IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10415

SECURE ELECTRONIC HEALTH RECORD SHARING WITH SENSITIVE BASE ACCESS CONTROL

Ms. P. Subha[1], M.E, G. Nishadevi[2], M. Periyanayaki[3], P. Vinotha[4], N. Navina[5]

Assistant Professor, Department of ComputeScience and engineering, Sri Bharathi Engineering College forWomen, Kaikkurichi, Pudukkottai-622303, Tamil Nadu, India[1]

B.E, Computer Science and engineering, Sri Bharathi Engineering College for Women, Kaikkurichi, Pudukkottai, 622303, Tamil Nadu, India[2-5]

Abstract: Cloud computing provides high performance, accessibility and low cost for data storing and sharing, provides a better consumption of resources. In cloud computing, cloud services providers compromise an abstraction of infinite storage space for clients to mass data. Electronic health record possesses the patient's medical details and their health history. The data owner has the capability to encrypt files and limiting access to only authorized data user.Data owner could add the users and distribute key for the verification of user.Key will be generated using Random Key Generation procedure. AES is implemented to provide security parameters to encrypt the data before store on cloud. We provide Role based authentication for medical data access.

Keywords: Medical Record Sharing, Advance Encryption Standard, Role Based Access Control, Attributes Based Access Control.

I. INTRODUCTION

Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. It is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable priced environment. The idea of cloud computing is based on a very fundamental principles of reusability of IT capabilities. The difference that cloud computing brings compared to traditional concepts of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to broaden horizons across organizational boundaries. Forrester defines cloud computing as: "A pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end customer applications and billed by consumption". It is a technology that uses the internet and central remote servers to maintain data and applications and allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth. Cloud computing examples are Yahoo email, Gmail, or Hotmail.

A. SERVICE MODELS OF CLOUD

Cloud Providers offer services that can be grouped into three categories.

- Software as a Service (SaaS)
- Platform as a Service (Paas)
- Infrastructure as a Service (Iaas)

a. Software as a Service

In this model, a complete application is offered to the customer, as a service on demand. A single instance of the service runs on the cloud & multiple end users are serviced. On the customers" side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained. Today SaaS is offered by companies such as Google, Salesforce, Microsoft, Zoho, etc.

b. Platform as a Service

Here, a layer of software, or development environment is encapsulated & offered as a service, upon which other higher levels of service can be built. The customer has the freedom to build his own applications, which run on the providers infrastructure. To meet manageability and scalability requirements of the applications, PaaS providers offer a

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10415

predefined combination of OS and application servers, such as LAMP platform (Linux, Apache, MySQL and PHP), restricted J2EE, Ruby etc. Googles App Engine, Force.com, etc. are some of the popular PaaS examples.

c. Infrastructure as a Service

IaaS provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data center space etc. are pooled and made available to handle workloads. The customer would typically deploy his own software on the infrastructure. Some common examples are Amazon, Go Grid, 3 Tera, etc.

B. ACCESS CONTROL

Access control is a security technique that regulates who or what can view or user resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization. There are two types of access control: physical and logical. These security controls work by identifying an individual or entity, verifying that the person or application is who or what it claims to be, and authorizing the access level and set of actions associated with the username or IP address. Directory services and protocols, including the Local Directory Access Protocol (LDAP) and the Security Assertion Markup Language (SAML), provide access controls for authenticating and authorizing users and entities and enabling them to connect to computer resources, such as distributed applications and web servers.

C. ADVANTAGES OF CLOUD-BASED ACCESS CONTROL SYSTEMS

Interest in cloud-based access control has surged in recent years, attracting business of different sizes and across industries. For anyone who has been seen the benefits of cloud-based systems, that's hardly a shock. From streamlines system management to pricing flexibility, cloud-based access control offers some very attractive qualities when compared with traditional, on-premise system. Some key examples are listed below.

a. Flexible cost management

Whereas traditional access control systems often come with high upfront installation and equipment costs, cloud-based services provide much greater flexibility in pricing. Instead of purchasing on-site equipment outright, users can opt to lease equipment from an authorized reseller, avoiding high capital expenditure costs in favor of modest ongoing operational costs.

