has been proposed which 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. Companies shares 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 .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 extra security for the confidential data or information. By using technologies "Location-based cryptography" and "Geo-Encryption algorithm" we can improve the security in cloud for data access.

A. Cloud Computing

Cloud computing is a phrase used to describe a variety of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. Such virtual servers do not physically exist and can therefore be moved around and scaled up or down on the becoming larger or smaller without being a physical object. In common usage, the term "the cloud" is essentially a metaphor for the Internet. Marketers have further popularized the phrase "in the cloud" to refer to software, platforms and infrastructure that are sold "as a service", i.e. remotely through the Internet. The major models of cloud computing service are known as software as a service, platform as a service, and infrastructure as a service. These cloud services may be offered in a public, private or hybrid network

B. Types of Cloud

1) Public Cloud

The idea is to host applications, Web applications in general, on shared environment with an unlimited number of users. The implementation of this type of cloud is managed by third parties (such as Amazon, Google, etc...)

2) Private Cloud

This is a deployed environment within an enterprise Thus; it must man- age its infrastructure alone. In this case, implement a private cloud signify transform the internal infrastructure using technologies such as virtualization to deliver services to request, more simply and faster. Eucalyptus, Open Nebula and Open Stack are examples of solution of the implementation of private cloud.

3) Hybrid Cloud

Hybrid cloud is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment

ISSN: 2278 – 1323

models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources. It allows one to extend either the capacity or the capability of a cloud service, by aggregation, integration or customization with another cloud service.

C. Types of Services

1) Software as a Service (SaaS)

SaaS software is used directly on the network, without being downloaded first in the local computer user environments. The software applications are available on the Internet via a SaaS provider, and are executed in the computing environment predefined from this supplier. Amazon S3 (Amazon Simple Storage Service) is an example of SaaS is a storage platform online. It uses a web interface to store and retrieve data

2) Infrastructure as a Service (IaaS)

IaaS is a complete computing infrastructure used as a service. To create and use their computing infrastructures freely, according to their needs and only when they need it, users or tenants, access to specific parts of a consolidated pool of federated resources. Amazon EC2 (Amazon Elastic Compute Cloud) is an example of IaaS allows rent virtual machines predetermined sizes to run the applications.

3) Platform as a Service (PaaS)

PaaS is a computing environment available and accessible, as needed, from an service provider. Used to develop and run software [4]. Hadoop is an example of PaaS for distributed applications and intensive management of huge amounts of data.

II. LITERATURE SURVEY

A. An Efficient Lossless Data Hiding Technique for Palette-Based Images with Capacity Optimization

Recently data hiding over images have drawn tremendous interest, using either loss or lossless techniques. Although loss techniques can allow large hiding capacity, host image cannot be recovered with high fidelity. Some applications require exact recovery of the host image as in medicine when personal data are hidden within the medical image. Lossless data hiding techniques suffer from limited capacity as the host image should be kept intact. In this paper a lossless embedding technique is proposed based on image histogram characteristics, zero and peak points are identified and manipulated to embed data. The new technique gives hiding capacity that can reach up to 50 percent of the host image size for images with large homochromatic regions (cartoons-like)

B. New Location based Authentication Technique in Access Management

In this paper, new space-time authentication techniques are proposed. Location-based authentication is a new direction in development of authentication techniques. At the first part advantages of location-based authentication are introduced. In the second chapter the main aspects of using user's position information are discussed, as user's mobility and user's privacy. The main part of the paper is focused on introducing of two new proposed authentication techniques. The first technique called STAT I (Space-Time Authentication Technique) uses GPS system for a position determination. The second technique (STAT II) uses proprietary communication technology IQRF for a position determination. Both newly designed authentication techniques use a pocket device described in the final section of the paper

III. SYSTEM

A. Existing System

A one-time password (OTP) is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords. The most important short- coming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will be no longer valid. On the downside, OTPs are difficult for human beings to memorize. Therefore they require additional technology to work

B. Proposed System

To overcome the drawbacks of the existing system we design our new system. In this system we are concentrating on the security of the confidential data. In our proposed system, it not only checks the authorized log in but also checks the location of the user at the time of log in. Because of this user is not able to download any files from anywhere, he must be in the location which is given at the time of registration. It provides more security than existing one. At the time of registration user fill its information. All the information is store into the database in the encrypted format. To encrypt this data we are using AES algorithm. Also user has to set his location at the time of registration. We are using android phone as a GPS device in our system. To find the co-ordinate of location of user, we are using localize intelligence algorithm.

