

Secure Role Based Access Control Using Blockchain And ECC Cryptography

Mr. Joseph S¹, Ms. Karthika M², Ms. Abirami P³, Mrs. Roy Sudha Reetha P⁴

¹Assistant Professor, Dept of Electronics and Communication Engineering

^{2,3}Dept of Electronics and Communication Engineering

⁴Assistant Professor, Dept of Artificial Intelligence and Data Science

^{1, 2, 3}Christian College of Engineering and Technology

⁴PSNA College of Engineering and Technology.

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. 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 model which provides flexible controls and database management by having users mapped to roles and roles mapped to privileges on data objects. The proposed solution is to make use of the emerging technology of blockchain to data storage. First, define the system model of blockchain-based data storage with block and hash creation in the setting of blockchain. 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. If the group member can be revoked means, automatically change public keys of existing group and no need encrypt again the original data. 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- Cloud Networking, RBAC Communication.

I. INTRODUCTION

A. ABOUT THE PROJECT

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 to kPSMens or other authentication factors. Multifactor authentication, which requires two or more authentication factors, is often an important part of layered defense 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.

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.

B. PROBLEM DEFINITION

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.

C. PROJECT SCOPE

The goal of access control is to minimize the risk of unauthorized access to physical and logical systems. Access control is a fundamental component of security compliance programs that ensures security technology and access control policies are in place to protect confidential information, such as customer data. Most organizations have infrastructure and procedures that limit access to networks, computer systems, applications, files and sensitive data, such as personally identifiable information and intellectual property.

Access control systems are complex and can be challenging to manage in dynamic IT environments that involve on-premises systems and cloud services. After some high-profile breaches, technology vendors have shifted away from single sign-on systems to unified access management,

which offers access controls for on-premises and cloud environments.

D. OVERVIEW

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.

II. LITERATURE SURVEY

Román-Martínez, Isabel, and Rafael M. Estepa-Alonso, et al. [1] propose a service oriented architecture, backed by blockchain technology, that enables: (1) tamper-proof and immutable storage of subject of care consents; (2) a fine-grained access control for protecting health data according to consents; and (3) auditing tasks for supervisory authorities (or subjects of care themselves) to assess that healthcare organizations comply with GDPR and granted consents. Standards for health information exchange and access control are adopted to guarantee interoperability. Access control events and the subject of care consents are maintained on a blockchain, providing a trusted collaboration between organizations, supervisory authorities, and individuals. A prototype of the architecture has been implemented as a proof of concept to evaluate the performance of critical components. The application of subject of care consent to control the treatment of personal health data in federated and distributed environments is a pressing concern. Blockchain-based support for auditing services that could be used by supervisory authorities or SoCs for assessing GDPR compliance. Using blockchain brings an immutable and tamper-proof ledger for consent and access control decisions for auditing. Fine-grained backward access control model and service to protect personal health data in healthcare SOA. This direct auditing method eases third-party assessment of GDPR compliance performed by organizations storing personal health data. In addition, a fine-grained backward access control decision model is proposed to address the requirements of complex FHIR interactions. Furthermore, the adoption of standards enhances the interoperability and openness required for distributed environments. Finally, the experimental results validate the feasibility of using a blockchain-supported architecture for consent management, access control, and auditing in the health domain.

Fugkeaw, Somchart, et al. [2] implemented a lightweight collaborative ciphertext policy attribute role-based encryption (LW-C-CP-ARBE) scheme to support a fine-grained and lightweight access control for mobile cloud environment. Apply CP-ABE approach as a core cryptographic access control and introduce a new proxy re-encryption (PRE) protocol to reduce data re-encryption and decryption cost for the mobile users. In LW-C-CP-ARBE, we extend the CP-ABE scheme and develop more supporting protocols to support both read and write access with the

preserved data privacy and secure policy sharing in the mobile cloud environment. The relying parties (DOs, DUs, Proxy) can call the functions from LW-C-CP-ARBE to execute the crypto operations (key generation, encryption, decryption). The system manages the user decryption keys (UDKs) generated from the attributes issued by AAs in the way that all UDKs are delivered to the users upon their access. Hence, DUs do not need to hold their UDKs, they are only responsible to retain the private key issued by the CA. This supports flexibility and scalability of user key management. In the mobile cloud access control system, we introduce the proxy to perform the heavy crypto operations (decryption, re-encryption) of CP-ABE. When there is a re-encryption request, the proxy will check the privilege of user through the encrypted access control policies sent by the LW-C-CPARBE. If the user has the write privilege, he/she can use their mobile devices to update and re-encrypt the data efficiently with the assistance of the dedicated proxy and our LW-C-CPARBE.