b. Reduced burden on user staff

Maintaining a business system takes time and effort, particularly for mission-critical ones like access control. By turning over the hosting and maintenance of on-site PCs, servers, data-redundancy infrastructure and related processes to the integrator, users can dramatically decrease the burden on their own IT staff. Depending on the application itself, a cloud-based system can reduce IT involvement by 97%. Should the user desire, management of the cloud system can be turned over partially or fully to the integrator as well.

c. System reliability

Storing all data on site can be quite risky: unless the user has strong safeguards in place, a power surge or network failure can impact system operation or result in the destruction of that data. To that end, cloud-based access control systems generally utilize centralized data centers that are equipped with robust backup power and storage systems to ensure the safety and integrity of the system and data.

II. RELATED STUDY

Pritam et al, [1] proposed a paper related toEnforcing Role-Based Access Control for Secure Data Storage in Cloud. In this paper encryption scheme is proposed which incorporates the cryptographic approaches with RBAC and also an anonymous control scheme to address the privacy in data as well as the user identity privacy in current access control schemes. A real-time method is provided to maintain a secure communication in cloud computing which ensures security as well as trust-based access to cloud. The proposed model contains algorithms to explain data protection and user authentication problems. A secure RBAC based cloud storage system is proposed in this paper. In our system, the Data Owner encrypts the data in such a way that only the data Users with relevant access policies can decrypt and view the data. The cloud service provider (who stores the data) will not be able to see the content of the data without the specified access policy. To prevent the admission of malicious Data Owner to cloud, an Admission Policy is proposed. Based on this policy, only genuine Data Owners can get admission to cloud which is based on voting by existing Data Owners. The authentication mechanism plays a vital role in security enhancement. Authentication mechanism is like an entrance door and will allow only the trusted individuals to enter in the cloud premises. The mechanism should be robust enough to ensure availability by letting the right person in, any time and any place. Authentication mechanism can be combined with cryptographic techniques to ensure confidentiality of data. Zhou et al, [2]proposed a paper related toAchieving secure role-based access control on encrypted data in cloud storage.Proposed a role-based encryption (RBE) scheme that integrates the cryptographic techniques with RBAC. Their RBE scheme allows RBAC policies to be enforced for the encrypted data stored in public clouds. Based on the proposed scheme, they present a secure RBE-based hybrid cloud storage architecture that allows an organization to store data securely in a public cloud, while maintaining the sensitive information related to the organization's structure in a private cloud. In this paper, they

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10415

present the design of a secure RBAC based cloud storage system where the access control policies are enforced by a new role-based encryption (RBE) that they proposed in the paper. This RBE scheme enforces RBAC policies on encrypted data stored in the cloud with an efficient user revocation using an broadcast encryption1 machan.The owner of the data encrypts the data in such a way that only the users with appropriate roles as specified by a RBAC policy can decrypt and view the data. The role grants permissions to users who qualify the role and can also revoke the permissions from existing users of the role. The cloud provider (who stores the data) will not be able to see the content of the data if the provider is not given the appropriate role. Their RBE scheme is able to deal with role hierarchies, whereby roles inherit permissions form other roles. A user is able to join a role after the owner has encrypted the data for that role. The user will be able to access that data from then on, and the owner does not need to re-encrypt the data. A user can be revoked at any time in which case, the revoked user will not have access to any future encrypted data for this role. With their new RBE scheme, revocation of a user from a role does not affect other users and roles in the system. In addition, they outsource part of the decryption computation in the scheme to the cloud, in which only public parameters are involved. By using this approach, their RBE scheme achieves an efficient decryption on the client side.

