IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205321 |

Privacy Preserving Public Auditing for Secure Data Sharing with Confidential Information Hiding using Cloud Computing

Darshan Raut[1], Akash Wadghane[2], Sameer Pathan[3], Prof. Avhad G.T[4]

Student, Department of Computer Engineering, Vishwabharati Academy's COE, Ahmednagar, Maharashtra India[1-3]

Assistant Professor, Department of Computer Engineering, Vishwabharati Academy's COE, Ahmednagar, Maharashtra, India[4]

ABSTRACT: Nowadays, data integrity maintenance is the major objective in cloud storage. It includes auditing using a third-party auditor for unauthorized access. To implements this work for protecting the data and regeneration of data if someone mishandles it. This job will be assigned to a Proxy server. User's confidential data will be stored in public and private areas of the cloud. So that only public cloud data will be accessed by the user and private cloud will remain more secure. As soon as any unauthorized modification is made, the original data inside the private cloud might be retrieved with the aid of theProxy server proxy server and could be back to the consumer. Cloud storage generally provides different redundancy configurations to users to maintain the desired balance between performance and fault tolerance. Data availability is essential in distributed storage systems, especially when node failures are common in real life. This research work explores secure data storage and sharing using the proposed AES 128 encryption algorithm and Role Base Access Control (RBAC) for secure data access schemes for the end-user. This work also carried out a backup server approach it works like a proxy storage server for ad hoc data recovery for all distributed data servers. The experiment analysis has been proposed in public as well as a private cloud environment.

KEYWORDS: Advanced Encryption Standard (AES), Proxy Key Generation, Role Base Access Control (RBAC), SHA256 encryption scheme; Secure user access policy, etc.

I. INTRODUCTION

Now a day's cloud storage is used to store and retrieve data that is based on the internet, instead of local storage devices for more reliable, secure, and availability of data. But data is very important and should not be revealed to any unauthorized person, for this purpose encryption method is used to convert this plain data into ciphertext and a decryption method is used to convert that cipher text into plain text to get back the original data. So, the encryption algorithm plays the most important role to make data more secure [2]. This research work explores secure data storage and sharing using the proposed AES 256 bit encryption algorithm and SHA-256 algorithm for Role Base Access Control (RBAC) for a secure data access scheme for the end-user. This work also carried out a backup server approach it works like a proxy storage.Server for ad hoc data recovery for all distributed data blocks. The experimental analysis has been proposed in public as well as private server storage environments. [1] Fig.1 shows the overall system overview.

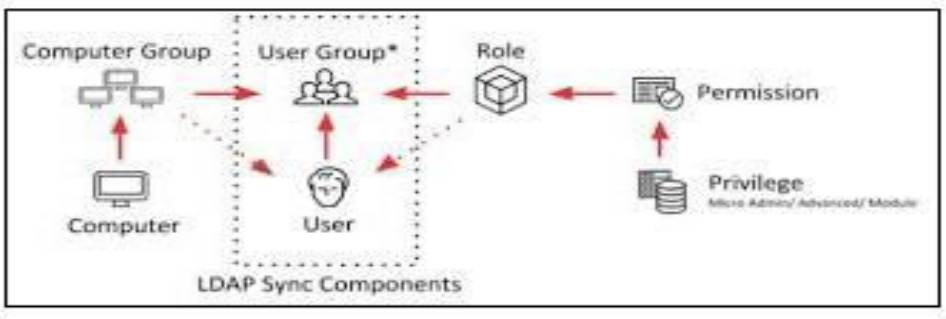


Fig.1: System Overview

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205321 |

The system depicts the principle plan objectives of the proposed plan including key circulation, information secrecy, access control, and effectiveness as takes after: Key Distribution: The prerequisite of key transportation is that clients can competently get their personal / private keys from the gathering director without a Certificate Authorities. In other existing plans, this purpose is skillful by expecting that the communication channel is secure, on the other hand, in our plan, the system can accomplish it without this solid thought. Access control: first, gather individuals can employ the cloud asset for records stockpiling and data sharing. Second, unapproved clients can't get to the cloud asset each time, and disavowed clients can be unfitted for utilizing the cloud asset again as soon as they are renounced [5].

