International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Multi Authority Access Control Mechanism for Role Based Access Control for Data Security in the Cloud Environment

Mahesh B Gunjal[1], Dr.Vijay R Sonawane[2]

Submitted: 26/10/2022 **Revised:** 24/12/2022 **Accepted**: 22/01/2023

Abstract: There has been an increasing tendency toward storing vast amounts of data on the cloud, which can be attributed to the rapid advancements that are taking place in cloud computing. As a result, the critical concern of how to manage and prevent unauthorized access to data that is kept in the cloud has been raised as a result of this. We present a secure data sharing approach, which, by utilizing Role-Based Access Control and the AES encryption method, is capable of achieving secure key distribution & information sharing for dynamic groups. The data is protected by our system, which also allows for its regeneration in the event that it is mishandled by an unauthorized user. A Proxy server will be given responsibility for completing this task. The information pertaining to the users would be kept in both the public and the private portions of the cloud storage. Users will only be able to access the data stored in the public cloud, allowing the private cloud to maintain its higher level of security. The original data that was stored in the private cloud would be collected by the Proxy server as soon as any unauthorized changes are made, and it will then be given back to the user. Users of cloud storage are typically provided with a variety of redundancy configuration options in order to achieve the optimal level of performance while also maintaining an acceptable level of fault tolerance. The system has the ability to concurrently achieve the highest possible level of both security and privacy. The results of our experiments have led us to the conclusion that computations on the client side that involve encryption and decryption can produce accurate results.

Keywords*: Role Based Access Control, AES, Cloud data security, Multi Authority Access Control*

1. Introduction

The word "Cloud" can also relate to the Internet or a network. To put it another way, we could say that the cloud represents something that is located in a distant place. The cloud has the capability to deliver services over networks, such as public or private networks, such as wide area networks, local area networks, or virtual private networks. Email, online conferencing, and customer relationship management are some examples of programs that can be run in the cloud. Cloud computing is the process of managing, customizing, and gaining access to software programs using the internet. It provides cloud storage, infrastructure, and applications over the internet. The fact that we do not have to install any programs on our local computer is one of the ways in which cloud computing gets around problems with platform dependencies. As a result, thanks to cloud computing, our business applications are becoming more cooperative and mobile [17].

Cloud computing invariably introduces new and challenging potential threats for a wide range of reasons, which is problematic from the point of view of information security, which has been an essential component of service quality. To begin, standard cryptographic elements cannot be directly accepted for the goal of protecting data security since users lose control of their data while using cloud computing. This makes it impossible to directly adopt these primitives. As a result, validation of accurate data storage on the cloud needs to be carried out without foreknowledge of the entirety of the data. The difficulty of validating the accuracy of data the cloud's storage is made even more difficult when one considers the numerous kinds of data that are saved for every user in the cloud as well as the necessity for long term ongoing guarantee of the data's safety. Second, contrary to popular belief, cloud storage is not merely a data storage facility run by a third party. The users have the ability to often update the data that is kept in the cloud, which may include insertion, removal, modification, adding, reordering, and other similar operations [3]. Therefore, ensuring that the storage is correct when dynamic data is being updated is of the utmost importance. Furthermore, due to the dynamic nature of the feature, standard methods of integrity insurance are rendered useless, necessitating the development of new alternatives. The last point to mention, but perhaps not the least important, is that the implementation of cloud computing is driven by data centers operating in a parallel, cooperative, and dispersed

[1]*Research Scholar: Department of Computer Science and Engineering, Dr. A. P. J Abdul Kalam University Indore (MP)*

maheshgunjal2010@gmail.com

manner. The data belonging to each user is duplicated and kept in a number of different locations so as to further lessen the risks to the data's integrity. As a result, networked protocols enabling storage accuracy assurance will be of the utmost importance in order to accomplish the goal of developing a dependable and safe cloud system for storing data in the reality. However, such an essential topic has not yet been thoroughly researched in the existing literature.

Recent study works have shed light on the significance of preserving the distant data's integrity, which has been emphasized as an increasingly important task [12, 16]. These methodologies, while they may be helpful to ensure the accurateness of the storage without allowing users possess the data, are limited in their ability to confront all of the security risks associated with cloud data storage because they are all centered on the circumstance of a single server, and the majority of them do not take into account the dynamic data operations. Academics have also suggested distributed methods for the purpose of maintaining storage integrity across numerous servers or peers. This is an additional solution that researchers have presented. To emphasize, not a single among these distributed methods is aware of the existence of dynamic data processing. Because of this, the extent to which they can be utilized for data storage on the cloud may be severely constrained.

The preservation of the data's integrity should be the primary focus of cloud storage. Our proposed work is carried out with the goal of protecting data and regenerating it in the event that it is mishandled. A Proxy server will be given responsibility for completing this task. The information pertaining to the users would be kept in both the public and the private sections of the cloud storage. Users will only be able to access the data stored in the public cloud, allowing the private cloud to maintain its higher level of security. The original data that was stored with in private cloud would be recovered by a Proxy server as soon as any unauthorized changes are made, and it will then be given back to the user. Users of cloud storage are typically provided with a variety of redundancy configuration options in order to achieve the optimal level of performance while also maintaining an acceptable level of fault tolerance. It is essential for data to be accessible within distributed storage systems, which is especially true in situations where node failures are common in real life. This study effort investigates secure information storage and sharing by employing a proposed encryption method called AES 128, as well as Role Base Access Control (RBAC) and a cloud snapshot-based method for forensic examination for a secure data access strategy. This work has implemented a backup server technique, in which the server functions as a proxy storage server in order to provide ad hoc retrieval for all dispersed data servers. The research's analysis is carried out in both public and private cloud environments respectively.

Before beginning development on the suggested system, we conducted an analysis of several previously developed methods that had research gaps. Existing computer systems frequently suffer from issues concerning the amount of time spent, the amount of space used, and the length of the procedure required to generate matrices. After conducting this gap analysis, we came up with a system that will address the following challenges.

• There have been no balancing methods in any of the previous academic work on cloud storage

• There are problems with data leaking out in environments with several clouds

• Another factor that might contribute to a rise in the total execution overhead is parallel processing.

• A problem with the unnecessary consumption of resources in cloud computing and distributed databases that use proxy servers

This study report is divided up into a few different sections. In the second part of this series, we will go over the history of cloud data security and several approaches to protecting it. The relevant work and research gap of a number of different existing systems is covered in greater depth in part 3. In the part 4 of the series, our proposed research technique of multi-authority access control method for role base access control for information security in the cloud System is discussed in more detail. The results of the experiments and their interpretation are explained in part 5. In the final section of we concluded our system.

2. Background

2.1 Data Security in Cloud Computing

Data encryption is only one component of cloud computing's comprehensive approach to data security. The three different service models—SaaS, PaaS, and IaaS—each have different requirements for the level of data protection that must be met. Data that is "at resting," which refers to information that is kept in the cloud, and data that is "in transit," which refers to information that is flowing between and within the cloud, are the 2 data states that typically pose a risk to the cloud's security. The type of the data protection systems, methods, and processes determines the extent to which data can maintain its integrity and confidentiality. The most important thing to address is the vulnerability of data in the two states that were just highlighted [8, 9,13].