III. PROPOSED WORK

A new method known as Role with Sensitive Based Access Control (RSBAC) was introduced. Role based Access Control (RBAC) determines user's access to the system based on the Job role with data sensitive level. The role a user is assigned to be basically based on the least privilege concept. The role is defined with the least amount of permissions or functionalities that is necessary for the job to be done. Permissions can be added or deleted if the privileges for arole change. However, problems became apparent when RBAC was extended across administrative domains. And it proved difficult to reach an agreement on what privileges to associate with a role. Accordingly, a policy-based access control known as Attribute Based Access Control (ABAC) came into existence. In ABAC, access is granted on attributes that the user could prove to have such as date of birth or national number. However, reaching to an agreement on a set of attributes is very hard, especially across multiple agencies or domains and organizations. All access control methods rely on authentication of the user at the site, as well as, at the time of request. Sometimes they are labeled as authentication-based access control. In all these methods, tight coupling among domains are required. This is done to merge identities or define the meaning of AES or roles. AES used for encrypting the shared data. In this proposed approach the user can access data, with their satisfied attribute key and role verification. Unauthorized access could be identified with the help of key verification and also role mismatch process. This proposed approach will enhance the security of group data sharing with different hierarchical based access structures.

- Only one user with a satisfied attribute set with their role can access the data.
- This method ensures that no unprivileged data user will gain access to any part of the data.
- It allows data owner to selectively share their data files among multiple data users.
- It minimizing the required cloud storage space needed to store the encrypted data segment.

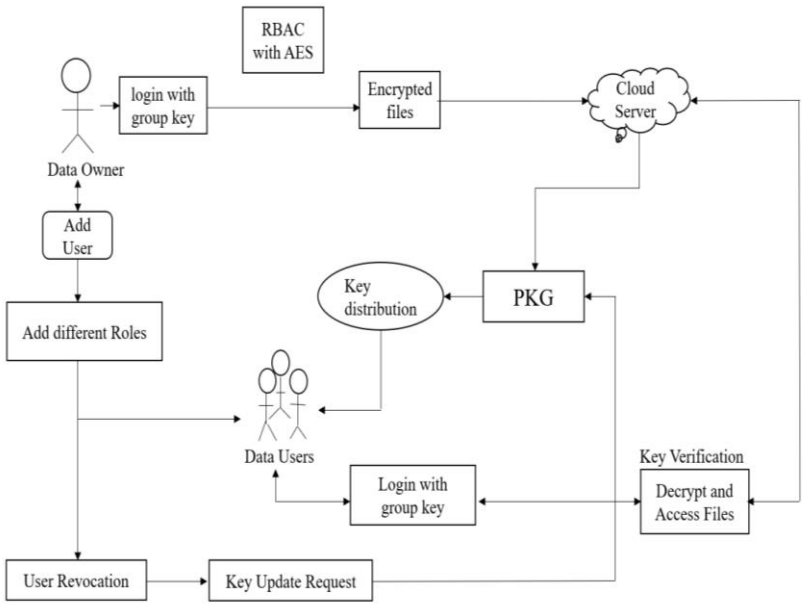

Fig 1. Proposed Architectural Design

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10415

A.Cloud Framework Construction

In this module, create a local Cloud and provide priced abundant storage services. Once get space from cloud the users can upload to share data in the cloud. In this work, the cloud storage can be implemented with high secure. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Proposed secure data sharing framework provides communication between group owner and group members. Group Owner takes charge of followings,

1. System parameters generation

2. User registration

3. User revocation

4. Revealing the data owner identity

Therefore, the group owner is fully trustily the other parties. The Group owner is the admin. The group owner has the logs of each and every process in the cloud. The group owner is responsible for user registration and also user revocation too.

B. Data Upload and Encryption

Group owner is a cloud client who registers with the CSP (Cloud Service Provider). Owner outsources data to cloud in encrypted form. Group owner anonymously get authenticated to cloud while getting duly authenticated. It is the duty of the Group owner to prevent the admission of malicious group owner's to cloud. The encrypted data is uploaded to the cloud by the group owner. The group owner can encrypt the file using AES encryption technique. The choice of encryption is of the group owner.

C. Sensitive with Role based Access Control

RBAC is nothing more than the idea of assigning system access to users based on their role within an organization. The system needs of a given workforce are analyzed, with users grouped into roles based on common job responsibilities and system access needs. Access is then assigned to each person based strictly on their role assignment. With tight adherence to access requirements established for each role, access management becomes much easier.

