E-ISSN: 2583-9667
Indexed Journal
Peer Reviewed Journal
https://multiresearchjournal.theviews.in

Received: 08-01-2024
Accepted: 19-02-2024

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH IN MULTIDISCIPLINARY

Volume 2; Issue 2; 2024; Page No. 204-210

Secure role-based access control with blockchain technology

[1]Dr. S Subashree, [2]Dr. M Priya and [3]R Srividhya

[1-3]Department of Computer Science and Engineering, E.G.S. Pillay Engineering College Nagapattinam, Tamil Nadu, India

DOI: https://doi.org/10.5281/zenodo.11514811

Corresponding Author: Dr. S Subashree

Abstract

Better resource utilization, quick speed, affordability, and accessibility for data exchange and storage are all provided by cloud computing. However, security concerns become the main barrier as data storage-possibly sensitive data-is increasingly outsourced to cloud businesses. Preserving data files encrypted before customers upload them to the cloud is a shared approach to safeguarding data confidentiality. Customers who use cloud storage services can save money on data management maintenance expenses. Data confidentiality is the main issue when outsourcing customer data to cloud storage providers. To prevent misuse of firm data, an access control system is also required. Regretfully, it might be difficult to develop a safe and efficient data exchange plan, especially for firms that are dynamic. First, in a secure way, recommend Role Based Access Control (RBAC). or key distribution without the need for any secure lines of communication, and group managers can safely provide group keys to users. One well-known access control paradigm is rolebased access control (RBAC), which maps users to roles and roles to privileges on data objects to provide flexible restrictions and database management. Using blockchain technology, an emerging technology, for data storage is the suggested remedy. First, describe the blockchain-based data storage system paradigm that includes hash and block creation. This work proposes an ECC based encryption system to solve user identity privacy and data privacy in the current access control techniques. It incorporates an anonymous control mechanism along with RBAC and cryptographic techniques. If a group member can be removed, the current group's public keys will be instantly modified, preventing the original content from needing to be re-encrypted. Individuals who are part of the group can access the cloud source; users whose access has been canceled cannot access the cloud again. Keywords: Elliptic Curve Cryptography, Cloud Storage Process, Group Creation, Role-Based Access Permission, Data Sharing, Data Encryption, Secure Data Access.

Keywords: Blockchain, affordability, data exchange, management, RBAC

Introduction

The objective of access control is to minimize the risk of unauthorized entry into both logical and physical systems. Access control is an essential aspect of security compliance programs as it guarantees the use of security technology and access control policies to safeguard private information, such as client data. Organizations typically restrict access to files, applications, computer systems, networks, and sensitive data, such as intellectual property and personally identifiable information, by implementing certain architecture and protocols. Maintaining access control systems in dynamic IT settings that combine on-premises and cloud services can be problematic due to their inherent complexity. Following many prominent cyber attacks, technology vendors transitioned from using single sign-on systems to adopting unified access management, which provides access restrictions for both on-premises and cloud environments. The objective of access control is to reduce the probability of unauthorized access to both logical and physical systems. Access control is an essential aspect of security compliance programs as it guarantees the implementation of security technologies and procedures to safeguard private information, such as client data. Many companies restrict access to their files, applications, computer systems, networks, and sensitive data, such as intellectual property and personally identifiable information, using their architecture and protocols. The complexity of maintaining access control systems in dynamic IT settings that combine on-premises and cloud services might provide challenges. The providers of technology have undergone a transformation.

Access Control Methods

Restricting access to both the resources and the system itself is the initial measure in safeguarding the data and resources of a system. Access control, however, involves more than simply restricting the individuals (subjects) who are allowed to access specific computer and network resources. Access control manages and regulates access to files, people, and other resources. It controls a user's permissions to access resources (objects) or files. Access control systems require several essential processes to be executed prior to allowing access to resources or objects in a broad sense. These processes encompass identity verification, authentication, authorization, and accountability. From the beginning of the development of computing and information technology, researchers and technologists recognized the significance of preventing users from disrupting each other on shared systems. A multitude of access control models were developed. The main determinant for authorizing users to access the system or its resources was their identification. The method was referred to as Identification Based Access Control (IBAC). However, as networks and users grew, it became evident that IBAC was inadequate to sustain such rapid growth.