2.2 Major Data Security Challenges in Cloud

Because multiple computers and users are involved, which is what is meant by the term "multi-tenancy," it is undeniably difficult to safeguard and assure the safety of computers that are connected to one another. The providers of cloud-based services including cloud computing as a whole are forced to contend with a great deal of conflict, especially in the field of resolving safety concerns. As a result, it is of the utmost importance to take into consideration how these issues are imitated and how security methods are applied in order to guarantee the safety of customers and provide a risk-free setting for cloud computing. The following are the most significant difficulties:

- **Inappropriate governance**

The provider of the cloud computing services retains complete control over the process. When this control is given to the provider, there is a risk that the loss of supervision over authority specifications could possibly lead in security being infiltrated, resulting in issues in terms of information access and the usage of the assets. This risk exists because transferring this control to the supplier creates a loss of influence over authoritative parameters. This security risk comes with additional threat, which is the potential to create a gap in security cover in situations in which Service Level Agreements aren't in place well with service supplier. Additionally, the conditions of use are accessible to the liberty of the user, which means that access to the data can be utilized in a relatively straightforward manner [22].

- **Lock-in**

Inadequate norms of data format, a shortage of operating techniques, and a paucity of tools are additional obstacles that, when combined, result in limited portability amongst applications and services between many service suppliers. As a consequence of this, the relationship between the consumer and the vendor must be unassailable [21].

- **Isolation failure**

The resource sharing that arises as a result of the multi-tenancy feature of cloud computing in and of itself is a problematic quality. It might be disastrous for companies not to have adequate space for separate storage. Other concerns including guest hopping assaults and accompanying complications are regarded to be a significant barrier to the utilization of cloud computing apps and their deployment [11].

- **Destructive attacks from management internally**

It is possible for the infrastructure of cloud computing platforms to provide hazards to the customers' privacy and security [2]. Even if this situation only rarely occurs, it is extremely challenging to mitigate this risk. For instance, the managers and admins of cloud service providers can occasionally pose a security risk to their customers by behaving in a malevolent manner and posing a threat to the clients that use cloud computing services.

- **Insecure or insufficient data erasure**

When customers request that certain data be removed entirely or in part, this situation raises the issue of whether or not it will be possible to remove the desirable output of their data packet with precision. The customers will have a more difficult time subscribing to the cloud computing services because of this [4].

· **Data interception**

When using cloud computing, as opposed to traditional computing, the data is divided and disseminated while it is being transferred. The weakness and volatility of the computer technologies, in specific sniffing as well as spoofing, third party assaults, and reply assaults [4], makes this a more dangerous situation than it would have been otherwise.

- **Compromise of management interface**

Because the functions of cloud computing are supplied remotely over the Web and the assets are available to the service supplier, third party access can lead in malware attacks [16]. Cloud computing services are available to the service provider. As a direct consequence of this, the risks associated with vulnerabilities, manipulation of services, and engagement of the service provider are increased. For example, a cloud computing application's use case may involve the client seizing control of the computers, while the provider may seize control of the situation by instituting restrictions on some areas of the system.

2.3 Safeguarding Information Through the Use of Encryption

Encryption algorithms for data-at-rest and data-in-transit can be distinct. For instance, cryptographic keys for data that is in transit may have a relatively limited lifespan, whereas cryptographic keys for data that is at rest may be stored for significantly longer lengths of time.

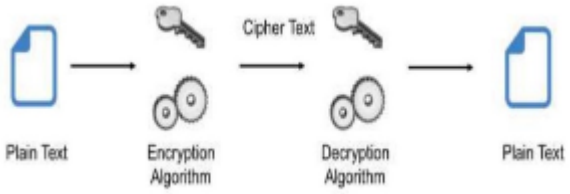

Fig. 1: Process Involved in Cryptography

These days, many methods of cryptography are utilized in order to encrypt the data that is being stored. The use of cryptography has resulted in an increase in the level of information protection that is necessary to guarantee the authenticity of content and its accessibility. The most fundamental implementation of cryptography involves converting plaintext into cipher text with the help of an encryption key, and then decrypting the cipher text that was produced with the help of a decryption key, as shown in Figure 1. There are typically four primary applications of cryptography, which are as follows:

2.3.1 Block Ciphers - An approach for encrypting information (to generate cipher text) known as a block cipher is one in which an encryption key and technique are used to a block of data rather than one bit at a time. This process produces cipher text. When a message is encrypted using this method, related sections of text are prevented from being encoded in the same manner as one another. In a typical scenario, the cipher text from either the prior encrypted block is transferred to the block that comes next in a sequence. The plain text is broken up into blocks of data, which are typically 64 bits in length. After that, these data blocks are encrypted with the use of an encryption key so that a cipher text can be produced.

2.3.2 Stream Ciphers - This method of encrypting information is also known as a state cipher because it is dependent on the present state of the cipher. Stream ciphers are used to encrypt data streams. Instead of encrypting entire blocks of data, this method encrypts each individual bit. An encryption key as well as an algorithm are individually applied, one bit at a time, to every single bit of the data. Because of the reduced computational complexity of the hardware required to run them, stream ciphers typically have a higher performance capacity than block ciphers. In the event that this method is not implemented correctly, however, it poses a significant risk to one's data security. Stream ciphers, encrypt individual bits of data using encryption keys rather than entire blocks of text. The resulting cipher text is a sequence of encrypted bits, which may be decrypted at a later time with the help of the decryption key to generate the plain text as it was originally written.

2.3.3 Hash Functions - Within the context of this method, the process of converting an input text into an alphanumeric string is handled by mathematical functions known as a hash function. Typically, the length of the resulting alphanumeric string remains constant. Using this method, you may be certain that no two texts will ever produce the same alphabetic or numeric string as a result. Even if the two strings that are being used as input are just very slightly distinct from one another, there is still a possibility that the output string that is formed from them will be very different. This hash function may take the form of a fairly straightforward mathematical operation, such as the one depicted in equation (1), or it may take on a more involved form.

$$F(y) = y \ *\mathrm{mod}\ 10 \quad (1)$$

The encryption of data stored in the cloud typically makes use of all of the approaches and techniques described above. This helps to ensure that the data is kept secure. The application of these strategies differs depending on the context of the situation. It is strongly advised that data security be ensured in both public and private clouds, regardless of the method that is employed to accomplish this.

2.4 Advanced AES Technique for Data Security in Cloud

Information can be encrypted using the Advanced Encryption Standard (AES), which is often referred to as Rijindael. The Advanced Encryption Standard (AES) is indeed a symmetric block cipher which has been thoroughly analyzed and is commonly used these days. In order to accomplish this goal, we make use of the AES symmetric key encryption technique with a key length of 128 bits. Seeing how AES is the standard encryption method for cloud storage these days. First, the user makes the decision to make use of cloud services and move his data to the cloud, as stated in the deployment proposal. The next step is for the user to share his service needs with a Cloud Service Provider (CSP), after which the user selects the best specialized services that are being provided by the provider. Whenever the data migration to the selected CSP really takes place, and throughout the future anytime any application publishes any information to the cloud, the information will first be encrypted using the AES

technique, and then they will be delivered to the provider. Any attempt to view the data will take place only after it has been decrypted on the user's side, at which point the user will be able to read the plain textual information. Data is stored in the cloud once it has been encrypted. The data are never stored anywhere on the cloud in plain text format. This encompasses all different kinds of data. This encryption technique is completely undetectable by the program and can be rapidly and easily implemented without requiring any modifications to the application itself. The key has never been stored in the same location as the encrypted data, because doing so could endanger both the key and the contents. Installing an actual key management server in the user's location allows for safekeeping of the keys in that location. This encryption safeguards both the information and the keys, ensuring that they will always be under the control of the user and they will never be revealed either in storage or even in transit. The Data Encryption Standard (DES) has been replaced as the accepted standard by the Advanced Encryption Standard (AES).