D. User Key Verification

Key Generation is the process of generating secret key for group owner and group members. After completion of registration secret key is generated using random key generation process and send to the corresponding user through email. During login user should enter their secret key that will be verify with database. If user does not have valid user id they will not allowed accessing application. The concept of group signatures was performed by PKG (Public Key Generation). A group signature scheme allows any member of the group to share messages while keeping the identity secret from verifiers. Besides, the unique group manager can display the identity of the signature's originator when a dispute happens, that is denoted as traceability. Here, a variant of the group signature updating scheme will be used to perform anonymous access control, as it supports efficient group user revocation.

E. Privilege based Data Access

User must be authenticated to access the service from cloud. The commonly used security mechanism for data access is to check username and password pair. User provides the username and password to the cloud server and then cloud server checks the authenticity of user. If user is authorized service provider will allow user to search file from cloud otherwise the user will not be allowed to search files. User can be extracting the stored data anywhere from cloud storage. If a new member is added to the group, this system can be granted access to the file and sharing the group key to the added member wherein he can directly download the decrypted data file, when they are downloading the file a secret key is generated and sent to their own mobile number, using that key user can download the data.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10415

IV. SIMULATION RESULTS

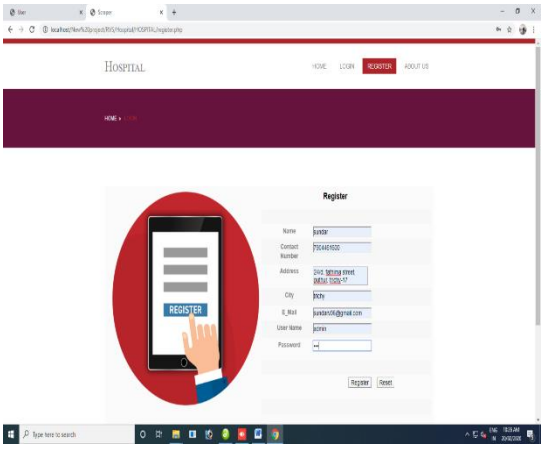

Fig 2. User Register

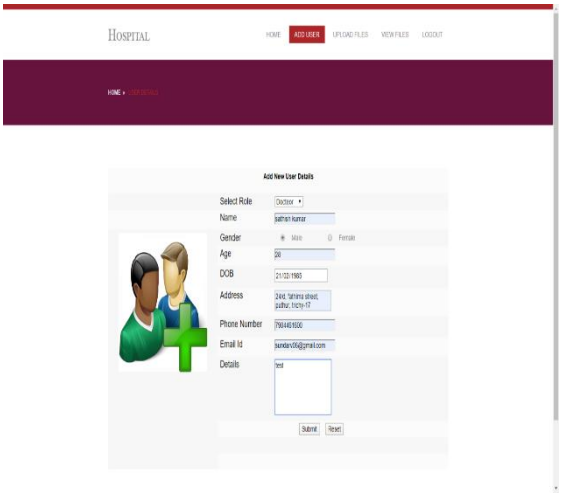

Fig 3. Add User Details

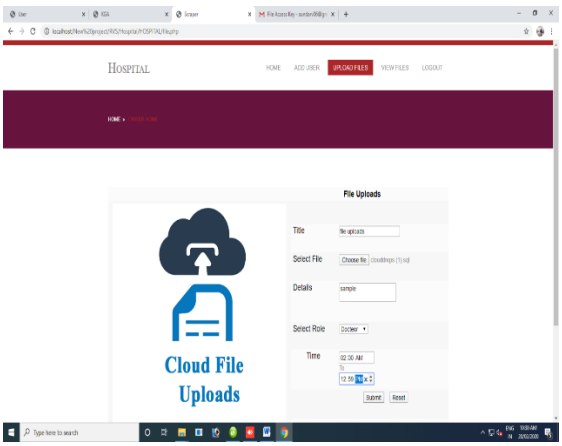

Fig 4. File Upload

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10415

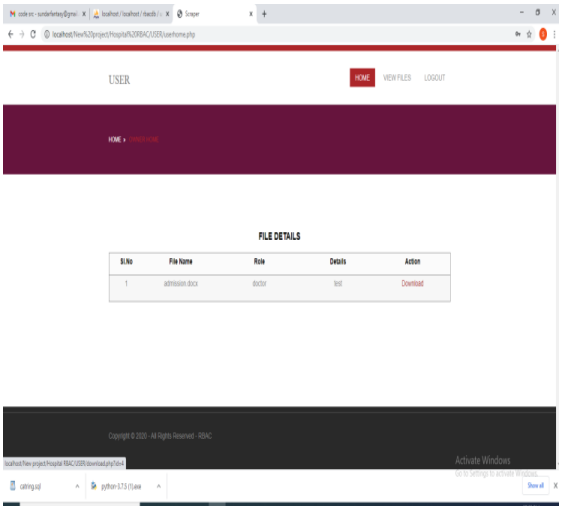

Fig 5. File Download

V. CONCLUSION AND FUTURE WORK

The secure data sharing mechanism can be used in many different areas of the healthcare system, such as for storing and sharing medical records and insurance information both in healthcare venues and in mobile applications and remote monitoring systems, and for clinical trials.Our project provides efficient access control policy based on user's role also implement secure encryption using AES encryption algorithm. The cloud storage requires secure access control to preserve privacy of data. We proposed a RBAC based model which allows an organization to store data securely in a public cloud. The proposed (Role Based Access Control with Encryption) model performs the user revocation and decryption operations efficiently.