II. RELATED WORK

In the existing system, a user can be a Data Owner and a Data Consumer simultaneously. Masteryis assumed to have effective computation competencies, and they're supervised by way of authorities places of work due to the fact some attributes partially comprise users' personally identifiable data records. The whole attribute set is split into N disjoint sets and controlled by means of each authority, consequently each authority is aware about most effective a part of attributes. A Data Owner is the entity that wishes to outsource encrypted data files to the Cloud Servers [4]. The Cloud Server, which is assumed to have adequate storage capacity, does nothing but storing them. Newly joined statistics clients request private keys from all of the authorities, and they do now not recognize which attributes are manage dthrough which authorities. When the Data Consumers request their private keys from the authorities, authorities together create the corresponding private key and send it to them [3]. All Data Consumers can download any of the encrypted data files, but only the ones whose private keys fulfill the privilege tree Tp can execute the operation related with privilege p. The server is delegated to execute an operation p if the person's credentials are proven through the privilege tree Tp.

III. ALGORITHMS & METHODOLOGY

A. AES Algorithm (Advanced Encryption Standard):

Now a day's cloud storage is used to store and retrieve data that is based on the internet, instead of local storage devices for more reliable, secure, and availability of data. But data is very important and should not be revealed to any unauthorized person, for this purpose encryption method is used to convert this plain data into ciphertext, and a decryption method is used to convert that cipher text into plain text to get back the original data. So, the encryption algorithm. plays the most important role to make data more secure. To achieve these operations some mathematical calculations are made and it is also possible to explain them practically. To encrypt and decrypt, data will be divided into a chunk of the block while performing this operation, there are various algorithms also available which are categorized into two different types. The first one is the symmetric encryption method, in which data can be encrypted and decrypt with the same key. After performing the encryption method data is converted into an unreadable form, to get the original message back intended user must have the key which is used while the encryption process. Then this method reverses its process and data will available in an understandable form. The second one is the asymmetric encryption method, where two keys are generated, one for encryption and the second for decryption [6].

Advanced Encryption Standard (AES) is also known as the Rijndael algorithm which works up to 128 bits of the block length. This algorithm allows the key length of three different bits which are 128, 192, 256 bits. To convert plain text into cipher, this encryption is dependent on key length where this algorithm repeats its method several times called rounds to enhance the security of data. For 128 bits it uses 10 rounds, for 192 bits it uses 12 rounds, and for 256 bits it uses 14 rounds. Excepting the last round in every case, the rest of the rounds are equal to each other [7]. After performing this operation on data encrypted data block is obtained, this is in an unreadable form. To get the original data back the reverse procedure of the AES algorithm is required to perform on encrypted data.To implement such a secure system, we are using Advance Encryption Standard to make data more secure and keep data out of reach from the attackers shown in fig.2.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205321 |

