APPLYING GEO-ENCRYPTION AND ATTRIBUTE BASED ENCRYPTION TO IMPLEMENT SECURE ACCESS CONTROL IN THE CLOUD

Abu Salim[1], Sachin Tripathi[2] and Rajesh Kumar Tiwari[3]

[1]Department of Computer Science, College of CS & IT, Jazan University, Jazan, Kingdom of Saudi Arabia (KSA)
[2]Department of Computer Science Engineering, Indian Institute of Technology, Dhanbad, Jharkhand, India
[3]Department of Computer Science and Engineering, RVS College of Eng. & Tech., Jamshedpur, Jharkhand, India

ABSTRACT

Cloud computing is utility-based computing provides many benefits to its clients but security is one aspect which is delaying its adoptions. Security challenges include data security, network security and infrastructure security. Data security can be achieved using Cryptography. If we include location information in the encryption and decryption process then we can bind access to data with the location so that data can be accessed only from the specified locations. In this paper, we propose a method based on the symmetric cryptography, location-based cryptography and ciphertext policy – Attribute-based encryption (CP-ABE) to implements secure access control to the outsourced data. The Symmetric key is used to encrypt that data whereas CP-ABE is used to encrypt the secret key and the location lock value before uploading on the server. User will download encrypted data and the symmetric secret key XORed with the Location Lock value, using his attributes based secret key he can obtain first XORed value of Symmetric secret key and location lock value. Using anti-spoof GPS Location lock value can be obtained which can be used to retrieve the symmetric secret key. We have adopted Massage Authentication Code (MAC) to ensure Integrity and Availability of the data. This protocol can be used in the Bank, government organization, military services or any other industry those are having their offices/work location at a fixed place, so data access can be bounded to that location.

KEYWORDS

Cloud Computing, Secure Access Control, Security issues, Cryptography, Geo Encryption, Attribute-Based Encryption, CP- ABE.

1. INTRODUCTION

Cloud computing is an emerging field, since its inception, cloud computing gained widespread popularity in the industry as well as academia [1]. It offers many benefits which include the reduced cost on technical support for data backups, saving electric power and maintenance cost. These benefits encourage the organization to shift their operations to the cloud. Cloud storage is one of the most promising services which are utilized by these organizations. Despite several benefits offered by the cloud it also poses many challenges, in which the security of outsourced data is paramount.

DOI: 10.5121/ijcnc.2019.11407

Security of the data in the cloud environment can be achieved using cryptographic methods; several cryptographic techniques are available which can be used to enforce confidentiality, integrity, availability and access control of the outsourced data. Confidentiality of the data can be achieved by encrypting the data before outsourcing to the cloud storage, encryption of the data also encompasses many challenges, which includes, key distribution to the user, user revocation, scalability of the data, performing search operations on the data, a number researcher has addressed these issues in their research work. To ensure the integrity of the data a number solution is purposed mainly based on the Message Authentication Code (MAC), the digital signature. Where MAC only ensures the integrity of the data, digital signature can be used to ensure authenticity, non-repudiations along with the integrity of the data. To ensure Availability the researchers purpose many schemes, these schemes are based on proofs of retrievability (PoRs) [2]/provable data possession (PDP) [3] and either private verifiable or public verifiable. PoRs can correct the small error using the error correcting code and it detects large corruption using spot checking whereas PDP only checks the availability of files which means it detects only corruption no error correcting code. To achieve secure access control of outsourced data Cipher Policy-Attribute based encryption can be used, in which the users which pose only certain attribute and satisfy the access structure associated with the data can access the data. We enhance this scheme by binding the data with the geographical location, so that, not only attributes needs to be satisfied by the users but the presence of the user at certain locations also needs to be satisfied. To achieve confidentiality, integrity along with the access control, we purposed to use symmetric key cryptography, Ciphertext-Attribute Based Encryption, Geo Encryption, and MAC.

The remainder of the paper is as follows, Section 2 provides an introduction of cloud computing, characteristics of cloud computing, Service delivery, deployment model and security challenges. In section 3, we have discussed an introduction to cryptography, Symmetric, and Asymmetric cryptography, Ciphertext-Policy Attribute Based encryption and Geo-Encryption. Section 4 discusses related works. In section 5, we discussed purposed work whereas in section 6 and 7 security discussion and conclusion respectively.

2. CLOUD COMPUTING

Cloud computing is a utility-based computing, According to NIST [4] ," Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

This cloud model is composed of five essential characteristics, three service models, and four deployment models

2.1. Characteristics of cloud computing

Cloud computing has the following essential characteristics.

