SECURING DATA IN CLOUD ENVIRONMENT USING TRUSTED THIRD PARTY

[1]D.Thiruveni, [2]K.Prabhakar, [3]E.Thangadurai

[1]PG Scholar, IT Department, Vivekanandha College of Engineering for Women (Autonomous) Tiruchengode, India

[2]Assistant Professor, IT Department, Vivekanandha College of Engineering for Women (Autonomous) Tiruchengode, India

[3]Assistant Professor, IT Department, Vivekanandha College of Engineering for Women (Autonomous), Tiruchengode, India

dthiruveni@gmail.com, k.prabhakar86@gmail.com, kapildurai@gmail.com

Abstract: Cloud computing is a computing standard which connects a group of systems in private or public networks, to offer robustly scalable infrastructure for data, application and storage. Although its growing influence increases in the field of cloud computing, concerns regarding still remain. Especially security is needed more when it includes third party as a service provider is having the chances of getting hacked whole data at a time .To overcome this issue, a secure environment was provided by the trusted third party which consists of ECC encryption. Using this encryption technique the authorized data was given only to the authorized user. The proposed architecture which performs the cryptographic operations using trusted third party and the key was stored separately in another server. Initially the cloud computing technology was outlined and finally the security and privacy problem can be solved by the trusted third party method.

Index Terms: Cloud computing, cloud service provider, sender, trusted third party

1. INTRODUCTION

With the explosive growth of cloud computing, security is the main issue which prevents the more number of users from this field. Forrester defines the term cloud computing as "A pool of abstracted, highly scalable, and managed compute infrastructure having the ability of hosting end-customer applications and billed by consumption."The issues which prevents the users to accept cloud computing are in terms of security, privacy, reliability. To achieve more security in the computing paradigm trusted third party was included which restricts the unauthorized access of users. The third party will enhance the data confidentiality in the cloud infrastructure. The data must be encrypted before storage to improve the security and confidentiality. The direct way of transferring data to the cloud that needs more level of security and trust. The third party prevents the intruders those who decrypt the encrypted data in the storage. The sender and receiver will not perform the cryptographic operations. The large data files were also transmitted using the ECC encryption technique with this third party in a secure manner. The encryption scheme used here was Elgamal which does not rely on a user's public key infrastructure (PKI) and the algorithm is uncomplicated and more capable to encrypt any size of data. The rest of paper is organized as follows Section 2 explains cloud computing models and Section 3 explains related work Sections 4 represents proposed plan and Section 5 represents Conclusion respectively.

2. CLOUD COMPUTING MODELS

Generally the models are classified into two types in cloud computing which are deployment model and service model. The cloud providers offer various services which can be divided into three categories which are SaaS, PaaS and IaaS.

2.1 Service Model

In cloud computing there are mainly three service models which are Platform as a service, Infrastructure as a service and Software as a service.

Infrastructure as a service (IaaS)

IaaS is the model which delivers the infrastructure to the clients on a demand basis. In IaaS a third party provider hosts the hardware, software, server, storage and other infrastructure components. The tasks such as software maintenance and backup can also be handled

here. Instead of purchasing and managing fully dedicated infrastructure, clients are renting a virtual serve space for providing that infrastructure. The cloud provider is responsible for the maintenance of infrastructure and provides the access to the clients through virtualized ip address. Examples of IaaS are Amazon EC2, Go Grid and Rack space Cloud.

Platform as a service(PaaS)

PaaS provides the application development platform which includes the programming languages, libraries and development tools. The Clients need not maintain the hardware resources such as storage, servers, programming tool kit but the users are having the control on the deployed applications. Examples of PaaS are Microsoft Windows Azure, Google App Engine and Amazon Web Services.

Software as a Service(SaaS)

Saas is a software distribution model in which the vendor or service provider hosts the applications and made available to the customers through internet. The main advantage of this model is multinenancy which supports multiple users to access at a time .It provides the authorization to access the software for a particular period and they can pay based on their usage. Here the clients are not responsible for the maintenance and control of the infrastructure. Examples of SaaS are Google Apps, Gmail, and Google Docs[11][12].

2.2 Deployment model

In cloud computing the deployment model characterize the type of access to the cloud which are public cloud, private cloud, community cloud and hybrid cloud.

Public Cloud

Public clouds are owned and operated by third parties; they distribute superior economies of scale to customers, as the infrastructure costs are widen among a mix of users, giving each individual client an attractive low-cost, "Pay-as-you-go" model. One of the benefit of a Public cloud is that they may be larger than an enterprises cloud, thus providing the facility to scale seamlessly, on demand.

Private cloud

Private clouds are built entirely for a single enterprise. They aim to tackle concerns on data security and suggest greater control, which is typically lacking in a public cloud.