The advanced topics presented were access control for owner, group, and public. Distributed systems were shown to have problems with IBAC as well. Managing access to resources and the system became challenging and prone to errors. A revolutionary mechanism called Role Based Access Control (RBAC) has been created. The system grants a user's access based on Role-based Access Control (RBAC), which is contingent upon their employment role. The least privilege principle fundamentally dictates the specific role that is allocated to a user. The position is determined by the minimum level of functionality or permissions necessary to accomplish the current task. Permissions can be added or removed when the privileges of a role are modified. However, complications developed when RBAC was deployed in different administrative domains. Reaching an agreement on the specific rights that pertain to each function was similarly challenging. As a result, a policy-driven access control system known as Attribute Based Access Control (ABAC) was created. ABAC access is granted based on verifiable user attributes, such as their date of birth or national identification number. However, reaching a consensus on a specific set of attributes can be difficult, particularly when working together with several organizations, fields, and government bodies. Every type of access restriction depends on the user's authentication upon login to the website and when making requests. They receive intermittent phone calls.

Related Work

Bhatt, *et al.*, [1] propose a formal attribute-based access control (ABAC) model for AWS IoT. This model is an extension of the existing access control model for AWS IoT, known as AWS-IoTAC model. This distinctive Attribute-Based Access Control (ABAC) paradigm facilitates the creation of detailed security policies by including attributes from many entities, such as virtual objects, themes, and Internet of Things devices. The proposed ABAC architecture utilizes the current cloud Identity and Access Management (IAM) entities, as well as components of AWS-IoTAC, with novel access control components. Here, create virtual objects in AWS IoT to represent each physical device. These things are accompanied by shadows. Multiple shadows can coexist for each object in AWS IoT. However, it is important to consider the presence of a shadow for each object in this particular situation. Attributes are assigned to each physical device, its corresponding virtual IoT item, and their shadows based on the properties of these entities. The ABAC authorization policies utilize these attributes and their corresponding values. Furthermore, categorize the objects into groups and subgroups based on their unique qualities for each category. This enables the inheritance of attributes and establishes a hierarchical structure of groups. These tasks are of an administrative nature, and the Administrative Phase will provide further detailed information about them at a later time. Physical devices need to initially register with the Amazon cloud. After being registered, these devices create a link with AWS Greengrass, which duplicates the representations of physical devices. These virtual things are on the brink. The AWS Greengrass service enables local computing by storing all device data on the edge. Data is synchronized with the cloud periodically when there is an Internet connection and/or when a user or administrator actively initiates the syncing process. The oil refinery's services and operations, such as message sending and receiving and notifying certain entities, are limited by attribute-based permission regulations. For the purpose of ensuring the safety and protection of these entities and operations, it is necessary to have policies implemented at one or more levels. In the smart oil refinery, certain policy rules are established to provide for precise access control for each type of refinery instrument. These rules enable or limit specific actions on specified devices and transmit messages to the relevant set of staff.

Chaudhry *et al.* [2] introduced a certificate-based enhanced lightweight access control and key agreement mechanism called iLACKA-IoT to ensure smooth and secure access control for Internet of Things devices. Furthermore, they claimed that LACKA-IoT has the ability to endure numerous attacks. The proposed method provides the requisite level of security and performance without necessitating any expensive pairing-based operations. A has complete control over the participants' insecure channel, allowing them to replay, erase, snoop on, and change any transmitted data. In addition, an individual can impersonate another device within the system in order to transmit a message to any other device. Power analysis can be employed to expose the parameters stored on a physically seized device. A may be an external entity or an inside one—a inquisitive mechanism. Both individuals with privileged access and those without privileged access have the ability to obtain the public system parameters, which encompass public keys and the identities of all entities inside the system (such as devices engaged in communication and certificate authorities). The private key of the certificate authority (CA) is safe and cannot be disclosed by A. The security of the proposed scheme is validated by both formal and informal methods. Specifically, it possesses reduced computation and communication expenses compared to LACKA-IoT and successfully addresses its limitations, all while providing superior security and performance in comparison to similar approaches. The access control and key establishment phases are completed by the proposed iLACKAIoT system in a brief duration of 22.4512 milliseconds, through the exchange of 2944 bits.

