Enhanced Algorithm to Improve the Security Level in Cloud Computing using Location Based Encryption

Shamshekhar S. Patil
Associate Professor, CSE Department.
Dr. AIT
Bangalore, India

Tania Clarke
M.Tech, CSE Department.
Dr. AIT
Bangalore, India

***Abstract*— One of the most challenging issue in cloud computing is regarding its security and access control. As there is a growing trend of using cloud computing for its storage and data processing needs, more and more people and companies are joining the cloud hence causing major security concerns. The existing solutions that use pure cryptographic techniques to mitigate these security and access control problems suffer from heavy computational overhead on both the data owner as well as the service provider for key management and distribution. In this paper we add an extra level of security to the existing security measure and thus prove our method is secure in terms of confidentiality, authenticity, simplicity and practicability. As a result the proposed approach can thus improve the security and confidentiality in location based encryption.**

Keywords—Cloud Computing , Security ,2-layer encryption ,Geo encryption, confidentiality

I. INTRODUCTION

Companies are rapidly moving onto cloud because they can now use the best resources available on the market in the blink of an eye and also reduce their operations cost drastically. But as more and more information is moved onto the cloud the security concerns have started to develop . In such scenarios, we need to secure the data present within the cloud. The most common way is by using encryption technique, like Hashing , Symmetric and Asymmetric encryption[2] . But nowadays this isn't sufficient in securing the data . It takes no time for the hackers to hack the keys and decrypt the data . Thus looking into the problem we can derive to a conclusion that all the encryption strategies henceforth used were location independent . Not only network security is important but also physical security needs to be taken into consideration . Because a person from any location can accesse the data , in which the identity of the person need not be the same-Imposter. For Ex: In many places, The 12^{th} examination board sends question papers to various districts and remote places physically, by transporting them through a vehicle . But these question papers can be leaked, either through human intervention by hijacking the vehicle or through some anti-social elements (people) who themselves leak the papers for some profit.

Hence we can draw from the above example that , Physical security is equally important to that of network security .First let us know, what is physical security?? Physical security can be described as a security measure that is designed to deny unauthorized access to any equipment, building or networking components and to protect, personnel and property from damage or harm (such as espionage, theft or any form of attacks) . By which physical security adds as an extra layer of protection to the existing network security . Examples of Physical security include, address of a person (Location), fingerprints & retinal scan(Biometrics), locks, CCTVs, surveillances, security guard etc. Remember that network security starts at the physical level. An intruder cannot be stopped by any kind of firewall in this world, who is able to gain physical access to your network and computers. So physical security cannot be ignored. No information security guide is complete without a chapter about securing physical access to information resources. Physical access, after all gives even the common unskilled attacker access to the network, workstations, servers, and hardcopy information just waiting for someone to come by and pick it up. Thus in this paper we provide physical security with respect to location and time constraints, which means a person only within that geographic location and time can have access to the data. Hence this can be termed as Location based encryption. Location based encryption enhances security by integrating position and time into encryption and decryption processes. From a security perspective we find that, it is not enough to simply have decryption based on location and time; these aspects must be integrated into the key construction process, which will be explained further.

Furthermore, keys or files in transit should not reveal anything regarding their locations/times of applicability . After reviewing the objectives of location-based encryption, The paper focuses on geo-encryption[1]. The described geo-encryption approach builds on established cryptographic algorithms and protocols in a way that provides an additional layer of security beyond that provided by conventional cryptography. There are many applications, however, which require more than just protecting the data at a single level. For those applications, it is necessary to provide multilevel security that can accommodate the different sensitivity levels of information as well as the different clearance levels of the users. Hence we come to a conclusion that inorder to improve the security one needs to increase the security levels[9].

II. CLOUD COMPUTING

A. *Definition of cloud computing*

It describes the means of delivering any to all information technology - from computing power to computing infrastructure , applications , Business processes and personal collaboration – to end users as a service wherever and whenever needed[3].