Zhang, Yiran, and Li Lu, et al. [3] proposed an efficient data integrity verification scheme for multi-cloud storage services by using blockchain technology. The overall verification can verify the integrity of multiple CSPs, which solves the problems of low computational efficiency. Local verification can trace the source to the specific damaged CSP, which is more secure and reliable. Since the information on the blockchain can be regarded as immutable and traceable, this paper puts the data verification process directly in the blockchain for public execution and provides data integrity verification services without the assistance of any third-party audit platform, avoiding the security problems caused by untrusted TPA. In addition, the integrity verification of multiple CSPs for multiple DOs is realized by the overall verification, which solves the problems of low computational efficiency. The specific CSP with integrity damage is traced by local verification, which solves the problem of tracing malicious CSPs in distributed cloud storage. This scheme stores the aggregate signatures and local signatures of encrypted data in the blockchain, and the verification process is carried out publicly in the blockchain. Therefore, anyone in the blockchain network can serve as a public auditor, and the verification results can be repeatedly authenticated by them, resulting in the extensive recognized of verification results. In addition, the blockchain will publish the CSP with missing data integrity to supervise the CSP to guarantee the data integrity.

Hao, Jialu, and Xuemin Shen, et al. [4] presented an efficient attribute-based access control with authorized search scheme (EACAS) in cloud storage by extending the anonymous key-policy attribute-based encryption (AKP-ABE) to support fine-grained data retrieval with attribute privacy

preservation. Specifically, by integrating the key delegation technique into AKP-ABE, EACAS enables data users to customize search policies based on their access policies, and generate the corresponding trapdoor using the secret key granted by the data owner to retrieve their interesting data. In addition, a virtual attribute with no semantic meaning is utilized in data encryption and trapdoor generation to empower the cloud to perform an attribute-based search on the outsourced ciphertext without knowing the underlying attributes or outsourced data. The data owners can achieve fine grained access control on their outsourced data, and the data users are flexible to search their interesting data based on protected attributes through customizing the search policies. The ciphertext is generated as two parts: (1) the original data encrypted under the original attribute set; (2) a trivial data “1” encrypted under the original attribute set added with the virtual attribute. While in the trapdoor, the virtual attribute is bound with the root node of the search tree through an AND gate, which makes it prerequisite for successful matching. When performing search on the ciphertext, DSS is able to retrieve the ciphertext whose attribute set satisfies the search policy by testing whether the trivial data “1” can be recovered, but cannot decrypt the ciphertext of the original data which is encrypted without the virtual attribute. As a result, EACAS is able to achieve fine-grained access control with authorized search on the data outsourced to cloud; simultaneously the data confidentiality and attribute privacy are protected effectively.

Bakas, Alexandros, and Alexandr Zaliztko, et al. [5] the proposed solutions are based on the properties of the underlying ABE scheme and hence, the revocation costs grow along with the complexity of the policies. To this end, here use these two cryptographic techniques that squarely fit cloud-based environments to design a hybrid encryption scheme based on ABE and SSE in such a way that we utilize the best out of both of them. In the Setup phase, all entities receive a public/private key pair that will be used to establish secure communication channels. During the Initialization phase, a data owner encrypts her data using the SSE scheme, uploads the encrypted files to the CSP, and encrypts the SSE key using an ABE key. The ciphertext of the key is bound by a policy specified by the user and it is stored on the Key Tray. In the Key Sharing phase, different users contact the Key Tray and request for the ciphertext of the symmetric key. Upon receiving the ciphertext, they can decrypt it if and only if their attributes satisfy the policy bound to the key. If the decryption of the key is successful, then the Data Processing phase commences where the users can search for different files, add new ones or delete existing ones, according to their access right (scopes). Finally, in the Scope Management phase, a data owner can modify the scopes of the users and even fully

revoke their right to access the encrypted dataset. Proposed construction allows a data owner to share her data in a privacy-preserving way and manage the access rights of the rest of the users. Moreover, here show that we can rely on the functionalities offered by Intel SGX, to design an access control mechanism that is agnostic to the underlying cryptographic primitives. In addition to that, we strongly believe that cloud-based services will rely less on traditional decryption of information, and more on computations over encrypted data.