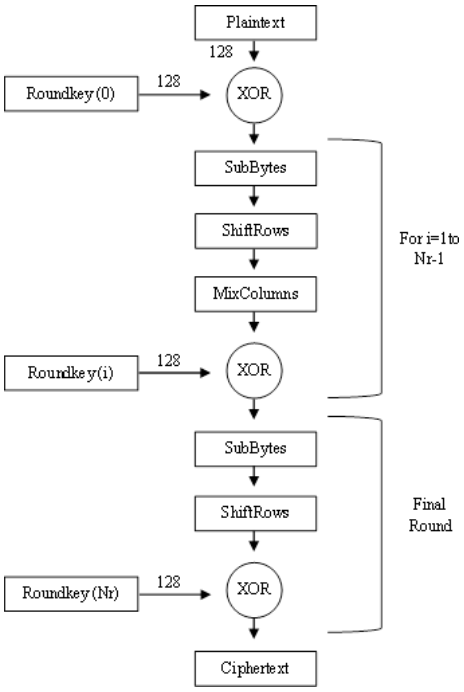

Fig. 2: Advanced Encryption Standard

Consider Figure 2, which depicts the flowchart of AES technique. The Data Encryption Standard was replaced by the Advanced Encryption Standard in 2001 at the recommendation of the National Institute of Standards and Technology (NIST). The Advanced Encryption Standard (AES) is one of the most effective symmetric algorithms.**}**

2.5 Role Based Access Control

The term "cloud computing" refers to a model of data storage and processing that pools several computing resources located throughout the internet and bases its operations on open protocols, services, and standards. These resources come together to form a large number of data warehouses and computation centers, which offer secure, blazing-fast, and hassle-free data storage, network computing, and a variety of other specialized services for a wide range of consumers [1]. The terms "confidentiality," "integrity," and "availability" are all connected to network security in some way, and each of these concepts is very significant. In the environment of cloud computing of today, maintaining confidentiality and privacy is the criterion that is prioritized the highest. Cloud computing has a number of characteristics, including those having to do with network security requirements and access control. There have been numerous proposals made for systems of access control for cloud technology; nevertheless, the vast majority of these models lack important qualities such as adaptability, flexibility, and trustworthy access control effectively. Controlling access is a manner of expressly enabling or restricting a capability in some way, and is referred to as an access mechanism. Not only does computer-based access control determine who or what processes are allowed to just have access to a certain system resource, but it could also determine the sort of access that is allowed for that asset. RBAC is a security system that bases choices on access to resources on the responsibilities that individual users play within an organization. When it comes to access controls, the idea of user groups is strongly related to the notion of roles.

In contrast to user groups, which are commonly understood to simply refer to a collection of users, roles bring combined, on the one hand, a group of users and, on the other hand a group of privileges. Discretionary Access Control (DAC) & Mandatory Access Control (MAC) are two distinct frameworks of access control that were developed as a result of differences in the necessities for military and business security protocols. These disparities in necessities resulted in the creation of these two distinct types of procedures. These models suffer from a number of shortcomings, which prompted the development of alternative models like the RBAC. However, due to the fact that each of these systems was developed for a unique setting in order to satisfy the consumers' security standards, it is feared that they may not function properly in cloud computing.

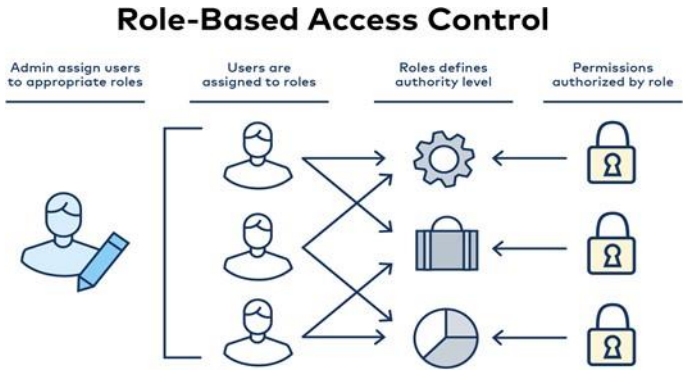

Fig. 3: Role Based Access Control

Consider the figure 3 which depicts the Role Based Access Control mechanism. A company requires a method to limit access to employees in order to keep sensitive data from being used improperly, changed improperly, or deleted improperly. The term "role-based access control" refers to a way of controlling data access depending on the role that a person plays in the organization. By utilizing RBAC, individuals will only have access to the resources and data that are necessary for them to carry out their duties. The tasks that they are responsible for determine whether their credentials permit or limit access, thereby reducing the likelihood that sensitive data will be mishandled. RBAC methods can be enormously beneficial in organizations that are larger in scale and in businesses that work with independent contractors. It may become challenging to give individual credential configurations for each individual if the quantity of authorized suppliers is subject to change and the quantity of employees continues to grow. When a role-based access control system is utilized, administrators have the ability to categorize workers or contractors within pre-existing categories, which are referred to as roles, and provide them access to a certain group of resources. This access is just limited, as the employees' membership in the group may be terminated once the task at hand has been finished. Admins also have the ability to reset the authorization levels for such groups, which enables them to better supervise personnel on a large scale, increase performance, and even enhance compliance.

RBAC gives administrators the ability to categorize users into groups according to the many functions that they play, and an individual user can belong to several distinct groups at the same time. Access granted to employees usually takes into account the individual's active status and responsibilities, as well as any security needs and rules already in place. The optimal policy is to only grant a user the minimum amount of authority necessary for them to do their duties. This is known as "minimal authorization." This approach, which contributes to the safety of one's data and is called as the concept of access privileges,

2.5.1 Benefits of RBAC

The RBAC system is the best approach to use for optimal safety in many different types of businesses. These types of firms are typically divided into various departments, and their hundreds of staff frequently have their own personal computers. There are several benefits that can accrue to your team as well as the broader organization if RBAC is executed successfully [1].

- **Decreases in the amount of work done in administrative areas and in IT support**

Role-based access management removes the necessity for time-wasting documentation and the requirement to change passwords in order to grant and revoke network access whenever a new worker is employed, whenever an existing worker alters his employment position, or whenever he moves to a different department. Instead, you may utilize RBAC to swiftly add and switch roles, as well as apply them globally throughout operating

systems, platforms, and apps. This is all possible with just one tool. In addition to this, it lowers the likelihood of making a mistake while allocating user access. One of the many financial advantages brought about by RBAC is a reduction in the amount of time being spent on administrative responsibilities. By assigning pre-defined responsibilities to third-party users, it is possible to facilitate a smoother integration of those individuals into the network [4].