Yang *et al.* [3] created a non-interactive access control solution for Internet of Things environments that uses blockchain technology and PSI technology. In addition, the privacy of the data holder and user is safeguarded by hiding their characteristics, as well as protecting the confidentiality of their attributes and the access policy of both parties. In the proposed work, the data holder maintains possession of the data resources on the cloud server. In order to gain access to the data resources, a user is required to initiate a transaction to the blockchain by utilizing their own unique attribute set secret. The blockchain's smart contract will automatically execute the private set intersection (PSI) protocol to ascertain if the attribute set meets the data holder's access structure. As per the suggested approach, the data owner will establish their own blockchain access policy and a smart contract that automatically verifies the eligibility of users, instead of relying on user interaction to certify their qualifications. The data holder transfers data to a cloud server. In order to analyze the data, a user must initially submit the attributes as a transaction to the blockchain. The PSI protocol is thereafter executed by a smart contract to ascertain if the attribute set meets the threshold structure requirements. Provided that the conditions are fulfilled, the data recipient is permitted to retrieve the data held by the data provider.

After encrypting the data using their public key, the data holder then provides the user with the encrypted data address.

The BCHealth architecture suggested by Hossein *et al.* [4] enables data owners to select the access controls they prefer for their personal health information. In the field of Health, data transactions and access policies are stored in separate chains. Health encompasses two distinct chains: the data chain and the access control (policy) chain. The access control chain in a private blockchain stores the patient's defined access policies together with their medical information. The confidentiality of the data is ensured by storing the patient's data hash as transactions in the data chain. In order to regulate the access to data, patients also maintain their preferred access policy in a distinct chain. This guarantees that both the access restrictions imposed by the data owner and the availability of patient data will remain unchanged. Instead of employing a Cluster Head (CH) for each cluster, establish a hierarchical structure. Assign the initial two bytes of the data packet to the cluster number linked to that data. Upon receiving the data packet, every member of the cluster will be capable of determining its own cluster affiliation. This novel technique minimizes the unnecessary dependence on a central hub, thereby mitigating the risk of a single point of failure and reducing delays. BCHealth has implemented an emergency alarm system to promptly alert the relevant medical staff when a patient's condition requires urgent attention.

BCHealth can promptly provide information about the COVID-19 pandemic to medical professionals upon detection of the disease.

Banerjee, along with other individuals, provides a robust and comprehensive solution for controlling user access to Internet of Things data, ensuring its security. The proposed user access control technique utilizes a three-factor authentication system and is compatible with multi-authority attribute-based encryption (ABE). Since the quantity of ciphertext needed for the authentication request and the ABE key stored on the user's smart card remain constant regardless of the number of characteristics, the system is highly scalable. The gateway node(s) in this Internet of Things architecture provide connections between the different smart devices and the internet, allowing them to collaborate and create a smart environment. Once the authentication process is over, registered users can use the gateway node(s) to access the services of the chosen smart devices. It is crucial to remember that a user may exhibit characteristics that are specified in several intelligent settings. The most rational course of action to address this issue is to adopt CP-ABE, as previously suggested. It is assumed that each gateway node is linked to an attribute authority, and the registration process enables the configuration of a smart device's access policy P. A user can be assigned many roles based on the authorities derived from different smart networks. Consequently, it is required to establish a set of qualities and global access policies. In the proposed design, a user can register with any of the gateway nodes, which are also known as attribute authorities. However, all the gateway nodes that have the relevant attributes must collaborate to establish the secret credentials for the user.