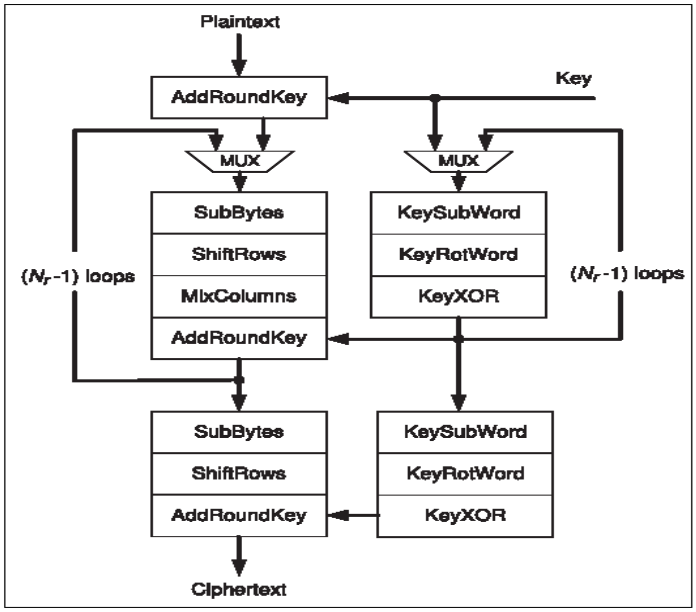


Fig.2: AES Algorithm Structure

- **Key Expansion:** This process involves in taking the words as initial key and create array of 44 words, then use with series of keys for every next round for encryption process.
- **Add Round Key:** Key expansion is done to make 10 keys by method called key schedule. This is done with XORing with resulted data to make input for the next round.
- **Substitute bytes:** Here, whole words are coded in such a way that one letter after of current word in alphabet. For example, hello changes to ifmmp.
- **Shift Rows:** As name give idea for this concept, each next row is moved one row back means.
- second row is shift in space of first row; third row is shift in space of second row and so on.
- **Mix Columns:** Each column has some value which is given by the previous stages of algorithm. Likewise, this mixing of column is performed.
- **Add Round Key (again):** This block takes input from previous block and add round key which are derived at the beginning of encryption.
- At the end of this step, we get encrypted data. To get the original data back reverse operation of encryption is performed on encrypted data and the resultant data would be our original data. [2]

B. SHA-256 bit:

The SHA-256 algorithm is a hashing algorithm that performs on data in one-way and it is developed by Ron Rivist. It is an evolution of previous algorithms such as SHA 0, SHA 1, SHA 256, SHA 384. Hashing is also known as compression or message summary function which takes the entire variable length and changes it into a binary sequence of fixed length. The concept of a hashing algorithm is shown in Fig.3.

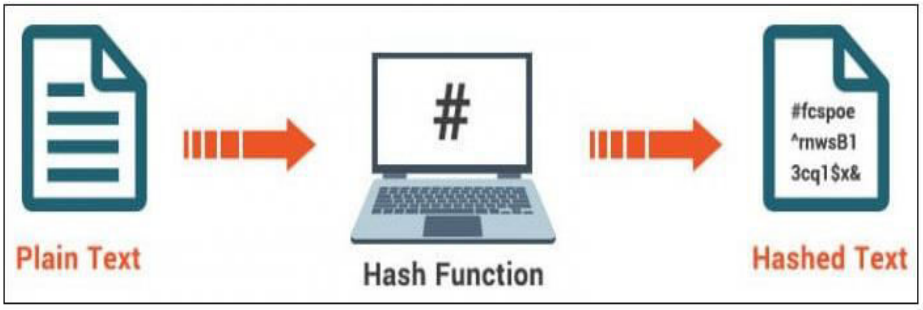


Fig.3: Working of hashing algorithm.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

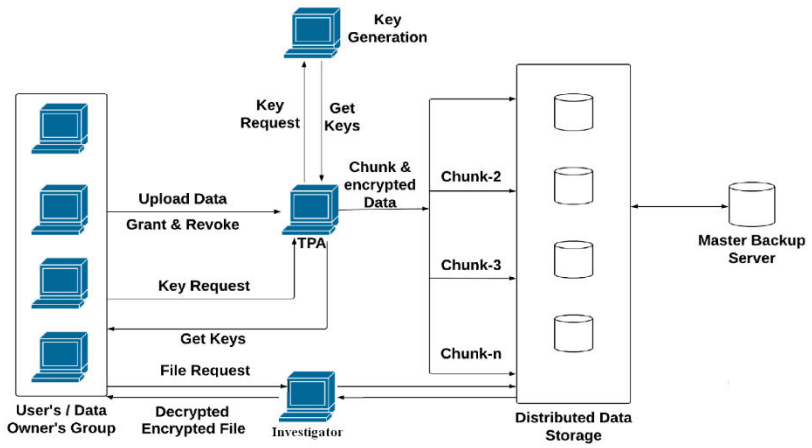
| DOI: 10.15680/IJIRCCE.2024.1205321 |

Working of SHA-256 algorithm is given as follows:

The first step is to add a bit as per algorithms rules. It is the first step in all the algorithms. Then SHA-256 algorithm process the block of a message in the block of 512 sizes. The next step is to add bits again with the original message; the addition of bits in the message is 128-bits. SHA-256 is a construction where data is absorbed into the sponge and then the output is derived as a squeezed from the input. In the absorbing stage, data is XORed and in the squeezing, stage data is altered with state transformation.With the help of AES and Hashing algorithm, we have designed an architecture where users upload data to the cloud server, and with the help of a private key, the receiver can retrieve that data. [4]

IV. PROPOSED SYSTEM

In the proposed system we use three different entities data Owner, User, TPA, cloud server, and the attacker is an untrusted entity. In this module first data owner uploads the data file to the cloud server using the cryptography algorithm once data has been stored into the database; the owner gets the notification about file storage successfully [8]. The data owner has full access to specific data file he can share or access, so the data owner can share any file with any user who can request the file then it will automatically access the particular user only normally; but in that one more access policy is there when Owner share a particular file that time user can't access these file without a key, so the user can request for a key to TPA and TPA can accept the user's request if it is trusted then TPA grant access and send the key to user & that time user access particular file [9]. The shared user can access each file anytime by the cloud server. In the first phase if the data owner revokes any user from access the file then he can't access such file. If he can try and generate any collusion attack the usage of SQL injection queries, even our system will prevent such attacks. The second data owner can share and revoke files to the individual user to a specific user, and third, once any user revokes system will automatically generate proxy key generation that means existing keys will expire. Finally, if any un-trusted user can alter or hack any file



As shown in fig.4 here in the proposed model the data owner stores data on the cloud server. The cloud server is always remaining an attractive point for an intruder to steal valuable data. For security purposes, a key is shared by the owner to the data used to access that data. To make that data unreadable to intruder AES algorithm is used. So, intruders are not able to steal the data. With the help of hashing algorithm, SHA-512 data blocks are linked to each other and if data blocks are found to be missing, we have developed a system which data user can know which data block is attacked by the hackers. from the server that time our system easily recovers that file and give access to the user. The overall approach improves the system efficiency as well security on a drastic level [10].

The user gives the required information of him to the owner i.e. request to the owner for access to particular files. It's up to the owner to approve the request of the user to use its services as well as to access that file. Once the owner allows using his services then the user can store data on the cloud server and access the files. Data stored on the server have a key that is created when data stored on the cloud server, so the user required that key to get that data. To access data that is stored on the cloud server user needs to send a request to Key Manager i.e. TPA to access the file. If it denies sending a private key then it is not possible for to use to access and download the file. All the users who wish to

