A SECURE GROUP DATA SHARING IN CLOUD WITH DATA INTEGRITY VERIFICATION USING THIRD PARTY AUTHENTICATION

Dinesh E¹, Muniyarasu A², Dinesh Babu B J³, Nithish R⁴
¹Assistant Professor, ²,³,⁴UG Scholar
Department of Electronics and Communication Engineering, M.Kumarasamy College of Engineering, Karur, Tamil Nadu, India.
¹dineshe.ece@mkce.ac.in

ABSTRACT

Cloud computing provides high performance, accessibility and low cost for data storing and sharing, provides a better consumption of resources. However, as we now outsource the storage of potentially sensitive data to cloud providers, security issues become the primary constraint. To safeguard the confidentiality of personal information, both parties agree before uploading the encrypted data, to encrypt data files to the cloud. Cloud storage services can assist customers in lowering their data management costs and maintenance costs. 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, designing a secure and efficient information sharing scheme, particularly for dynamic businesses in the cloud, is far more difficult. We propose an AES-based encryption scheme that incorporates cryptographic methods and RBAC in this paper. as well as an In existing access control schemes, a system of anonymous oversight is used to protect both the privacy of data and the privacy of a user's identity. The existing group's public keys will be automatically changed if a group member's membership can be revoked, and the original data will not need to be encrypted again. Anyone in the system company can access the source in the cloud, and revoked users are unable to access the cloud if they've been revocation. Finally, use TPA to implement a data auditing scheme to track the modification of shared information on the cloud.

Keywords: Secure Data Sharing, Role with Time based access control, AES encryption, Group member revocation, Key Updation, Data Auditing, TPA Verification.

I. INTRODUCTION:

In the field of computing, access control is a security tactic that limits who or what has access to certain areas see or make use of certain information. It is a basic notion in the field of security reduces the danger to the environment company or organization. Access control can be manipulated in two ways: physically and logically. Access to universities, houses, rooms, and IT property can all be restricted. Connections to computer networks, files, and data are restricted by logical access control. By examining the necessary login credentials, such as passwords, PINs, biometric scans, security tokens, or other forms of authentication components, access control systems identify, authenticate, and authorize customers and entities. Multifactor authentication, which requires the use of multiple authentication factors, is commonly used as access to manipulate systems is protected as part of layered security.

Unauthorized gain access to physical and logical structures is minimized through access control. Because it ensures that Access control rules and surveillance information Access control is a critical component of security compliance since it protects private records such as client information programmes. Many companies now have infrastructure in place that limits access to networks, computers, packages, files, and sensitive information such as personally identifiable information and intellectual property.

Control access structures are they complicated in addition difficult to manipulate IT settings that are still changing with premises-based structures as well as cloud services. Following a series of as a result of high-profile
data breaches, technology companies are moving away from single sign-on systems and toward unified access control, which oversees access to both on-premises and cloud environments.

**BENEFITS OF ACCESS CONTROL**

Interest in cloud-based access to manipulate has surged in recent years, attracting businesses of various sizes and throughout industries. For everybody who has been seen the benefits of cloud-based systems, that’s hardly a surprise.

From streamlined system management to pricing flexibility, cloud-primarily based access manipulates offers some very interesting characteristics while compared with conventional, on-premise structures. Some key examples are listed underneath.

*Accessibility from anywhere with an Internet connection*

While some conventional access control systems provide some remote connectivity, cloud systems are designed with mobile accessibility in thoughts. Authorized users may view or manage device interest by logging into the appropriate access to control app, web portal, or network. This allows consumers to receive alerts and take action in the event of an incident or emergency, in addition to providing convenience.

*Flexible cost management*

Whereas conventional access control systems frequently include due to the high upfront costs of installation and equipment, cloud-based services provide much greater price flexibility. Instead of buying online equipment outright, users can prefer to lease equipment from an authorized reseller, avoiding large capital expenditures in favour of low ongoing operational costs.

*Reduced burden on user staff*

Maintaining a business service takes time and effort, especially for undertaking-critical ones like access control. By turning over the hosting and renovation of on-web site PCs, servers, facts-redundancy infrastructure and associated processes to the integrator, customers can dramatically decrease the weight on their very own IT personnel. Depending on the software itself, a cloud-based system can reduce burden of IT involvement by means of 97%. Should the consumer preference, the integrator may also be entrusted with part or all of the management of cloud services.

*System reliability*

Storing all records on a website can be a dangerous task: unless the person has strong safeguards in place, a power outage or network failure will disrupt service or result in data loss. Cloud-based access control systems traditionally use centralised data centres with effective backup energy and storage systems to ensure the security and integrity of the cloud service and information.

*Round-the-clock updates and monitoring*

Software updates and patches are critical for ensuring that the access control system is updated and that any vulnerability is addressed. However, these updates are only beneficial if they are implemented in a well-timed manner. Instead of forcing employees to handle updates, cloud-based access to manage systems allows them to be pushed out quickly and simultaneously across all machine devices. This improves device performance and security while reducing the likelihood of human error. Furthermore, many cloud-based systems provide 24/7 monitoring services, assisting in improving response times, providing peace of mind, and freeing up stop person workforce to address more pressing business issues.

