Enhanced Cloud Computing Adaption Framework with Cipher Text-Policy Attribute-Based Access Control for Data Security

#1G.Suganya,*2Dr. S. Arumugam
PG Scholar, *Professor
Department of Computer Science and Engineering
Nandha Engineering College(Autonomous),Erode.
[1]E-Mail : suganyagme@gmail.com [2]E-Mail : arumugamdote@yahoo.co.in

Abstract
Cloud computing is a prominent technology that enables flexible, on-demand and low-cost usage of computing resources. Though cloud computing provides various benefits to users, it brings some security challenges. Security is a major concern when entrusting an organization's critical information to cloud platforms not under the direct control of that organization. To securely manage the outsourced data, cipher text-policy attribute-based access control can be used .The fine-grained access control can be achieved by dual encryption mechanism.
Keywords-- Cloud computing, Security, Cipher text policy attribute based access control , Techniques

I. INTRODUCTION

Cloud computing is a revolutionary computing technique, by which computing resources are provided dynamically via Internet and the data storage and computation are outsourced to someone or some party in a 'cloud'. It greatly attracts attention and interest from both academia and industry due to the profitability [2].The cloud comprises of five essential characteristics ***on- demand self-service, Broad network Access, and Location Independent Resource Pooling, Rapid Elasticity and Measured service***. Cloud services can be deployed in four ways based on the customers' requirements:

- ***Public Cloud:*** A cloud infrastructure is provided to customers as common and is managed by a third party service provider. Multiple enterprises can work on the cloud infrastructure provided, at the same time.
- ***Private Cloud***: Cloud infrastructure, made available only to a specific set of customer within an organization and managed either by the organization itself or third party service provider
- ***Community cloud:*** Infrastructure shared by several organizations from same community (Ex: Hospitals) and that will be managed by them or a third party service provider.
- ***Hybrid Cloud***: A composition of two or more cloud deployment models, that transfers between them without affecting each other.

Cloud computing can save an organization's time and money, but trusting the system is more important because the real asset of any organization is the data. Cloud computing brings a number of attributes that require special attention when it comes to trusting the system. The trust of the entire system depends on the data protection and prevention techniques used in it. Numerous different tools and techniques have been tested and introduced by the researchers for data protection and prevention to gain and remove the hurdle of trust but there are still gaps which need attention and are required to be lined up by making these techniques much better and effective. Owing to the large quantity of entities and access points in a cloud environment, authorization is crucial in assuring that only authorized entities can interact with data. By avoiding the unauthorized access, organizations can achieve greater confidence in data integrity. Cloud computing providers are trusted to maintain data integrity and accuracy. However, it is necessary to build the third party supervision mechanism besides users and cloud service providers.[9]

The main enabling technology for cloud computing is virtualization. Virtualization software allows a physical computing device to be electronically separated into one or more "virtual" devices, each of which can be easily used and managed to perform computing tasks. Cloud computing provides the tools and technologies to build

data/compute intensive parallel applications with much more affordable prices compared to traditional parallel computing techniques. Cloud offers three primary Software-Platform-Infrastructure (SPI) framework services. The services providers are Amazon EC2(Infrastructure as a Service), Google App Engine(Platform as a Service) and Google Docs(Software as a Service) Figure 1 shows the cloud service models .

Figure 1: Cloud service models

Some of the cloud security threats are:

DoS Attack

Denial-of-service attack (DoS attack) is a an attack where the attacker seeks to make a machine or network resource unavailable temporarily or indefinitely disrupting services to users. Denial of service is typically accomplished by flooding the targeted machine with requests in an attempt to overload systems.

Cross site scripting (XSS)

Cross-site scripting (XSS) is a type of security vulnerability in web applications. XSS enables attackers to inject client-side scripts into web pages which can be viewed by other users. A cross-site scripting vulnerability used by attackers to bypass access controls.

SQL Injection

SQL injection is a code injection technique in which depraved SQL statements are inserted into an entry field for execution. SQL injection must exploit security vulnerability in an application's software.

II. RELATED WORKS

Multi-factor Authentication as a Service for Cloud Data Security

To protect data access by unauthorized users, authentication plays an important role. Authentication is a first step for data security, through which user can establish proof of identities prior data access from system. Multi-Factor Authentication (MFA) scheme has been proposed which integrates more than one factors like knowledge, possession, location and time, for cloud user authentication. The architecture offers security as a service to cloud customers which can help to build trust to adopt cloud infrastructure without any fear to security threats [1].

Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption

A semi anonymous privilege control scheme AnonyControl has been proposed to address not only the data privacy, but also the user identity privacy in existing access control schemes. Anony Control decentralizes the central authority to limit the identity leakage and thus achieves semi anonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. Subsequently, that presents the AnonyControl-F, which fully prevents the identity leakage and achieves the full anonymity [2].

