© 2017 IJSRSET | Volume 3 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Secured Storage using AES Algorithm and Role Based Access in Cloud

M. Saraswathi,T. Bhuvaneswari
[1]Assistant Professor, Department of CSE,SCSVMV University,Kanchipuram, Tamilnadu, India
[2]Assistant Professor, Department of Computer Applications,Queen's Mary College, Chennai,Tamilnadu, India

ABSTRACT

Cloud computing provides lot of advantages such as on demand service, cost effectiveness, elasticity, scalable, pay per use .One of the main drawback of cloud computing is data security .when data migrate to the cloud , is fully controlled by cloud service provider not by the data owner .As a result user data is not secure at the server side.The main contribution of this paper to designed a prototype which uses a encryption technique to store data and Retrieve data using access control .Instead of applying encryption technique to the whole dataset, we are applying attribute based encryption to only any confidential data in the database and the same encrypted data sent to cloud server. Accessing of data by authorized users via access control methods and polices. Finally achieve data confidentiality and integrity in cloud computing.

Keywords: Cloud Computing, Data Storage, Access Control, Data Confidentiality, Integrity

I. INTRODUCTION

The Cloud Computing refers to "Computing over the Internet". The cloud computing expertise derived from Grid,Utiity and software as service .The cloud model comprises five vital characteristics are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured services. It also offers main three service models such as software as a service (SaaS),Platform as a service (PaaS), and infrastructure as a service (IaaS)and four deployment models such as public, private, community, or hybrid Cloud. Cloud based services should be scalable, service oriented and shared, metered by use, customer focused, use internet technologies in cloud. Cloud computing provides lot of advantages such as access the data remotely at anytime, from anywhere and gives permission to authorized users to share the data.

Access Control is nothing but giving the authority to users to access the specific resources, applications and system. Access control is the process of enforcing these policies in order to achieve the desired level of security. There are three important access control models, such as MAC (Mandatory access control model), DAC (Discretionary access control model) and RBAC Role based access control models. Which also add access control feature only a valid users are able to decrypt the stored information. The most important issues are how to control and prevent unauthorized access to data in the cloud. The mostly used access control methods are identity based access control models.

II. METHODS AND MATERIAL

A. Problem Statement

In an organization, for the employees to be given access to the section of data based on their company security policies. The other employee working in the same organization cannot access the same data. For that, various encryption techniques and key management mechanisms are used to ensure that data are shared to only with the valid users. Apart from that Cloud, computing has several major issues and concerns such as data security, user access control, data integrity, and trust and performances issues. In order to solve these problems, many schemes are proposed under different systems and security models.

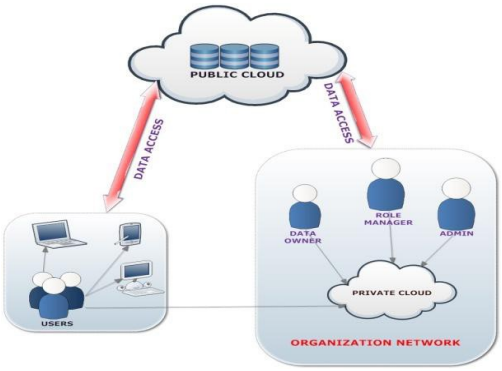

Figure 1. Secure Cloud storage system

B. Literature Review

Data privacy and security is a major issue in cloud computing. Storage of data and access mechanism proposed by various researchers' data to preserve its integrity, confidentiality, authentication, and nonrepudiation while facilitating availability. [1]. proposed a secure cloud computing model based on data classification. It minimizes the overhead and processing time needed to secure data through using TLS, AES and SHA based on the type of classified.[2] presented a data classification method for secure the data. This method describes three types of characteristics such as access control, content and storage. Based on type of content and access control parameter security levels are provided as per requirement of confidentiality of user data. [3]. proposed a K-NN classifier to classify the data in sensitive and nonsensitive data for data confidentiality in cloud. Then used RSA algorithm to encrypt sensitive data for protecting from unauthorized users.