Hybrid Cloud

Hybrid Clouds merge both public and private cloud models. With a Hybrid Cloud, service providers can exploit 3rd party Cloud Providers in a full or limited manner thus increasing the elasticity of computing [11].

3. RELATED WORK

Based on analyzing the various papers the encryption of the data is needed before storage which enhances the data security. Typically for securing the data more encryption algorithms and techniques are used. Here the trusted third party will only execute the encryption under the control of data owner.

3.1 Symmetric key Encryption

The symmetric key encryption is defined as the identical key used for encryption of data will be used again for the decryption of data .With a generator function the user encrypts the data in symmetric key encryption using secret key. The symmetric key system consists of two algorithms which are stream cipher and block cipher. The secret key is disseminated among the users those who need to access the shared data. Various symmetric key encryption algorithms are Advanced encryption standard (AES), Data Encryption standard (DES), 3DES, Blowfish and International Data Encryption Algorithm.

3.2 Role-Based Access control

Usually data owner stores the data in the cloud but the stored data was accessed by a variety of users which lead to unauthorized access. So there is a requirement of access list to limit the unauthorized user from accessing the data. Here the data objects are mapped to roles and those roles are further assigned to the authorized users. Based on the access list the requested data was given to the user those who have to access the file. The user revocation from authorized access leads to refute of access for unauthorized user.

3.3 APAC

Initially the sensed data is made obtainable only for an authorized user by enforcing APAC for strict access control. It provides sophisticated user with privacy protection .But the nonappearance of third party makes it less reasonable in practice.

3.4 Multi-keyword ranked search encryption (MRSE) privacy framework

To secure sensitive data before out sourcing and enabling encrypted cloud data search service, and to allowed multiple keyword search request by proposing MRSE scheme. It failed in checking the probity of rank order in search result by assuming that the cloud server is unreliable [3].\

3.5 DaSEC protocol

First the use of FADE protocol was done which lack in authenticating the client for file upload processes, so the DaSEC protocol was used instead which is more efficient and reliable than FADE and also used semi trusted third party by which the rise of intrusion collapsed. It also provided key management, access control, file assured deletion, but lacked in extending security for group shared data and secure data forwarding. The stored data provided from the third party to the client was also able to decrypt easily [1].

3.6 Key-policy attribute based encryption

The data owner encrypts the data and a set of attributes was used to decrypt the cipher text is known as key-policy attribute based encryption. The trusted authority sends the key for decryption and specifies the type of cipher text a user has access. The users having this essential set of attributes can only decrypt the data. This scheme is appropriate for organizations those who involve different type of access for various users.

3.7 Attribute-based encryption

A set of user attributes used to encrypt and decrypt the data is known as attribute-based encryption. The attributes which includes unique user attributes (id, mobile number) and other attributes such as user location, action attributes can be used to encrypt and decrypt the data. The data was encrypted and decrypted using the set of attributes instead of key [4].

3.8 Public key infrastructure

The technique which requires separate keys such as public key and private key for encryption and decryption is known as public key infrastructure. The data owner uses the private key secretly to decrypt the data and also for signing the document digitally. The public key was published publicly that used to confirm the digital sign and encrypt the data. For generating the cipher text various methods such as transposition, factorization is used [2].

3.9 Hierarchical Identity based encryption

The public and private key pairs are provided to the users without using CA. The unique identifiers are used as a public key. The private key generator generates the private key holds the master secret key called root PKG. Another version of identity based encryption is hierarchical identity based encryption relieves the root PKG from key generation. The root PKG is responsible for the private key generation in certain hierarchy.

4. PROPOSED SCHEME

As per analysis the various techniques being used along with all the work done the proposed architecture was proficient cost and time worthy method beneath cloud environment .It give a great idea to examine the method above and to recover the work further. For the method used for security in cloud for affix storage and access of data in cloud which is ECC seems more suitable and efficient algorithm for the further work to be proceeded. After the analysis from the literature survey, looking forward to various algorithms and environment. The plan is to provide authentication and encryption by ECC and to provide a secrete key to access the encrypted data using the same. By using ECC encryption and decryption we can either encrypt the desired data or the whole data. Data anonymization technique can provide confidentiality of data by letting only the authorized user see the data allotted to him. This is the overall work which is to be carried out.

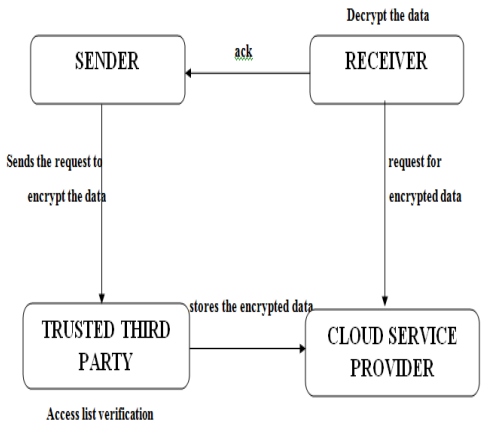

Figure 1: System Architecture

The sender and receiver will not perform the cryptographic operations. Initially the sender sends the request to the trusted third party to encrypt the data. The encrypted data was stored in the cloud storage. When the receiver requests to get the encrypted data was provided by service provider and decrypt the data to get a original content. Based on the access list verification the user will be authorized.otherise the user will be determined a unauthorized user.