Multilevel classification of security concerns in cloud computing

A novel multilevel classification model of different security attacks across different cloud services at each layer. It also identifies attack types and risk levels associated with different cloud services at these layers. The risks are ranked as low, medium and high. The intensity of these risk levels depends upon the position of cloud layers. The multilevel classification model leads to the provision of dynamic security contract for each cloud layer that dynamically decides about security requirements for cloud consumer and provider [3].

DNA Cryptography An New Approach to Secure Cloud Data

Cryptography is a method in which we protect data or information and transmit it into an unreadable format. A new approach of cryptography that is DNA cryptography has been proposed. DNA can be used to store and transmit data. The concept of using DNA computing in the fields of cryptography and steganography has been identified as a possible technology that may bring forward a new hope for unbreakable algorithms. Strands of DNA are long polymers of millions of linked nucleotides. These nucleotides consist of one of four nitrogen bases, a five carbon sugar and a phosphate group. The nucleotides that make up these polymers are named after the nitrogen base that it consists of; Adenine (A), Cytosine (C), Guanine (G) and Thymine (T) [4].

Data Security in Cloud Computing using Encryption and Steganography

This scheme revolves around the problem of data security and with the help of encryption at client side and steganography at server side provides a highly secure model that will not only solve the issue of data safety but also simple in its implementation and hence usage[5].

Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services

A new fine-grained two-factor authentication (2FA) access control system for web-based cloud computing services. Specifically, proposed 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both a user secret key and a lightweight security device. As a user cannot access the system if they do not hold both, the mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-based cloud services. Based on the attribute-based access control mechanism, the proposed 2FA access control system has been identified not only enable the cloud server to restrict the access to those users with the same set of attributes but also preserve user privacy. Detailed security analysis shows that the proposed 2FA access control system achieves the desired security requirements. Through performance evaluation, demonstrated the construction is “feasible”[6].

An Efficient Fuzzy Self-Classifying Clustering based Framework for Cloud Security

Fuzzy self-classifying clustering based cloud intrusion detection system which is intelligent to gain knowledge of fuzzy sets and fuzzy rules from data to detect intrusions in a cloud environment. The results of proposed approach are compared with other cloud intrusion detection systems based on K means, modified K means, and fuzzy self-constructing clustering algorithms. Using each of these algorithms, the intrusion detection training dataset is partitioned into several clusters with similar patterns belonging to same cluster [7].

Harnessing Encrypted Data in Cloud for Secure and Efficient Mobile Image Sharing

Secure and efficient cloud-assisted image sharing provides a mobile-friendly design that saves the transmission cost for mobile clients, by directly utilizing outsourced correlated images to reproduce the image of interest inside the cloud for immediate dissemination. Initially, secure and efficient index design that allows the mobile client to securely find from encrypted image datasets the candidate selection pertaining to the image of interest for sharing. Then design voting-based ranking mechanism and key management mechanism that support secure image reproduction from encrypted candidate selection. Bandwidth and energy consumptions at the mobile client can be saved, while achieving all service requirements and security guarantees[8].

III. EXISTING SYSTEM

Offering real-time data security for huge amount of data is important for cloud computing. The security of user‘s data has the highest priority as well as the main concern. This can be able to achieve with an approach that is systematic, adoptable and well-structured. The CCAF multi-layered security can protect data in real-time and it has three layers of security:

1) Firewall and access control
2) Identity management and intrusion prevention
3) Convergent encryption

The first layer is Access Control and firewall to allow restricted members to access. The second layer consists of the IDS (Intrusion Detection System) and IPS(Intrusion Prevention System). The aim is to detect attack, intrusion and penetration and also provide up-to-date technologies to prevent attacks such as DoS, anti-spoofing, port scanning, known vulnerabilities, pattern-based attacks, parameter tampering, cross site scripting, SQL injection and cookie poisoning. The identity management is enforced to ensure that right level of access is only granted to the right person. The third layer is convergent encryption. It produces identical cipher text from identical plain text. In convergent encryption identical files will always produce the same cipher data; a person with that exact original file could encrypt it and then identify instances of that file. Convergent encryption is also vulnerable to a partial-information attack

IV. PROPOSED SYSTEM

A. SYSTEM MODEL

The system architecture consists of four entities:

Data owner: This is a client who owns data, and wishes to outsource it into the external data server provided.

User: This is an entity who wants to access the outsourced data.

Service provider: It is an entity which provides a data outsourcing service. It is controlling the accesses from unauthorized users to the outsourced data and providing corresponding contents services.

Trusted Authority: It generates public and secret
parameters for the system. It provides differential access rights to individual users based on their attributes .Figure 2 system architecture of the data outsourcing system.