- *On-Demand Self-Service:* User of the cloud computing can access /control computing resources automatically as needed.
- *Ubiquitous Network Access:* Uniform access to the resources from the cloud using different devices like Computer, Laptop, PDA, etc.
- *Resource Pooling:* The resources can be shared between different Users; they can acquire or release resources as needed.

- *Rapid Elasticity:* Resources can be acquired and released automatically and quickly as needed.
- *Measured Service:* Uses of the resources on the cloud can be monitored and the user is charged based on the resources used.

2.2. Three Service Models

Cloud computing utilizes three service model to deliver services.

- *Software as a Service (SaaS):* Software as a Service (SaaS), in this model of computing user can use the software hosted by the third party without installing them on his system, most of the software can be accessed using web browser.
- *Platform as a Service (PaaS):* Platform as a Service (PaaS), this model provides a framework which can be used by the developer to develop or customize applications. It makes the development, testing, and deployment of software quick, simple, and cost-effective.
- *Infrastructure as a Service (IaaS):* Infrastructure as a Service, in this cloud service provider outsources the equipment like storage, hardware, servers, and networking components. The management of these components is done by the service provider and the client charged based on resources used by them.

2.3. Four deployments Model

Cloud computing utilizes four deployment model.

- *Private Cloud:* It belongs to some specific organization, resources are controlled by the Information Technology (IT) Departments of that organization.
- *Community cloud:* In this model of computing some organization those belong to a specific community can share the resources, for example, two government organizations working for the same goal can share the resources.
- *Public Cloud:* In this model of computing cloud services are available to the general public through the internet. Examples are Gmail, DropBox, office 360, etc.
- *Hybrid Cloud:* In this model Organizations may host some important data, application on the private cloud and less important data on the Public cloud; it is a combination of two models so referred to as Hybrid Cloud.

2.4. Security Challenges

Security is the major concern which delaying adoption of cloud computing, in the cloud computing software, data, infrastructure is not in the control of the user, it is under the control of cloud service provider, this unique model of computing raise several issues with respect to the data security, the security of the data may be compromised by the dishonest employee of service provider, the other client those using the same infrastructure. Data Security includes Confidentiality, Integrity, and availability of stored data. Due to cloud computing characteristic, some other issues also exist like Data Lock-In, Data Location.

- *Data Privacy:* Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveals themselves selectively [5]. The privacy of the data in the cloud should be not compromised.

- *Data Integrity:* Integrity means that assets can be modified only by authorized parties or in authorized ways and refers to data, software, and hardware. Data Integrity refers to protecting data from unauthorized deletion, modification or fabrication [6]. The integrity of the data must be intact in the cloud.

- *Data Availability:* Availability refers to the property of a system being accessible and usable upon demand by an authorized entity [6]. Data Availability is also a concern in cloud computing.

- *Data Lock-In:* Different CSP provider may use different framework and if the user wishes to change the CSP for one or another reason it will be difficult for him.

- *Data Location:* Location of data is also concerned in cloud computing. The CSP has their data center located across the different geographical region, because of the data privacy law in various countries this may be a matter of concern. Some data may be of a sensitive and they must not leave a certain country. In case of investigation, some data may be required and accessing those data may be a problem.

3. CRYPTOGRAPHY

Cryptography can be used to protect the data in transit, data at rest and during computation. Cryptography is a technique in which plain text (readable text) will be converted to ciphertext (unreadable text) with the help of the key and algorithm.

It can be categorized in two categories.

1. Symmetric Key Cryptography
2. Asymmetric Key cryptography

In the Symmetric key cryptography same key is used for encryption and decryption where as in the asymmetric key cryptography different key are used for encryption and decryption.

3.1. Symmetric encryption

A symmetric encryption [7] scheme consists of five elements (Figure 1).

- *Plaintext:* This is the message which is needed to be protected.
- *Encryption algorithm:* This algorithm converts plaintext (Original Message) to random stream of data using substitution and transformation
- *Secret key:* The secret key is fed to the encryption algorithm. The algorithm produces a different output (cipher Text) depends upon the key. The key does not have any relation with the encryption algorithm or plain text.
- *Ciphertext:* When the secret key and plain text feed (input) to the encryption algorithm we get a scrambled message, known as ciphertext, Different key produce different ciphertext.
- *Decryption algorithm:* It takes Secret key and ciphertext as input and produces plain text as an output.