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

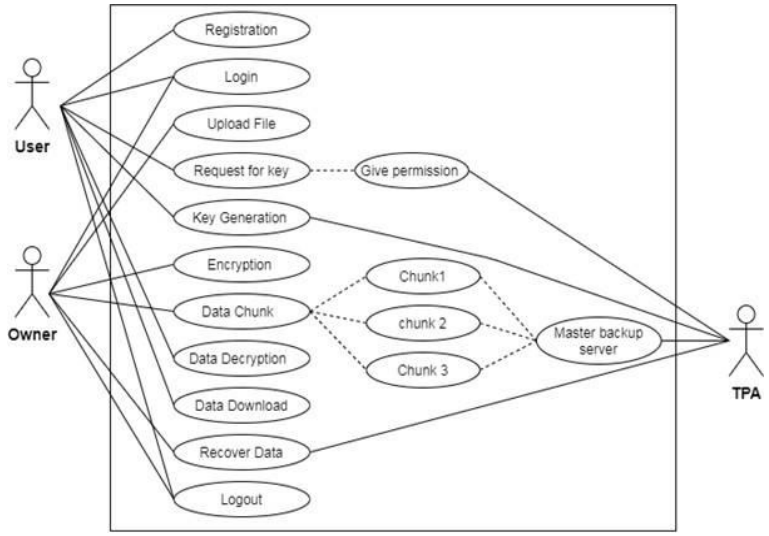
| DOI: 10.15680/IJIRCCE.2024.1205321 |

use data that is stored on cloud storage are requiring permission to access that data. Key Manager has the authority to share the key to the respective user to access the data on the cloud.

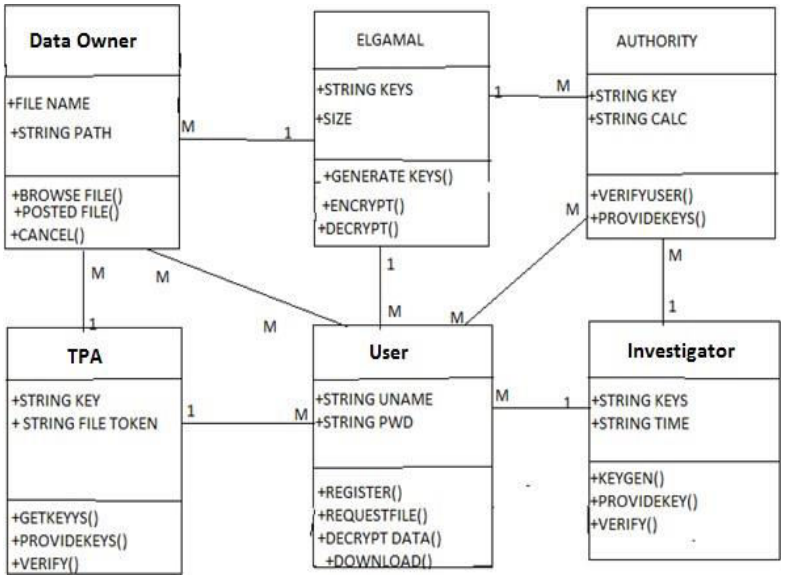
Objectives:

- To provide the better security all data into the cloud system.
- To provide the security to system from collusion attack, bruit force attack as well as malicious queries.
- To implement a new verification as well as authentication protocol between authorities and trusted third party.
- To improve the time efficiency.
- To provide the security to system from malicious queries.
- To provide highest security from any type external or internal attack like collusion attack, SQL injection attack etc.
- Successfully implementation of AES encryption scheme in proposed system architecture.

B. Use case Diagram:



C. Class Diagram:



International Journal of Innovative Research in Computer and Communication Engineering

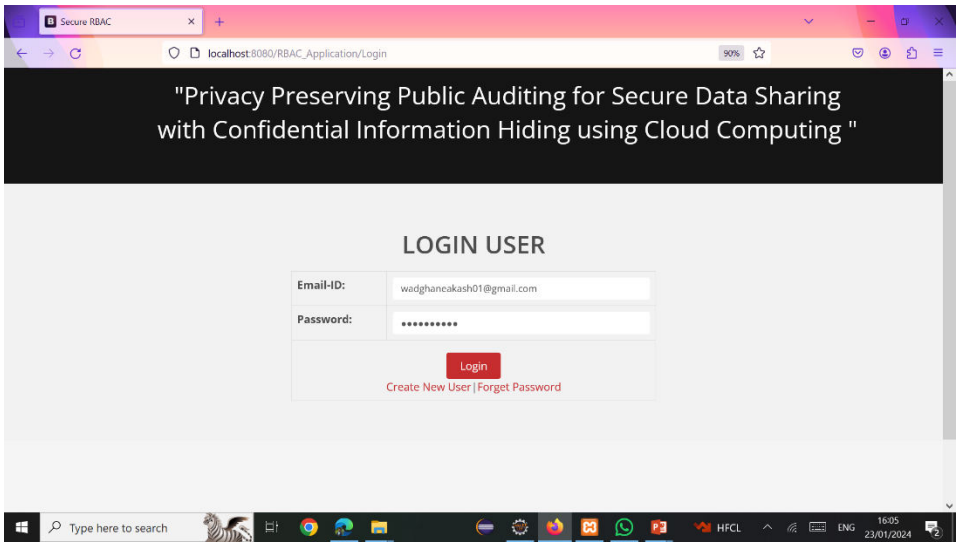
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