Sandeep K. Sood[4] .They proposed technique provides a way to protect the data, check the integrity and authentication by following the best possible mechanisms. First begin the division of data into different sections(Public.private&Limitted Access), Index builder,128-bit SSL encryption, Message authenticate code and a double authentication of user one by owner and other by cloud and verification of digital signature of the owner. This method achieves the availability, reliability and integrity of data traversing through data owner to cloud and cloud to user.

[5].They Designed a framework for secure the stored data in cloud. Before storing the sensitivity of the data is examine and the data a classified and segmented accordingly. Secondly, the data is protected from the malicious users by use of enciphering methods .Thirdly, the sensitive data is protected from unauthorized access users by the inclusion of Mandatory Access Control. Finally, all authorized and unauthorized access are recorded in the log register which can be analyzed for predict the attack.[10].Symmetric algorithms which should be used for Cloud based applications and services that require data and link encryption. Security issues by use of cryptography, authentication and distributing keys securely.

Proposed System

The proposed work provides complete security to the user data in the cloud environment. It has been divided into two phase i) Cloud Data storage ii) Data Access

Cloud data storage

In this proposed model, have three main entities. Owner,Cloud service provider ,user.Owner is the person who has the authority to upload the data securely using encryption algorithm to the cloud. Users will want to the access and decrypt the stored data from cloud.In this system applied attribute based encryption (ABE)technique to confidential data available in the database because any dataset it's contain only 20% of confidential data. According to that, no need to encrypt all the data it would be a waste of time for processing it and same as attribute based access control to be used to protect the confidential data from unauthorized users.

Data Access

When the user or owner want to access the data, applied role-based access control model with authentication technique. Data access is determined by the role within the organization. Individual users do not determine it. RBAC model is hybrid between MAC and DAC. The role can be a job position or group membership. Based on complexity of the system use multifactor authentication like password, secret key sent via mail, Digital signatures and generates One Time Password etc.

Module Description

Owner:
A data owner can be a user within the organization who has the authority to encrypt and upload data to the cloud storage and owners to specify who can access the data

according to the role-based policies. In the proposed model, owner performs the encryption using AES Algorithm. We applied client side encryption using AES Algorithm ensures that stronger cloud based secure storage.

In cryptography, the Advanced Encryption Standard(AES) is mostly used symmetric-key encryption standard.AES is a block cipher having block length of 128 bits block size, with key sizes of 128, 192 and 256 bits,respectively Encryption and Decryption for 128-bit keys needs 10 rounds of processing, for 192-bit keys needs 12 rounds of processing, and for 256-bit keys needs 14 rounds.All other rounds are identical for encryption and decryption except for the last round in each case.

Pseudo code of AES Algorithm

The AES algorithm performs a number N_r of cryptographic rounds depending on the actual key length. It has variable key length of 128, 192, or 256 bits.Each round consists of four byte-oriented cryptographic transformations Byte Substitution,Shifting rows of state array,Mixing data within a column of the state array and Round key addition to the state array

```
Cipher(byte[] input, byte[] output)
{
byte[4,4] State;
copy input[] into State[] AddRoundKey
for (round = 1; round < Nr-1; ++round)
{
SubBytesShiftRowsMixColumns
AddRoundKey
   }
SubBytesShiftRowsAddRoundKey
copy State[] to output[]
}
```

User:
Users are the employees of the organization who has particular job functionality according to role and wants certain data from the public cloud to perform this job functionality. The administrator of the secure cloud storage system authenticates each user. Users are not having authority to update the organization structure. They are allowed only for downloading the data assigned for their roles.