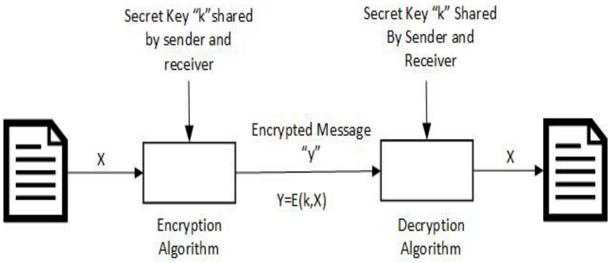
Secret Key "k"shared by sender and receiver
Secret Key "k" Shared By Sender and Receiver
X
Encrypted Message "Y"
Y=E(k,X)
X
Encryption Algorithm
Decryption Algorithm

Figure 1: Symmetric encryption

3.2. Asymmetric encryption

In Asymmetric encryption, encryption and decryption are performed using two different keys referred as public key and private key. It is also known as public-key encryption. In this, encryption algorithm public key is used to transform plaintext into ciphertext and private key is used to recover plaintext from ciphertext. Public key is made widely available through certificate authority, whereas private key is kept secret.
Symmetric key encryption technique is more efficient then asymmetric key cryptography but key distribution is a problem where as asymmetric key cryptography used different key for encryption and decryption so there is no need to exchange key but it is slow [8].

In cloud computing data can be encrypted with the help of symmetric key encryption and key can be encrypted with the asymmetric key encryption prior to distribution.

3.3. Ciphertext-Policy attribute-based encryption

Attribute-based encryption (ABE) can be used for fine-grained data access control, in which a group of recipients can be specified using a descriptive attribute [9]. ABE can be implemented in two ways Key Policy-Attribute Based Encryption (KP-ABE) and Ciphertext Policy-Attribute Based Encryption (CP-ABE), The KP-ABE was first introduced in [10] by Sahai at el., in this scheme, the attributes are associated with the ciphertext whereas in CP-ABE introduced in [9] the access structure is associated with the ciphertext. In KP-ABE, The attribute was encrypted along with the plain text to generate ciphertext and access structure was associated with the Key which was distributed to the user. In CP-ABE the access structure was encrypted along with the Plain text to produce ciphertext and the attribute was associated with the key so that different user having different set of attribute associated with the key can decrypt different set of data based on the access structure associated with the data (Ciphertext) so providing fine-grained access control to the data.

An Example of CP-ABE encryption is given in Figure 2, CP-ABE uses tree-based structure with a given set of attribute, in order to decrypt the data, attribute set must satisfy access structure which is associated with the data , it uses AND, OR and k of n operator to specify which attribute set(User) can decrypt the data. for example if the data is encrypted under the following attribute set (accountant, manager,clerk,a1,a2,a3 etc) and the access tree given in the Figure 2 is associated with the data and the different user group can be identified as User1: Manager,a2,a3 user2: accountant,a1 user3: clerk,a1,a3 etc.

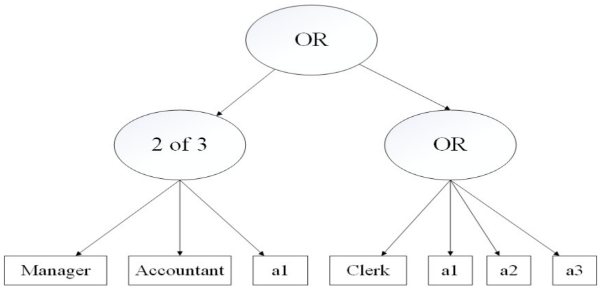

Figure 2: CP-ABE

if a user wants to decrypt the data he must poses two attributes from the manager, accountant, a1 or anyone from the clerk, a1,a2, a3.

3.4. Geo- Encryption

Identity is a very important component in the cryptography. It may constitute name, employee id, Adhar Number, Voter ID card, hand geometry, iris, retina, finger veins, etc beyond this traditional identity, We can also have another form of identity, presence of particular entity at the specified location for example in the bank we are verifying bank manager or account manager only due to their location without asking them their identity card. In the cryptography system, we can use this identity in which the identity of an entity is derived from the presence of the entity at a geographical location [11]. It allows data to be encrypted for a specific location which can be identified in terms of space and time, it is impossible to decrypt the data without the location information which can be obtained using antispoof GPS receiver, an anti-spoof GPS receiver has a selective availability spoofing module (SAASM) and the GPS signal includes encrypted binary codes Y. SAAMS receiver can track Y codes only when loaded with correct decryption key [12]. Location-based encryption or Geo-encryption can be used to ensure that data cannot be decrypted outside a particular facility, for example, at a particular theatre, bank, the headquarters of a government agency, military base or an individual's office or home.