In future, it can be implementing in any organization where role hierarchy plays an important role. The organizations which wish to upload the document to the cloud with security. It provides the full security to the documents. This project can be using in colleges or company need to provide the access to the file to appropriate role and to user.

REFERENCES

[1] Zhou, Lan, Vijay Varadharajan, and Michael Hitchens. "Achieving secure role-based access control on encrypted data in cloud storage." IEEE transactions on information forensics and security 8, no. 12 (2013): 1947-1960.

[2] Jiang, Tao, Xiaofeng Chen, and Jianfeng Ma. "Public integrity auditing for shared dynamic cloud data with group user revocation." IEEE Transactions on Computers 65, no. 8 (2015): 2363-2373.

[3] Pritam, Divya, and Madhumita Chatterjee. "Enforcing Role-Based Access Control for Secure Data Storage in Cloud Using Authentication and Encryption Techniques." Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org 6, no. 4 (2016).

[4] Fu, Anmin, Shui Yu, Yuqing Zhang, Huaqun Wang, and Chanying Huang. "NPP: a new privacy-aware public auditing scheme for cloud data sharing with group users." IEEE Transactions on Big Data (2017).

[5] Guo, Rui, Huixian Shi, Qinglan Zhao, and Dong Zheng. "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems." IEEE Access 6 (2018): 11676-11686.

[6] Dagher, Gaby G., Jordan Mohler, MateaMilojkovic, and Praneeth Babu Marella. "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology." Sustainable Cities and Society 39 (2018): 283-297.

[7] Mehmood, Abid, IynkaranNatgunanathan, Yong Xiang, Howard Poston, and Yushu Zhang. "Anonymous authentication scheme for smart cloud-based healthcare applications." IEEE access 6 (2018): 33552-33567.

[8] Wang, Hao, and Yujiao Song. "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain." Journal of medical systems 42, no. 8 (2018): 152.

[9] Sun, You, Rui Zhang, Xin Wang, Kaiqiang Gao, and Ling Liu. "A decentralizing attribute-based signature for healthcare blockchain." In 2018 27th International Conference on Computer Communication and Networks (ICCCN), pp. 1-9. IEEE, 2018.

[10] Gupta, Shubhi, Swati Vashisht, and Divya Singh. "Enhancing Big Data Security Using Elliptic Curve Cryptography." In 2019 International Conference on Automation, Computational and Technology Management (ICACTM), pp. 348-351. IEEE, 2019.