IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12347

SECURE ELECTRONIC HEALTH RECORD SHARING WITH SENSITIVE BASE ACCESS CONTROL

Nikhil. K[1], DR. Gobi Natesan[2]

Student, Department of Computer Science and IT Jain (Deemed to be) University Karnataka -560041, Bengaluru, India[1]

MCA, Computer Science and IT Jain (Deemed to be) University Karnataka -560041, Bengaluru, India[2]

Abstract: For data storage and sharing, cloud computing offers great performance, accessibility, and cheap cost, resulting in better resource usage. Cloud service providers compromise an abstraction of limitless storage space for clients to mass data in cloud computing. The patient's medical information and medical background are contained in the electronic health record. The owner of the data has the power to encrypt files and restrict access to only registered users. Users could be added, and keys could be distributed for user authentication. A random key generation process will be used to create the key. Data is encrypted before being stored in the cloud using AES, which is implemented to offer security measures. We offer role-based authentication for access to medical data.

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

I. INTRODUCTION

A vast number of systems are linked together in private or public networks to create a dynamically scalable infrastructure for application, data, and file storage, which is known as cloud computing. This technology has drastically decreased the cost of computation, application hosting, content storage, and distribution. It can change a data center from a capital-intensive setup to a variable priced environment, and it is a practical way to see immediate cost benefits. Reusability of IT capabilities is one of the core tenets on which the concept of cloud computing is built. Cloud computing differs from conventional ideas of "grid computing," "distributed computing," "utility computing," or "autonomic computing" in that it broadens perspectives outside of organizational boundaries. According to Forrester 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 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.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023
DOI: 10.17148/IJARCCE.2023.12347

II. ACCESS CONTROL

As a security measure, access control limits who or what can access resources in a computing system. It is a basic security principle that reduces risk to the company or organization. Access control comes in two flavors: logical and physical. These security measures operate by identifying a person or entity, confirming that they are who or what they say they are, and then approving the level of access and set of actions linked to their username or IP address. Access controls are provided by directory services and protocols, such as the Local Directory Access Protocol (LDAP) and the Security Assertion Markup Language (SAML), which allow users and entities to connect to computer resources, such as distributed applications, after being authenticated and authorized.

III. ADVANTAGES OF CLOUD-BASED ACCESS CONTROL SYSTEMS

Cloud-based access control has had a recent increase in popularity, drawing organisations of all sizes and from a variety of industries. That shouldn't come as a surprise to anyone who has experienced the advantages of cloud-based solutions. When compared to conventional, on-premise systems, cloud-based access control has some highly appealing qualities, such as simplified system management and pricing flexibility. These are a few crucial instances.

a. Flexible cost control

Cloud-based services offer significantly better price flexibility than traditional access control systems, which frequently have expensive upfront installation and equipment expenses. Users have the option to lease equipment from an authorized reseller rather than buying it altogether, avoiding high capital investment expenses in favor of low continuing operational costs. Reduced burden on user staff.

b. Reduced Burden on Staff

It takes time and effort to maintain a business system, especially one as crucial as access control. User can significantly lessen the workload on their own IT staff by handing over hosting and maintenance of on-site PCs, servers, data-redundancy infrastructure, and related processes to the integrator. A cloud-based solution can reduce IT involvement by 97%, depending on the application. The user has the option of giving the integrator partial or full control over the management of the cloud system.

C. System dependability

Keeping all data locally can be dangerous because, unless the user has robust security measures in place, a network outage or power surge could affect system performance or result in the loss of that data. So as to guarantee the security and integrity of the system and data, cloud-based access control systems typically make use of centralised data centres that are outfitted with reliable backup power and storage systems.

IV. RELATED STUDY

Enforcing Role-Based Access Control for Secure Data Storage in the Cloud is the subject of a paper that Pritam et al. [1] proposed. In order to address the privacy in data as well as the privacy of user identification in current access control systems, an encryption scheme is provided in this work that integrates cryptographic approaches with RBAC and also includes an anonymous control mechanism. In order to maintain safe communication in cloud computing, a real-time approach is offered that provides security and trust-based cloud access. Algorithms are included in the suggested model to explain issues with user authentication and data protection. In this paper, a secure RBAC-based cloud storage system is suggested. In our system, the data owner encrypts the information in a way that only users with the necessary access may decipher it.

V. PROPOSED WORK

Role with Sensitive Based Access Control (RSBAC), a novel technique, was introduced. According to the job description with the highest level of data sensitivity, role-based access control (RBAC) decides which users have access to the system.

The least privilege principle essentially governs the role that is given to a user.
The role is defined with the fewest rights or functions required to complete the task.
In the event that a role's rights change, permissions can be added or removed.
Nevertheless, when RBAC was expanded across administrative domains, issues emerged.

