IJERMT

International Journal of Engineering Research & Management Technology

ISSN: 2348-4039

January-February-2023 Volume 10, Issue-1

Email: editor@ijermt.org www.ijermt.org

ENHANCING CLOUD SECURITY USING GEO-ENCRYPTION AND ATTRIBUTE-BASED ENCRYPTION

M. Mohamed Ashik,

Research Scholar, School of Technology and Computer Science,

Glocal University Saharanpur (U. P.)

Dr. Rajeev Yadav,

Research Supervisor School of Technology and Computer Science,

Glocal University Saharanpur

ABSTRACT

The utility-based computing model of cloud computing has many benefits for the businesses that utilise it, but mainstream adoption is being slowed by worries about data security. There are security challenges in the fields of infrastructure security, network security, and data security. One way to guarantee the security of data saved is through the use of cryptography. Data can only be accessed from the locations that have been designated if location information is included in the method used for encrypting and decrypting the data. By doing this, we can link access to the data with the location. In this study, we present an approach for implementing symmetric cryptography, location-based cryptography, and ciphertext policy - attribute-based encryption (CP-ABE)-based safe access control to outsourced data. The data is encrypted with a symmetric key prior to uploading it to the server, and the secret key and location lock value are encrypted with the CP-ABE technique. The user will also receive the symmetric secret key that has been XORed with the Location Lock value in addition to the encrypted data. The user will be able to obtain the first XORed value of the Symmetric secret key and the Location Lock value using his attributes-based secret key. Anti-spoofing software can be used to extract a value for the GPS location lock, and this value can then be used to recover the symmetric secret key. To ensure the availability and integrity of the data, we choose to use the Message Authentication Code (MAC). This protocol can be used in a bank, a government agency, the military, or any other company with offices or work locations at a specific location so that data access is restricted to that area. It may also be applied to any other industry with a fixed location of employment.

Keywords- fine-grained access control, Cryptography, Geo Encryption, Security issues,CP- ABE, Cloud Computing, Attribute Based Encryption.

INTRODUCTION

Cloud computing has expanded rapidly since its introduction, both in the business sphere and among academic institutions [1]. It has several benefits, including decreased maintenance expenses, electricity cost savings, and technological support for data storage. These benefits encourage companies to shift their operations to the cloud. Cloud storage is one of the most promising services employed by these businesses. The cloud provides a lot of benefits, but it also has a lot of problems. Data security is especially crucial when it comes to outsourcing.

One way to guarantee the security of one's data while it is stored in the cloud is by using cryptographic techniques. There are numerous cryptographic techniques that can be utilised to guarantee the availability, integrity, secrecy, and access control of one's outsourced data. Encrypting the data can be used to safeguard its confidentiality before outsourcing. Data encryption, however, is fraught with challenges such as key distribution to the user, user revocation, data scalability, and the ability to conduct searches on the data. In their various works, a number of researchers have tried to address these issues. a range of technologies focused mostly on digital signatures with the Message Authentication Code (MAC). Digital signatures can be used to ensure authenticity and non-repudiation in addition to data integrity, in contrast to MAC, which just ensures the data's integrity. Researchers have proposed numerous techniques to guarantee availability. These methods are either private verifiable or public verifiable and are based on proofs of retrievability (PoRs) [2] and proven data possession (PDP) [3]. While PDP simply checks the availability of files, which means it only identifies corruption and does not utilise an error correcting code, PoRs can repair minute errors using an error correcting code and can spot-check large corruptions. Spot testing with PoRs can also find significant corruptions. It is possible to use the encryption technique known as Cypher Policy-Attribute to provide a secure access control on data that has been outsourced. This method grants users access to the data only if they possess a specific attribute and are compliant with the access structure that is linked to the data. We have connected the data with the geographic location, which enhances this approach. This means that for the system to function properly, not only must the user's characteristics be met, but also the user's physical presence in the designated locations. To achieve our objectives of protecting the data's secrecy, integrity, and access control, we planned to use symmetric key cryptography, Ciphertext-Attribute Based Encryption, Geo Encryption, and MAC.

The remaining sections of the essay are as follows: We introduce cloud computing in Section 2 along with its capabilities, service delivery, deployment models, and related topics.And the problems related to the security of cloud computing. We introduced cryptography, discussed symmetric and asymmetric cryptography, ciphertext policy attribute-based encryption, and geo-encryption in the third section. Section 4 of the document discusses the associated works. We talked about the anticipated work in part 5; however, the security discussion and the conclusion were covered in sections 6 and 7, respectively.