IV. LOCATION BASED CRYPTOGRAPHY

A. Location based identity

In cryptography "identity" Components are important to us. As a typical example we can mention the name and national ID card. So are scans of fingerprints or residential address, work address and so on. Data can be encrypted so that only the person who holds the private key can decrypt it (public key or private key). Here the question arises: can we have other forms of "identity"? What else can be used as an identity? Another question arises (in fact, it is the answer to the previous question): Can we use the place where we have a presence as our "identity"? Is it possible to use it in encryption? Physical presence in a particular location at a specific time, can be our "identity" in cryptography . For example, we know the role of a bank-teller behind a bullet-proof bank window not because she shows us her credentials but by merely knowing her location.Another question arises: for what applications is this method is more suitable? For example, assume military base "A" wants to communicate with military base "B" (obviously military communications must be confidential). In the traditional

ISSN: 2278 – 1323

approach the two bases can communicate by exchanging a secret key. One problem that arises is when an honest officer who carries the key is captured by enemy and he's tortured and he finally reveals the secret key. As a result with the secret key the enemy can decrypt the messages. We trust physical security more. So maybe we're able to guarantee somehow through some physical means that those who were inside a particular geographical region are approved. As a result (in the previous example) those who have physical presence in the military base "B" or get into it, are approved. So the message that is encrypted and sent from military base "A" to military base "B" will only be decrypted by a person or persons who have physical presence in a particular geographical location (military base "B") and no one else can't decrypt it.

B. *Location Based "Access Control"*

Another usage for the 'Location Based Cryptography' is

Access Control. A person who is physically present in a Particular location can make use of the resources. For example, individuals who are physically present in a particular room are able to use the printer. If they leave the room, they will not be allowed to access printers anymore and many such examples.

C. *Geo-Encryption Principles*

"Geo-Encryption" is a method based on adding a new Security layer on the available encryption protocols structure using the recipient's location information. Encrypted data can be decrypted and readout only on a particular geographical point at a specific time. The particular point can be exactly where we want the information to be decrypted, even with a radius of a few centimeters. It can also be within the walls of a room on a particular floor. Next-generation GPS and highly accurate GPS like the military types that are "Anti-Spoof", perform with an accuracy of 1 cm. They have the ability to measure a specific location very accurately with latitude, longitude and height. The idea of using "Geo-Encryption" was proposed and developed by "Logan Scott" and "Dorothy E Denning" for the first time. They used Geo-Encryption to encode files related to films in the manufacturer studios and send them to the cinema theaters through a wide network like the Internet. The sent files could be downloaded in all the areas which were covered. But they could be decrypted only on the location of the considered cinema theater at a specific time. The geographical information of the cinema theater must be matched with the information used in the sender's file.

As we know, using symmetric encryption (private key) in terms of computational and implementation is very fast. Asymmetric encryption (public key) method uses both the public and private keys and its security is very high. On the other hand due to the difficulty in computing its performing rate is low. Therefore in the "Geo-Encryption" algorithm a combination of symmetric and asymmetric encryption is used. The public key algorithm is used to secure and distribute session keys and the symmetric encryption algorithm is used to encrypt the information. The sender uses the session key (which is random) and a symmetric algorithm like "AES" to encrypt the desired data. Then using location information, time and speed of receiver (PVT) and a mapping table makes a certain code named "Geolock". Last the session key is encrypted by the certain code (Geolock) and by using an algorithm such as "RSA" the results are encrypted and sent. The receiver using their PVT information obtained via positioning tools (Anti-spoof GPS) and the mapping table, calculates the Geolock and then: Geolock encrypted key = Session key. The receiver using their PVT information obtained via positioning tools (Anti-spoof GPS) and the mapping table, calculates the Geolock and then: Geolock encrypted key = Session key.