- **Increasing operational performance**

RBAC systems can also be built to maximize operating efficiency as well as the strategic value that they add to businesses. They have the capability to streamline and standardize a large number of transactions and corporate processes, and they give users the tools they need to do their tasks more effectively, more quickly, and with a higher sense of individual responsibility [1]. Because of the implementation of RBAC systems, firms are in a better position to comply with their own legislative and regulatory standards for confidentiality and security. This is something that is absolutely necessary for enterprises that deal with health care & financial matters. Directors, executives, and IT workers are more capable of monitoring how information is being utilized and accessed, which allows for the preparation of more precise planning & budget models depending on the actual requirements.

- **Providing a robust security system in addition to a significant economic value**

RBAC is a security solution that is beneficial for both large and medium-sized businesses because it reduces the amount of money spent on maintenance while simultaneously boosting productivity. The operation is as follows: When all the employee roles have been added to the database, the next step is to develop role-based rules and deploy workflow engine components. Right from the workstation of the HR or IT manager, role-based permissions may be input and changed rapidly across numerous systems, platforms, apps, and geographical areas thanks to these aspects. The RBAC model offers a company - wide control method for managing IT resources while preserving the necessary level of security. This is accomplished by limiting the access that users have to specific IT resources according to the roles they play and the qualities that are associated to those roles.

- **Protecting Against Data Leaks Is Made Easier Due to Role-Based Access Control**

The potential damage that might be produced by a data breach can also be reduced with the use of roles. User access constraints, in addition to data encryption as well as other security procedures incorporated into the storage database, serve to shut off malicious hackers and prevent any harmful effects that may result from a breach. Users who are attempting to view data can be notified by companies that they do not have the appropriate access and prompted to get in touch with an administrator to receive further access. A large number of companies authenticate their users by utilizing single sign-on (SSO) systems that are integrated to Active Directory (AD). After that, staff members can access directly or log in via a virtual private network (VPN). After the data provided by the user is validated by the single repository, a digital signature representing the identity of the user and role is generated. It is essential to protect an employee's connection whenever the person is receiving information in the cloud-hosted data store from a remote location.

- **Improved adherence to security regulations**

Every organization must comply with the various regulations that exist at the state, federal, and municipal levels. Companies are in a better position to readily satisfy the regulatory standards for confidentiality and safety when they have RBAC systems in place. In addition, IT teams and managers have the authority to govern how information is accessed and used in their own organizations. This is especially essential for institutions that manage large amounts of sensitive data, such as those in the health care and banking sectors [1,4].

3. Literature Survey

This section will describe some of the different access control and information security measures that have been developed by a large number of researchers for use in cloud computing.

Yong Wang et al. [1] organized and carried out the implementation of an RBAC structure that was reliant on property encryption. The User job task as well as the job assent task procedure is both realized using attribute-based encryption. This is done with the goal that the entry decision isn't now relying upon unmistakable methodology decision centers, which ensures the trustworthy utilization of access methods. Within the meantime, their technique executes attribute-based client job roles and role permission allocations, which enables the access control procedure logically flexible. Additionally, their methodology attribute to the RBAC prototype. The reachability of the idea is demonstrated by the confirmation of its endorsement as well as the implementation testing of a prototype. The goals of security are needed to be taken into consideration in order to have a competent trust-based system. Mahdi Ghafoorian et al. [2] offered a novel reputation and trust based RBAC model that not only can properly endure the security risks of trust-based RBAC prototypes, but is also adaptable as it has logical execution time. After

that, researchers proceed to assess the proposed prototype by utilizing the well-known trust structure of the Advogato dataset. In the long run, they differentiated the proposed prototype from the late circulating ones to the extent that it meant an analogous error, the execution duration of complex trust figuring, and the features that were given. The findings of the cultivation reveal that the proposed prototype can be used under cloud circumstances that have been certified.

Muthunagai, Anitha's et al. [3] found that maintaining the customer data on a private storage device that is physically close by becomes a challenging operation. Cloud storage might potentially solve this problem by storing the files in a distant database, from which the user would then be able to retrieve their records no matter where they happen to be located. In this investigation, the aforementioned security concerns are addressed by first segmenting the information that is transmitted by the client, and then encrypting the segmented information using the enhanced attribute-based encryption approach that has been suggested. The encrypted information is then amassed in various locations. The privacy of secret data at several focuses helps to prevent the client's transferred information from being mediated by any unauthorized third parties. In the end, the information that was located at a certain spot was recovered with the help of a deciphering method. After that, it reduces the amount of system traffic that occurred during the process of recovering the client's information that was sent from a separate location.Gadouche et al., [4] describes a correct special technique of the attribute based access control (ABAC), which recommends applying the Event-B technique. The researchers make use of the earlier appropriate confirmation in order to produce the appropriate prototype in a step-by-step manner. The prototype illustrates the various levels of consideration that can be achieved through the completion of refining chores. Many of the ABAC qualities are described at every level of refinement, starting with the highest and most distinctive level and working down to the level which is the most solid. These qualities are stored within the conduct particular in the proofs. The procedure is outlined on the organizations that administer social insurance.

Chakraborty et al. [5] suggested that ABAC arrangement mining problem predict that attribute esteems for various compounds, such as clients as well as items in the framework, are given, in addition to the approval state, from where the ABAC method should be found. This recommendation was made in response to a question posed by the authors Chakraborty et al. In light of this one-of-a-kind condition, the developers formulate the ABAC RuleSet Availability problem and devise a computational as well as an unusualness evaluation for the answer to that question. The authors continue by presenting the concept of ABAC RuleSet Infeasibility Improvement along with a computation for the solution to the problem. An ABAC structure is recommended as a paradigm for human services, according to Majid Afshar et al. [6]. They implemented and maintained social insurance programs by utilizing the ABAC engine. In addition to that, we manage emergency situations using this technology. Yingjie Xue et al. [7] explored an exceptional attribute-based access control scenario in which multiple clients with unique attribute sets can perform together to obtain entrance permission if the data owner enables their combined effort in the access process. Specifically, the scenario focused on a scenario in which the clients were attempting to access a database. They suggested a strategy for attribute-based-controlled-synergistic access control, in which comprehension center points in the access hierarchy would be appointed. The results of the security evaluation indicate that their proposed strategy can protect the confidentiality of data and possesses a variety of other critical security qualities. The extensive evaluation of the plot's execution reveals that the proposed plan is effective to the extent as storage and count expenses are concerned.

In addition, Yang Xu et al. [8] proposed a method called feasible fluffy expanded ABAC (FBAC) to enhance the flexibility in great key approvals, so enhancing the asset's simplicity of use and the business's practicability. Researchers employ the fluffy appraisal procedure to assess the approach coordinating levels of the requests that don't adhere to strategy. This is done so that the structure can decide on distinct endorsement options in the same way to achieve unattended unusual approvals. In addition, they envisaged an assistant credit system that would be coupled with occasional credit modification checking in order to provide expeditious approvals for the purpose of mitigating risks. The FBAC approach improves asset promptness and comfort of use while simultaneously reducing the amount of controllable risk, as shown by both hypothetical studies and experimental assessments.N. Geetha et al. [9] proposed a technique that revolves around the SaaS cloud concept. Access Control and the Division of Strategies in the Creation of Services are the Two Primary Concerns in Software as a Model for the Delivery of Assistance. It is necessary to have a legitimate protection protecting access control prototype in order to have secure assistance provisioning and piece. Within the framework that has been proposed, the provision of secure assistance is made feasible through the positioning of probable networks of composite administrations according to the part that the client plays and the degree to which their data can be

affected. Services are chosen for arrangement and strategies are developed according to the role that a client plays in the process. In addition to this, the security of the client content is taken care of here.

