IJNRD.ORG ISSN : 2456-4184

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

DATA SHARING THROUGH MODIFIED BLOCKCHAIN IT ENABLE TO INCREASE SECURITY FOR DATA CUSTOMER

[1]Dr.V.Ravindra Krishna chandar, [2]Jeeva.v, [3]Kanna.P,[4]Madesh.R

[1]Assistant professor, [2]student, [3]student,[4]student
Department of computer science and Engineering
Paavai Engineering college (Autonomous)
Pacahal,Namakkal,Tamil Nadu.,India

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. Cloud storage services can help clients reduce their monetary and maintenance overhead of data managements**.** Data confidentiality becomes the main concern in outsourcing client data to cloud storages. There is also an essential for an access control mechanism for preventing data mistreatment within the organization

***IndexTerms* – DSA algorithm, ECC cryptography,blockchain technology,cloud application.**

INTRODUCTION

The first way a system provides security to its resources and data, is by controlling access to the resources and the system itself. However, access control is more than just controlling which users (subjects) can access which computing and network resources. In addition, access control manages users, files and other resources. It controls user's privileges to files or resources (objects). In access control systems various steps like, identification, authentication, authorization and accountability are taken before actually accessing the resources or the object in general. In early stages of computing and information technology, researchers and technologists realized the importance of preventing users from interfering each other on shared systems. Various access control models were developed. User's identity was the main index to allow users to use the system or its resources. This approach was called Identification Based Access Control (IBAC). However, with the growth of the networks and the number of users, IBAC was found to be weak to defend such a large growth. Advanced concepts in access control were introduced which included owner/ group/ public. IBAC proved to be problematic for distributed systems as well. Managing access to the system and resources became hard and vulnerable to errors.

A new method known as Role Based Access Control (RBAC) was introduced. Role based Access Control (RBAC) determines user's access to the system based on the Job role. 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 a role 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 attributes or roles. Furthermore, all these approaches make it difficult to assign subsets of privileges of an administrator.

RESEARCH METHODOLOGY

[1] Ravi Sandhu…..Develop a formal attribute-based access control (ABAC) model for AWS IoT by building upon and extending previously developed access control model for AWS IOT, known as AWS-IOTAC model. This novel ABAC model

support the specification of fine grained security policies using attributes of various entities, such as IoT devices, virtual objects, and topics. These attributes and their values are utilized in the ABAC authorization policies. Further, we group things into groups and sub-groups with specific attributes for each group. This forms a group hierarchy and allows attribute inheritance. These are administrative tasks and will be discussed later in detail in the Administrative Phase. First, physical devices need to be registered with the AWS cloud. Once the registration is complete, these devices connect to the AWS Greengrass which holds a copy of physical devices' shadows. These are edge virtual objects. All the data from the devices is stored at the edge on the AWS Greengrass service which allows local computation. The data is synced with the cloud periodically when the Internet connection is available and/or when user/administrator syncs data manually. The attribute-based authorization policies restrict access to services and operations in the oil refinery, such as sending and receiving messages, sending notifications to specific entities. There are single or multi-level policies needed for securing these entities and operations. For enabling fine-grained access in the smart oil refinery, here define policy rules for each type of refinery devices that allow or deny specified actions on specific devices and sending notifications to the relevant group of employees.

[2] Chaudhry,… Proposed a certificate based improved lightweight access control and key agreement scheme for IoT devices (iLACKA-IoT) to ensure smooth and secure access control and claimed LACKA-IoT to withstand the several attacks. The proposed scheme is free of any pairing based expensive operations and provides required security level and performance. The A has control over insecure channel being used among the participants for data exchange and A can eavesdrop, delete, replay or alter any data during transmission. A can also forge and transmit a message to any device pretending itself as another device of the system. A can expose the parameters stored on a physically captured device using power analysis. A can be an insider (a curious device) or an external entity. The public system parameters including public keys and identities of all the system entities (certificate authority and communicating devices) are accessible to insiders and outsiders. The private key of the certificate authority (CA) is safe and A does not have capabilities to expose the private key of the CA. The security of the proposed scheme is proved using formal and informal methods. The proposed iLACKA-IoT provides better security and performance than related schemes, specifically it has low computation, communication cost as compared with LACKA-IoT and it overcomes the weaknesses of the same. The proposed iLACKA-IoT completes the access control and the key establishment phase in just 22.4512 ms and by exchanging 2944 bits.