4. RELATED WORKS

Many techniques have been purposed by the various researchers for the secure Access control in the cloud [13, 14, 15], Geo-Encryption technique was first purposed by Logan Scott, Dr. Dorothy Denning [16] to secure digital film distribution. In this paper, they purpose a solution for secure digital film distribution. The purpose that by using Geographical location a key can be generated "Geo-Lock" which is used in the encryption process of digital film. This film can be sent at any location using the network but can be decrypted only at the location which is specified at the time of encryption. In geo-encryption two separate packets of data is sent to the receiving side, one is data encrypted with the symmetric key cryptography, and other is Geo-Lock value obtained using the geo-lock function where longitude, latitude and time constitute input, XORed with a symmetric key and encrypted with Asymmetric key cryptography. At the decryption side, the Geo-Lock values are computed after obtaining location information using the Anti Spoof GPS and XORed with the decrypted value of received Geo-Lock XORed with a symmetric key to recover symmetric key, which finally used to decrypt the data.

The idea of location-based encryption is further used by many researchers in their scheme to enhance security.

Ala Al-Fuqaha, Omar Al-Ibrahim [17] they use Geo-Encryption to ensure that message are exchanged between mobile nodes securely, by allowing the decryption of the message at the specified location and time.

Mahdi Daghmechi Firoozjaei, Javad Vahidi [18] uses A5 encryption to encrypt data between Mobile Subscriber and BTS. The key to A5 encryption is generated using Mobile subscriber location information and a random number. The decryption of data is only possible at the location to which GSM network is aware.

Prasad Reddy. P.V.G.D, K. R. Sudha, P Sanyasi [19] proposed a location dependent Image Encryption for Mobile Information System. In this paper, the mobile clients transmit a target latitude/longitude coordinate and an LDEA key is obtained for data encryption to the information server. The client can only decrypt the ciphertext when the coordinate acquired from GPS receiver matches with the target coordinate. They make the use of a random key (R-key) in addition to the LDEA key to improving security.

5. PURPOSED MODEL

We propose an idea of using Geo-Encryption for cloud computing, in which the data can be accessed only at the specified location. Data owner will calculate MAC using Secret Key and encrypt both data and MAC using Secret Key before storing on the cloud server, as public key cryptography is computation intensive as compared to symmetric key cryptography we will purpose to use Symmetric key cryptography for encryption, one of the widely used Symmetric key algorithms is RSA which can be used for the encryption of data and MAC. In our purpose model, attribute authority is responsible for the defining access structure associated with the data on the basis of the access policy, Data and MAC will be encrypted using a session key, session key is XORed with the location lock value which can be computed on the basis of intended user positions and then encrypted with the attribute policy using CP-ABE scheme, after encryption they are passed to the cloud storage, at the decryption site user will use secret key associated with his Attribute keys to decrypt and recover the XOR value of Location lock and the Secret key, Anti Spoof GPS will be used at the decryption side by the user to get the accurate location value , This Location Lock value will be XORed with the received value (XOR of Secret Key and intended Location Value) to recover the secret key. If the location obtained by Anti Spoof GPS is correct then the only user will get correct secret key which can be finally used to decrypt the data and MAC, if the location lock value is incorrect then the secret key obtained will be also incorrect and cannot be used for decryption. After retrieving DATA and MAC, the user will calculate MAC of the received data using a secret key, if computed MAC is the same as received MAC value and then the user can be sure that he received correct DATA.

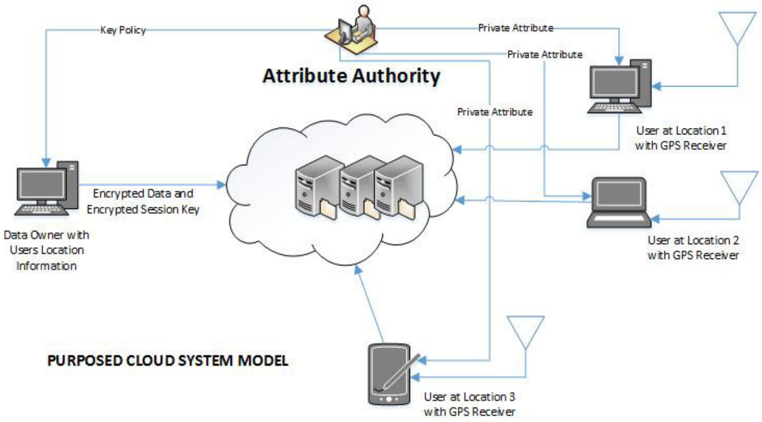

Figure: 3 Purposed Cloud System Model

Table 1 represents all the information which required encrypting the session key and the location lock value using CP-ABE scheme for which attribute policy is specified using the User Attributes.