Banerjee, along with a group of individuals [6], The Decentralized Lightweight Group Key Management (DLGKM-AC) architecture is an innovative approach to access control in the Internet of Things. The proposed system employs a hierarchical architecture including multiple Sub Key Distribution Centers (SKDCs) and a single Key Distribution Center (KDC) to alleviate the rekeying workload on the KDC and enhance the management of subscribers' groups. In addition, a novel approach to managing master tokens is introduced to control the distribution of keys among subscribers. When utilizing this protocol, the usage of join/leave events results in reduced processing, storage, and transmission overhead. The suggested method minimizes the risk of a single point of failure and facilitates a scalable design for the Internet of Things by lowering the burden of rekeying in the core network. A hierarchical framework consisting of a central Key Distribution Center (KDC) and many Sub Key Distribution Centers (SKDCs). DLGKM-AC lowers the overhead associated with join/leave membership changes by dividing key management responsibilities among multiple SKDCs. This allows for quicker computation and communication. Considering that the Key Distribution Center (KDC) is responsible for managing device groups and each Sub Key Distribution Center (SKDC) is responsible for managing user groups, the proposed Distributed Local Group Key Management - Access Control (DLGKM-AC) system is capable of being expanded or adjusted to accommodate growth or increased demand. In addition, the implementation of DLGKM-AC's new key management system allows users within the same group to reduce their need on rekeying. DLGKM-AC is an access management protocol that is both scalable and adaptable. It is constructed on the foundation of the GKM mechanism.

Shantanu, Pal, and others [7] Develop a delegation mechanism for the Internet of Things that is based on blockchain technology, does not require identity verification, operates independently of time constraints, and is distributed across multiple nodes. The utilization of blockchain technology has been found to have a substantial influence on the decentralized administration, verifiability, and regulation of Internet of Things (IoT) devices. Data that is immune to manipulation cannot be manipulated by a hostile actor. The primary idea is to utilize blockchain technology to streamline communication among various institutions and distribute access privileges through capabilities. The IoT devices authenticate their allocated capabilities when gaining access. As far as we know, this proposal is the first to utilize blockchain technology and capability-based access to allocate access rights in the Internet of Things without relying on a physical identity. An event is a distinct form of transaction within a blockchain network that is generated and linked to a smart contract. To ensure a reliable delegation verification, it is crucial that every event is generated by a distinct smart contract. All the fundamental security attributes of a blockchain transaction are conveyed to an event, encompassing ownership (pertaining to the smart contract responsible for its creation), immutability (the greater the difficulty in altering it, the more deeply the event is embedded in the blockchain), and shared (automatically accessible to all participants in the blockchain network). Event security and enforceability are ensured solely through ownership and immutability. The event generated by a smart contract will be securely associated with it. The event can only be utilized by the delegate, who must demonstrate ownership of the public key, which is unchangeable and includes the delegate's address. Given that a blockchain event is accessible to the whole public, it can be categorized as communicative. Ultimately, the confirmation can be obtained by simply verifying that the event was generated by a "valid" smart contract, since the delegate address included in the event is immutable. Verification occurs in a sequence of delegation.

The subject of discussion includes the panda species as well as other related topics [8]. Propose a strategy for the efficient and secure generation and upkeep of cryptographic keys to enable mutual authentication across communication entities. The suggested method employs a one-way hash chain technique to furnish a collection of public and private key pairs to the IoT devices. This enables the key pairs to autonomously authenticate themselves at any given moment. The architecture consists of three levels: the Device, Fog, and Cloud layers. The Device layer of the Internet of Things encompasses intelligent devices that are employed in many use cases, including wearable medical devices that are capable of remotely sensing, monitoring, and observing a patient's health status. These encompass gas and temperature sensors, along with security cameras designed for automated residences and commercial establishments. The implementation of the Fog layer aimed to enhance performance and reduce device overhead and computation time due to the inherent resource limitations of the devices. The Fog layer houses several access management nodes (AMNs) that possess shared computing and storage capabilities, which are used to control the devices in the Device layer. Devices with similar purposes are grouped into categories, each of which is supervised by an AMN. Similarly, under the Fog layer, a group of Autonomous Management Nodes (AMNs) are consolidated to establish a network. Their primary responsibility is to create, distribute, and oversee the secret keys for the devices that are linked to them. Furthermore, AMNs function as miners, consolidating device transactions that occurred within a designated timeframe into a fresh block. Subsequently, the Fog layer is connected to the Cloud layer by high-speed network connectivity. The cloud layer manages many blockchains, each belonging to the AMN network of the Fog layer. Consequently, a significant quantity of nodes possessing substantial computing capabilities, referred to as management nodes or MNs, are incorporated into the cloud layer to manage Internet of Things use cases that require high scalability and limited resources. The Access Management Nodes (AMNs) are responsible for managing communications within a specific network, while the Management Nodes (MNs) at the cloud layer are responsible for facilitating transactions between different networks. In addition, the MNs store the encrypted data generated by the lower layer devices, which can only be accessed after undergoing the necessary authentication procedure.