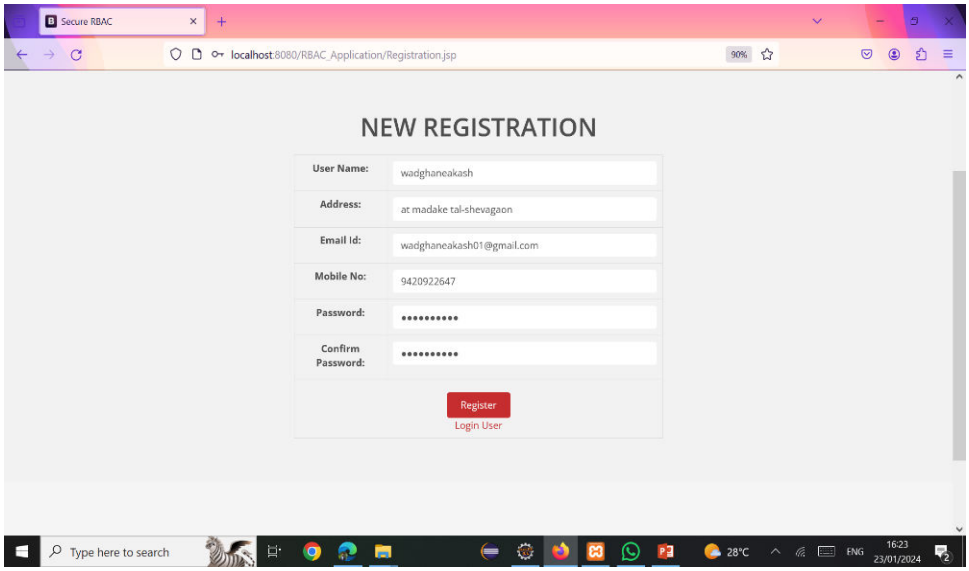
| DOI: 10.15680/IJIRCCE.2024.1205321 |

V. RESULT

1. Login page



2. Registration page



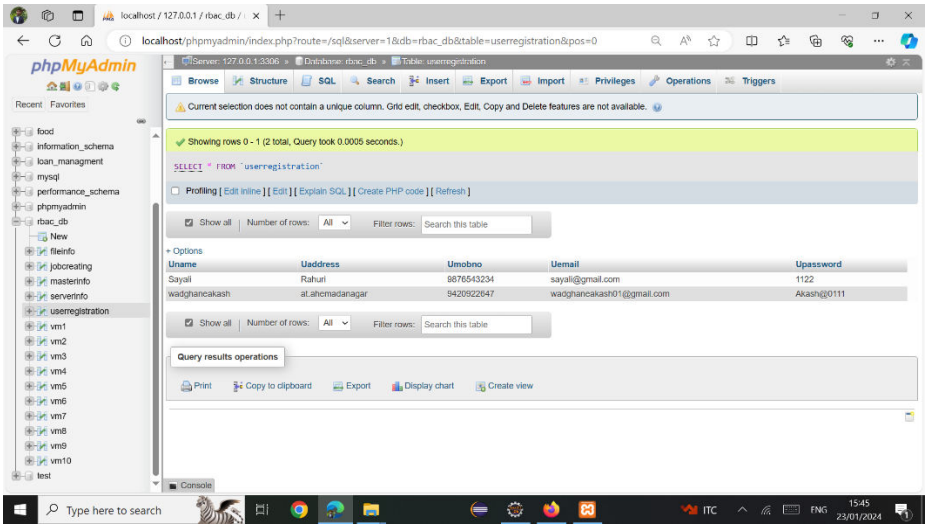
International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205321 |