The technique for uploading info or data into a cloud infrastructure was created by Viswanath, G., and Krishna, P. V. [10]. Before being sent to the cloud, the data were encrypted with the help of this algorithm. The outcomes of the simulation can also be found there with a total of 2630KB of data encrypted. In order to evaluate the efficacy of the algorithm, the authors made utilization of the real-time medical data collection. A technique of images reduction for compressive sensing, encryption method, and verification was proposed by Li, H., Yu, C., and Wang, X. [11], which can minimize added subcontracting of the expensive putting it away and entire amount. With the assistance of a stochastic process, the researchers develop a brand new encryption method for protecting the privacy of photos. AES, BRA, RC4, and Blowfish technique for block wise safety were explored by Bale et al. [12]. These techniques are a kind of symmetric cryptography, which means that they use the same key for both the encoding and decoding processes. In this article, a low latency parameter was accomplished with the assistance of the multithreading process. According to the authors' proposal, the encoding of text files required approximately 20 percent less time when compared to the AES technique.

Olanrewaju et al. [13] suggested a mixed algorithm consisting of the Advanced Encryption Standard (AES) and the Blowfish algorithm. This hybrid method offers robust encryption for the purpose of storing data on the cloud as well as reliability and enhanced comparative performance to the AES algorithm. In their suggested algorithm, they have already incorporated the ideas behind the AES and Blowfish algorithms. Bhardwaj et al. [14] Discussed about the concepts of block & stream cipher, symmetric method, and asymmetric method. The RSA algorithm and the Diffie-Hellman key exchange method were discussed by the authors, along with their respective functions in the context of security. They examine a variety of symmetric and asymmetric methods and come to the conclusion that MD5 is significantly faster than the others when it comes to encoding. Another privacy system was created about the same time [15], which would evaluate load offsetting, observations on security situations, and proactive operations in order to preserve the specified trust levels. A notoriety-based framework evaluated the reputation of specialist firms [16] by employing a trust evaluation formula that would take into consideration the clients' input, the server dismissal rate, and the server's outstanding responsibilities at hand. The trials demonstrate that the trust outcome is more effective as more time passes. Tawalbeh et al. [17] have reviewed the cloudlet engineering that was done for MCC. They noticed that making use of this model increased the display of a variety of apps and reduced the amount of idle time experienced by the system. When compared to non-cloudlet cloud engineering, using the cloudlet model results in significant improvements across a wide range of quality of service characteristics, including accessibility, flexibility, and throughput. In a similar vein, they developed a secure utilization and architecture for the cloudlet MCC concept by making use of the dynamic trust assignment mechanism. This was done in order to provide increased protection and safety for the client's data that was stored in MCC.

The reliability of data came under increased scrutiny as the protection of stored information became the top issue. It was proposed that identity-based encryption should be used on revocable storage elements (RS–IBE) [18], in order to guarantee the veracity of the data that was accessed. This forward security or backward safety of cyphertext demonstrated superior efficiency as compared to its competitors in terms of both efficiency and usefulness. On the other hand, [19] challenged the accuracy of this technique and suggested the use of self-updatable encryption as a way to improve the efficiency of the RS-IBE algorithm. The degree of accessibility became the next performance measure that garnered prominence after data security became practical and, frankly, required throughout all cloud storage access. As a result, a data security technique with a self-contained module that was given the name RBAC enhanced utilizing data centric attribute based encryption (DCRBAC) became quite popular [20]. The encryption was made even more secure by the addition of a trust value that was determined with the help of a Fuzzy Analytic Hierarchy Process (FAHP) [21], which offered improved granularity and flexibility. Therefore, adding a trust value appeared to be the ideal solution that can provide data protection that was both flexible and effective. The Ciphertext Policy Driven Attribute Based Encryption (CPABE) method was by far the most popular choice for use in access control applications. They serve as the foundation for numerous mobile applications that share multimedia data [22,23].

Moreover to other features, data creation as well as access to data is often considered to be an attribute which helps in the data access control as well as data security, validity, thereby boosting the CPABE one individual parameter at a time [24]. This is because both data creation as well as data access is regarded to be a characteristic that enables in dual control of data access and data security verifiability. After doing an in-depth

investigation of a variety of encryption techniques and access control systems, it has been abundantly evident that very few of these have addressed with trust factors as the primary component, and even among those that have, the idea of cyclic flipping is rarely discussed. The [25] Developing a blockchain-based spectrum trading and sharing system that addresses security concerns and maintains user privacy. Mobile network operators can exchange spectrum without relying on a third party using a Distributed Blockchain Consortium System (DBCS). As a result, data is well-protected from plaintext, stalker, and ciphertext attacks, making it easier to track, manage, and control services. Experimental; results showed that the proposed DBCS outperformed other conventional systems in terms of security and performance.

According to [26] hybrid clustering approach named HCMX to find clustering solution of multi-version XML documents which changes dynamically. the amount of document affected, rather than considering each coming document as new version. To find new clustering solution, after changes in preliminary one, instead of comparing all members of clustering solution, make the use of distance information during preliminary clustering phase, with the changes responsible for document version to produce. To improve clustering speed and response time homomorphic compression scheme used which retain documents original structure. The [27] Managing different servers platform (Windows and Linux), Hardware Inventory like how many Disks, Memory, CPU are in used currently. As well as we will monitor how many applications on server and relative services of it. Highlight max disk, memory, CPU usage servers. It will provide alerts configurations visually so Administrator troubleshoots issues and cause of issue quickly. A benefit of system is in very less time or at a time you can manage N number of server's activity. So Organizations Qos (Quality of services) will be increase and also the downtime. For Failure of any resource will be detected in very less time. Troubleshooting also be an easy, Single Human resource can manage complete N number of server. The [28] simple web site mining technique by mining product information from the pages of the e-commercial web site. For this taking the benefits of hierarchical structure of HTML language. First it discovers the set of product descriptions based on the measure of entropy at each node in the HTML tag tree of the retrieved web page. Afterward, a set of association rules based on heuristic features is employed for more accuracy in the product extraction.

4. Proposed System

We propose a reliable method of data sharing using Role Base Access Control for use in untrusted environments like those found in the cloud. The users of our system are able to obtain their master as well as private keys in a safe and secure manner from the middleware authority; TPA is responsible for providing and securing communication between multiple parties. Untrusted users will be able to benefit from the secure revocation that the scheme offers. In addition to that, the production of proxy keys is proposed in this study. When a data holder revokes access for a particular end user, the system will promptly expires any current keys and produce new ones for any shared users. By utilizing these kinds of strategies, the system is able to simultaneously attain the maximum possible level of security and privacy. It is a decentralized data access control method that can provide efficient attribute revoking for multi-authority cloud storage platforms. This system is revocable and decentralized. It gets rid of the burden of decryption that users have to bear as per attributes. This robust attribute-based encryption method is utilized for the purpose of providing robust data security in cloud storage environments. This strategy is a potentially useful method that can be implemented in a remote storage facility as well as online social networks, among other places.