The cloud in cloud computing is a set of hardware , software , networks , storage , services and interfaces that combine to deliver aspects of computing as a service. Shared resources , software and information are provided to computers and other devices on demand. It allows people to do things, whatever they want to do on a computer without the need for them to buy and build an IT infrastructure or to understand the underlying technology.

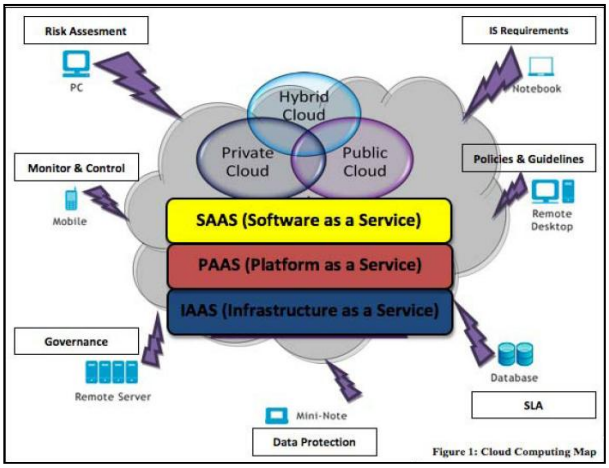


Figure 1: Cloud Computing Map

B. *Cloud delivery models*

- *Public clouds*: A business rents its capability and they pay for whatever they use . They are available to clients from a third-party service provider via the internet. Public clouds provide an elastic, cost effective means to deploy solutions and they take care of deploying , managing and securing the infrastructure[3] .

- *Private clouds*: A business essentially turns its IT environment into a cloud and uses it to deliver services to the users. These clouds are deployed into the companys firewall (on-premise data centers) and traditionally run by on-site servers. Private cloud provides a greater control of the cloud infrastructure and it improves security and resiliency because user access and the networks used are restricted and designated .

- *Hybrid clouds*: It's a combination of, an interoperating public and private cloud . Here, users typically outsource non-business-critical information and processings to the public cloud , as they keep business-critical services and data under their control. It offers the best of both cloud worlds – the scale and convenience of public cloud and the control and reliability of on-premises software and infrastructure.

C. *Types of cloud offerings*

- *Platform as a service (PaaS)* : This is the provisioning of hardware, frameworks, OS and database for which developers write custom applications. They provide foundation to build highly scalable and robust web-based applications. PaaS saves cost by reducing the upfront software licensing and infrastructure cost and by reducing ongoing operational costs for development, testing and hosting environments[3].

- *Software as a service (SaaS)* : This is the provisioning of OS, special purpose software and hardware made available through the internet. SaaS saves the cost by removing the effort of development, maintenance and delivery of software; eliminating up-front software licensing and infrastructure costs; and reducing the costs for maintenance and operational costs with respect to support and administration.

- *Infrastructure as a service (IaaS)* : This is the provisioning of hardware or virtual computers where the organization has control over the OS, thereby allowing the execution of arbitrary software. IaaS saves costs by eliminating the need to over-provision computing resources to be able to handle peaks in demand.

D. *Cloud computing issues and challenges, with regards to security*

As there are some real benefits of using cloud computing, which includes some key security advantages. There are also some key security challenges which prevents users from using the cloud [5].

Security challenges falls into 3 categories

Data Protection: We need to protect the data from Unauthorized access , Accidental loss and damage. Since, In cloud computing one outsources the data onto the cloud hence data needs to be protected not only when its stored in the cloud but also during its transit. To do so, you need to be confident about your cloud provider's security and one should be aware of where the data is being stored. Thus by the client encrypting the data, to be stored on the cloud and having access to the encryption keys being used for encryption and manipulating them, they will have full control over the data[6].

User Authentication: The data which resides in the cloud needs to be accessed only by authentic users who are authorized to use the data. Thus by having strong passwords and keys, one can prevent insiders attack or imposition, wherein other users who pretend to be the original users use the data.