1. PRELIMINARY

1.1 CLOUD COMPUTING

Cloud computing is a form of utility computing. Which is composed up of a total of five key features, as well as four deployment and three service model.

Computing in the cloud can be defined with these five characteristics

- Ubiquitous Network Access- The ability to uniformly access resources stored in the cloud using a variety of devices such as personal computers, laptops, personal digitalassistants, and so on.
- Resource Pooling- Users are able to pool resources with one another, and they have the ability to acquire or release resources based on their own needs.
- On Demand Self-Service- This feature enables users of cloud computing to accessand control computer resources automatically according to their requirements.
- Rapid Elasticity- enables resources to be swiftly and autonomously obtained andreleased in response to changing demand.
- Measured Service- This kind of service allows for the user's use of cloud-basedresources to be tracked and then billed to the user.

The delivery of services in cloud computing is accomplished via the use of three differentservice models.

- Platform as a Service (PaaS): Platform as a Service (PaaS), sometimes known as "platform as a service," is a paradigm that gives developers access to a frameworkthat can be used to build or customize apps. The process of creating, testing, and deploying software is accelerated, simplified, and made more efficient as a result.
- Software as a Service (SaaS): Software as a Service (SaaS) is a model of computing in which a user may use the software hosted by a third party without installing themon his system. The majority of the software can be accessed using a web browser. SaaS is becoming more popular.

- Infrastructure as a Service (IaaS): With Infrastructure as a Service, the cloud service provider outsources the equipment such as storage, hardware, servers, and networking components. IaaS is also known as "cloud computing infrastructure." The service provider is responsible for managing these components, and thecustomer is paid based on the resources that are actually used by the service provider.

Four different deployment models are used by cloud computing.

- Private Cloud: A private cloud is one that is owned by a single company or organization and whose resources are managed by the Information Technology (IT) Departments of that company or organization.
- Community cloud: This form of computing allows organizations that belong to the same community to share resources with one another. For instance, two governmentorganizations that are working towards the same objective might share resources withone another using this model.
- Public Cloud: This kind of cloud computing makes cloud services accessible to the broader public over the internet. Gmail, DropBox, Office 360, and other similar services are some examples.
- Hybrid Cloud: In this approach, organizations may host certain vital data andapplications on the private cloud and less important data on the public cloud. Becausethis model is a blend of the private and public cloud models, it is known as the hybridcloud.

1.2 CRYPTOGRAPHY

The data may be protected by cryptography while it is in transit, while it is at rest, and while it is being computed. The plaintext (the text that can be read) is changed into the ciphertext (the text that cannot be read) by the use of a key and an algorithm in the process of cryptography, which is a technology.

It is possible to divide it into two distinct groups.

1. Cryptography Based on Symmetric Keys
2. Cryptography with an Asymmetric Key

In the case of symmetric key cryptography, the same key is used for both the encrypting anddecrypting processes, but in the case of asymmetric key cryptography, separate keys are employed for each process.

2.2.1. Symmetric encryption

A symmetric encryption [4] technique contains a total of five elements (Figure 1).

- Plaintext: This is the Message that Needs to be Protected.
- Ciphertext: A scrambled message is produced by an encryption algorithm when a secret key and plain text are fed into it as input. This message is referred to as ciphertext. Different keys create different ciphertext.
- The secret key: Secret key is input into the encryption algorithm. Depending on the key, the algorithm will create a uniquely ciphered text with each iteration. There is no connection whatsoever between the key and the encryption technique or the plaintext.
- Encryption algorithm: This method takes the plaintext, also known as the Original Message, and transforms it into a stream of random data by employing substitution and transformation.
- Decryption algorithm: Decryption algorithm requires the inputs of the Secret key and the ciphertext, and it produces plain text as the final result.

2.2.2. Asymmetric key encryption

In asymmetric encryption, the processes of encrypting and decrypting data are carried out with the assistance of two distinct keys: a public key and a private key. Public-key encryptionis another name for this method. In this scenario, the public key of the encryption method isused to convert the plaintext into the ciphertext, and the private key is used to retrieve the plaintext from the ciphertext. While the private key is guarded as a closely guarded secret, the public key is made publicly accessible via the use of certificate authorities.

The symmetric key encryption approach is more effective than the asymmetric keycryptography, but it is difficult to distribute the key. On the other hand, the asymmetric key cryptography technique uses a distinct key for encryption and decryption, so there is no needto share the key [5]. However, this method is much slower.

Prior to delivery, data in cloud computing may be encrypted using symmetric key encryption,and the key can be encrypted using asymmetric key encryption. Alternatively, the data can be encrypted using both types of encryptions.