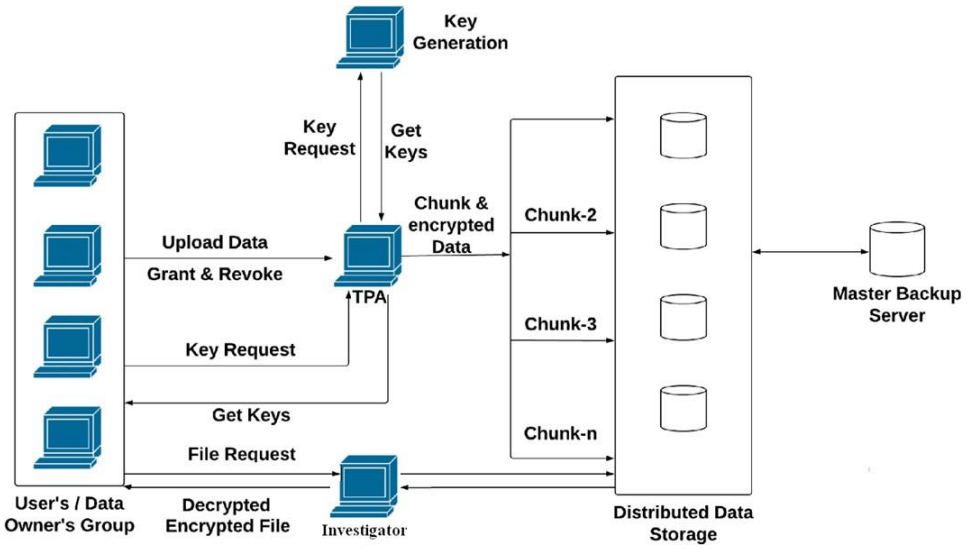

Fig. 4: Proposed Systems Framework

Figure 4 illustrates the matrix construction framework that is used for the administration and evaluation of the cloud data hierarchy. The architecture of an administrative broadcast channel is included in the architecture that has been presented. A node domain controller is also included. Data packets are moved from terminals to data sources at regular intervals or when a task is planned. We have incorporated additional self-address calibration unit into the CaCo design in order to facilitate the decoding of data and the retrieval of addresses. Our proposed solution prioritizes cutting down on wait times while simultaneously increasing the system's overall efficiency. In the beginning, the system will calculate the values for (k,m,w), where k stands for the total number of chunks, M stands for the matrix nodes, and w is the sum of k and m. When all of the k, m, and w vectors are followed, the file can then be uploaded. When k = 4, m = 2, and w = 6, the system will generate 4 chunks in which to save the encrypted data and will use data nodes to do so. When it comes time to save the information, it will generate a [8 * 8] matrix for every algorithm. Every data chunks are saved on data node as well as matrix are placed into master mode. When a failure of any kind happens in the system, the data can be recovered with the assistance of the matrix and any rest of the data nodes.

Module Description

- **Registration and Authentication:** CA accepts registrations from any and all entities. Each individual, including the data owner, AAs, TTPs, and users, has the ability to construct their own profile under CA.
- **Data Uploading:** The data owner is able to upload the file after identity verification of user has been completed. The Elgamal encryption method is utilized to encrypt the data, and during this process, both keys are communicated to the TTP as well as AA's.
- **Data Sharing:** The owner of the data is responsible for data sharing. The owner of the data can choose to share any file with any member of the cloud group.
- **Access Control & Revocation:** In the access control, every user with the appropriate permissions can view or access a file that another user has shared with that user. During the revocation process, the owner of the data can remove a user's access to a particular file.
- **File request & download:** the user is able to send the download demand to the cloud server at the exact same time that the TTP and AA's verification are being done.

Experimental Findings and Discussion

Our trials were carried out on a cluster of three computers, each of which has a quad-core Hp Q6600 2.40 Gigahertz processor, 4 GB of RAM, and two 7200 RPM hard disks. These computers were connected to one another via gigabit switched Ethernet. let's take a look at the length of the ciphertext. The summary of the RBE scheme reveals to us that the ciphertexts do not encompass any user-related data; rather, they are calculated using variables that encompass the identities of each of the ancestor responsibilities of the target role. To determine the size of the ciphertext, we compare the situation in which the target role does have 10, 100, and 1000 ancestor roles correspondingly.

Table I presents the lengths of the ciphertext when the plaintext sizes are 1000, 10000 and 100000 bytes accordingly. To begin, we make the observation that the size differences between both the plaintext and the ciphertext remain constant. Second, regardless of the amount of ancestor roles that are used, the total size of the ciphertext will not change. We have come to the conclusion that the size of the ciphertext is directly proportional to the width of the plaintext. This holds true regardless of the amount of roles or users that are capable of deciphering the ciphertext.

Table I: Ciphertext Length in Bytes

Plaintext Length	10 Roles	100 Roles	1000 Roles
1000	1342	1342	1342
10000	10342	10342	10342
100000	100342	100342	100342

Another crucial aspect of the cloud-based storage system is the length of the decryption key. According to the findings of our experiments, the length of the decryption key was 48 bytes, which has a size that is convenient for users. When a decryption key is not of a constant size, it is typically challenging for users to determine the memory needs that must be met on client devices in order for those devices to be able to hold encryption keys. The issue in question does not exist in our system.

The operations of encryption & decryption are the ones that are called upon the most frequently in the system. Because we have separated the decryption method so that it may be run in both the client and the cloud, the first thing that we did was measure how long it took for the cloud to perform the decryption. The time it takes for the cloud to decrypt data is measured from the moment the public cloud obtains the determined role variables from the private cloud until the moment it begins transmitting the ciphertext to the user. This is how the time is calculated. The decryption of cloud data was a computationally intensive task, therefore we broke it up into numerous threads. This strategy helps to cut down on the amount of time needed to decrypt data in the cloud by taking advantage of the fact that the cloud might have several processing cores running numerous threads at once. Through the course of our research, we have simulated a growing number of processor cores by elevating the total number of active threads. As a result of the fact that the calculation process utilizes a single thread as that of the master thread, the quad-core server is only capable of simulating a maximum of three cores.

Figure 4(a) depicts the amount of time that a cloud server used implementing a decryption method on the ciphertext of just a 1KB file. This time varies based on the number of users who are in the position that the user who is conducting the decryption corresponds to. In this particular instance, four other roles have been established as this role's ancestor roles. Growing the amount of users has the same effect on cloud decryption duration as increasing the amount of ancestor roles does. Increasing the amount of ancestor responsibilities has the exact same influence on cloud decryption duration as increasing the density performs. On the other hand, it is essential to keep in mind that the amount of roles is typically a far more manageable proportion of the total number of users participating in each job.