Disaster and Data Breach: With the cloud serving as a single centralized repository for a company's mission-critical data, There are several risks of the data being compromised due to data breach or temporarily made unavailable due to a natural disaster are real concerns. Additionally, companies should also have contingency plans in place,when events such as their cloud provider fails or goes bankrupt. At that point of time, whether the data can be easily retrieved and migrated to a new service provider or to a non-cloud strategy is a question ? What happens to the data and its access mechanism if the provider gets acquired by another company?[5]

Security Issues fall in two categories,

Security issues faced by cloud provider: When the organization elects to store the data or host the applications on the cloud, it loses its ability to have physical access over the data. As a result , confidential data is at risk from insiders attack. Thus the provider must ensure that their infrastructure is secure and that their clients data and applications are protected[5]

Security issues faced by customers: In order to save the resources, reduce the cost, and maintain efficiency, Cloud Service Providers often store more than one customer's data on the same server. Hence there is a possibility that one user's private data can by viewed by other users (possibly even competitors). In order to prevent such type of situation, cloud service providers should ensure proper data isolation and logical storage segregation [5]

III. EXISTING SYSTEM

The term "Geo-encryption" is a Location based data encryption, where the cipher text can only be decrypted at a specified location. If an attempt is made to decrypt the data at another location, the decryption process fails and reveals no information about the plaintext. In this method, the key depends on target geographic location which powers it to be used in real time applications. [1]

The "Geo-Codex GeoEncryption" algorithm is a combination of symmetric and asymmetric encryption. The public key algorithm is used to secure and distribute session keys and the symmetric encryption algorithm was 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" (Fig. 4). 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 XOR encrypted key = Session key [1].

The existing system is a combination of both symmetric and asymmetric encryption, in which the disadvantages of one is overcome by the advantages of the other. Hence they form a perfect solution for cryptography .But, it's quite complex for users to understand and implement. Key management is quite cumbersome and confusing.

As the use of session keys makes the system more secure, it also has some fallbacks as in - A series of numbers generated from a truly random process, called the RNG(Random Number Generator) and one of the key problems is deciding whether or not the generating process is truly random. They are generally slow, especially since the typical computer application may require millions of numbers per sec. The numbers obtained from such type of devices are not always truly random. Another major shortcoming is the lack of reproducibility. Reproducibility is needed for debugging codes that use random numbers for making co-related computations. Computational methods which use mathematical formula or precalculated tables to produce sequence of numbers that appears random can be easily trapped. Since computer follows an deterministic algorithm to generate these numbers which can be predictable [7].

A. *Security requirements of the existing approach:*

The security requirements of the existing approach are as follows[2]:

Confidentiality: Only the registered users and the data owner shares the session key, which keeps on changing. Thus as long as the registered users and the data owner are updated with it, confidentiality remains. If as said above, the RNG is truly not random or some computational methods are used to generate these session keys, confidentiality no more remains as these session keys can be guessed/trapped through direct cryptanalytic attacks, input based attacks, state compromise extension attacks etc…[7]

Authentication: The user must know the correct session key and GeoLock to decrypt the data. If the user forgets the session key he would never be able to access the data, even though he is at the correct location.

Simplicity: Since the use of both symmetric and asymmetric encryption is used, it is highly secure. But its very complex and not easily understandable by the users .

Practicability: The mapping function which converts the position, time and velocity to a unique value called a lock. Here, the lock is calculated by dividing the coordinates by the decryption region which is a square. Hence, other than the square no other decryption regions can be used like circle, triangle etc.. [8]

Hence as this provides a single level of security which is not enough to be secure. In our proposed approach we are adding an extra level of security, called the 2 layer encryption scheme in order to enhance the security.

IV. PROPOSED SYSYTEM

In our proposed approach, we define the location parameters as latitude, longitude, Start time and End time instead of using postion, velocity and time(PVT) parametrs as used in the existing system . Thus here we call these location parameters as Access policy.

Here we are providing a 2 layer encryption, to make the Location based encryption system more secure than the existing one. Fig(2) shows the block diagram of the file uploading process, from the data owner to the cloud. The data owner selects the file to be uploaded and decides on the access policy the file needs to have. From the access policy a key is generated, which is XORed with the file .Hence, the first cipher text is formed. Then, as we are providing a 2 layered encryption, at the second layer we are performing AES encryption, on the cipher text 1 and an AES key which is further encrypted to form cipher text 2.