2.2.3 Ciphertext Policy attribute-based encryption

ABE, also known as attribute-based encryption, may be used for the purpose of providingfine-grained control over data access [9]. Within this kind of encryption, a set of receivers can be designated by means of a descriptive property. There are two different approaches to put ABE into practise. KP-ABE, or Key Policy-Attribute Based Encryption, and CP-ABE, or Ciphertext Policy-Attribute Based Encryption, are both types of attribute-based encryption. In this method, the attributes are associated with the ciphertext, while in the CP-ABE that was established in [6], the access structure was associated with the ciphertext. TheKP-ABE was initially presented in [7] by Sahai at el. The attribute, together with the plain text, was encrypted in KP-ABE in order to create ciphertext, and the access structure was associated with the Key, which was then given to the user. In CP-ABE, the access structure was encrypted along with the plain text in order to produce ciphertext. The attribute was associated with the key in order to ensure that different users, each with their own unique setof attributes associated with the key, would be able to decrypt different sets of data dependingon the access structure that was associated with the data (Ciphertext). This would result in fine-grained access control being applied to the data.

Figure 2 shows an example of CP-ABE encryption. CP-ABE employs a tree-based structure with a predetermined set of attributes. In order to decrypt the data, the attribute set first needsto meet the access structure that is linked with the data. CP-ABE makes use of the AND, OR,and k of n operators to specify which attribute set (User) is able to decrypt the data. for instance, if the data is encrypted using the following attribute set (Director, Teacher, Full time) and the access tree shown in Figure 1 is associated with the data, data sets, then the various user groups can be identified as follows: User1: Director, User2: Teacher and User 3: Teacher, Full Time.

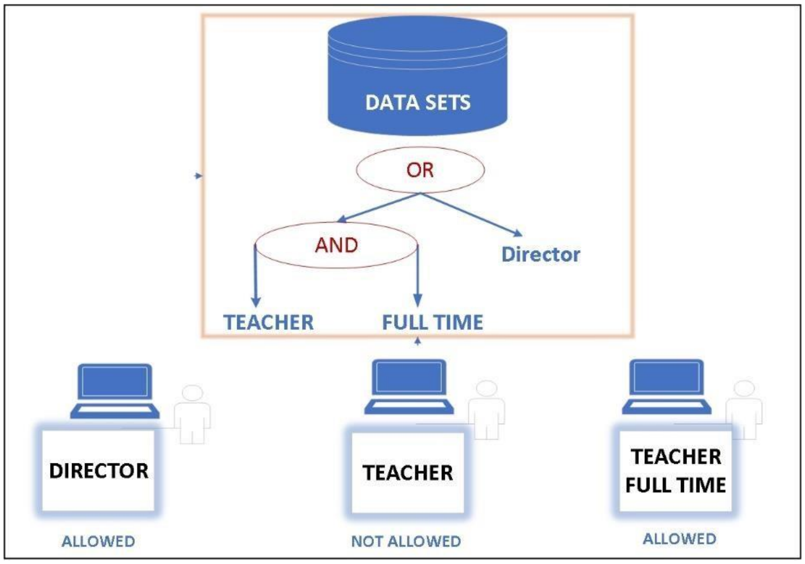

Figure 1: CP-ABE

In order for a user to decrypt the data, he has to possess attributes: director or Teacher, Fulltime.

2.2.4 Geo- Encryption

Identity is a key element in identity protection with encryption. It might contain information like a person's name, social security number, Aadhaar number, voter ID number, geometry, iris, retina, finger veins, and so forth. We are able to have a distinct kind of identity in addition to these conventional forms of identification, which is the actual physical presence of a person at a particular location. For instance, in the bank, we can confirm account managers and bank managers based purely on their location without asking them for their ID card. This identification method, in which an entity's identity is inferred from the fact that it exists at a specific location, is one that might be applied to the cryptography system we are developing [8]. Without the coordinates, which can be obtained by utilising an anti-spoof GPS device, the data cannot be decrypted. A selective availability spoofing module (SAASM) is present in an anti-spoof GPS receiver, and the GPS signal contains encrypted binary codes Y. Data for a particular location that may be located in both space and time can be encrypted. A SAAMS receiver can only follow Y codes after receiving the correct decryption key [9]. Geo-encryption, commonly referred to as location-based encryption, is a technique that can be used to ensure that data cannot be decoded outside of a specific facility. This might be the case, for instance, at a specific theatre, bank, government agency's main office, a military base, or a person's place of employment or residence.

