ISSN: 2321-7782 (Online)
Volume 2, Issue 10, October 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Security in Cloud Computing: Using Geo-Encryption Authentication and Time Based Data Access

Nilesh B. Jondhale[1]
Student
Computer Engineering
Jaihind College of Engineering
Kuran, Pune – India

Sonal K. Kadam[2]
Student
Computer Engineering
Jaihind College of Engineering
Kuran, Pune – India

Shweta B. Shinde[3]
Student
Computer Engineering
Jaihind College of Engineering
Kuran, Pune – India

Amol N. Dumbare[4]
Assistant Professor
Department of Computer Engineering
Jaihind College of Engineering
Kuran, Pune – India

Abstract: ***The term "geo-encryption" or "location-based encryption" refer to a security algorithm that limits the access or decryption of information content to specified locations and/or times. There are many challenges in the cloud computing. In our paper we are focused on the security and data access control. Now-a-days hackers can easily hack any confidential data. These become major issue in the cloud computing to resist these we are providing new security level by location based authentication. This is very useful in the corporate area, bank, institution, military, etc.***

Keywords: cloud computing; security; geo-encryption; cryptography; location-based.

I. INTRODUCTION

The Cloud computing is a concept that combines several technologies for deliver different services. Users are no longer owners of their computer servers but may gain many services online scalable without having to manage the underlying infrastructure, often complex. The Cloud computing enlarged the area of distributed computing systems by providing advanced Internet services complement and complete functionality of distributed computing provided by the Web, grid computing and Peer-to-Peer. The cloud computing systems provide an infrastructure for large-scale IT has high performance that dynamically adapts to the user and application needs.

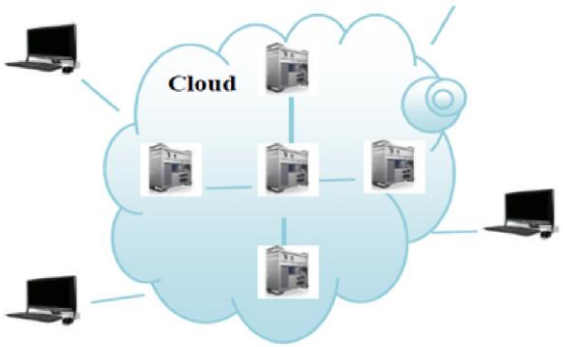

Fig 1: Cloud Computing

What Is 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 without affecting the end user, somewhat like a cloud 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.

Types of Clouds:

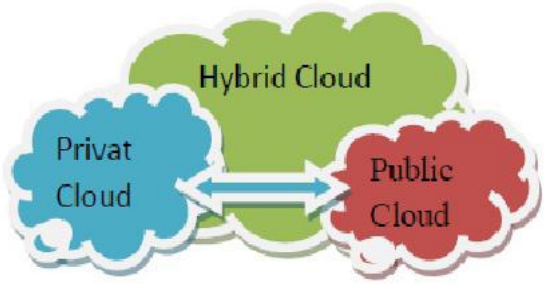

Fig 2: Types of Cloud

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...)

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.

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 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.

Types of services:

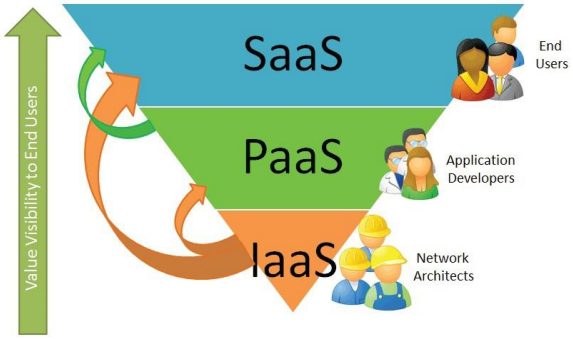

Fig 3: Types of Services

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 [2].

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.

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 [3].