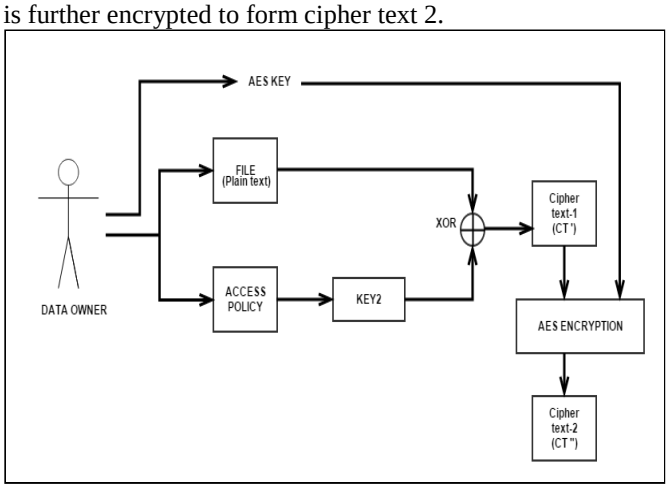
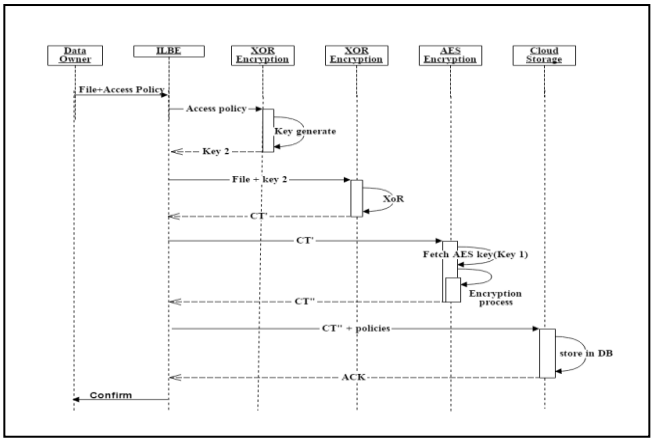


Fig .2 Block diagram of the Upload process

At the very first layer we are using XOR encryption, which gives the cipher text 1 and above that we are providing an extra level of security by using a symmetric encryption algorithm (AES), which is the strongest among all symmetric encryption algorithms having a key size of 128bits.

Cipher text 2 cannot be decrypted without one getting the AES key , which cannot be hacked even with the brute force attack. Thus taking advantage of this we add an extra level of security by introducing another encryption called XOR encryption, which further contains the key of the access policy.



Figs .3 Sequence diagram of the File upload process

Fig .3 shows that , The Data Owner selects the file and defines the necessary access policy (Latitude, Longitude, Start and End time) for it. From the Access policy a key is generated, called Key 2.The File and the key2 are XORed using XOR encryption which gives, Cipher text(**CT'**).Since we are providing a 2 layer encryption, AES encryption is used with CT' and AES key which is present with the data owner , Hence which produces cipher text(**CT"**) .CT" along with the access policies are stored in the cloud. Thus the ACK will be sent to the ILBE(Intelligent Location Based Encryption) , which would be further confirmed to the Data Owner.

At the downloading end, the user uses the AES key through symmetric encryption which is being shared between the data owner and the user and thus decrypts cipher text 2. Hence by providing his correct access policy he unlocks the KEY2 and fetches the file and thus decrypts cipher text 1 .

Data Owner : He selects the files to be uploaded and defines the access policy(latitude, longitude, start time and end time) for it.

Key2 : This key is obtained from the access policy. The key generation is shown below in fig(3), first XOR operation is performed on the latitude and longitude and then separately another XOR operation is performed on the start time and end time. Finally, Both the operations are combined to form a final XOR which forms the key.