B.CIPHER TEXT POLICY ATTRIBUTE BASED ACCESS CONTROL

Cipher Text policy attribute based access control resolves the issue of fine grained access control over the outsourced data where the data owner can have the direct control over a data. Each user is assigned with a set of attributes .The data owner chooses an access structure (AS) and encrypts the message under the AS.

A user is able to decrypt the cipher Text only if set of attributes associated with the user's key satisfies the AS of the ciphertext.

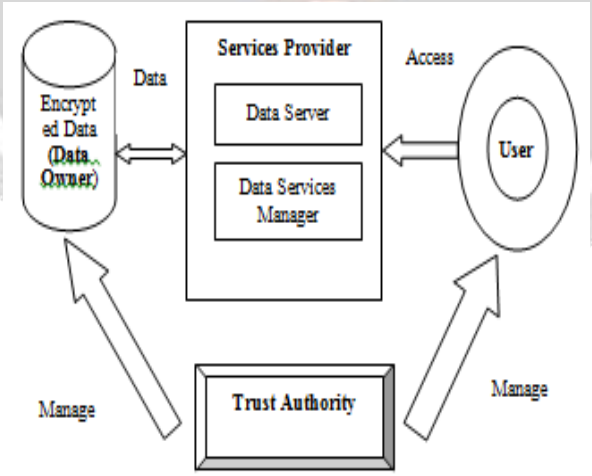

Figure 2: System Architecture

Setup: It takes the implicit security parameter as an input and outputs the public key PK and a master key MK.
.
AKeyGen(MK;A;U)→SK: It takes as input the master key MK, a set of attributes and a set of user
indices. It outputs a set of private attribute keys SK for each user in U. The trusted authority generates attribute keys for a set of users

KEKGen(U): It takes as input a set of user indices U, and outputs KEKs for each user in U.

Encrypt(PK;M;AS)→CT: It takes as input the public parameter PK, a message M, and an access structure AS and outputs a ciphertext CT. The algorithm enforces attribute-based access control on the outsourced data

ReEncrypt(CT;G)→CT': It takes as input the ciphertext CT including an access structure AS, and a set of attribute groups G and outputs a re-encrypted ciphertext .

Decrypt(CT';SK;K_A): The decryption algorithm takes as input the ciphertext CT' which contains an access structure AS, a private key SK.

Bilinear Maps

We present a few facts related to groups with efficiently computable bilinear maps.

Let G_0 and G_1 be two multiplicative cyclic groups of prime order p. Let g be a generator of G_0 and e be a bilinear map, $e : G_0 \times G_0 \rightarrow G_1$.

The bilinear map e has the following properties:

1. Bilinearity: for all $u,v \in G_0$ and $a,b \in Zp$, we have $e(u^a, v^b) = e(u,v)^{ab}$

.

2. Non-degeneracy: e(g,g) not equals to 1.

We say that G0 is a bilinear group if the group operation in G0 and the bilinear map $e : G_0 \times G_0 \rightarrow G_1$ are both efficiently computable. Notice that the map e is symmetric since $e(g^a, g^b) = e(g,g)^{ab} = e(g^b, g^a)$.

V. RESULTS

Data integrity is one of the most critical elements in any information system. Generally, data integrity means protecting data from unauthorized deletion, modification, or fabrication. Managing entity's admittance and rights to specific enterprise resources ensures that valuable data and services
are not abused, misappropriated, or stolen[9].

Triple DES (3DES) which applies the DES cipher algorithm three times to each data block. Triple DES uses a "key bundle" that comprises three DES keys, K1, K2 and K3, each of 56 bits (excluding parity bits). The encryption algorithm is:

ciphertext = EK3(DK2(EK1(plaintext)))

i.e., DES encrypt with K1, DES decrypt with K2, then DES encrypt with K3.

Decryption is the reverse:

plaintext = DK1(EK2(DK3(ciphertext)))

i.e., decrypt with K3, encrypt with K2, then decrypt with K1.

Each triple encryption encrypts one block of 64 bits of data [10].

In attribute key generation the possible operations (access policies) performable by the users are defined.

Figure 3: Attribute Key Generation

Encryptions process outputs the ciphertext which is performed by the data owner.

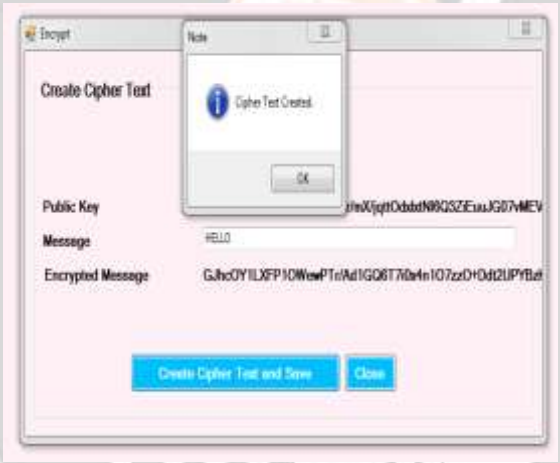

Figure 4: Encryption

Cipher text is reencrypted with the given group by considering group of attributes and access structure