Amazon EC2 (Amazon Elastic Compute Cloud) is an example of IaaS allows rent virtual machines predetermined sizes to run the applications.

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 Review

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) [5].

B. New Location-Based Authentication Techniques in the 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 [6].

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 [7].

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. ALGORITHMS

1. AES (Advanced Encryption Standard) Algorithm:

AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. However, the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively.

The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of its counterpart in the encryption algorithm. The four stages are as follows:

1. Substitute bytes
2. Shift rows
3. Mix Columns

The tenth round simply leaves out the Mix Columns stage. The first nine rounds of the decryption algorithm consist of the following:

1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

Again, the tenth round simply leaves out the Inverse Mix Columns stage [8].

2. **Localize Intelligence Algorithm**:

Location Tracking is becoming very popular in the modern era. In Today's world, the development of smartphones is gaining significant progress in the market. Navigation and positioning is one of the most enormous features available today. GPS is a navigation system using worldwide. It gives accurate precision and higher accuracy. We are using Localize Intelligence Algorithm which is implemented on android mobile phone. The steps of algorithm are as follows:

1. The Android Client receives the Signals and Coordinates from the Satellite.
2. We will design a Localized Location Engine. The Engine works in two parts:-

(a) The Location Engine: The Engine works in coordination with Android Location API. The Process is as follows:-

(i) Get Coordinates: It will take Coordinates of Android Client received from satellite.

(ii) Reverse Geocoding: The received Coordinates are then converted into geographical place.

(iii) Localized Refinement: Each geographical place is now matched with Localized data (user defined locations). The User defined Locations or pre-specified Locations are stored in Database called SQLite hosted on android Server. The result provides the relevant and refined Locations. Ex: Retech Society is nearby Vasundra.

(iv) Plotting engine: This Engine takes the Refined Locations and plotted them on map. The Engine works in coordination with Google map API [9].

V. System Design

A. Data Storage in Cloud:

- Data can be store on the cloud.
- Check authentication of user's location using GPS device.
- Give access to the authorize user.
- Check current time, date and time, date of file at the time of downloading.

B. User:

- At the time of registration user have to enter username, password, IMEI and location.
- At the time of login he has to enter username, password and GPS device must connect to system to get current location and IMEI.
- User can upload or download file.
- Users have to enter start date, time and end date, time of file when he want to upload file.
- User can download file only if file is within time period otherwise he get error of access denied.

C. Global Positioning System (GPS):

- Get the exact location co-ordinate (longitude and latitude) of user.
- It will give the location of user after every 15 sec.

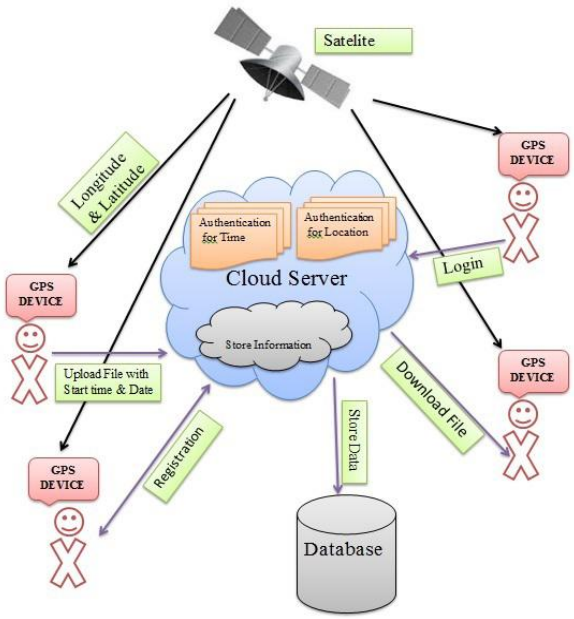

Fig 4: Architecture of System

D. Database

Store the username, password, IMEI, location of user. Whenever user want login to system server match the details of user with stored details.