[3] Mingrui Zhang,..Develop a non-interactive, attribute-based access control scheme that applies blockchain technology in IoT scenarios by using PSI technology. In addition, the attributes of data user and data holder are hidden, which protects the privacy of both parties' attributes and access policy. In proposed work, the data holder stores the data resources in the cloud server. When a user wants to access the data resources, the user first sends their own attribute set confidentially to the blockchain as a transaction. Subsequently, the smart contract of the blockchain will run the private set intersection (PSI) protocol to automatically determine whether the attribute set meets the access structure of the data holder. When the element number of the intersection achieves the threshold set by the data holder, the user is given access to the data holder's cloud data. In our scheme, instead of interacting with data users to verify that a data user is qualified, the data holder deploys their own access policy on the blockchain, and a smart contract automatically determines whether a user is qualified or not. A data holder uploads data to a cloud server. If a user wants to access the data, the data user first writes attributes to blockchain as a transaction. Next, the PSI protocol is run by a smart contract to determine whether the attributes set meets the threshold structure. If the condition is met, the data user is allowed to access the data holder's data. Then, the data holder uses the selected user's public key to encrypt the data address and sends it to the user.

[4] Tooska Dargahi,..Propose an architecture (so called BCHealth) that enables data owners to define their desired access policies over their privacy-sensitive healthcare data. BCHealth is composed of two separate chains for storing access policies and data transactions. BCHealth introduces the usage of two different chains, namely, data chain and access control (policy) chain. Data chain stores patient's healthcare data and access control chain stores the patient's defined access policies in a private BC. It preserves the confidentiality of the data by storing the hash of patient's data as transactions in the data chain. At the same time, to control access over data, patients store their desired access policy in another chain. This ensures that the data owner's access policies will remain unaltered, and access to patient's data will be controlled as expected. BCHealth uses a new clustering approach to increase the BC network throughput and improve the scalability of the network. Here, instead of considering a Cluster Head (CH) for each cluster, we introduce a hierarchical structure. Here allocate the first two bytes of the data packets to the cluster number associated with that data. Upon receiving a data packet, each cluster member will be able to identify the cluster that this data belongs to. This new approach reduces the unnecessary reliance on a CH which imposes delay and risk of a single point of failure. BCHealth is equipped with an alarm system for emergency situations, which will notify corresponding medical staff if urgent action is required based on the patient's health condition. For example, in the case of the COVID pandemic, BCHealth
could help in informing the medical staff as soon as identifying the disease symptoms for them to take appropriate actions.

[5] Ashok Kumar Das,..Present a secure fine-grained user access control scheme for data usage in the IoT environment. The proposed scheme is a three-factor user access control scheme, which supports multi-authority ABE and it is highly scalable as both the ABE key size stored in the user's smart card and ciphertext size needed for authentication request are constant with respect to the number of attributes. Under this IoT architecture, multiple smart devices together form a smart environment in which the devices are connected to the internet through the gateway node(s). The registered users can access the services of the designated smart devices through the gateway node(s) after the authentication process is completed. It is worth noting that a user may have attributes defined under multiple smart environments at the same time. In order to provide fine-grained access control in the described architecture, it is needed to define how a user is eligible to access different smart devices. As discussed previously, a natural solution to deal with this problem is the use of CP-ABE. We envision an attribute authority associated with each gateway node, and the access policy P of a smart device can be defined during its enrollment process. a user can have different roles defined by attribute authorities from different smart networks. This demands that a set of attributes, and consequently, the access policies need to be defined globally. In the proposed architecture, a user is registered with any one of the gateway node(s) (also known as the attribute

authorities), but the secret credentials should be composed with the help of all relevant (under which the user has the defined attributes) gateway node(s).

PROBLEM DEFINTION

Modern organizations encounter formidable challenges in managing their data securely within cloud environments. The paramount concern lies in preserving the confidentiality of sensitive information amidst the inherent risks of unauthorized access and data breaches. Access control management further compounds these issues, as the complexity of granting and revoking permissions for diverse user roles often leads to inefficiencies and potential security lapses. Moreover, the secure distribution of encryption keys among authorized users remains a critical hurdle, necessitating innovative solutions to ensure data integrity and privacy. Traditional centralized data storage solutions are increasingly deemed inadequate due to vulnerabilities to single points of failure and manipulation. Consequently, there is an urgent need for a comprehensive approach that integrates cutting-edge technologies to address these challenges. This project endeavors to develop a robust solution by harnessing blockchain-based data storage, ECC-based encryption, Role-Based Access Control (RBAC), and a secure key distribution mechanism. By decentralizing storage, fortifying encryption methods, streamlining access management, and ensuring secure key distribution, the project aims to provide organizations with a holistic framework for secure and efficient data management in cloud environments.