Yang and his colleagues, The user's text is "[9]". Develop a data access control plan that ensures fairness and equality for edge blockchain-enabled smart grid applications. In a consortium blockchain system, the edge nodes are responsible for processing the computational activities that are not performed by the end user devices. Implement an on-chain/off-chain technique in this scenario to ensure adaptable data sharing. It is recommended to integrate edge computing and blockchain technology to delegate computing tasks to the consortium blockchain using smart contracts. To ensure the precision of the computation results, edge nodes, who serve as endorsers, are responsible for executing smart contracts. Moreover, using the blockchain technology to ensure accountability for malicious conduct. Specifically, the proposed plan can ensure fairness in holding all semi-trusted entities accountable by including them within its scope. The combination of the (t, n) secret sharing approach with CP-ABE enables the implementation of distributed authority-based data access control. The proposed method is suitable for facilitating data transfer across IoT devices with varying levels of computational capacity, as it offloads the processing tasks of end user devices to edge nodes in EB. Blockchain ensures the traceability of computing results, thereby holding individuals liable for any misconduct. In order to ensure equitable responsibility, the accountability scope encompasses all semi-trusted entities. Moreover, the decentralized authority has the ability to bypass the centralized authority's vulnerability of having a single point of failure.

Khan and his colleagues [10]. This work aims to develop a robust and streamlined Attribute-Based Encryption (ABE) architecture that delegates complex encryption and decryption tasks while ensuring high levels of security. In order to put the suggested method into practice, it replaces expensive pairing processes with elliptic curve scalar point multiplication as the underlying technology of Attribute-

Based Encryption (ABE). The MAA serves as the primary source for generating cryptographic keys and is the sole entity in the system paradigm that is completely trusted. KGC oversees the registration process for all system users. When Su is given a set of characteristics, it generates secret key components (SK), public parameters (PARAMS), and a system master key (SMK) as part of the startup process. DSP provides a limited decryption service to MDUs that are interested, without having knowledge of the precise data contents. Consider the honest-but-curious threat paradigm, which is commonly employed by most ABKS schemes. This approach involves executing the algorithm in a truthful manner and deducing confidential information based on the already accessible facts. The suggested system paradigm completely trusts the medical attribute authority and the data owner (DO) as authoritative entities. Another concern pertains to the interactions among users who possess corrupted data (DU). The selective-set security model is commonly used to demonstrate the security of an Attribute-Based Encryption (ABE) system. This model involves a game where an attacker (A) and a challenger (C) participate. In order to address the underlying security assumption of this game, the attacker must successfully overcome the difficulties presented by the challenger.

Background Work

The primary subjects of the proposed architecture, known as Dynamic Secure Access Control utilizing Blockchain (DSA-Block), are the secure access control and secure data sharing facilitated by blockchain technology. Hyper elliptic curve cryptography (HECC) is employed for the purpose of authenticating nodes and users. The entities involved are maintained in a private local ledger (LL) to enhance security and mitigate the effects of external attacks. Authentication-based request filtering, implemented through a Gateway (GW), reduces latency and increases throughput by verifying the legitimacy of requests using a timestamp. The edge server utilizes Rock Hyraxes Swarm Optimization (RHSO) to delegate access, considering factors such as trust, energy, load, and resource availability (RA). Blockchain is utilized to assess the level of trust, hence enhancing the efficiency of consensus, block validation, and response times. The data is securely shared by uploading it to the cloud server and employing a differential privacy method to enhance the attack detection rate. Revocation is now implemented for both users and user characteristics to enhance security. User attributes are revoked based on the trust value, which also increases the rate of detecting attacks. The revocation process considers the expiry time and attribute updating.