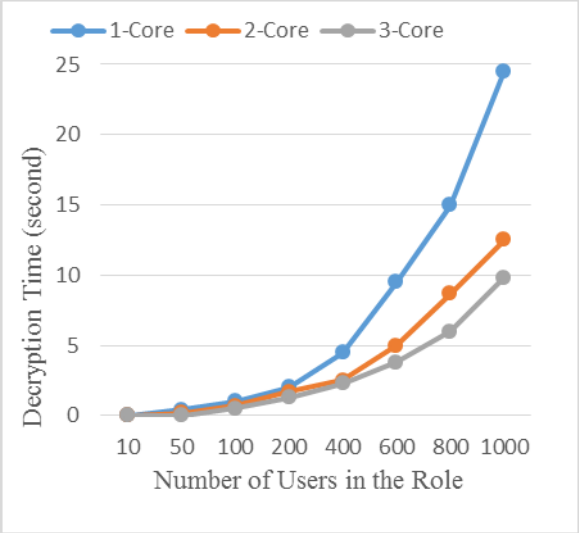

Fig. 5(a) Decryption Time of Public Cloud

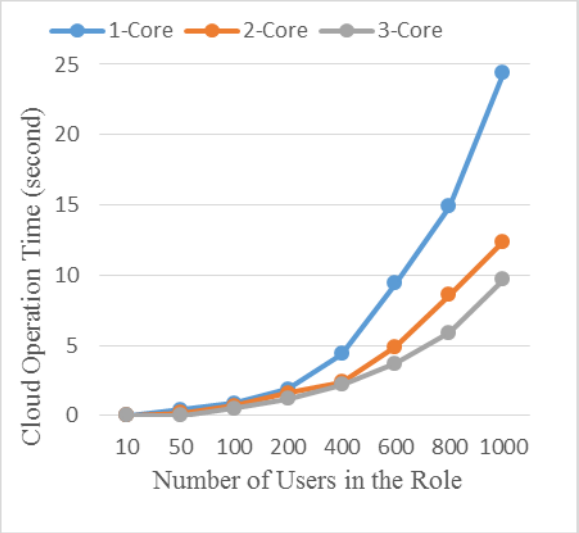

Fig. 5(b) Operation Time of Public Cloud in User Management

We found the cloud decryption duration is the amount of time it takes for the cloud to respond to decryption requests from users. After users have sent decryption queries to the cloud, users have to wait for this amount of time before the requests are processed. This time needs to be minimized so that users can have a positive experience when utilizing this cloud storage solution. In order to successfully decrypt the message, we have run a series of tests using 1, 2, and 3 processor cores. According to the findings, we have discovered that reducing the amount of time required for the cloud to respond can be accomplished by expanding the number of processing cores that are involved in the decryption. We consider that the cloud reaction rate can be managed to a reasonable range that is suitable to the users when it is implemented in a real cloud system that has a big amount of virtual processor cores. This range may be made suitable to the users. The outcome of the cloud decryption is stored in the cloud's cache. Therefore, it is not necessary for it to analyze for each and every decryption demand, which further minimizes the amount of time that is typically required for cloud decryption.

In our system, the calculations that are related to user management are some of those that are outsourced to the cloud. This is done by the role managers. The amount of time that the cloud has spent working together with the role administrators on this computation can be seen in Figure 4(b). For the intention of this experiment, we have established four roles that serve as the role's ancestors. In a manner analogous to the decryption performed by the cloud, the amount of time required for this calculation can be decreased by expanding the number of processing cores. The time spent operating the client is our next focus. On the client side, the amount of time required to encrypt and decrypt files of varying sizes is depicted in Fig. 5(a). For the sake of this study, we came up with 5 roles and assigned 10 users to each role. After selecting the file that needs to be encrypted, the owner clicks on the share button in the Java Applet. Once the file upload is finished, the owner gets a reaction from the cloud denoting that the transaction was effective. During our tests, we measured the amount of time it takes for the encryption process. The length of time required to decode a message was considered as a measure at which a user begins to receive ciphertext as from cloud to the point at which the plaintext is successfully written to a file on the user's local disk drive.

Because our solution makes use of the stream cipher ISAAC, the process of encrypting and decrypting data can take place even as the data is being sent from one location to another over a network. A key is generated and utilized in the RBE program's symmetric encryption method, which is part of the technique for encrypting and decrypting data using the RBE scheme. As can be seen in Figure 5(a), when the length of the plaintext is less than 100KB, the amount of time required for symmetric encryption and decryption, along with the transfer of data, is negligible in comparison to the amount of time required by the RBE method for the production of symmetric keys. As a result, the time according to our measurement does not change. When the length of the plaintext is greater than 1 megabyte, the amount of time required for symmetric encryption and decryption grows to be on the same order as the amount of time required for symmetric key creation. As a result, we observe that the amount of time required increases in tandem with the length of the plaintext.

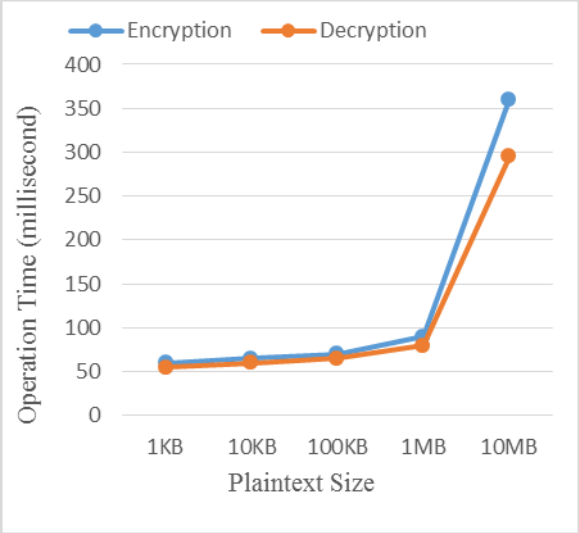

Fig. 6 (a) Various Plaintext Size

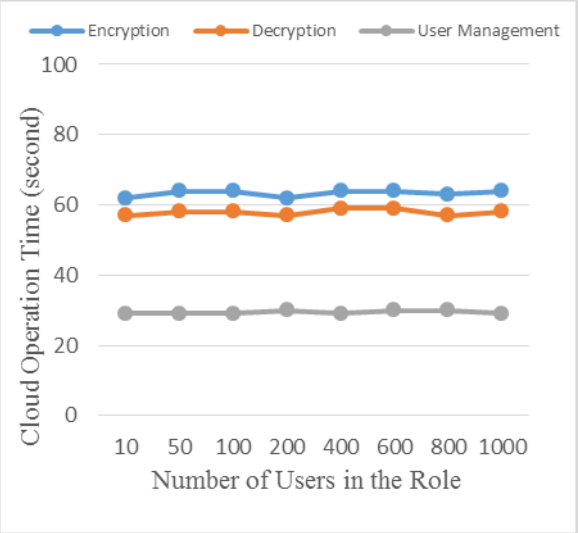

Fig. 6 (b) Various Number of Users

The time it takes customers to complete their activities is drastically cut down when clients' labor-intensive computations are sent to the cloud for processing. The amount of time that we spent measuring the encryption of 1Kilobyte of data by the data owner, the decryption of 1Kilobyte of data by users, and the user management of role managers is depicted in Figure 5(b) (when a role has a variable number of users assigned to it). Once more, there are four different ancestor roles for such a particular position. According to the findings, the amount of time required for these activities is quite stable, independent of the number of individuals or roles that are participating in the computation. As a result, it would be feasible to execute these procedures on portable devices with a reduced amount of necessary computing capabilities.