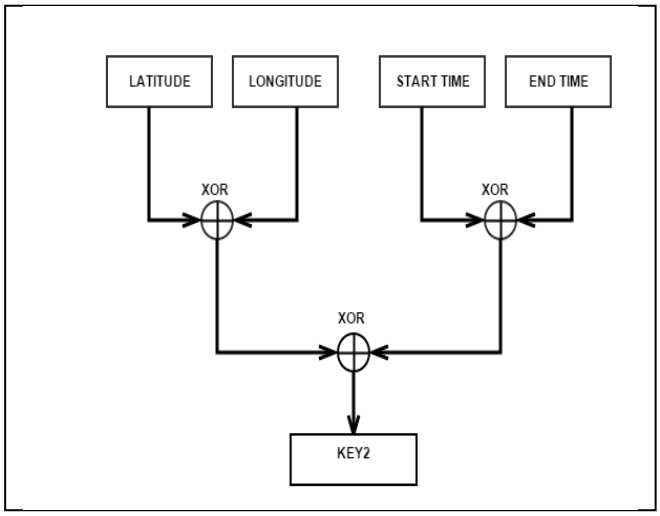


Fig .4 key generation from the access policy

Xor Encryption : XOR is a symmetric cipher . A string of text can be encrypted by applying bitwise XOR operator to every character using a key. To decrypt the output, we merely apply XOR function with the key which will remove the cipher[6]. XOR encryption is then performed on the file and the KEY2, which produces cipher text1 (CT').

Aes Encryption : AES is a symmetric block cipher. Which indicates that it uses the same key for both encryption and decryption. However, AES uses a block length of 128 bits and a key length that can be 128, 192, 256 bits. A number of AES parameters depend on the key length. For example, if

the key size is 128 bits 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 decryption algorithm contains the following first nine rounds,

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 [6].

Thus the input to the AES encryption is the CT' and a AES key of length 128bits is used (which the user owns), which produces cipher text 2(CT").

A. Security requirements of the existing approach:

The security requirements of the proposed approach are as follows[2]:

Confidentiality: the AES key and the Access policy key is shared between the owner and the users. Hence even if either is compromised the confidentiality still remains as it is a two level security .

Authenticity: Firstly, the username and password identifies the users authenticity with the data owner. Secondly, the key he contains and finally, his location information adds for the user to prove his identity.

Simplicity: In our proposed approach we use simple XOR encryption and symmetric algorithm such as AES which is highly secure and easily understandable.

Practicability: Here we do not explicitly define the decryption region. A tolerance value of 100m is taken and accuracy is tolerable.

CONCLUSION AND FUTURE WORK

Traditional encryption technology cannot restrict the location of users for data decryption. In order to meet the demand of security in cloud computing, a modified location dependent data encryption algorithm is proposed in this paper. The location based encryption or Geo encryption were reviewed. Finally a new security level was added to the existing security measures using location based encryption. Thus by providing an extra level of security we are improving the security and confidentiality in cloud computing. This method can be useful in several places such as during examination conduction, companies and banks.

In future research work, Quantum mechanics can be used to encrypt and decrypt data at a secure location without pre-sharing any cryptographic keys.

REFERENCES

[1] Abolghasemi M.S,Sefidab M.M,Atani,R.E "Using location based encryption to improve the security of data access in cloud computing", Advances in Computing,communications and informatics(ICACCI) 2013 International conference.

[2] Karami R,Kalantari M "Enhancing security and confidentiality in location-based data encryption algorithm", Roedunet international conference(RoEduNet)2011,10th.

[3] Dr.Kumar Saurabh, "CLOUD COMPUTING", First edition:2012, ISBN:978-81-265-3603-0

[4] http://www.wisegeek.org/what-are-the-different-types-of-encryption-methods.htm

[5] http://www.webopedia.com

[6] http://www.ictknowledgebase.org.uk/cloudcomputingdataprotection

[7] http://en.wikipedia.org

[8] Gongjun Yan, Jingli Lin, Danda B. Rawat, Weiming Yang, A Geographic Location-based Security Mechanism for Intelligent Vehicular Networks,(*Unpublished*)

[9] Jongdeog ,Sang H., Mukesh Singhal "Design of an Architecture for Multiple Security Levels in Wireless Sensor Networks"