5. ELLIPTIC ELOAMAL CURVE CRYPTOSYSTEM

We implement Elliptic Curve Cryptography (ECC) was projected by Koblitz [4] and Miller [2] in 1980s. ECC is a public key cryptographic scheme. It uses properties of Elliptic Curves to develop cryptographic algorithms. An elliptic curve is a plane curve defined by an equation of the form:

$$Y^2=x^3+ax+b$$

The Elliptic cryptosystem procedures Curve EIGamal (EC-EIGamal) is composed of the following

5.1 Set up

A finite field Fp is first selected. After that, two integers a and b defining an elliptic curve E over Fp are chosen so that the cardinality of E(Fp) has a large prime factor q.Finally, a point P of order q is taken as a generator of the order q cyclic subgroup of E(Fp). The values (p, E, P, q) are made public.

5.2 Key generation

Given the set up parameters, a private key is generated by randomly choosing an integer d in the range [1, q-I]. Next, its related public key Q is computed as Q = d . P.

5.3 Encryption

A plaintext M consisting of a point of E(Fp) is encrypted under public key Q by computing EQ(M) = C = (A, B)=(r . P,M + r . Q),where r is an integer selected randomly in the range[I, q - I].

5.4 Decryption

If the private key d is known, a cipher text C can be decrypted by computing Dd(C)= B - d . A. The clear text M is obtained as a result. The EC-EIGamal cryptosystem has an homomorphic property. Let C I = (A I, 8 I) and C2 =(A2, 82) be two cipher texts encrypting M 1 and M2,respectively. They are aggregated by computing, C= C 1 + C2 = (A 1 + A2, 81 + 82). The decryption of C will provide M I +M2 as a result.

6. CONCLUSION

The ECC Algorithm was proposed for cloud storage security system to issue key management, access control, and file poised deletion with the help of trusted third party and data Anonimyzation.The data anonymization increases the integrity of encryption by changing the encryption pattern within a few seconds which make it difficult to break. The barrier which prevents the users to accept mobile computing is in terms of reliability, security and privacy. The trusted third party method will only perform those cryptographic operations which restricts the unauthorized access of users. This technique enhances the secure sharing of data between the user and cloud using trusted third party method.

REFERENCES

[1] R. Nicole, “Tit[1] Lan Zhou, Vijay Varadharajan, and Michael Hitchens, “Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage,” IEEE Transactions On Information Forensics And Security, Vol. 8, No. 12, December 2013.

[2] Zhifeng Xiao and Yang Xiao, “Security and Privacy in Cloud Computing,” IEEE Communications Surveys & Tutorials, Vol.15, No. 2, Second Quarter 2013.

[3] Niroshinie Fernando, Seng W. Loke, WennyRahayu,”Mobile cloud computing: A survey,”Future Generation Computer Systems (2013)

[4] Ming Li, Shucheng Yu, , Yao Zheng, KuiRen, and Wenjing Lou, “Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,” IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No.1, January 2013.

[5] "Intel Trusted Execution Technology" Hardware-based Technology for Enhancing Server Platform Security, White Paper.

[6] Boyang Wang, Baochun Li and Hui Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud".

[7] Piotr K. Tysowski, M. Anwarul Hasan "Re-Encryption-Based Key Management towards Secure and Scalable Mobile Applications in Clouds".

[8] "A Survey on Data Storage Security in Mobile Cloud Computing Environment" Manoj M. Chavan, Poonam Gupta International Journal of Science and Research (IJSR) ISSN(Online): 2319-7064

[9] Novel Design of Fair Exchange Protocol for Semi-trusted Server and Its Application in Cloud Environment. Chih-Hung Wang,Chien-Ming Wang.

[10] Trusted Third Party for Data Security in Cloud Environment. Noopur Katre, Deepti Theng International Conference on Advancesin Electrical, Electronics, Information,Communication and Bio-Informatics (AEEICB16).

[11] Encryption as a service for securing data in mobile cloud computing , [btihal Mouhib 2015 15th International Conference on Intelligent Systems Design and Applications (ISDA).

[12] R. Karthikeyan and A. Prabha, "A Novel Approach for Load Balancing in the Cloud Computing", International Journal of Innovations in Scientific and Engineering Research(IJISER), Vol. 2, No. 4, April 2015.