OVERVIEW OF THE PROJECT

The proposed project aims to revolutionize data management in cloud environments by integrating advanced technologies to ensure security, confidentiality, and efficiency. Leveraging blockchain-based data storage, ECC-based encryption, Role-Based Access Control (RBAC), and a secure key distribution mechanism, the project seeks to address the pressing challenges faced by organizations in safeguarding their data assets. At its core, the project focuses on decentralizing data storage to mitigate the risks associated with centralized solutions. By utilizing blockchain technology, data is distributed across a network of nodes, ensuring tamper-proof storage and resilience against single points of failure. Concurrently, ECC-based encryption techniques are employed to provide robust security for data transmission and storage. Each user and group is assigned a unique public-private key pair, ensuring secure communication and safeguarding data integrity.

Access control management is streamlined through the implementation of RBAC, where users are assigned roles based on their organizational responsibilities. Access rights are then granted or revoked based on these roles, reducing complexity and minimizing the risk of data misuse. Additionally, a secure key distribution mechanism is devised to facilitate the sharing of encryption keys among authorized users. Employing techniques such as Shamir's Secret Sharing Scheme ensures the protection of keys during distribution, even in the absence of secure communication channels. Through comprehensive testing and analysis, the project aims to evaluate the performance, security, and scalability of the proposed solution. The expected outcomes include enhanced data security, improved access control, secure key distribution, decentralized data storage, and scalability to accommodate organizational growth. Ultimately, the project endeavors to provide organizations with a robust framework for secure and efficient data management in cloud environments, paving the way for a new era of data security and integrity.

INTERFACE CONSTRUCTION

The storage scheme of medical data uses blockchain based cloud storage technology to achieve safe storage and sharing. In this module, create a local Cloud and provide priced abundant storage services. Data storage and access control are the main transactions in the medical blockchain. It would be optimal to be able to hold all medical data on the blockchain. Once get space from cloud the users can upload to share data in the cloud. In this work, the cloud storage can be implementing with high secure using block chain technology. 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

Therefore, the group owner is fully trusted by 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.

GROUP KEY VERIFICATION

Group key defines the verification key shared using as the message passing interface that used to exchanging messages to multiple systems in a parallel processing. Here proposed a new approach to access cloud using login credential and group verification based secret key for secure access of cloud storage. PKG is responsible for generating secret key and use MPI for distribution of secret keys to the user. The secret key sharing based on message passing is the concept of group authentication and verification module in cloud security system.

DATA UPLOAD AND ENCRYPTION

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

Elliptical Curve Cryptography

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. Elliptic curves are an algebraic structure and their use for cryptography. They feature properties which allow the setup of a problem similar to the well-known discrete logarithm problem of finite fields – also known as Galois fields (GF). ECC includes key agreement, encryption, and digital signature algorithms. The key distribution algorithm is used to share a secret key, the encryption algorithm enables confidential communication, and the digital signature algorithm is used to authenticate the signer and validate the integrity of the message:

ECC Algorithm Steps

Assume that those who are going through this article will have a basic understanding of cryptography (terms like encryption and decryption).

The equation of an elliptic curve is given as,

$$y^2 = x^3 + ax + b$$

Few terms that will be used,

E -> Elliptic Curve

P -> Point on the curve

n -> Maximum limit (This should be a prime number)

Key Generation

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.Now, we have to select a number **'d'** within the range of **'n'**.Using the following equation we can generate the public key

Q = d * P

d = The random number that we have selected within the range of (**1 to n-1**). **P** is the point on the curve.

'Q' is the public key and 'd' **is the private key.**

Encryption

Let 'm' be the message that we are sending. We have to represent this message on the curve. This has in-depth implementation details. All the advance research on ECC is done by a company called certicom.

Consider *'m'* has the point *'M'* on the curve *'E'*. Randomly select 'k' from [1 – (n-1)].

Two cipher texts will be generated let it be **C1** and **C2**.

C1 = k*P, C2 = M + k*Q.C1 and C2 will be send.

Decryption

We have to get back the message 'm' that was send to us,

M = C2 – d * C1 M is the original message that we have send.

Proof

How do we get back the message?

M = C2 – d * C1

'M' can be represented as 'C2 – d * C1'

C2 – d * C1 = (M + k * Q) – d * (k * P) (C2 = M + k * Q and C1 = k * P)= M + k * d * P – d * k *P (canceling out k * d * P)= M (Original Message)

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. The Data User is provided with Role-based Access Control (RBAC) policy. In our proposed system, the privileges of the Data User are reduced and the DU can only download data from the cloud. In the proposed system, to protect the sensitive information the Data Owner specifies their own access privacy policies. Access can be restricted to certain information. Apart from this, it also helps the customer to increase his confidence and provides continuous data access with the touch of a button from anywhere at any time

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 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.