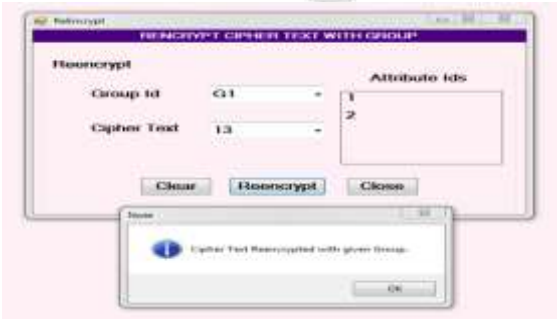

Figure 5:ReEncryption

The user who satisfies the access structure and having appropriate key can decrypt the data.

Figure 6:Decryption

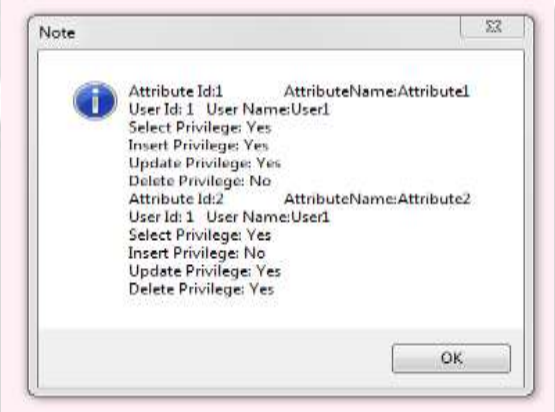

Figure 7: Attribute based Access Control

VI. CONCLUSION

Cloud computing is a prominent and emerging technology. The hindrance towards the growth of cloud computing are data security and privacy issues. To provide data security in the outsourced system Cipher Text Attribute based access control has been implemented. It allows the definition of access policies based on users' roles. So, it provides control of data and avoids data owner to rely on the cloud server. It provides data confidentiality and collusion resistance.

ACKNOWLEDGMENT

I am thankful for the timely and consistent cooperation given by my guide Dr.S.Arumugam for preparing this paper. I hope this paper will help to understand about cipher text policy attribute based access control with the aspect of secure cloud platform.

REFERENCES

[1]. Sajjan Rajani1, Vijay Ghorpade, Madhuri Dhange," Multi-factor Authentication as a Service for Cloud Data Security", International Journal of Computer Sciences and Engineering Volume-4, Special Issue-4, June 2016 E-ISSN: 2347-2693

[2]. Taeho Jung, Xiang-Yang Li, Senior Member, IEEE, Zhiguo Wan, and Meng Wan, Member, IEEE, *Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption*, IEEE Transactions 0n Information Forensics And Security, Vol. 10, No. 1, January 2015

[3]. Syed Asad Hussain , Mehwish Fatima , Atif Saeed , Imran Raza , Raja Khurram Shahzad , "Multilevel classification of security concerns in cloud computing", Applied Computing and Informatics Volume 13, Issue 1, January 2017

[4]. Vinay kumar Pant , Ashutosh Kumar , "DNA Cryptography An New Approach to Secure Cloud Data" , International Journal Of Scientific & Engineering Research, Volume 7, Issue 6, June-2016

[5]. Karun Handa, Uma Singh, "Data Security in Cloud Computing using Encryption and Steganography" , International Journal of Computer Science and Mobile Computing, Vol.4 Issue.5, May- 2015

[6]. Joseph K. Liu, Man Ho Au, Xinyi Huang, Rongxing Lu and Jin Li, "Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services", IEEE Transactions On Information Forensics And Security, Vol. 11, No. 3, March 2016

[7]. Sivakami Raja, Jaiganesh M, Saravanan Ramaiah, *An Efficient Fuzzy Self-Classifying Clustering based Framework for Cloud Security* , International Journal of Computational Intelligence Systems · January 2017

[8].Helei Cui,, Xingliang Yuan,and Cong Wang ,"Harnessing Encrypted Data in Cloud for Secure and Efficient Mobile Image Sharing", IEEE Transactions on Mobile Computing (Volume: 16, Issue: 5, May 1 2017)

[9]**.**Yunchuan Sun, Junsheng Zhang,Yongping Xiong, and Guangyu Zhu*,"Data Security and Privacy in Cloud Computing",* International Journal of Distributed Sensor Networks Volume 2014

[10] https://en.wikipedia.org/wiki/Triple_DES

[11]. Victor Chang and Muthu Ramachandran, Member, IEEE, *Towards Achieving Data Security with the Cloud Computing Adoption Framework*, IEEE Transactions On Services Computing, Vol. 9, No. 1, January/February 2016