Steps:

1. Firstly, users have to register to the system.

2. During registration user has to set his location i.e. longitude & latitude. Here all the data is keep in encrypted format in database using AES algorithm.
3. After completing this registration process user can log on to system.
4. Whenever, user wants to log in system, system must authenticate his location using GPS device (i.e. android phone). To get the co-ordinates of particular location we are using Localize Intelligence Algorithm, if authentication get failed, user unable to log in system.
5. When user get authorized log in, he can upload/download file on/from cloud server.
6. At the time of uploading file user has to give start date, time and end date, time.
7. At the time of downloading file user must be authorized then only he can download the file.
8. There is also another condition that he can download only that file which is in the valid time and date duration, otherwise he failed to download it.
9. After completing all the processes he has to log out from system.

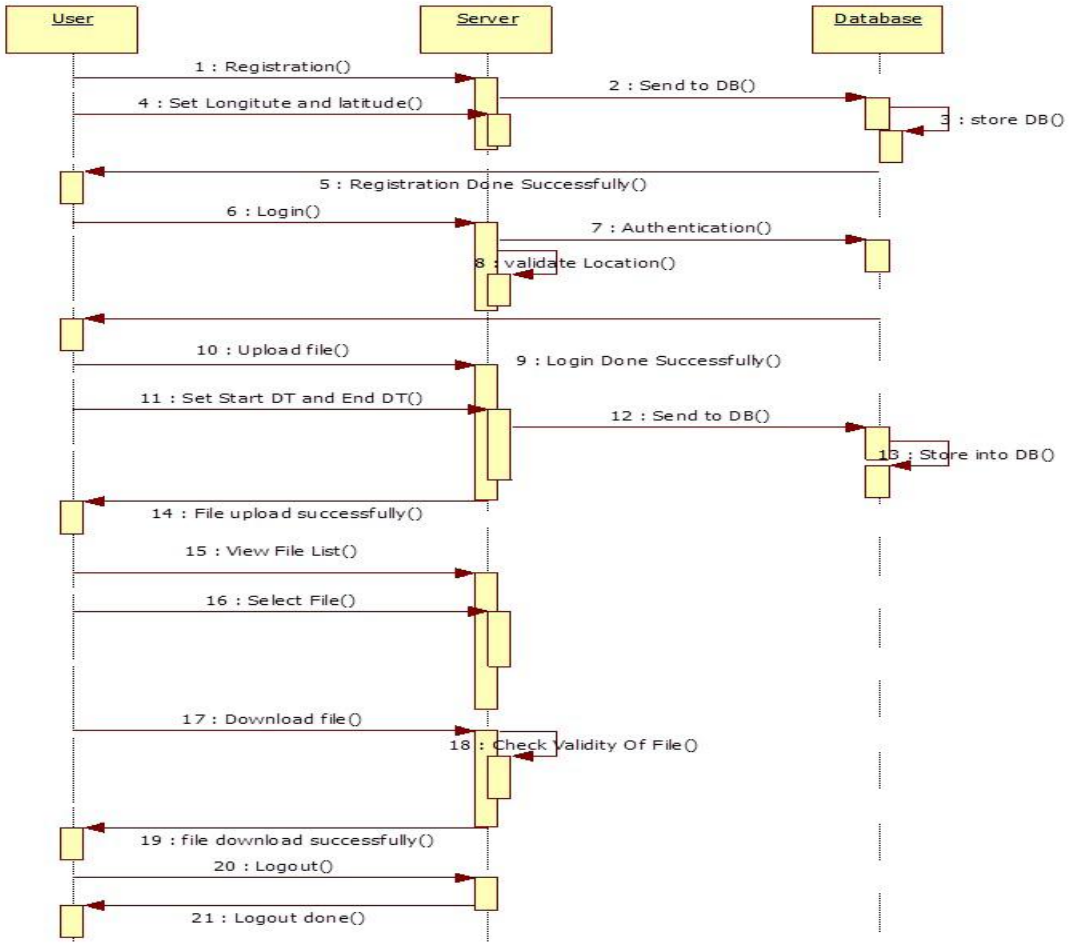

Fig 5: Sequence Diagram of Proposed System

E. Advantages

In this we get authentication of user with help of location and time when the user can access the system. File security contains the upload and download file with start date, time and end date, time. Private cloud storage is use for file storage and all file users can access after authentication of location and IMEI.