Table1. Information used to encrypt session key

Data Tag	User Attributes				Location Lock Value (Calculated using hash function Longitude, Latitude as input)
	Att1	Att2	Att3	Att4	
T1	A	B	C	d	Location Lock Value 1
T2	C	F			Location Lock Value 3
Tn	A	C	G		Location Lock Value n

5.1 Protocol for Encryption and Decryption

Our Scheme is based on the CP-ABE and Geo Encryption, In CP-ABE a message is encrypted under an access structure *A* over the set of possible attributes set and users secret key S_k is associated with an attribute sets. A secret key S_k can decrypt the message encrypted under the access structure if attribute sets satisfy access structure associated with the ciphertext. Our scheme consist of four entities, an Attribute Authority, Data Owner, Users, Cloud Service Provider, and CP-ABE uses four algorithms as defined in the [2].

Setup(*K*): This function is run by the Attribute Authority. It takes a security parameter *K* as input and outputs the public key *PK* and a master key *MK*.

Keygen(*MK, S*): This function is also run by the Attribute Authority. It takes master key MK and a set of attributes S as inputs. The algorithm outputs a secret key S_k associated with S.

E_{cpabe} (*PK, K_c, A*): This function is run by the data owner to encrypt the data, this algorithm takes public key PK , a message K_c, and an access policy *A* as inputs and outputs ciphertext $C_{y2,}$ the users who have the secret key associated with attributes that satisfy the access policy *A* will be able to decrypt the message.

D_{cpabe} (*PK, C_{y2}, S_k*): This function is run by the users to decrypt the data. It takes ciphertext C_{y2}, Public Key *PK*, a secret key S_k associated with the particular user attribute sets as input, and outputs a message K_c.

To calculate Location Lock Value, we will use one-way hash function which takes, latitude and longitude of the location as inputs and converts to a fixed value known as the location lock value.

The proposed scheme uses the following assumption and notations in this paper.

Table 2. Notation Used In this Paper

Notation	**Explanations**
K_{sec}	Secret key based on the Symmetric key Cryptography used for Encryption and Decryption
M	MAC function, use secret key K_{sec} to compute MAC.
D	Data block or Message transferred
E_{sem}	Symmetric Encryption Function
D_{sem}	Symmetric Decryption Function
E_{cpabe}	*CPABE* Encryption function
D_{cpabe}	*CPABE* Decryption function
C_{y1}	*D* || *MAC* encrypted with K_{sec}
L	Location Lock Value, computed using Hash Function, Longitude and Latitude as inputs obtained from GPS Receiver
K_c	$XOR_{ing,}$ K_{sec} and *L*
C_{y2}	K_c encrypted under Access Structure *A*.
C_y	Concatenated value of C_{y1} and C_{y2}
A	Access Structure associated with the Ciphertext, received from Attribute Authority
PK	Public key used in *CPABE*, used to encrypt data under *CPABE* with *A*.
MK	Master key used in *CPBE*, used to create S_k using user attribute set
S_k	User secret key based on his Attribute Set.

5.1.1 Protocol for Encryption at the Data Owner Location

Figure 4 shows the basic protocol for the encryption.