Several crucial user and device characteristics were utilized to authenticate devices, users, gateways (GWs), and edge nodes (ENs), hence enhancing security for both users and nodes. The HECC method is employed to produce both private and public keys, enabling the use of smaller keys while maintaining security. This strategy can be advantageous in IoT scenarios with restricted resources. The hierarchical architecture-based strategy utilizes both global domain authorities (GDAs) and local domain authorities (LDAs) to achieve the decentralized management of authorization. The RHSO method is utilized to select the delegator nodes based on their trust value, energy level, traffic load, and RA, ensuring an efficient selection process. The consensus process utilizes selected delegator nodes to execute access control, hence enhancing network scalability. Initially filtering the queries reduces the burden on the gateway. The Trusted PBFT protocol selects trusted nodes to achieve consensus. The greatest number of nodes that can participate in the consensus is limited by the total number of nodes. This reduces the time required for block validation and provides protection against malicious nodes.

Role based access control and user revocation with blockchain technology

It is crucial that only individuals with proper authorization are able to access data stored in the cloud in order to allow the sharing of data. Cloud-based secure group sharing. The main objective of the proposed undertaking was the application of Blockchain Technology. When a data owner desires to distribute their data to the group, they transmit the encryption key to each member of the group. Group members have the ability to retrieve encrypted data from the Cloud and decrypt it using a key, eliminating the need for assistance from the data owner. The proposed work focuses on decentralized blockchain-based Electronic Health Records (EHRs) that utilize an ECC encryption approach. Each authority is responsible for utilizing their designated Role to retrieve data within their own system. Put simply, the user's different duties are granted increased power based on their respective positions. The hybrid cloud architecture comprises a public cloud where encrypted data and public parameters pertaining to the role-based access control with encryption system are stored, and a private cloud that holds sensitive hospital role hierarchies and patient memberships. Interactions between users seeking access to encrypted data and data owners who wish to encrypt their own data exclusively on the public cloud. The administrator specifies the role managers responsible for overseeing user membership relationships and the role hierarchy. Develop a mechanism for upgrading cryptographic keys and establish a procedure for securely revoking user access. When a user is removed from the group, the group key is modified and distributed to all users in the current data access pattern. Moreover, it is difficult to allocate specific portions of administrative authority across all of these systems.

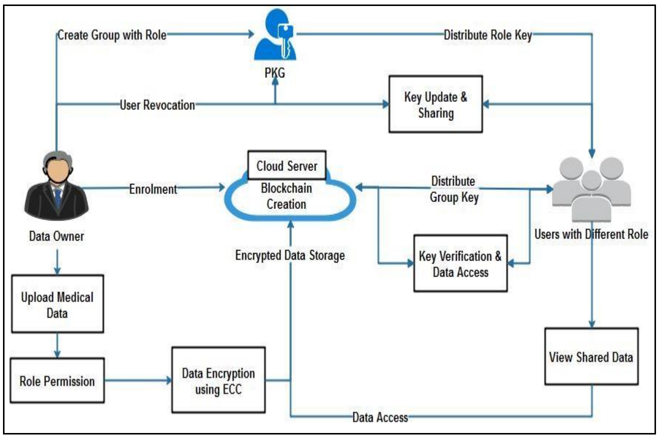

Fig 1: Proposed Framework

Interface Construction

The medical data storage plan employs blockchain-based

cloud storage technology to guarantee secure storage and sharing. Create a localized cloud infrastructure that provides affordable and abundant storage services within this module. Access control and data storage are the main transactions in the medical blockchain. Storing all medical data on the blockchain would be optimal. Once users have available storage space on the cloud, they can upload and share data with others. This project employs blockchain technology to establish a highly secure method for implementing cloud storage. The proposed secure data exchange architecture will enable group owners and members to engage in communication with one another.
Group Owner takes charge of followings,

1. System parameters generation
2. User registration
3. User revocation

As a result, everyone else has complete faith in the group owner. The admin is the group owner. All cloud-based process logs are accessible to the group owner. Both user registration and user revocation are under the purview of the group owner.