Also, deciding which privileges to assign to each role proved challenging. As a result, Attribute Based Access Control (ABAC), a policy-based access control, was developed.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12347

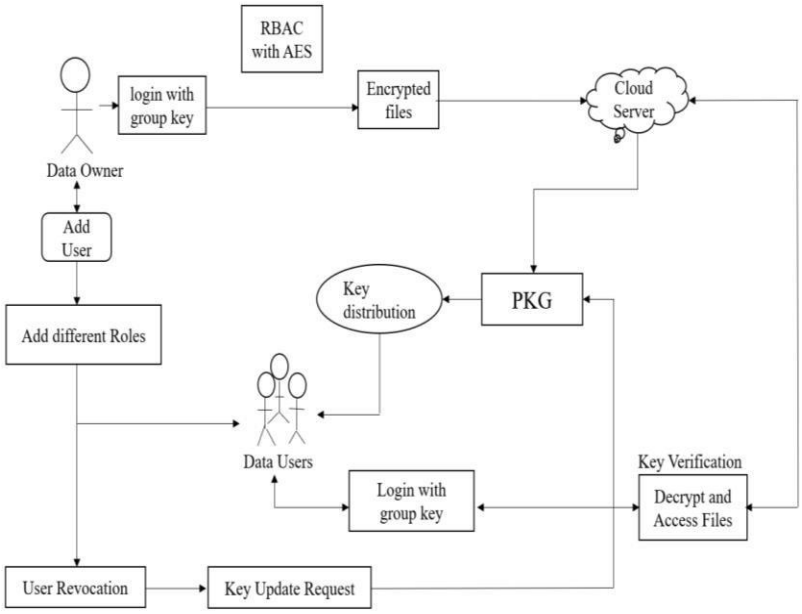

FIG 1. PROPOSED ARCHITECTURAL DESIGN

A. Cloud Framework Development

Create a local cloud in this module and offer reasonably priced, ample storage services. Once users have cloud storage, they can upload and exchange data there. The implementation of cloud storage is highly secure in this work. Yet, because CSPs are almost certainly outside of the cloud users' trusted domain, consumers do not fully trust the cloud. The proposed infrastructure for secure data sharing enables interaction between group owners and members. Group Owner is responsible for the following:

1.Generating system parameters
2. User registration
3. User revocation
4. Identifying the data owner.

As a result, the group owner is completely trusted by the other parties. The group is under the admin's management. The group owner is in charge of the logs.

B. Uploading Data and Encryption

A cloud client who registers with the CSP is the group owner (Cloud Service Provider). Owner uploads encrypted data to the cloud. Group owner receives proper authentication while receiving anonymous cloud authentication. The group owner has a responsibility to stop harmful group owners from joining the cloud. The group owner uploads the encrypted data to the cloud. The file can be encrypted using the AES encryption method by the group owner. The group owner selects the encryption method.

C. Receptive to Access control based on roles

Nothing more than the concept of allocating system access to users in accordance with their organizational roles constitutes RBAC. Users are categorized into roles based on common job tasks and system access requirements, after which the system requirements of a specific workforce are examined. Then, according solely to their specified roles, access is granted to each individual. Access management is made considerably simpler with strict respect to the access restrictions set forth for each position.

D. User Key Verification

The process of creating a secret key for the group owner and members is known as key generation. Following registration, a secret key is generated using a random key generation process and sent via email to the appropriate user. Users must enter their secret key at login so that it may be verified against the database. If a user's user ID is invalid, they will not be able to access the program me. PKG invented the idea of group signatures (Public Key Generation). Any group member can share messages using a group signature technique while maintaining anonymity from verifiers.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023
DOI: 10.17148/IJARCCE.2023.12347

Additionally, the traceability of the unique group manager enables it to reveal the identity of the signature's creator in the event of a disagreement. This is a different group signature.

E. Access to data depending on privileges

To access the service via the cloud, the user must be authenticated. Checking a user's login and password is a standard security measure for data access. The cloud server requests the user's username and password from the user before verifying the user's identity. The user will only be permitted to seek files from the cloud if the service provider has given them permission; otherwise, they will not be permitted. Users can access their stored data from cloud storage from any location. This method can allow access to the file whenever a new group member joins, sharing the group key with the new member so he can immediately download the encrypted.

VI. CONCLUSION AND FUTURE WORK

The secure data sharing method can be applied to numerous different aspects of the healthcare system, including clinical trials, mobile applications, remote monitoring systems, and the storage and exchange of insurance and medical record data.

Our technology implements secure encryption using the AES encryption method and offers effective access control policies based on user roles. To protect data privacy, cloud storage requires secure access management.

We suggested an RBAC-based paradigm that enables a business to safely store data on a public cloud.

The user revocation and decryption processes are effectively carried out by the suggested (Role Based Access Control with Encryption) methodology.

It can be implemented in the future in any organization where position hierarchy is significant.

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.