3. Security Challenges

In cloud computing, the user does not have control over the software, data, or infrastructure;rather, it is under the control of the cloud service provider. This distinctive model of computing raises a number of concerns with regard to the data's safety. The safety of the datacould be jeopardized by a dishonest employee of the service provider or by another client that is using the same infrastructure. The confidentiality, integrity, and availability of the databeing stored are all components of data security. Because of the characteristics of cloud computing, additional problems such as data lock-in and data location are also present.

- Data Privacy: Privacy refers to a person's or group's capacity to conceal themselves or information about themselves, and to reveal themselves only in a manner that is chosen by the individual or group [10]. The confidentiality of the data stored in the cloud should under no circumstances be jeopardized.

- Data Integrity: Integrity in data, software, and hardware indicates that assets may only be manipulated by authorized persons or in authorized methods. Integrity refers to the fact that data, software, and hardware can only be modified in certain ways. The term "data integrity" refers to the process of defending stored information against unauthorized changes, deletions, or fabrications [11]. The data in the cloud must maintain their integrityat all times.
- Availability of Data: Availability is the property of a system that allows it to be accessed and used on demand by an authorized entity [11]. Availability refers to the fact that data isavailable and useful. Cloud computing raises a number of concerns, one of which is the availability of data.
- Data Lock In: Each CSP provider may utilize a unique framework, and if a user wants to switch CSPs for one reason or another, it will be impossible for him to do so.
- The Location of Data: The cloud computing model takes the physical location of data into consideration. Since different nations' laws regarding data privacy may be in conflict withone another, the fact that the CSP's datacenters are dispersed throughout many geographicregions may raise some privacy concerns. Because of the potentially sensitive nature of particular data, it is imperative that information does not leave the nation. In the event of an inquiry, certain data could be requested, and getting access to that data can be difficult.

4. Related Works

Many methods have been developed by a variety of researchers in order to provide secureaccess control in the cloud [12, 13, 14]. The Geo-Encryption method was first developed byLogan Scott and Dr. Dorothy Denning [15] in order to provide security for the distribution of digital films. Within the scope of this work, they propose a method for the safe distributionof digital films. They believe that it will be possible to develop a key called "Geo-Lock" by making use of geographical position, and that this key will be used in the process of encrypting digital film. This movie may be sent to any site by using a network, but it can only be decrypted at the particular place that was chosen before it was encrypted. In geo- encryption, two separate packets of data are sent to the receiving side: one is data encryptedwith the symmetric key cryptography, and the other is Geo-Lock value obtained using the geo lock function where longitude, latitude, and time constitute input. This value is then XORed with the symmetric key and encrypted using the asymmetric key cryptography. At the decryption side, the Geo Lock values are calculated after getting position information using the Anti Spoof GPS. These values are then XORed with the decrypted value of receivedGeo-Lock, XORed with symmetric key, and ultimately used to recover symmetric key, whichis then used to decode the data.

The concept of location-based encryption is employed even further by several researchers to improve security.

Geo-Encryption is used by Ala Al-Fuqaha and Omar Al-Ibrahim [16] to guarantee that messages sent between mobile nodes are securely transmitted. This is accomplished by onlyallowing the message to be decrypted at the time and place that have been predetermined.

A novel CP-ABE approach that allows disguised access policy was introduced by Pallavi

[17] et al. They employed inner product encryption in conjunction with attribute concealingin order to ensure unlink ability and increase the privacy of patient data.

For encrypting data between mobile subscribers and base transceiver stations (BTS), Mahdi DF and Javad V [18] employ the A5 encryption algorithm. The key for A5 encryptionis created by using information about the precise location of mobile subscribers in conjunction with a random number. Data can only be decrypted at a place of which the GSMnetwork is aware in order for it to be decrypted there.

Again, using a hidden access policy, Zhong [19] et al. presented a decentralized multi- authority CP-ABE approach. This system has relatively low costs associated with both communication and computing.

A location-dependent image encryption for mobile information systems was suggested byPrasad Reddy, P.V.G.D, K. R. Sudha, and P. Sanyasi [20]. In this particular research study, the mobile clients provide an information server an intended latitude and longitude coordinate, and the information server also obtains an LDEA key for data encryption. Whenthe coordinate that was obtained from the GPS receiver coincides with the destination coordinate, the client is then able to decode the ciphertext. For the purpose of increasing the level of protection offered, they use the usage of a random key, often known as an R-key.