Group Key Verification

The phrase "group key" refers to a shared verification key that is used as a means of communication for exchanging messages simultaneously with many systems. This article presents an innovative approach to securely accessing cloud storage. It involves employing a secret key that is based on group verification, together with login credentials. PKG is responsible for generating cryptographic keys, which are subsequently disseminated to users through MPI. The group authentication and verification module in cloud security systems operates by exchanging secret keys through message transit.

Data Upload and Encryption

DO is a cloud customer who enrolls with the cloud service provider, also known as CSP.The data sent by DO is encrypted before being transmitted to the cloud. When acquiring the required authentication, ensure that you authenticate yourself to the cloud in an anonymous manner. The role of the DO is to prevent the addition of harmful DOs to the cloud. The individual or entity who possesses the data transfers the data that has been transformed into a coded form to the cloud storage system. The Data Owner (DO) has the capability to utilize encryption.

Role Based Access Control

Role-based access control (RBAC) is a system that grants users access to a system based on their organizational roles. An analysis is conducted on the system requirements of a workforce, and users are categorized into roles based on shared job duties and system access requirements. Subsequently, individuals are granted access solely in accordance with the job they have been designated. Complying strictly with the access requirements provided to each role greatly simplifies access management. The Data User is assigned the Role-based Access Control (RBAC) policy. The proposed method curtails the privileges of the Data User and confines them to solely retrieving data from the cloud. The proposed method enables the Data Owner to define their own access privacy policies to protect confidential data. There may be restrictions on accessing some information.

Data Access

In order to utilize the cloud service, a user must undergo the process of authentication. The predominant security approach for accessing data involves authentication through the verification of login credentials, including the combination of a username and password. The user provides their login and password to the cloud server, which then authenticates the user's identity. Users can only search files from the cloud if they have been authorized by the service provider; otherwise, they are not allowed to search files. Users can get their stored data from cloud storage from any location. When a new individual joins the group, this procedure can be utilized to obtain the file and distribute the group key to the new member, allowing them to promptly receive the encrypted data file. A cryptographic key is generated and transmitted to the user's cellphone number when the file is being downloaded. This key can subsequently be used by the user to retrieve the data.

User Revocation

Once a group member is expelled, the cloud has the ability to reassign the blocks that were previously signed by the expelled user and inform the PKG (Public Key Generator) to generate a new signing key. Consequently, the efficiency of user revocation may be greatly increased, and the computer and communication resources of present users can be readily preserved. Currently, the signature of a user whose access has been revoked can only be modified to match that of another user within the same block by the cloud. However, it is important to note that this cloud is not within the same trusted domain as each user.

Methodology

Elliptic Curve Cryptography

Elliptical curve cryptography (ECC) is a cryptographic method for generating public key encryption keys that is faster, more compact, and more efficient. The foundation of this is rooted on the principles of elliptic curve theory. ECC leverages the characteristics of the elliptic curve equation instead than relying on the conventional approach of generating keys through the multiplication of extremely large prime numbers. The majority of public key encryption algorithms, such as RSA and Diffie-Hellman, are compatible with the system. According to several researchers, ECC has the capability to attain a security level equivalent to that of a 1,024-bit key in other systems, using just a 164-bit key. The utilization of ECC in mobile applications has become increasingly common due to its ability to provide comparable security with reduced battery consumption and computing resources. An elliptic curve, which is an algebraic structure, is used in cryptography. A problem similar to the widely recognized discrete logarithm problem in finite fields, commonly referred to as Galois fields (GF), can be created based on their characteristics.Elliptic Curve Cryptography (ECC) encompasses methods for establishing shared secret keys, encrypting data, and verifying digital signatures. The digital signature method ensures the integrity of the message and confirms the identity of the signer, while the key distribution algorithm facilitates the sharing of a secret key and enables secure private communication:

General Procedure of ECC

- Both parties consent to certain publicly available data elements.
- The equation for an elliptic curve
- Values of *a* and *b*
- Prime, *p*
- The elliptic group determined by using the equation for the elliptic curve
- A base point from the elliptic group, B
- Comparable to the generator employed in contemporary cryptosystems o Every user creates their own pair of public and private keys.
- Private Key = an integer, x, selected from the interval [1, p-1]
- Public Key = product, Q, of private key and base point (Q = x*B)

Encryption

1. Explain what a curve is.
2. For both the sender and the recipient, generate a public private key pair using that curve. 3. From the key pair, create a shared secret key.
3. Create an encryption key using that shared secret key.
4. Encrypt the data you want to send using the asymmetric encryption technique and that encryption key.

Decryption

The sender and recipient will equally utilize the equal curve form, or the sender and recipient will share the curve. Additionally, sender will give recipient access to its public key.

1. Using the same curve as the receiver, generate a public personal key pair.
2. Using the sender's public key and the recipient's private key, regenerate a shared secret key.
3. Create an encryption key using that shared secret key.
4. Decrypt the data using the symmetric encryption algorithm and that encryption key.

Conclusion

This research project utilizes the ECC encryption technique to produce secure encryption and provides efficient access control policies based on users' roles. In order to safeguard the confidentiality of data, it is imperative to implement robust access control measures for cloud storage. Our organization offers a Role-Based Access Control (RBAC) framework that allows for secure storage of data on a public cloud. The proposed RBE solution, which combines Role Based Access Control with Encryption, effectively manages user revocation and decryption. To ensure safe communication, we also provide group verification to both the user and the data owner. Time-based access permissions can be employed to improve access control. The proposed system integrates the traditional Role-Based Access Control (RBAC) concept with the Risk-Based Evaluation (RBE) method. The role hierarchy is utilized to enhance the efficiency of user revocation and decryption procedures. Consequently, this system will provide enhanced security.

References

1. Bhatt S, Pham TK, Gupta M, Benson J, Park J, Sandhu R. Attribute-based access control for AWS internet of things and secure industries of the future. IEEE Access. 2021;9:107200-107223.
2. Chaudhry SA, Yahya K, AlTurjman F, Yang MH. A secure and reliable device access control scheme for IoT based sensor cloud systems. IEEE Access. 2020;8:139244-139254.
3. Yang Q, Zhang M, Zhou Y, Wang T, Xia Z, Yang B. A non-interactive attribute-based access control scheme by blockchain for IoT. Electronics. 2021;10(15):1855.
4. Hossein KM, Esmaeili M, Dargahi T, Khonsari A, Conti M. BCHealth: A novel blockchain-based privacy-preserving architecture for IoT healthcare applications. Computer Communications. 2021;180:31-47.
5. Banerjee S, Roy S, Odelu V, Das AK, Chattopadhyay S, Rodrigues JJPC, Park Y. Multi-authority CP-ABE-based user access control scheme with constant-size key and ciphertext for IoT deployment. Journal of Information Security and Applications. 2020;53:102503.
6. Dammak M, Senouci SM, Messous MA, Elhdhili MH, Gransart C. Decentralized lightweight group key management for dynamic access control in IoT environments. IEEE Transactions on Network and Service Management. 2020;17(3):1742-1757.
7. Pal S, Rabehaja T, Hitchens M, Varadharajan V, Hill A. On the design of a flexible delegation model for the Internet of Things using blockchain. IEEE Transactions on Industrial Informatics. 2019;16(5):3521-3530.
8. Panda SS, Jena D, Mohanta BK, Ramasubbareddy S, Daneshmand M, Gandomi AH. Authentication and key management in distributed IoT using blockchain technology. IEEE Internet of Things Journal. 2021;8(16):12947-12954.
9. Yang W, Guan Z, Wu L, Du X, Guizani M. Secure data access control with fair accountability in smart grid data sharing: An edge blockchain approach. IEEE Internet of Things Journal. 2020;8(10):8632-8643.
10. Khan S, Iqbal W, Waheed A, Mehmood G, Khan S, Zareei M, Biswal RR. An efficient and secure revocation-enabled attribute-based access control for eHealth in smart society. Sensors. 2022;22(1):336.