3. Database



VI. CONCLUSION

In this work, the system proposes a secure Role Base Access Control (RBAC) data sharing scheme for the untrusted environment in the cloud. In our scheme, the users can securely get their private keys from middleware authorities; TPA provides and secures communication between multi-users. Also, our scheme can provide secure revocation for the untrusted user. The proxy key generation has also been proposed in this work. When the data owner revokes any specific end-user system automatically expired the existing keys and generates new keys for all shared users. The system can achieve the highest level of security as well as privacy through such approaches [7].

It's a revocable decentralized data access control system that can support efficient attribute revocation for multi-authority cloud storage systems. It eliminates the decryption overhead of users according to attributes. This secures attribute-based encryption technique for robust data security is being shared in the cloud. This revocable multi-authority data access scheme with verifiable outsourced decryption and is secure and verifiable. This scheme will be a promising technique, which can be applied in any remote storage systems and online social networks etc.

REFERENCES

1. Rubina Ghazal, Ahmad Kamran Malik, NaumanQadeer, BasitRaza, Ahmad RazaShahid, and Hani Alquhayz, "Intelligent Role-Based Access Control Model and Framework Using Semantic Business Roles in Multi-Domain Environments". IEEE Access, 2020.
2. Wei Li, KaipingXue, YingjieXue, and Jianan Hong, "TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage", IEEE Transactions on parallel and distributed systems, VOL.24, NO. 06, October 2017.
3. Jianan Hong, KaipingXue and Wei Li, "Comments on "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems"/Security Analysis of Attribute Revocation in Multi-Authority Data Access Control for Cloud Storage Systems", IEEE transactions on information forensics and security, VOL. 10, NO. 06, June 2017.
4. Taeho Jung, Xiang-Yang Li, Zhiguo Wan, and Meng Wan, "Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption", IEEE transactions on information forensics and security, VOL. 10, NO. 01, January 2017.
5. Kan Yang and Xiao huaJia, "Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage", IEEE Transactions on parallel and distributed systems, VOL. 25, NO. 07, July 2014.
6. S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proceedings of the 14th Financial Cryptography and Data Security. Springer, 2010, pp. 136-149.
7. R. Ostrovsky, A. Sahai, and B.Waters, "Attribute-based encryption with non-monotonic access structures," in Proceedings of the 14th ACM conference on Computer and communications security. ACM,2014, pp. 195-203.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205321 |

8. N. Attrapadung, B. Libert, and E. Pana_eu, "Expressive key policy attribute based encryption with constant-size ciphertext," in Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography. Springer, 2011, pp. 90-108.
9. T. Jung, X. Li, Z. Wan, and M. Wan, "Privacy preserving cloud data access with multi-authorities," in Proceedings of The 32nd IEEE International Conference on Computer Communications. IEEE, 2013, pp. 2625-2633.
10. Z. Liu and Z. Cao, "On efficiently transferring the linear secret sharing scheme matrix in ciphertext-policy attribute-based encryption," IACR Cryptology ePrint Archive, vol. 2010, p. 374, 2010.
11. S. Patil, P. Vhatkar, and J. Gajwani, "Towards secure and dependable storage services in cloud computing," International Journal of Innovative Research in Advanced Engineering, vol. 1, no. 9, pp. 57-64, 2014.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details