International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

SECURE CLOUD DATA SHARING: ROLE BASED ACCESS CONTROL

Mr.D.Vijayakumar [1], P.Jenith [2], A.Jeyasurya [3], T.Sabarivasan [4], S.Kishore [5]

[1] Assistant Professor, Department of Information Technology, Dhanalakshmi Srinivasan Engineering College(Autonomous), Perambalur, Tamil Nadu.

[2,3,4,5] UG - Department of Information Technology, Dhanalakshmi Srinivasan Engineering College(Autonomous), Perambalur, Tamil Nadu.

E-Mail: vijaydsecit@gmail.com[1], jenith2703@gmail.com[2], jeyasuriya170@gmail.com[3], sabarikavi083@gmail.com[4], kishorepmt123@gmail.com[5]

ABSTRACT

Cloud computing provides high performance, accessibility and low cost for data storing and sharing, provides a better consumption of resources. However, security concerns develop the main constraint as now outsource the storage of data, which is possibly sensitive, to cloud providers. To preserve data privacy, a mutual approach is to encrypt data files before the clients upload the encrypted data into the cloud. There is also an essential for an access control mechanism for preventing data mistreatment within the organization. Unfortunately, it is difficult to design a secure and efficient data sharing scheme, especially for dynamic groups in the cloud. To overcome the problem, here propose a secure data sharing scheme for frequently changed groups. First, propose Role Based Access Control (RBAC) with a protected way for key distribution without any secure communication channels, and the users can securely obtain their group keys from group manager. Role-based access control (RBAC) is one of the familiar access control models which provides flexible controls and database management by having users mapped to roles and roles mapped to privileges on data objects. In this work, an ECC based 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. Any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked.

Keywords: Interface Construction, Group Key Verification, Data Upload and Encryption, Role based access control, Data Access, User Revocation.

INTRODUCTION

Access control is a security technique that regulates who or what can view or use 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. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.

Access control systems perform identification authentication and authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers (PINs), biometric scans, security tokens or other authentication factors. Multifactor authentication, which requires two or more authentication factors, is often an important part of layered defence to protect access control systems. 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. Organizations use different access control models depending on their compliance requirements and the security levels of information technology they are trying to protect.

PURPOSE

The purpose of the proposed project is to enhance the security and efficiency of data storage and sharing in cloud environments. Some of the project purposes are given below.

Data Privacy: Ensure the privacy and confidentiality of sensitive data by employing encryption techniques to protect data both during transmission and storage in the cloud.

Access Control: Implement robust access control mechanisms, such as Role-Based Access Control (RBAC), to restrict data access based on users' roles and privileges, thereby preventing unauthorized access and misuse of data.

Key Distribution: Develop a secure method for distributing encryption keys within dynamic groups without relying on secure communication channels, ensuring that authorized users can securely access encrypted data.

Blockchain Integration: Leverage the decentralized and immutable nature of blockchain technology to enhance the security and transparency of data storage and access control mechanisms, providing a tamper-proof record of data transactions and access activities.

Efficiency: Design efficient data sharing schemes, especially for dynamic groups, to facilitate seamless collaboration and resource utilization in cloud environments while minimizing overheads associated with data management.

Revocation: Implement a robust revocation mechanism to revoke access privileges for users who are no longer authorized to access cloud resources, ensuring that data remains secure even in the event of user changes or revocations.

User Privacy: Incorporate anonymous control schemes to protect the privacy of user identities while maintaining the integrity and security of access control mechanisms, thus ensuring compliance with privacy regulations and standards.

OBJECTIVES

Role-Based Access Control (RBAC) with ECC encryption for secure data sharing is a powerful framework that helps organizations manage and control access to their sensitive information. The objectives of implementing RBAC with ECC encryption in the context of secure data sharing, along with user revocation capabilities, include:

Granular Access Control: Assign specific roles to users based on their responsibilities and job functions. Define fine-grained permissions associated with each role, ensuring users only have access to the information required for their tasks.

Data Confidentiality: Use ECC encryption to protect the confidentiality of shared data. ECC is a widely used asymmetric encryption algorithm that ensures secure data transmission and storage.

Data Integrity: Implement mechanisms to maintain data integrity, ensuring that data remains unchanged and trustworthy throughout its lifecycle.

Secure Data Sharing: Enable secure sharing of sensitive data within the organization by allowing access only to authorized users with the appropriate roles and permissions.