USER REVOCATION

Once a user in the group is revoked, the cloud is able to resign the blocks, which were signed by the revoked user and intimate PKG to generate re-signing key. As a result, the efficiency of user revocation can be significantly improved, and computation and communication resources of existing users can be easily saved. Meanwhile, the cloud, which is not in the same trusted domain with each user, is only able to convert a signature of the revoked user into a signature of an existing user on the same block

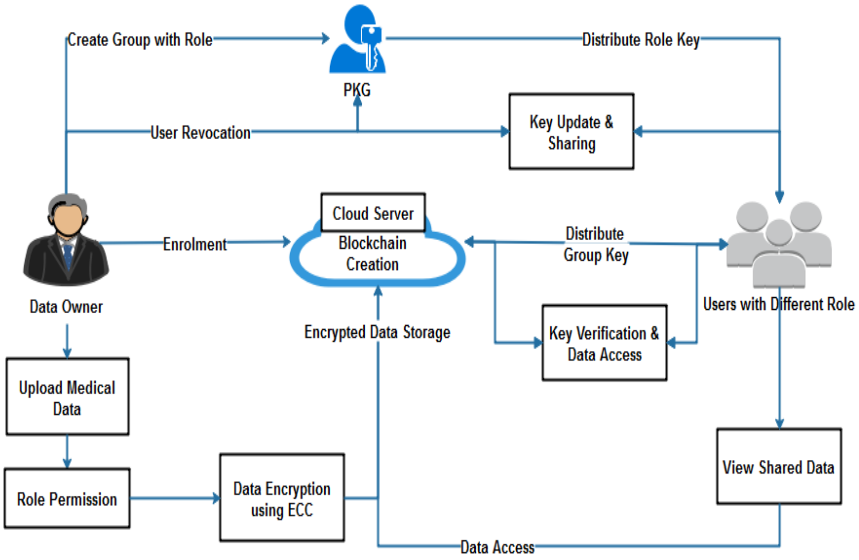
PROPOSED SYSTEM

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.

SYSTEM ARCHITECTURE

System architecture involves the high level structure of software system abstraction, by using decomposition and composition, with architectural style and quality attributes. A software architecture design must conform to the major functionality and performance requirements of the system, as well as satisfy the non-functional requirements such as reliability, scalability, portability, and availability. Software architecture must describe its group of components, their connections, interactions among them and deployment configuration of all components.

System architecture can comprise system components, the externally visible properties of those components, the relationships (e.g. the behavior) between them. It can provide a plan from which products can be procured, and systems developed, that will work together to implement the overall system. There have been efforts to formalize languages to describe system architecture; collectively these are called architecture description languages (ADLs).



CONCLUSION

This research work provides efficient access control policy based on users 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

Acknowledgment

We are grateful to Dr.v.Ravindra Krishna chandar.,Assiatant professor,CSE Department,Paavai Engineering college(Autonomous) for mentoring us to present this paper successfully

REFERENCES

[1] Bhatt, Smriti, Thanh Kim Pham, Maanak Gupta, James Benson, Jaehong Park, and Ravi Sandhu. "Attribute-based access control for AWS internet of things and secure industries of the future." IEEE Access 9 (2021): 107200-107223

[2] Banerjee, Soumya, Sandip Roy, Vanga Odelu, Ashok Kumar Das, Samiran Chattopadhyay, Joel JPC Rodrigues, and Youngho Park. "Multi-authority CP-ABE-based user access control scheme with constant-size key and ciphertext for IoT deployment." Journal of Information Security and Applications 53 (2020): 102503.

[3] Chaudhry, Shehzad Ashraf, Khalid Yahya, Fadi Al-Turjman, and Ming-Hour Yang. "A secure and reliable device access control scheme for IoT based sensor cloud systems." IEEE Access 8 (2020): 139244-139254.

[4] Dammak, Maissa, Sidi-Mohammed Senouci, Mohamed Ayoub Messous, Mohamed Houcine Elhdhili, and Christophe Gransart. "Decentralized lightweight group key management for dynamic access control in IoT environments." IEEE Transactions on Network and Service Management 17, no. 3 (2020): 1742-1757.

[5] Hossein, Koosha Mohammad, Mohammad Esmaeil Esmaeili, Tooska Dargahi, Ahmad Khonsari, and Mauro Conti. "BCHealth: A novel blockchain-based privacy-preserving architecture for IoT healthcare applications." Computer Communications 180 (2021): 31-47.

[6] Pal, Shantanu, Tahiry Rabehaja, Michael Hitchens, Vijay Varadharajan, and Ambrose Hill. "On the design of a flexible delegation model for the Internet of Things using blockchain." IEEE Transactions on Industrial Informatics 16, no. 5 (2019): 3521-3530.

[7] Panda, Soumyashree S., Debasish Jena, Bhabendu Kumar Mohanta, Somula Ramasubbareddy, Mahmoud Daneshmand, and Amir H. Gandomi. "Authentication and key management in distributed iot using blockchain technology." IEEE Internet of Things Journal 8, no. 16 (2021): 12947-12954.