Delegate and Verify Pool Based Policy IBE Using Composite Cryptosystem

Sujatha T
M.Tech Scholar, Dept of CSE RRIT, Bangalore.

Poornima U.S
Assistant Professor, Dept of CSE, RRIT, Bangalore.

Abstract – Cloud offers the populace, an opportunity to share data, resources and services. Among many issues, security is the most challenging issue and research has been going on to make more strengthen. Encryption is one of the methods to secure data at any level in cloud. This paper presents such a technique to achieve stored data confidentiality and access control using policy based encryption. During the delegation, cloud server may cheat the authorized users or may tamper the data stored or may replace the data for cost saving. So, proposed Hybrid VPABE schema achieves data confidentially and fine grain access control.

Index Terms – Encryption, Verifiable delegation.

1. INTRODUCTION

Cloud computing is a lucrative technology which every sector interested to adapt to make computation at ease. It involves dramatically scalable and virtualized resources such as bandwidth, software and hardware on demand to customers which leads the customers to use application or services on clouds using internet. Users are connected with cloud with web browser or web services. It provides a way for utility computing [1]. Even though, cloud has many advantages it suffers from security issues. This could happen in any types of cloud.

1.1 Types of cloud

Private cloud*:* This framework is exclusively operated for an organization or enterprise. Private clouds are more secure than public cloud since resources and virtual applications are provided by cloud dealer of that organization.

Public cloud**:** This framework is for general purpose in which user buy a service from cloud on the basis of pay, use and go.

Public clouds are less secure than others because they are more subjected to attacks [2]

Hybrid cloud*:* This framework is like a combination of private cloud and third party. Hybrid clouds are less vulnerable to attacks**.**

Community cloud*:* This framework is shared to several organizations from specific group with specific computing functions.

1.2 Delivery models in cloud.

Software as a service (SaaS): This model eliminates the need of installing and run application on user system instead it provides the user to access the software from cloud provider and pay as u use. SaaS applications are accessible through web browsers. SaaS offers enterprise services like workflow management, customer relationship management etc

Infrastructure as a service (IaaS): In this model customers have control over operating system, deployed applications and storage not with cloud infrastructure, since IaaS provides cloud infrastructure it greatly reduces the investment of hardware such as servers networking devices and processing power.

Platform as a service (PaaS): This model works like IaaS, user has control over deployed application and application hosting environment configurations. PaaS is not useful when applications must be moveable, when proprietary programming languages are used or when the underlying hardware and software must be customized to improve performance of application. Since security is a major issue in cloud computing, research has been going on to make the cloud more secured at different levels of cloud.

This paper addresses the one of the security issue in cloud computing.

The paper is organized as below. Section II explains the issues in cloud computing section III highlights the security measures taken and section IV focus on conclusion.

2. CHALLENGES IN CLOUD COMPUTING

Many issues faced by cloud computing are as follows

1 Security

2 Resource management

3 Interoperability and standardization

In this paper, gaining the trust of data owners and users in cloud environment is highlighted. Better solutions involve data encryption, good infrastructure and data recovery facility. Data in storage is susceptible to attacks, so special attention has to

be taken to protect data storages. Data replication is necessary to ensure proper functioning when system fails. Data encryption protects the data in storage it has to be decrypted for later processing on demand.

There are different layers of security

1 Web application security: it involves security against phishing, SQL injection and cross site scripting.

2 Network layer security: This layer involves security against Domain name service (DNS) attack, sniffer attack, and IP address-spoofing attack.

3 Application layer security: This layer Involves hardware and software resources and distributed denial of service attack (DDOS), cookie hijacking.

One such security measures [3] is to deploy encryption at data level. It not only provides data confidentiality but also provides the access control and scalability so that user can access data at anytime and anywhere.

There are different encryption mechanisms to protect data. Those are encipherment, digital signature, access control, data integrity, authentication exchange, and so on. Cryptosystem is divided into symmetric based encryption and asymmetric based encryption. Symmetric key systems use a common key for encryption and decryption of data whereas asymmetric system uses a different key for encryption and decryption.

3. LITERATURE SURVEY

Attribute based encryption is a public key encryption. It has two forms KP-ABE, CP-ABE. In KP-ABE, key distributor is responsible for decision of access policy instead of encipher, whereas in CP-ABE every cipher text is associated with an access structure, keys are labeled with a set of attributes.

Authors of [4] proposed a new idea to ABE in which user provide single transformation key to cloud so that cloud can translate any ABE cipher text satisfied by attribute, thus reduces the computation cost during decryption.

Authors of [5] proposed a new construction which is provable under deffie helman bilinear assumption in which access policies are not sent along with cipher, thus preserve the privacy of encryptor.

To reduce the computing of decryption task to cloud, ABE with delegation concept emerges out in research field. During delegation, cloud server may cheat corresponded users by telling them that they are unauthorized. Cloud server may change the cipher text and respond fake computing results. So, verifiable delegation is used to protect eligible users from being deceived by the cloud server.

4. SECURITY AS HYBRID VD-ABE

Authors of [6] proposed HABE model which consists of root manager (RM) and Domain manager (Dm). It has certain drawbacks performance. Delegation mechanism between attributes authorities was not provided. It demands users to heavily depend on admin authority (AA).

Authors of [7] proposed distributive server concept which provides security to both communication channel and system. One time password is used in this concept to keep data secure, but it has high execution time.