User Authentication: Implement robust user authentication mechanisms to ensure that only authorized individuals can access the system. This helps prevent unauthorized access to sensitive information.

User Revocation: Provide the capability to revoke user access when necessary, such as when an employee leaves the organization or changes roles. This ensures that former users cannot access sensitive data after their roles change or they leave the organization.

Scalability and Flexibility: Design the RBAC system to be scalable and adaptable to changing organizational needs. This includes accommodating new roles, updating permissions, and ensuring the system can grow with the organization.

EXISTING SYSTEM

The proposed dynamic secure access control using the blockchain (DSA-Block) model focuses on secure access control and secure data sharing using blockchain.1) Authentication of nodes and users is carried out via hyper elliptic curve cryptography (HECC) and the entities are stored in the private local ledger (LL) to enhance the security, which helps to mitigate external attacks. Authentication-based request filtering is performed through a GW by verifying the legitimacy with a timestamp and freshness of the requests, which increases throughput and reduces latency. Access delegation is achieved through the edge server using rock hyraxes swarm optimization (RHSO) by considering trust, energy, load, and resource availability (RA), in which the trust value is evaluated using blockchain, which reduces the block validation time, response time, and consensus time. The data are shared securely manner by uploading the data to the cloud server with the help of a differential privacy mechanism, which increases the attack detection rate. Finally, revocation is performed for both user attributes and users to enhance security. The user attributes revocation is performed by considering expiry time and attributes updating, and user revocation is performed based on the trust value, which also increases the attack detection rate.

The authentication of devices, users, GWs, and ENs was carried out based on several significant user attributes and devices attributes that increase the degree of security of the nodes and users. Private and public keys are generated by using the HECC algorithm, which enables reduced key size without any compromise on security. This algorithm is suitable for resource-constraint IoT environments. The hierarchical architecture-based approach is implemented, in which the decentralized management of authorization is performed by using both a global domain authority (GDA) and a local domain authority (LDA). The delegator nodes are selected by using the RHSO algorithm for the trust value, energy level, traffic load, and RA; this contributes to the effective selection of nodes. Access control is executed by the consensus operation using the selected delegator nodes, which increases the network scalability. The burden of the GW is reduced by initially filtering the requests. The Trusted PBFT is utilized, in which trusted nodes are selected for consensus. The number of nodes participating in the consensus is restricted to a particular value based on the number of nodes. This provides resistance to malicious nodes and also reduces the block validation time. The dual revocation is executed, in which the revocation of attributes is carried out based on the attribute expiry time, and the revocation of users is performed based on the trust threshold value. The overloading and resource wastage of blockchain nodes is mitigated by filtrating incoming requests. The authenticity and timestamps of the requests are validated to ignore the malicious requests.

DISADVANTAGES

- This is limited to a single delegator node section, which means block validation takes more time.
- When the number of delegator nodes increases, the time consumption for the consensus also increases.
- This system may not easily adapt to blockchain integration.
- It is leading to higher implementation costs and potential disruptions during the transition.
- Managing cryptographic keys securely, especially in a large-scale IoT environment, can be challenging.

PROPOSED SYSTEM

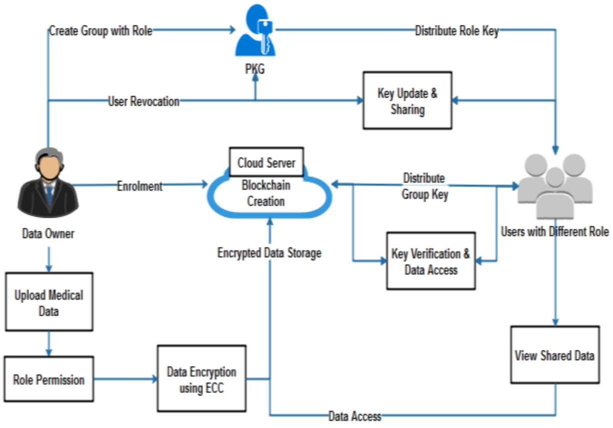
To enable data sharing in the Cloud, it is essential that only authorised users are able to get access to data stored in the Cloud. Proposed work focused on Secure Group Sharing in Cloud with Blockchain technology. When the data owner wants to share their own data to a group, he/she sends the key used for data encryption to each member of the group. Any of the group members can then get the encrypted data from the Cloud and decrypt the data using the key and hence group member does not require the interference of the data owner. Proposed work designed decentralized blockchain based EHRs with ECC encryption scheme. In their scheme, each authority is in charge of accessing data using their Role. That is to say, the different roles of the user are issued to more authority based on their roles. It is a hybrid cloud architecture comprising a private cloud which is used to store sensitive role hierarchy of the hospital and patient memberships, and a public cloud storing the encrypted data and public parameters associated with the Role based access control with encryption system.