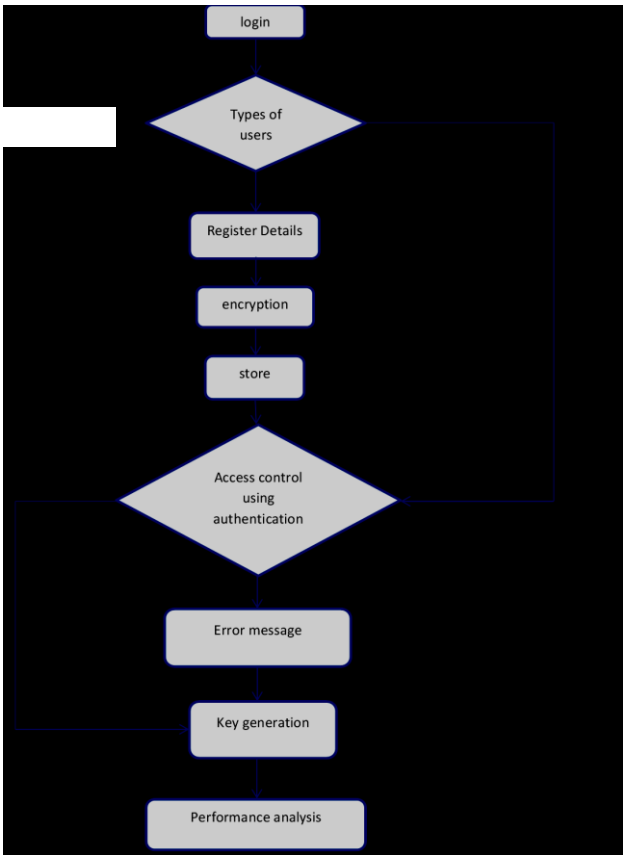

Figure 2. Control flow diagram

C. Deployment to Cloud

The system can be deployed to any type of cloud ie either public or private or hybrid cloud.Most familiar cloud service providers are Microsoft Windows Azure,Amazon Webservices,Salesforce.Comgivingdifferent resources like network,storage,Memory,middleware,database and application.

Public Cloud

Public cloud is a third party cloud provider, which resides outside the infrastructure of the organizations and organizations outsource their users' encrypted data to the public cloud. Since the public cloud is untrusted, data storedin the public cloud could be accessed by unauthorized parties,such as employees of the cloud provider and users from otherorganizations who are also using services from the cloud. An untrusted public cloudmay deny a user's request for accessing stored data in thecloud or provide users with incorrect data. Such behaviours will result in the users not being able to

access the data stored in cloud but will not cause violation of RBAC policies.

Private Cloud

Private cloud is built on an internal data centre that is hosted and operated by a single organization. The organization only stores critical and confidential information in this private cloud.The private cloud only provides interfaces to the administrator and role managers of the role-based system and to the public cloud.

Hybrid Cloud

This cloud is a mixture of the two or more clouds. In thisthe public cloud and private cloud both are used. In this it integrates the advantages of each one for overcoming the others obstacle. The private cloud will not be available for the user. The user will only interact with the public cloud and the administrator of the system will be allowed to access the private cloud. This model is managed by both the third party entity and organization. It can be placed in the onsite or offsite location.

III. RESULTS AND DISCUSSION

Experiment Result

We were taken the input is patient data in the hospitalformation system. Designed the system with front end as Visual studio 2012 and backend as SQL server 2012 database.Information stored in the database patient personal details like name,age,typeofpatient(inpatient,outpatient),address,disease etc and billing details have billed,patient id, patient name ,date, amount and concession fee.Each record have at least one confidential data ie patient disease, patient name or date we paid the amount and concession fee.weshown the screenshot of our work ids displayed in fig 3.

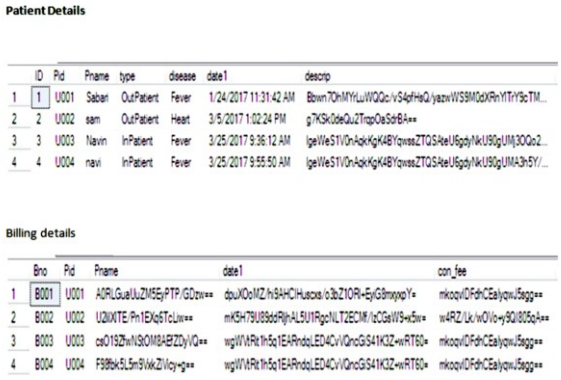

Figure 3. Data Encryption

To view the patient details by the respective role assigned by Admin ,he/she view their details using of patientID and password generate by admin with two factor authentication. It can be shown in fig 4.