F. Disadvantages

GPS device is a core requirement because without GPS device user unable to log in the system. There is also another case i.e. cloudy environment. If there is cloudy environment then GPS device unable to find the perfect location of user. There may be problem occur while log in to system.

G. Applications

1. **Universities**:

   In universities there is major problem of paper leak. To avoid it university can upload all paper on the server. Server stores all the paper. When files are uploading we are giving start date, time and end date, time. So, no one is able to download that files before the given time and only authorize user can log in the system because we are providing location based encryption.

2. **Corporate Area:**

   In corporate area there is major problem of hacking of confidential data. Company stores the confidential data on server but still it is not safe. To protect data we are providing location based encryption. The person who want to download the data, firstly he has to match his location then only he can log in to server. Secondly, if the date and time limit get expire then he unable to download the file, error will occur.

3. **Military Based Application:**

   Assume military base A wants to communicate with military base B (obviously military communications must be confidential). In the traditional 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.

VI. Conclusion

Geo encryption provides control access to file based on location, time and date. In this paper we are discussed about the concept of clouds and its challenges. AES algorithm and Localize Intelligence Algorithm are also reviewed. Finally a new security level is added to the existing system using location, date and time encryption.

References

1. http://mysaas.fr/2010/10/04/private-cloud-publique-cloud-et-hybrid-cloud/.
2. http://www.emc.com/corporate/glossary/software-as-a-service.htm
3. http://www.emc.com/corporate/glossary/infrastructure-as-a-service.htm
4. http://www.emc.com/corporate/glossary/platform-as-a-service.htm
5. "An Effcient Lossless Data Hiding Technique for Palette-Based Images with Capacity Optimization", Published in: Systems, Signals and Image Processing, 2007 and 6th EURASIP Conference focused on Speech and Image Processing, Multimedia communications and services.
6. "New Location-Based Authentication Techniques in the Access Management", Published in: Wireless and Mobile Communications (ICWMC), 2010
7. http://en.m.wikipedia.org/wiki/one-time-password
8. http: //www.google.co.in / search ? site = & oq = aes + pdf & aqs = mobile-gws-lite.. & q = aes+pdf
9. Shaveta Bhatia1, Saba Hilal" A New Approach for Location based Tracking", IJCS International journal of Computer Science Issues, vol. 10, Issue 3, No 1, May 2013.

AUTHOR(S) PROFILE

Mr. Nilesh B.Jondhale currently persuing B.E in Computer Engineering from Jaihind College of Engineering, Kuran, Pune (Savitribai Phule Pune University, Pune). He is also good in programming.

Miss. Sonal K. Kadam currently persuing B.E in Computer Engineering from Jaihind College of Engineering, Kuran, Pune (Savitribai Phule Pune University, Pune). She is also good in presenting the technical topics.

Miss. Shweta B. Shinde currently persuing B.E in Computer Engineering from Jaihind College of Engineering, Kuran, Pune (Savitribai Phule Pune University, Pune). She is good in academic and she is punctual.

Prof. Amol N. Dumbare received the B.E. degree in Computer Engineering from Pimpri Chinchwad College of Engineering, Akurdi in 2012 and currently persuing M.Tech in Computer Science Engineering from Jawaharlal Nehru Technical University, Hyderabad. He is having 1.5 years of experience in teaching. Presently working as an Assistant Professor at Jaihind College of Engineering, Kuran (Savitribai Phule Pune University, Pune).