5. Purposed Model

We offer a notion of employing geo-encryption for cloud computing, in which the data can only beviewed at the designated place. This keeps the data secure while yet allowing it to be accessible remotely. Data owner will calculate MAC using Secret Key and encrypt both data and MAC using Secret Key before storing on the cloud server. Since public key cryptography requires a significant amount of computation in comparison to symmetric key cryptography, we will purpose to use symmetric key cryptography for encryption. One of the most widely used symmetric key algorithms is RSA, which can be used for the encryption of data and MAC. According to our purpose model, theattribute authority is in charge of designing the access structure that is connected with the data basedon the access policy. Data and MAC will be encrypted using a session key. The session key will thenbe XORed with the location lock value, which can be computed on the basis of intended user positions. Finally, the session key will be encrypted with the attribute policy using the CP-ABE scheme. After encryption, the data and MAC will be sent to cloud storage. At the decryption site, theuser will use the secret key associated with his attribute keys in order to decrypt and recover the XOR value of the If the location received by Anti Spoof GPS is right, then only the user will get the propersecret key, which can eventually be used to decrypt the data and MAC. However, if the location lockvalue is erroneous, then the secret key obtained will also be incorrect, and it will not be possible to use it for decryption. After getting data and MAC, the end user will next evaluate the MAC of the data that was received by using a secret key. If the calculated MAC value is identical as the MAC value that was obtained, then the user is certain that he got the proper data.

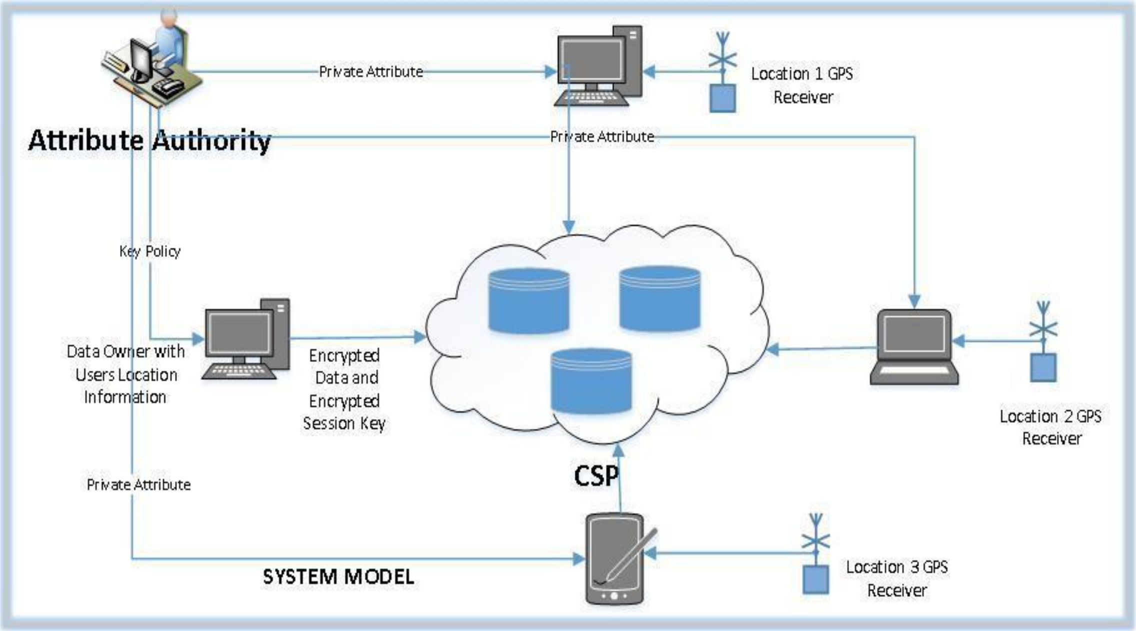

Figure: 2 Purposed Model

5.1 Procedure for Encryption and Decryption

CP-ABE and Geo Encryption form the basis of our scheme. In CP-ABE, a message is encrypted using an access structure *A* over the set of potential attributes set, and a users secretkey *Sk* is linked with an attribute set. If the attribute sets fulfil the access structure associatedwith the ciphertext, a secret key *Sk* will be able to decode the message that was encrypted using the access structure. The Attribute Authority, Data Owner, Users, and Cloud Service Provider make up the four entities that make up our scheme. The CP-ABE employs the fouralgorithms that are outlined in [2].

$F_{setup}(K)$: The Attribute Authority is in charge of executing this function. As input, it accepts a securityparameter known as K, and as output, it provides both a public key K_{pk} and a master key $K_{mk.}$

$F_{keygen}(K_{mk}, S)$: The Attribute Authority is also in charge of running this function. As inputs, it requiresa master key, denoted by K_{mk}, and a collection of attributes, denoted by S. An encrypted key, S_k thatis associated to S is produced by the algorithm.