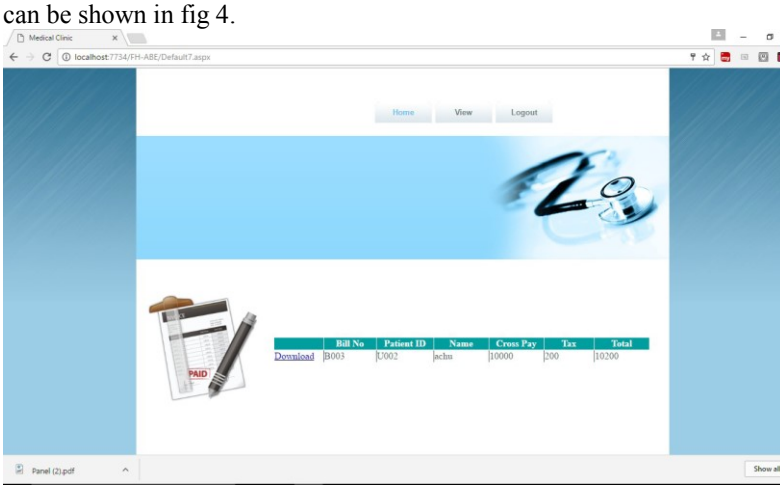

Figure 4. Role based Access

IV. CONCLUSION

In this paper, we propose a framework on secure storage and authenticate user access in cloud.The proposed scheme provides two-factor protection mechanism to enhances the confidentiality of outsourced data. If a user wants to recover the outsourced data, this user is required to hold sufficient attribute secret keys with respect to the access policy and authorization key with regard to the outsourced data. In addition, the proposed scheme provides the user-level revocation for data owner in attribute-based data access control systems.

V. REFERENCES

[1]. Darwazeh, Nour S., Raad S. Al-Qassas, and Fahd AlDosari. "A Secure Cloud Computing Model based on Data Classification." Procedia Computer Science 52 (2015):,pp. 1153-1158.

[2]. Shaikh, Rizwana, and M. Sasikumar. "Data Classification for Achieving Security in CloudComputing." Procedia Computer Science (2015): pp. 493-498.
[3]. Zardari, Munwar Ali, Low Tang Jung, and Nordin Zakaria. "K-NN classifier for data confidentiality in cloud computing." In Computer and Information Sciences (ICCOINS), 2014 International Conference on, IEEE, 2014, pp. 1-6
[4]. Sandeep K. Sood A combined approach to ensure data security in cloud computing Journal of Network and Computer Applications 35 (2012) 1831–1838
[5]. Sudha Devi Dorairaj and Thilagavathy Kaliannan An Adaptive Multilevel Security Framework for the DataStored in Cloud Environment Hindawi Publishing Corporation Scientific World JournalVolume 2015, Article ID 601017, 11 pageshttp://dx.doi.org/10.1155/2015/601017
[6]. A Study on Data Storage Security Issues in Cloud ComputingNaresh vurukonda1, B.Thirumala Rao
[7]. S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute Based Data Sharing with Attribute Revocation,” Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 261-270, 2010.
[8]. Bokefode J.D, Ubale S. A, Apte Sulabha S,Modani D. G, Analysis of DAC MAC RBAC Access Control based Models for Security, International Journal of Computer Applications, Volume 104 – No.5, October 2014.
[9]. Yang, P. Lai, J. Lin, Design role-based multi-tenancy access control scheme for cloud services.
[10]. International Conference on Computational Modeling and Security (CMS 2016)Security Algorithms for Cloud Computing