The users who wish to access the encrypted data and the data owners who wish to encrypt their data only interact with the public cloud. The role hierarchy and user to role mappings related to the organization are maintained in the private cloud which is only accessible to the administrator of the hospital system. The administrator specifies the role hierarchy and the role managers who manage the user membership relations. Also implement secure user revocation process with key update system. When a user removed from existing group, group key gets updated is distributed to all users present in current data access pattern. Furthermore, all these approaches make it difficult to assign subsets of privileges of an administrator.

ADVANTAGES

- Only one user with a satisfied attribute set with their role can access the data.
- Shared group key together with user's roles, determines whether the user satisfies the policy.
- Resolve problem of data modification using block chain technology.
- With the help of ECC algorithm key generation and distribution process are implemented in easy and secure way.

SYSTEM ARCHITECTURE



FUTURE ENHANCEMENT

In future this policy 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. This policy 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.

CONCLUSION

This research work provides efficient access control policy based on user's role also implement secure encryption using ECC encryption algorithm. The cloud storage requires secure access control to preserve privacy of data. Here propose a RBAC based model which allows an organization to store data securely in a public cloud. The proposed (Role Based Access Control with Encryption) RBE model performs the user revocation and decryption operations efficiently. Also provide group verification for both data owner and user for secure communication. Time based access permission can be implemented to improve access control. The proposed system combines RBE scheme with traditional RBAC model. The role hierarchy is used to improve efficiency of decryption and user revocation operations. Thus, in this system we will provide the higher security than previous models.

REFERENCES

[1] Román-Martínez, Isabel, Jorge Calvillo-Arbizu, Vicente J. Mayor-Gallego, Germán Madinabeitia-Luque, Antonio J. Estepa-Alonso, and Rafael M. Estepa-Alonso. "Blockchain-based service-oriented architecture for consent management, access control, and auditing." IEEE Access 11 (2023): 12727-12741.

[2] Fugkeaw, Somchart. "A fine-grained and lightweight data access control model for mobile cloud computing." IEEE Access 9 (2020): 836-848.

[3] Zhang, Yiran, Huizheng Geng, Li Su, and Li Lu. "A Blockchain-Based Efficient Data Integrity Verification Scheme in Multi-Cloud Storage." IEEE Access 10 (2022): 105920-105929.

[4] Hao, Jialu, Jian Liu, Huimei Wang, Lingshuang Liu, Ming Xian, and Xuemin Shen. "Efficient atStribute-based access control with authorized search in cloud storage." IEEE Access 7 (2019): 182772-182783.

[5] Bakas, Alexandros, Hai-Van Dang, Antonis Michalas, and Alexandr Zalitko. "The cloud we share: Access control on symmetrically encrypted data in untrusted clouds." IEEE Access 8 (2020): 210462-210477.

[6] Li, Qi, Youliang Tian, Yinghui Zhang, Limin Shen, and Jingjing Guo. "Efficient privacy-preserving access control of mobile multimedia data in cloud computing." IEEE Access 7 (2019): 131534-131542.

[7] De Oliveira, Marcela Tuler, Lúcio Henrik Amorim Reis, Yiannis Verginadis, Diogo Menezes Ferrazani Mattos, and Sílvia Delgado Olabarriaga. "Smartaccess: Attribute-based access control system for medical records based on smart contracts." IEEE Access 10 (2022): 117836-117854.

[8] Chiquito, Alex, Ulf Bodin, and Olov Schelén. "Attribute-Based Approaches for Secure Data Sharing in Industrial Contexts." IEEE Access 11 (2023): 10180-10195.

[9] Jaiman, Vikas, and Visara Urovi. "A consent model for blockchain-based health data sharing platforms." IEEE access 8 (2020): 143734-143745.

[10] Yang, Caixia, Liang Tan, Na Shi, Bolei Xu, Yang Cao, and Keping Yu. "AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud." IEEE Access 8 (2020): 70604-70615.