$F_{ecpabe}(K_{pk}, K_m, A)$: The data owner uses this method to encrypt the data; it accepts a public key K_{pk}, amessage K_m,, and an access policy A as inputs and produces ciphertext C_{e2}. Only users who possess the secret key linked to attributes that meet the requirements of the access policy A will be capable todecrypt the message.

$F_{dcpabe}(M_{pk},C_{e2},S_k)$: Users are the ones that decrypt the data by running this function on theircomputers. It accepts as input ciphertext C_{e2}, Public Key K_{pk}, and a secret key S_k connected with thespecific user attribute settings, and it produces a message K_m as output.

We are going to use a one-way hash function to generate the location Lock value. This function takesthe latitude and longitude of the place as its inputs and converts them into a single number that is referred to as the location lock value..

Notation used in the protocol are listed below
K_{sec}: Secret key F_{mac}: MAC
functionD_s: Data set
F_{esem}: Symmetric Encryption Function F_{dsem}:
Symmetric Decryption Function F_{ecpabe}: CPABE
Encryption function F_{dcpabe}: CPABE Decryption
function V_{ll}: Location Lock Value
K_c: XORing, K_{sec} and V_{ll}
C_{e2}: K_m encrypted under Access Structure A. C_e:
Concatenated value of C_{e1} and C_{e2}
A: Access Structure associated with the CiphertextK_{pk}: Public key
used in CPABE
K_{mk}: Master key used in CPBE
S_k: User secret associated with Attribute Set.V_{mac}: MAC
Value.

5.1.1 Protocol for Encryption at the Data Owner Location

The Figure 3 shows the basic protocol for the encryption.

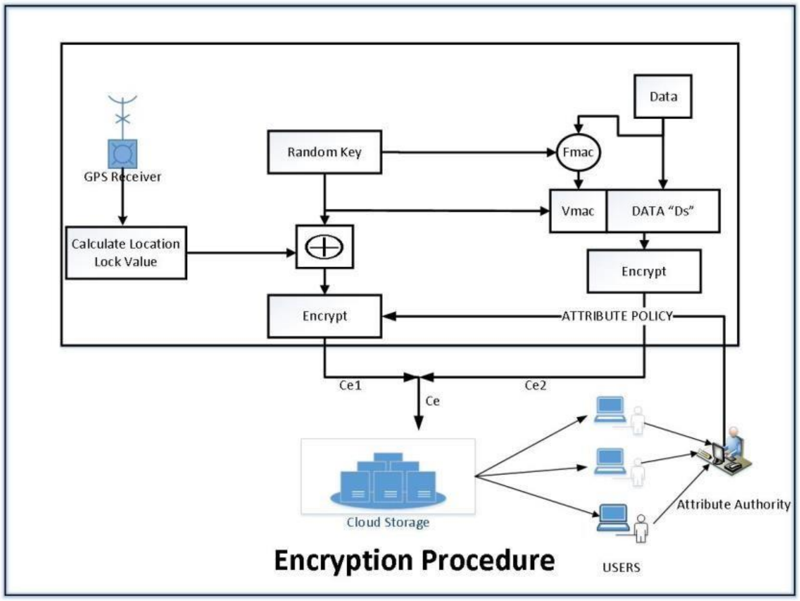

Figure 3: Protocol for Encryption

The following procedures will be used to carry out encryption at the premises of the DataOwner:

- Secret Key *Ksec* is generated.
- Calculate V_{mac} using F_{mac} on the Data *"D_s"* using K_{sec}.
  $V_{mac} = F_{mac}(K_{sec}, D_s)$
- Calculate C_{e1}. on *"D_s"* using $\mathrm{V}_{\mathrm{mac}}$ and K_{sec}.
  $C_{e1} = F_{esem}\ (K_{sec}, D_s \parallel V_{mac})$
- The Key K_{sec} is XOR_{ed} with the $\mathrm{V}_{\mathrm{llv}}$, producing combined key K_c.
  $K_c = K_{sec} \oplus V_{ll}$
- Key K_c is encrypted under the attribute policy to produce C_{e2}.
  $C_{e2} = F_{ecpbe}\ (K_{pk,}\ \ , A)$
- C_{e1} and C_{e2} is combined to form *Ce*.
  $C_e = C_{e1} || C_{e2}$
- Then C_e is stored on the cloud server.

5.1.2 Protocol for Decryption at the User Location

Figure 4 illustrates the fundamental procedure that must be followed in order to decode thedata.