In most of cases Cipher text is at a risk of being tampered. To enhance the security, Hybrid VD-ABE Model is proposed. Verifiable delegation [8] protect certified user being cheated by cloud.

4.1 Algorithm for verifiable delegation

Step1: Data owner encrypts message M with some access policy f

Step 2: Computes the complement circuit $\bar{f}$

Step 3: Encrypt a random element R of same length to M with some access policy $\bar{f}$

Step 4: Extended encryption assures that users can obtain either message M or R

Table 1. List the roles of different Hybrid VD-ABE Model.

Roles of Hybrid VD-ABE Model	
Authority	Trusted one
Data owner Data Users	Both Registered entities. Got private keys from authority

Table 1 Roles of Hybrid VD-ABE Model

The roles of different users in this model are briefed as below.

1. Authority: He is a super user who creates the data owner user and maintains cloud server configuration. He can insert, edit, and delete any number of data owners.

2. Data owners: He is a person who will store the files in cloud which in turn accessed by authorized data customers. Whenever file is uploaded, it will be encrypted by system using owner encryption key. Data owner has to specify the access policy for each and every file. Access policies are set using Domain attributes and sub domain attributes.

3. Data user: Data users are the data access users. They receive identity token through emails with help of access key. User can able to download the files for which they have access. Access control is set by data owner.

4.2 How the model Works:

Suppose data consumer wants to download any file, first he has to select the file from list and system asks for the access key. After system getting the access key, it will separate the attribute set from key and check for access rights. If the user has access, he can download the encrypted file which in turn decrypted using decryption key and download to data consumer local system.

The cipher text of Hybrid VD-CPABE system is divided into components CP-ABE for circuit f, complementary circuit $\bar{f}$ which makes up KEM, Symmetric encryption and encrypts then MAC. Each KEM encrypts random group element and maps it via key derivation function into symmetric encryption key (Dk) and a onetime Verified key (Vk). Then by using that random element (Dk), we encrypt the message of any length (Vk) and data owners Ids are used to verify the MAC of cipher text. The user could be able to properly validate Mac only when server sends original cipher text and respond a correct partial decryption cipher text.

In Hybrid VD-CPABE, we come across C-CPABE, Symmetric encryption Schema and encrypt then MAC. It is a tuple of algorithms (setup, hybrid encrypt, keygen, transform, verify-Decrypt)

1 Setup: This phase is executed by authority. It takes input Security Parameter(q),number of attributes(n), maximum depth of circuit(h) Outputs Public parameter(Pk), Master Key(Mk)(secret)

2 Hybrid encrypt: This phase is executed by data owner. To achieve verifiable delegation we used key delegation mechanism (KEM) and authenticated symmetric encryption (AE). KEM takes input public parameter (Pk) and access structure f ,performs complement circuit $\bar{f}$ then choose random string R Thus generates Km={dkm,vkm}, Kr={dkr,vkr} outputs CP-ABE cipher text (Ckm ,Ckr).AE takes a input message M, Random string R,symmetric key Km and Kr. Outputs a cipher text.

3 Key Gen: This phase is executed by authority. It takes input Master key Mk and a bit string x, outputs private key Sk and transform key Tk

4 Transform: This paper is executed by cloud server, it takes transformation key(Tk) and Cipher text(Ct) outputs partially decrypted cipher text.

5 Verify-Decrypt: This phase is executed by users, it takes secret key (Sk) and decrypted cipher text (CT') then it verifies for validity of cipher text if f(x)=1 then Mb=M else Mb=R.

5. CONCLUSION

Security to encrypted data plays a prominent role in cloud. Our proposed Hybrid VPABE has CPABE for circuit f, complement of circuit f then it selects random element of same length with certain access policies, symmetric encryption and encrypt then Mac mechanism thus ensures data confidentiality and fine access control and verifiable delegation in cloud.

REFERENCES

[1] M.Armbrust,A.Fox,R.Griffith,A.D.Joseph,R.H.Ratz,A.Konwinski,G.Le l,D.APatterson, A.Rabkin, I.Stoica And M. Zaharia,"Above The Clouds: A Berkeley View Of Cloud Computing", University Of California, Berkley, Technical Report No.UCB/EECS-2009-28,2009

[2] Ramgovind, Eloff MM, Smith E," The Management Of Security In Cloud Computing" University Of South Africa,978-1-4244 IEEE

[3] Abhisek Kumar, Srivastav, Irman Ali,"An Emerging Security Issues In Cloud Computing" IIT, Allahabad volume 4, issue 2 IJARCSSE, Feb 2014

[4] M. Green, S. Hohenberger And B .Waters," Outsourcing The Decryption Of ABE Cipher text" In Proc. USENIX Security symp,San Francisco,CA,USA 2011.

[5] A.Balu, K.Kuppuswamy,"Cipher text Policy Attribute Based Encryption with Anonymous Access Policy", Tamilnadu, India.

[6] Guojun Wang, Qin Liu, Jie Wu," Hierarchical Attribute Based Encryption For Fine Grained Access Control In Cloud Storage Service" Temple University 978-1-4503-0244, Dec 2010.

[7] Kawser Wazed Naïf, Tonny Sheka Kar, Sayed Anisul Hoiue, Dr.M.M.A. Hashen"A New User Authentication, File Encryption And Distributed Server Based Cloud Computing Security Architecture" IJACSA Vol 3, No.10,2012