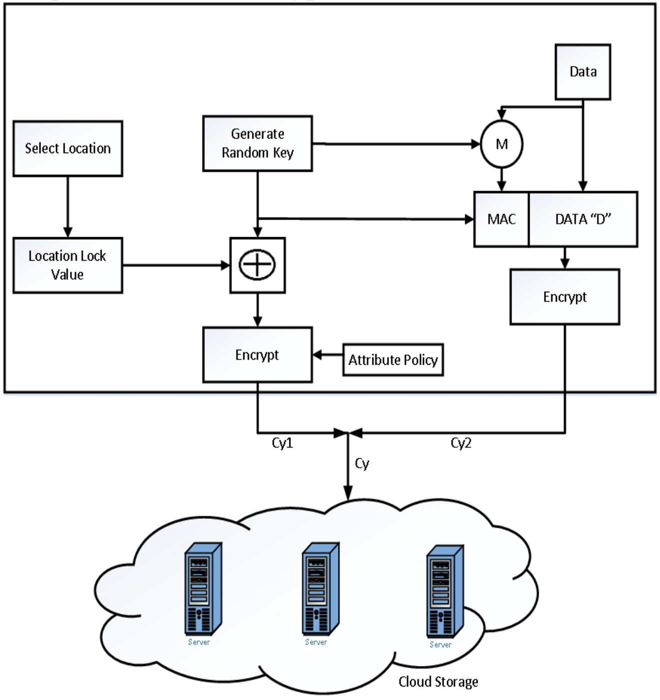

Figure 4: Protocol for Encryption

Encryption at Data Owner location will be carried out in the following ways

1. A Ksec is generated.
2. A MAC is calculated using MAC function *"M"* on the Data *"D"* using K_{sec}.

$$MAC = M(K_{\sec}, D)$$

3. The Data "D" and MAC will be encrypted with the key K_{sec} to produce C_{y1}.

$$C_{y1} = E_{sem}(K_{\sec}, D \,||\, MAC)$$

4. The Key K_{sec} is XOR_{ed} with the location lock value, producing combined key K_c.

$$K_c = K_{\sec} \oplus L$$

5. Key K_c is encrypted under the attribute policy to to produce C_{y2}.

$$C_{y2} = E_{cpabe}(PK, K_c, A)$$

6. C_{y1} and C_{y2} is combined C_{y1}|| C_{y2} to form C_y.

$$C_y = C_{y1} \,||\, C_{y2}$$

7. Then C_y is stored on the cloud server.

5.1.2 Protocol for Decryption at the User Location

Figure 5 shows the basic protocol for the decryption.

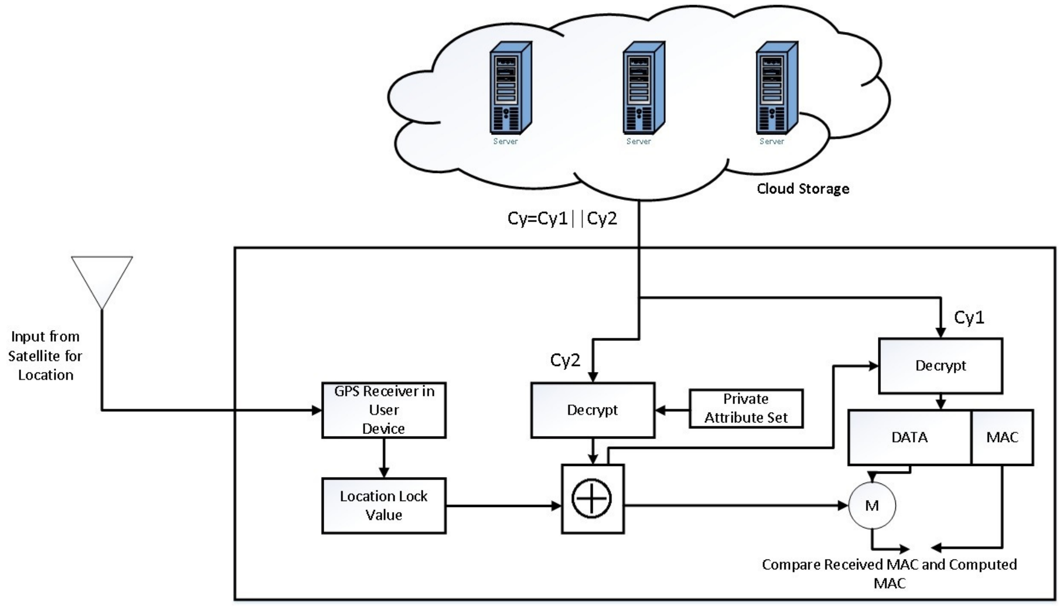

Figure 5: Protocol for Decryption

Decryption at User location will be carried out in the following ways

1. At the user side C_y will be downloaded by the user.
2. After downloading the C_{y2} will be recovered and decrypted under the private attribute set to recover key Kc .

$$K_c = D_{cpabe}(PK, C_{Y2}, S_K)$$

3. Lock values is calculated after obtaining the location value L from the GPS receiver.
4. Ksec is obtained by $XOR_{ing,}$ K_c and location lock value L.

$$K_{\sec} = K_c \oplus L$$

5. Data “D” and MAC will be obtained after decryption of Cy1 under the key Ksec.

$$D \,\|\, MAC = D_{sem}(K_{\sec}, C_{Y1})$$

6. Apply MAC function “M” using Ksec to obtain MAC of received Data.

$$MAC_1 = M(K_{\sec}, D)$$

7. Compare this MAC with the MAC$_1$ received.

8. If there is no change found means Integrity of data is preserved and it is not modified intentionally or accidentally.