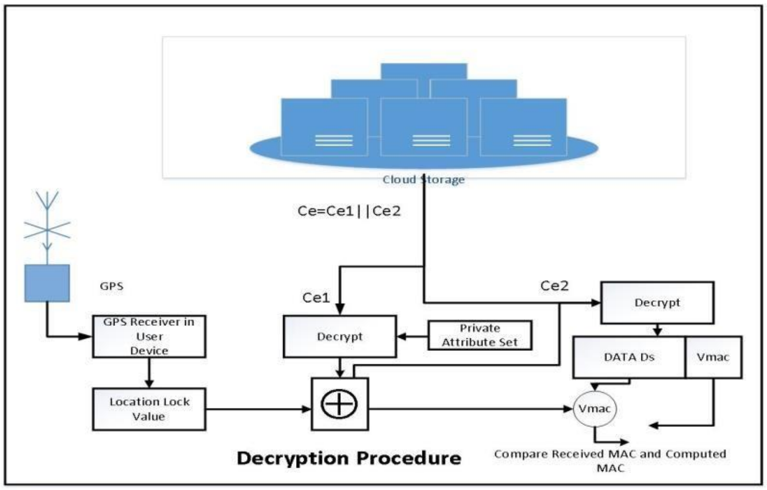

Figure 4: Protocol for Decryption

- The following procedures will be used to carry out decryption at the premises of theData Owner:

- At the user side C_e will be downloaded by the user.
- Now recover C_{e2} and decrypted under the private attribute set to recover key K_c.
  - $K_c = F_{Dcpabe}(K_{pk}, C_{e2}, S_k)$
- Location Lock values V_{ll} is calculated after obtaining the location value from the GPSreceiver.
- K_{sec} is obtained by $XOR_{ing,}$ K_c and location lock value V_{ll}.
  - $K_{sec} = K_c \oplus V_{ll}$
- Data "D_s" and V_{mac} will be obtained after decryption of C_{e1} under the key K_{sec}.
- $D_s \parallel V_{mac} = F_{dsem}(K_{sec}, C_{e1})$
- Apply MAC function F_{mac} using Ksec to obtain MAC of received Data.
  - $V_{2mac} = F_{mac}(K_{sec}, D_s)$
- Compare this V_{mac} with the V_{2mac}.
- If there is no change found means Integrity of data is preserved and it is not modifiedintentionally or accidentally.

6 Security Discussions

There are two kind of attacks that may be made against cloud computing: internal attacks and externalattacks. Internal assaults are a major cause for worry when it comes to the safety of data stored in cloud computing. An employee of a cloud service provider who is acting maliciously may carry out an internal attack by gaining access to confidential client information. They could risk compromisingthe sensitive information in order to get financial gains. An external attack is one that originates fromoutside of the cloud service provider and is carried out by a wicked user. They are able to use the internet to launch a variety of active and passive forms of assault. Phishing, port scanning, IP spoofing, and DNS poisoning are some of the attack methods that may be used to obtain access to cloud services. If a wicked user, whether it be an insider or an outsider, was successful in performingassaults on the cloud resources, this might lead to the company incurring a significant amount of damage, either in terms of money or in terms of the trustworthiness of the service provider.

The recommended systems have largely been developed with the goal of securing access control in order to defend against the many different kinds of internal and external threats. This method not onlysafeguards the data's confidentiality and integrity, but it also has the capability of ensuring the data'savailability.

6.1 Ensuring the data's confidentiality

The data is encrypted using a symmetric key, and this symmetric key together with the XOR value ofthe location are encrypted with the CP-ABE technique before being uploaded to the cloud server. This protocol guarantees that the data will remain confidential since it encrypts the data with a symmetric key. Therefore, it is secure from eavesdropping both while it is being sent and when it is being stored. The user requires both the Private key that is associated with the attribute set as well asthe location lock value in order to decrypt the data.

6.2 Access control

This protocol is able to establish fine-grained control over the access granted to data because it makesuse of CP-ABE and Geo-encryption. Specifically, the data D is first encrypted with the symmetric key Ksec, and then CP-ABE is used to encrypt XOR of Location lock Vll and Symmetric key.

$$K_c = K_{sec} \oplus V_{ll}$$

$$C_{e2} = F_{ecpabe}\ (K_{pk}, K_c, A)$$

To begin the process of decrypting the data D_s, the user must first obtain K_c using theCP-ABE Decryption algorithm.

$$K_c = F_{dcpa}(K_{pk}, C_{e2}, K_{sec})$$

After recovering K_C, the symmetric key K_{sec} may be reconstructed with the help of this valueas well as the location-lock value that was acquired by using anti-spoof GPS.

$K_{sec} = K_c \oplus V_{ll}$

MAC and data value will be retrieved using K_{sec}.