5. Conclusion and Future Scope

We proposed an encryption method using AES 128, Role Base Access Control and a cloud snapshot-based method for forensic examination for a secure data access strategy. The users of our system are able to obtain their master as well as private keys in a safe and secure manner from the middleware authority; TPA is responsible for providing and securing communication between multiple parties. Untrusted users will be able to benefit from the secure revocation that the scheme offers. In addition to that, the production of proxy keys is proposed in this study. When a data holder revokes access for a particular end user, the system will promptly expires any current keys and produce new ones for any shared users. By utilizing these kinds of strategies, the system is able to simultaneously attain the maximum possible level of security and privacy. From the experimental findings, we have discovered that computations involving encryption and decryption are effective on the client side. Furthermore, the amount of time required for decryption in the cloud can be shortened by having several processors, which is typical in a cloud setting. We consider that the proposed framework has the ability to be useful in business settings because it can capture real-world access policies depending on roles in a dynamic way and it can focus on providing secure data storage with in cloud that enforces these access control policies. As a result, we consider that the proposed framework has the possibilities to be useful in business settings.

References

[1] Y. Wang, Y. Ma, K. Xiang, Z. Liu and M. Li, “A Role-Based Access Control System Using Attribute-Based Encryption,” in IEEE Int. Conf. Big Data Artific. Intellig. (BDAI), June 2018, pp. 128-133.

[2] M. Ghafoorian, D. Abbasinezhad-Mood and H. Shakeri, “A thorough trust and reputation based RBAC model for secure data storage in the cloud,” IEEE Tran. Paral. Distribut. Sys., vol. 30, pp.778-788, 2018.

[3] S. U. Muthunagai and R. Anitha, “Secure Access Control Method in Cloud Environment Using Improved Attribute Based Encryption Technique,” Int. J. Engineer. Adv. Tech. (IJEAT), 2019.

[4] H. Gadouche, Z. Farah and A. Tari, “A correct-by-construction model for attribute-based access control,” Clust. Comp., pp. 1-12, 2019.

[5] S. Chakraborty, R. Sandhu and R. Krishnan, “On the feasibility of attribute-based access control policy mining,” in IEEE 20th Int. Conf. Inf. Reuse Integrat. Data Sci. (IRI), July 2019, pp. 245-252.

[6] M. Afshar, S. Samet and T. Hu, “An attribute based access control framework for healthcare system,” J. Phy. Conf. Ser. vol. 933, 2018, p. 012020.

[7] Y. Xue, K. Xue, N. Gai, J. Hong, D. S. Wei and P. Hong, “An attribute-based controlled collaborative access control scheme for public cloud storage,” IEEE Tran. Inf. Forens. Security, vol. 14, pp. 2927-2942, 2019.

[8] Y. Xu, W. Gao, Q. Zeng, G. Wang, J. Ren and Y. Zhang, “A feasible fuzzy-extended attribute-based access control technique,” Sec. Comm. Net., 2018.

[9] N. Geetha and M. S. Anbarasi, “Role and attribute based access control model for web service composition in cloud environment,” in IEEE Int. Conf. Computat. Intelligenc. Data Sci. (ICCIDS) June 2017, pp. 1-4.

[10] Viswanath, G., & Krishna, P. V. (2020). Hybrid encryption framework for securing big data storage in multi-cloud environment. Evolutionary Intelligence, 1-8.

[11] Li, H., Yu, C., & Wang, X. (2020). A novel 1D chaotic system for image encryption, authentication and compression in cloud. Multimedia Tools and Applications, 1-38.

[12] Bala, B., Kamboj, L., & Luthra, P. (2018). Secure file Storage in Cloud Computing Using Hybrid Cryptography Algorithm. International Journal of Advanced Research in Computer Science, 9(2).

[13] Olanrewaju, R. F., Abdullah, K., & Darwis, H. (2018, November). Enhancing Cloud Data Security Using Hybrid of Advanced Encryption Standard and Blowfish Encryption Algorithms. In 2018 2nd East Indonesia Conference on Computer and Information Technology (EIConCIT) (pp. 18-23). IEEE.

[14] Bhardwaj, A., Subrahmanyam, G. V. B., Avasthi, V., & Sastry, H. (2016). Security algorithms for cloud computing. Procedia Computer Science, 85, 535-542.

[15] V. K. Prasad, M. Shah, N. Patel and M. Bhavsar, “Inspection of trust-based cloud using security and capacity management at an IaaS level,” Procedia Computer Science, vol. 132, no. 1, pp. 1280–1289, 2018.

[16] P. S. Challagidad, V. S. Reshmi and M. N. Birje, “Reputation-based trust model in cloud computing,” Internet Things Cloud Computing, vol. 5, no. 1, pp. 5–12, 2017.

[17] L. A. A. Tawalbeh, F. Ababneh, Y. Jararweh and F. AlDosari, “Trust delegation-based secure mobile cloud computing framework,” International Journal of Information and Computer Security, vol. 9, no. 2, pp. 36–48, 2017.

[18] J. Wei, W. Liu and X. Hu, “Secure data sharing in cloud computing using revocable-storage identitybased encryption,” IEEE Transactions on Cloud Computing, vol. 6, no. 4, pp. 1136–1148, 2016.

[19] K. Lee, “Comments on secure data sharing in cloud computing using revocable-storage identity-based encryption,” IEEE Transactions on Cloud Computing, vol. 8, no. 4, pp. 1299–1300, 2020.

[20] B. Lang, J. Wang and Y. Liu, “Achieving flexible and self-contained data protection in cloud computing,” IEEE Access, vol. 5, pp. 1510–1523, 2017.

[21] C. Gu, F. Luo, Y. Li and W. Ding, “Dynamic access control model based on FAHP in cloud environment,” in IEEE 4th Int. Conf. on Computer and Communications, Chengdu, China, pp. 1938–1943, 2018.

[22] Q. Li, Y. Tian, Y. Zhang, L. Shen and J. Guo, “Efficient privacy-preserving access control of mobile multimedia data in cloud computing,” IEEE Access, vol. 7, pp. 131534–131542, 2019.

[23] S. Zhou, G. Chen, G. Huang, J. Shi and T. Kong, “Research on multi-authority CP-ABE access control model in multi-cloud,” China Communications, vol. 17, no. 8, pp. 220–233, 2020.

[24] Q. Zhang, S. Wang, D. Zhang, J. Wang and Y. Zhang, “Time and attribute-based dual access control and data integrity verifiable scheme in cloud computing applications,” IEEE Access, vol. 7, pp. 137594– 137607, 2019.

[25] Liu, L., Shafiq, M., Sonawane, V. R., Murthy, M. Y. B., Reddy, P. C. S., & kumar Reddy, K. C. (2022). Spectrum trading and sharing in unmanned aerial vehicles based on distributed blockchain consortium system. Computers and Electrical Engineering, 103, 108255.

[26] Sonawane, V., & Rao, D. R. (2015). HCMX: AN EFFICIENT HYBRID CLUSTERING APPROACH FOR MULTI-VERSION XML DOCUMENTS. Journal of Theoretical and Applied Information Technology, 82(1), 137.

[27] Sonawane, V. R., Singh, L. L., Nunse, P. R., & Nalage, S. D. (2015, December). Visual monitoring system using simple network management protocol. In 2015 International Conference on Computational Intelligence and Communication Networks (CICN) (pp. 197-200). IEEE.

[28] Sonawane, V. R., & Halkarnikar, P. P. Web Site Mining Using Entropy Estimation. In 2010 International Conference on Data Storage and Data Engineering.