6. SECURITY DISCUSSIONS

We can divide attack on cloud computing in two groups, internal attack and external attack. Internal attacks are a serious concern to the security of data in cloud computing, the internal attack is carried out by the malicious employee of a cloud service provider accessing sensitive customer data. They may compromise the sensitive information for the monetary benefits. The external attack is carried out by the malicious user outside of the cloud service provider. They can use the internet to launch the various type of active or passive attack. Port scanning, IP Spoofing, DNS poisoning, phishing are performs to gain access to cloud resources. If insider or outsider malicious user succeeded to perform attacks on the cloud resources, this may lead to incur huge amount of loss to the business in terms of money/reliability to the service provider.

The proposed schemes have been primarily designed to secure access control to counter the various internal and external attacks. This scheme also protects the confidentiality, integrity and can be used to ensure Availability of the data.

6.1. Access control

In this protocol fine-grained data access control is achieved, it uses CP- ABE and Geo-encryption for this, the data *D* is first encrypted with symmetric key K_{sec} and *XOR* value of Location lock *L* and Symmetric key is encrypted with the CP-ABE scheme.

$$K_c = K_{\sec} \oplus L$$

$$C_{y2} = E_{cpabe}(PK, K_c, A)$$

In order to decrypt the data *D* user has to first retrieve *Kc* using CP-ABE Decryption.

$$K_c = D_{cpabe}(PK, C_{Y2}, SK)$$

After retrieving K_C, this value and location-lock value which is obtained using Anti Spoof GPS is used to recover Symmetric key K_{sec}.

$$K_{\sec} = K_c \oplus L$$

This K_{sec} will be used to retrieve data along with the MAC value,

Using this scheme a fine-grained access control is achieved, decryption of the data is not only required proper attribute set but also needs to be present at the specified location, hence adding another layer of security, which is the presence of the user at the specified location.

It is safe from both the internal attack as well as the external attack, to be internal attack successful, the adversary required both Private key associated with the attribute set which should comply access structure and Location Lock value which can be obtained only using Anti Spoof GPS at the specified location. To be external attack successful, the adversary required to be present at the location which is specified during the encryption process and the having Private Key associated with the attribute set which should satisfy access structure. If the user which poses attribute got kidnapped by some criminals, they can’t forcefully get any information from the user, as to decrypt the data, user needs to be present only at the location which is specified during the encryption process.

6.2 Confidentiality of the data

In this protocol, the confidentiality of the data is ensured as the data is encrypted using Symmetric key, and this symmetric key and the XOR value of Location is encrypted using CP-ABE scheme prior to uploading on the cloud server. So it is safe from eavesdropping during transmission as well as at the rest (storage). To decrypt the data user needs both the Private key associated with the attribute set and location lock value.

6.3 The integrity of the data

The integrity of the data is also ensured from accidental or intended modification from Internal attackers as well as the internal attack as the MAC is stored along with the data in the encrypted form.

$$MAC = M(K_{\sec}, D)$$
$$C_{y1} = E_{sem}(K_{\sec}, D \,||\, MAC)$$

After downloading data from the server user can calculate MAC value and match with the received MAC value if both are the same this means that data is not modified.

6.4 Availability of the Data

As the MAC value is stored on the data owner location, user can challenge randomly any data block to the cloud server and ask him to send the data block and associated MAC value, the user will calculate received data block MAC value and if it is matched with the received MAC value this means the data block is not modified and it is available on the server. MAC Value can't be changed as it is stored in encrypted form.

7. CONCLUSIONS

Due to many advantage more and more organization shifting towards cloud computing platform. But there are also many challenges are associated with it. Security is a one of the major challenge in the adoption of cloud computing, in this paper we discussed various security challenges to the stored data in the cloud computing, also we have reviewed cryptography, some cryptographic scheme. This protocol purposed a method of data access control using the Location Based Cryptography-Geo Encryption [12], Attribute-Based Encryption Scheme-CP ABE [2] and the symmetric key cryptography [14]. This protocol ensures that data can be accessed only at the location which is specified by the data owner, so Location based Encryption adds another layer of security beyond the security which is provided using Symmetric Key cryptography and CP-ABE.

Conflict of Interest: The authors declare that they have no conflict of interest.