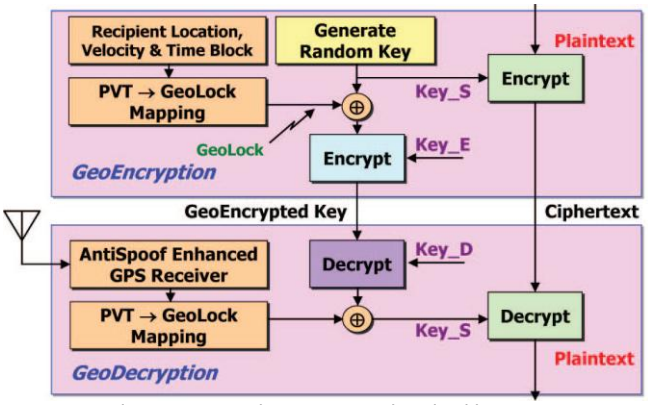

Figure 3. GeoCodex GeoEncryption algorithm

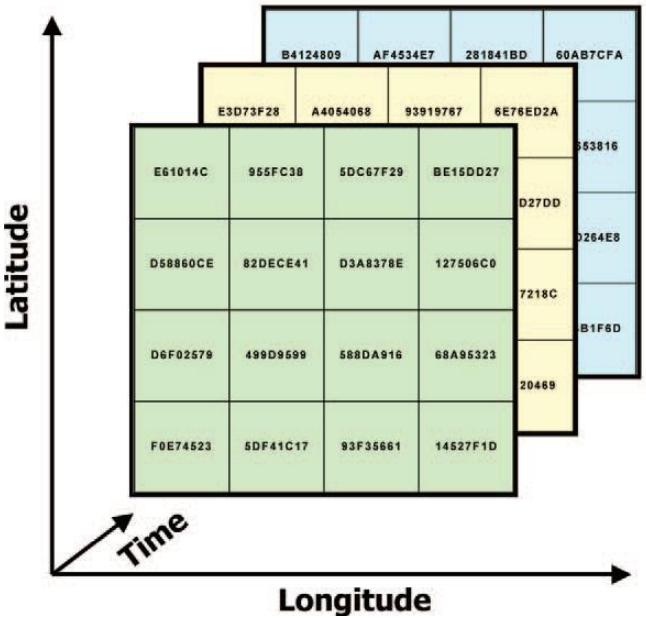

Figure 4. PVT GeoLock mapping function .

V. CONCLUSION

ISSN: 2278 – 1323

One of the most challenging issues in cloud computing is data access control. Because of the benefits of the cloud computing more people and more companies turn to this technology every day. Like almost every proposed procedure, there are challenges as well as the advantages present in this technology. In this paper, cloud security and its challenges are briefly discussed. Location based encryption and "Geo-Encryption" algorithm were also reviewed. Finally a new security level was added to the existing security measures using location-based encryption.
This method can be used in several places such as banks, big companies, institutions and have the desired performances.

VI. REFERENCES

[1] Nilesh B. Jondhale,Sonal K. Kadam,Shweta B. Shinde,Amol N. Dumbre,"Security in Cloud Computing: Using Geo-Encryption Authentication and Time based Database",International Journal of Advanced Research in Computer Science and Management Studies, Volume 2,Issue 10,October 2014,ISSN:2321-7782
[2] Pawar Sumedha D., Parade Priya B., Jagdale Supriya K., Goikar Vandana T. "Use Location to improve Security in Cloud Computing",International Journal of Advanced Research in Computer Science Engineering and Information Technology,Volume 4, Isuue 3,April 2015 ISSN:2321-3337
[3] Goikar Vandana T., Jagdale Supriya K., Parade Priya B., Pawar Sumedha D,Prof. Nalawade V.S."Improve Security of data access in Cloud Computing using Location ",Vol. 4 Issue. 2, February 2015, pg.331 – 340
[4] Meer Soheil Abolghasemi, Mahdi Mokarrami Sefidab, Reza Ebrahimi Atani ,"Using Location Based Encryption to Improve the Security of Data Access in Cloud Computing", 2013, International Conference on Advances in Computing, Communications and Informatics (ICACCI)

ISSN: 2278 – 1323