By using this approach, a fine-grained access control can be accomplished. For the data to be decrypted, the user not only has to have the appropriate attribute set, but they also need to be presentat the place that has been provided. This adds an additional layer of security in the form of the presence of the user at the location that has been specified.

It is safe from both internal and external attacks; for an internal attack to be successful, the adversarymust have both the Private key associated with the attribute set that should comply access structure and the Location Lock value, which can be obtained only by using Anti Spoof GPS at a specified location. This makes it safe from both types of attacks. In order for an external assault to be effective,the adversary must both be present at the location that is indicated during the encryption process andpossess the Private Key that is connected with the attribute set that must meet the access structure. To be able to decode the data, the user has to be present only at the place that was indicated during the encryption process. If the user who possesses the attribute were to be abducted by some criminals,the criminals would be unable to coerce the user into providing any information since the user wouldneed to be present only at the location that was stated during the encryption process.

6.3 Integrity of the data

Because the MAC is kept with the data in encrypted form, the data's integrity is protected not just against accidental or deliberate modifications by internal attackers but also from the internal attack itself because the MAC is encrypted when it is placed alongside the data.

$V_{mac} = F_{mac}(K_{sec}, D_s$

$C_{e1} = F_{sem}\ (K_{sec}, D \parallel V_{mac}$

After downloading the data from the server, the user may compute their MAC number and compare it to the one they have received; if they are the same, this indicates that the data hasnot been altered.

6.4 Availability of the Data

The user may challenge every data block to the cloud server at arbitrarily and request him tosend back the data block along with its MAC value. The user will calculate the received datablock MAC value and if it matches the received MAC value, it indicates that the data block has not been modified and is available on the server. Since MAC Value is kept in encryptedform, it cannot be changed.

7. Conclusions

Due to its many advantages, a growing number of firms are switching to the cloud computing platform. However, it also has a lot of drawbacks. Security is one of the main barriers to cloud computing adoption. We looked at a number of security concerns regarding the data held there in this article. Additionally, we discussed several encryption algorithms. This protocol utilises the Location Based Cryptography-Geo Encryption [9], Symmetric Key Cryptography [13], and Attribute Based Encryption Scheme-CP ABE [2] to control access to data. This protocol ensures that only the location that the data owner designates may be used to read the data. The security provided by symmetric key cryptography and CP- ABE is therefore enhanced by location-based encryption.

References

Sadiku M.,Musa S., Momoh O., “Cloud computing: opportunities and challenges,” IEEE Potentials ,pp.34–36,2014.

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

Ateniese G. at el. “Provable data possession at untrusted stores,” Proceedings of the 14th ACM conferenceon Computer and communications security, Alexandria, Virginia, USA, November 02-October 31, 2007.

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

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.

Bethencourt J, Sahai A, Waters B., “Ciphertext-policy attribute-based Encryption,” IEEE Symposium on Security and Privacy, 2007.

Sahai A., Waters B., “Fuzzy identity-based encryption,” In EUROCRYPT, pp. 457-473, 2005.

Chandran N. at el.,“Advances in Cryptology. CRYPTO 2009 Lecture Notes in Computer Science,” Volume 5677, pp 391-407, 2009.

https://www.novatel.com/tech-talk/velocity/velocity-2013/understanding-the-difference-between-anti-spoofing-and-anti-jamming/.

Chandran N., Arulkumar S.,“Utilization of Random Key and Sobel Filter Based Edge Detection for SecureData Transmission,” IJIRCCE, Vol. 1, Issue 10, pp. 2376-2380, 2013.

Dimitrios Z., Dimitrios L., “Addressing cloud computing security issues,” Future Generation Computer Systems, Vol. 28, Issue 3,pp. 583–592, 2012

Hong H, Sun Z , “Achieving secure data access control and efficient key updating in mobile multimediasensor networks”. Multimedia Tools and Applications 77(4):4477–4490, 2018.

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.

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

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

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

Patil, P.A.; Joshi, S. “Hidden CP-ABE to Enhance Patient Data Privacy in Smart Healthcare Systems”. Int.J. Appl. Eng. Res. 2017, 12, 3950–3960.

Firoozjaei MD., Vahidi J, “Implementing Geo-encryption in GSM Cellular Network,” IEEE,pp. 299- 302,2012

Zhong, H.; Zhu, W.; Xu, Y.; “Cui, J. Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage”. Soft Computing. 2018, 22, 243–251.

Reddy P., Sudha KR., Sanyasi P., “A Modified Location-Dependent Image Encryption for MobileInformation System,” IJEST,pp. 1060-1065,2010.