REFERENCES

[1] Sadiku M.,Musa S., Momoh O., "Cloud computing: opportunities and challenges," IEEE Potentials ,pp. 34–36,2014.

[2] Juels A., Burton J., Kaliski S., "Pors: proofs of retrievability for large files," in: Proc. of ACM CCS, Alexandria, VA, October 2007.

[3] Ateniese G. at el. "Provable data possession at untrusted stores," Proceedings of the 14th ACM conference on Computer and communications security, Alexandria, Virginia, USA, November 02-October 31, 2007.

[4] The NIST Definition of Cloud Computing: https://www.nist.gov/sites/default/files/documents/itl/cloud/cloud-def-v15.pdf. Accessed on 05 Sep 2017.

[5] Chandran N., Arulkumar S.,"Utilization of Random Key and Sobel Filter Based Edge Detection for Secure Data Transmission," IJIRCCE, Vol. 1, Issue 10, pp. 2376-2380, 2013.

[6] Dimitrios Z., Dimitrios L., "Addressing cloud computing security issues," Future Generation Computer Systems, Vol. 28, Issue 3,pp. 583–592, 2012

[7] Stallings W., Cryptography and Network Security: Principles and Practice, 6th edition, Pearson Education.

[8] Mandal P.C., "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish," Journal of Global Research in Computer Science, Volume 3, No. 8,pp. 67-70, 2012.

[9] Bethencourt J, Sahai A, Waters B., "Ciphertext-policy attribute-based Encryption," IEEE Symposium on Security and Privacy, 2007.

[10] Sahai A., Waters B., "Fuzzy identity-based encryption," In EUROCRYPT, pp. 457-473, 2005.

[11] Chandran N. at el.,"Advances in Cryptology. CRYPTO 2009 Lecture Notes in Computer Science," Volume 5677, pp 391-407, 2009.

[12] https://www.novatel.com/tech-talk/velocity/velocity-2013/understanding-the-difference-between-anti-spoofing-and-anti-jamming/ , Accessed on 20-04-2019.

[13] Hong H, Sun Z , "Achieving secure data access control and efficient key updating in mobile multimedia sensor networks". Multimedia Tools and Applications 77(4):4477–4490, 2018.

[14] Qiu S, Liu JQ, Shi YF et al . " Hidden policy ciphertext-policy attribute-based encryption with keyword search against keyword guessing attack". Volume 8880 of the series Lecture Notes in Computer Science. Inf Syst Secure 60:052105,2017.

[15] Li LF, Chen XW, Jiang H et al. " P-CP-ABE: Parallelizing Ciphertext-Policy Attribute-Based Encryption for clouds". 2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/ Distributed Computing (SNPD), 575-580, 2016

[16] Scott L., Dorothy E. Denning, "Location Based Encryption & Its Role in Digital Cinema Distribution", Proceedings of ION GPS/GNSS , pp. 288-297, 2003.

[17] Fuqaha A., Ibrahim O.," Geo-encryption protocol for mobile networks," Computer Communications, pp. 2510–2517, 2007.

[18] Firoozjaei MD., Vahidi J, "Implementing Geo-encryption in GSM Cellular Network," IEEE,pp. 299-302,2012

[19] Reddy P., Sudha KR., Sanyasi P., "A Modified Location-Dependent Image Encryption for Mobile Information System," IJEST,pp. 1060-1065,2010.

AUTHORS

Sachin Tripathi received his M.Tech & PhD degree from IIT (ISM) Dhanbad. He joined Indian School of Mines, Dhanbad on 21st November 2005 and currently he is working as Associate Professor in the Department of Computer Science and Engineering. Before that he joined, Haldia Institute of Technology, Haldia, West Bengal, in July 2005, as a Lecturer in the Department of Computer Science and Engineering. His reserch interest is focussed on Computer Networks, Internet multicasting applications, Mobile IP.

Rajesh Kumar Tiwari received his MCA from Nagpur University in 2002 and PhD in the field of Data Security form Birla Institute of Technology, Ranchi in the year 2010. Currently, he Professor and Head of Department Computer Science and Engineering at R.V.S. College of Engineering and Technology, Jamshedpur, Jharkhand, India. His research is focused on data security, network security, cloud computing and database management system.

Abu Salim received his B.Tech (CSE) from Dr. RML Avadh University, Faizabad in 2003 and M.Tech from JNTU Kakinada in 2009. Currently he is pursuing PhD from IIT (ISM) Dhanbad as Part Time Research Scholar and working as Lecturer in the Jazan University, KSA. His research is focused on data security, network security and cloud computing.