III. 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.

IV. 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.

A.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.

V. SYSTEM DESIGN

The System Design describes the system requirements, operating environment, system and subsystem architecture, files and database design, input formats, output layout, detailed design, processing logic, and external interfaces, if applicable. A further view sees system analysis as a problem-solving method that splits down a system into its element pieces for the idea of the studying how well those component parts work and interact to accomplish their purpose.

Systems design entails a systematic approach to the design of a system. Systems design is the progression of defining elements of a system like modules, architecture, components and their interfaces and data for a system based on the specific requirements. It is the procedure of defining, developing and scheming systems which satisfies the specific requirements and necessities of a business or organization.

System design is “The process of studying a procedure or business in order to identify its goals, purposes and create systems and procedures that will achieve them in an efficient way”; Another view sees system analysis as a problem-solving technique that breaks down a system into its component pieces for the purpose of the studying how well those component parts work and interact to accomplish their purpose.

The field of system analysis relates closely to requirements analysis or to operations research. It is also “an

explicit formal inquiry carried out to help a decision maker identify a better course of action and make a better decision than she might otherwise have made”.

Systems design is the process of defining the architecture, modules, interfaces, and data for a system to satisfy specified requirements. Systems design could be seen as the application of systems theory to product development. There is some overlap with the disciplines of systems analysis, systems architecture and systems engineering.





Design Notation:

Design notations are used when planning and should be able to communicate the purpose of a program without the need for formal code. Commonly used design notations are:

- Data Flow Diagram
- Entity Relationship Diagram

A. DATA FLOW DIAGRAM

A data flow diagram is a two-dimensional diagram that explains how data is processed and transferred in a system. The graphical depiction identifies each source of data and how it interacts with other data sources to reach a common output. Individuals seeking to draft a data flow diagram must identify external inputs and outputs, determine how the inputs and outputs relate to each other, and explain with graphics how these connections relate and what they result in. This type of diagram helps business development and design teams visualize how data is processed and identify or improve certain aspects.

Symbol	Description
	An entity . A source of data or a destination for data.
	A process or task that is performed by the system.
	A data store , a place where data is held between processes.
	A data flow .

Data flow Symbols:

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

Level 0

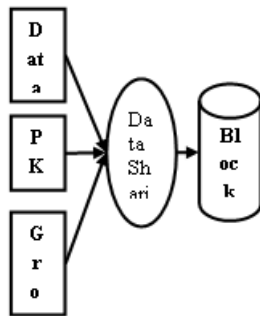


Fig 1 DFD LEVEL 0

Level 1

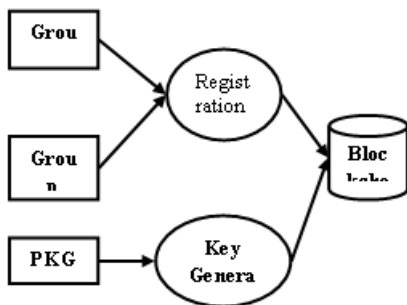


Fig 2 DFDLEVEL 1

Level 2

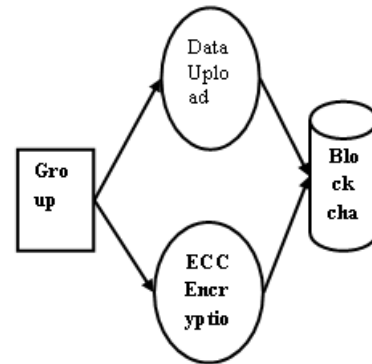


Fig 3 DFD LEVEL 2

Level 3

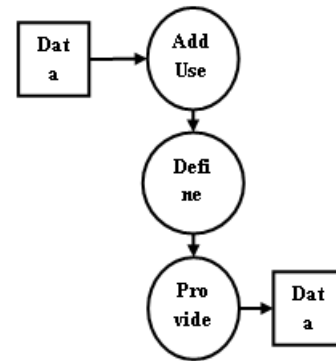


Fig 4 DFD LEVEL 3

Level 4

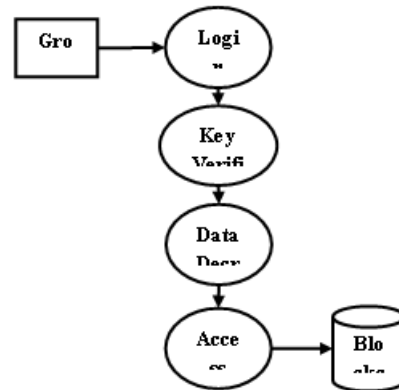


Fig 5 DFD LEVEL 4

Level 5

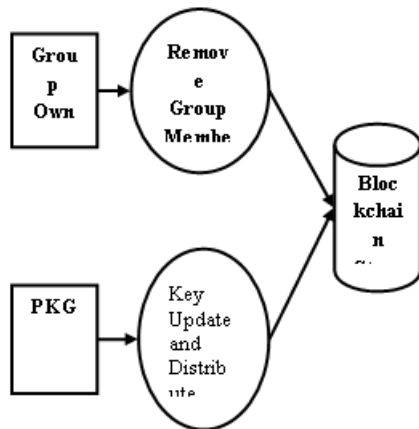
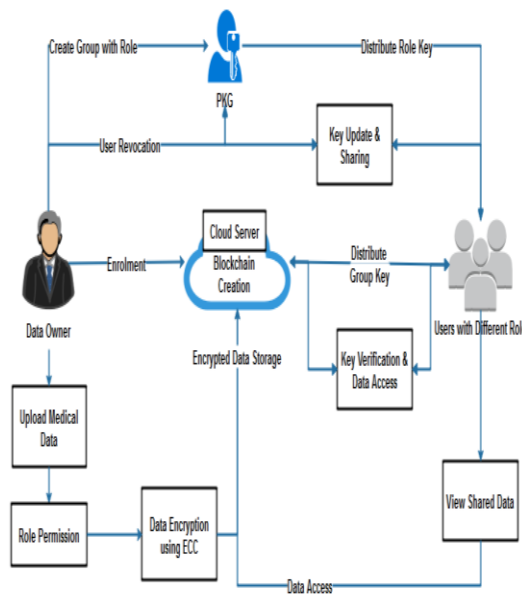


Fig 6 DFD LEVEL 5

VI. BLOCK DIAGRAM



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.

A. INPUT DESIGN

In an information system, input is the raw data that is processed to produce output. During the input design, the developers must consider the input devices such as PC, MICR,

OMR, etc. Therefore, the quality of system input determines the quality of system output. Well-designed input forms and screens have following properties –

- It should serve specific purpose effectively such as storing, recording, and retrieving the information.
- It ensures proper completion with accuracy.
- It should be easy to fill and straightforward.
- It should focus on user’s attention, consistency, and simplicity.
- All these objectives are obtained using the knowledge of basic design principles regarding –

- What are the inputs needed for the system?
- How end users respond to different elements of forms and screens.

Objectives for Input Design

The objectives of input design are –

- To design data entry and input procedures.
- To reduce input volume
- To design source documents for data capture or devise other data capture methods.
- To design input data records, data entry screens, user interface screens, etc
- To use validation checks and develop effective input controls.

B. OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user.

Efficient and intelligent output design improves the system’s relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2. Select methods for presenting information.

3. Create document, report, or other formats that contain information produced by the system.

VII. 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.

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] 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.
- [3] Yang, Qiliang, Mingrui Zhang, Yanwei Zhou, Tao Wang, Zhe Xia, and Bo Yang. "A non-interactive attribute-based access control scheme by blockchain for IoT." *Electronics* 10, no. 15 (2021): 1855.
- [4] 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.
- [5] 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.
- [6] 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.
- [7] 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.
- [8] 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.
- [9] Yang, Wenti, Zhitao Guan, Longfei Wu, Xiaojiang Du, and Mohsen Guizani. "Secure data access control with fair accountability in smart grid data sharing: An edge blockchain approach." *IEEE Internet of Things Journal* 8, no. 10 (2020): 8632-8643.
- [10] Khan, Shahzad, Waseem Iqbal, Abdul Waheed, Gulzar Mehmood, Shawal Khan, Mahdi Zareei, and Rajesh Roshan Biswal. "An efficient and secure revocation-enabled attribute-based access control for eHealth in smart society." *Sensors* 22, no. 1 (2022): 336.