As with traditional access control system, cloud-based solutions vary from commercial enterprise to enterprise, as do the benefits that customers care maximum about. The most exciting benefit of all is that consumers can find new ways to not only improve facility security, but also to maximize IT and other commercial enterprise-wide activities.

**ROLE BASED ACCESS CONTROL**

Controlling access to resources and the device itself is the first way a system provides protection to its sources and data. Access control to handle, on the other hand, is more than just deciding which users (subjects) have
access to which computing and network resources. Access control also keeps track of clients, files, and other resources. It manages a person's access to documents or sources (objects). Several steps, including identity, authentication, authorization, and transparency, are taken in access management systems before achieving honest access to resources or objects in general. However, as the networks and the number of users grew, IBAC was discovered to be vulnerable to one of these large increases. Access control ideas that covered the proprietor, group, and general public were presented. IBAC also proved to be a problem for dispensed structures. Managing device and source access has become more complex and prone to errors. RBAC (Role Based Access Control) is a brand-new tactic that has been implemented. RBAC (role-based access control) determines a user's system access based on his or her position. The position to which a person is assigned is based on the principle of least privilege. The function is specified with the fewest permissions or functionalities that are required to complete the task. If the privileges for a position exchange, permissions can be added or removed. When RBAC was extended across administrative domains, however, problems became apparent. It was also difficult to come to an agreement on what privileges should be associated with each role.

II. RELATED WORK

Chard, et.al.,[1] Because online social network relationships are frequently founded on genuine-life relationships, they can be utilized to construe a degree of trust among clients. Here's how you can use these connections to build a dynamic system called "Social Cloud," in which individuals can share a wide range of assets inside the setting of an interpersonal organization. Furthermore, the inherent socially remedial instruments (motivations, disincentives) can be utilized to create a cloud-based system for long haul sharing that has less protection and security worries than traditional cloud conditions. Sale frameworks are managed by the DRIVE meta scheduler. A converse Vickrey sell off convention module is utilized since the most well-known offering approach (truth telling) is all the more socially driven. It additionally recommends that "antis" is censorious.

Yang, et.al.,[2] Allow the server to register the evidence as a moderate estimation of the check (controlled by the test stamp and direct mixes of information blocks) with the goal that the inspector can check the verification utilizing this transitional worth in the proposed strategy. As a result, this technique would significantly decrease the evaluator's figuring load by moving the reviewer's processing to the cloud worker. To improve the adequacy of an inspecting framework, we utilize the Data Fragment Technique and Homomorphic Verifiable Tags. Information fracture diminishes capacity overhead and upgrades framework proficiency by lessening the quantity of information labels. The worker just answers to the examiner with the amount of information blocks and the result of labels, whose size is steady and equivalent to just a single information block, paying little mind to the number of information blocks are challenged, when utilizing homomorphic obvious labels. The cost of communicating is eliminated as a result.

Wang et al., et al., et al., et al. [3] Numerous factors should be viewed as when imparting information to an enormous bunch of people, like productivity, information trustworthiness, and the information proprietor's protection. Ring mark is a promising possibility for building an unknown and dependable information sharing framework. It permits an information proprietor to confirm his information namelessly, after which it very well may be put away or investigated in the cloud. In a conventional public key foundation (PKI), then again, the exorbitant testament check turns into a bottleneck for the versatility of this arrangement. An identity-based (ID-based) ring signature, which does not require certificate verification, may be used instead. In this job, add forward security to ID-based ring signatures to improve security: All previously generated signatures containing this user remain valid regardless of whether the user's secret key is undermined. This property is particularly valuable in any enormous scope information sharing framework, since it is difficult to request that all information proprietors re-confirm their information if a single user's secret key is compromised. In response to real-world data sharing needs, we proposed a new idea called Forward Secure ID-Based Ring Signature. In an ID-based ring mark plot, it permits forward security. This is the first time that a ring signature has been used in an ID-based environment.

Zhou et al., et al., et al., et al., et al. [4] Propose an RBE scheme that incorporates cryptographic and RBAC techniques. Our RBE scheme can be used to apply RBAC policies for encoded information put away in broad daylight mists. In light of the proposed conspire, we present a protected RBE-based crossover distributed storage design that empowers an association to safely store information in a public cloud while keeping up delicate data about the association's construction in a private cloud. This paper describes the plan of a safe RBAC-based distributed storage framework, with access control arrangements presented utilizing another job based encryption (RBE) method that we propose. This RBE plot implements RBAC approaches on encoded information put away in the cloud while also allowing for quick user revocation. The data in our RBE scheme can only be decrypted.

www.turkjphysiotherrehabil.org
and viewed by users with the proper positions as specified by an RBAC policy. Users who meet the role's criteria will be granted or denied permissions by the job. The cloud supplier (who stores the information) won't see the information's substance until he or she is assigned the appropriate role. Role hierarchies, in which roles inherit permissions from one another, will be handled by the proposed RBE scheme. A user should access the role if the proprietor has encoded the information for it. The client will actually want to get to the information from here on out, and the proprietor won't be needed to re-encode the information. A client's admittance to future encoded information for this job can be denied whenever, and the eliminated client will lose admittance to it. This technique allows our RBE scheme to achieve successful client-side decryption.

Fu, et.al.,[5] A Create a homomorphic undeniable bunch mark to propose another security mindful public evaluating component for shared cloud information. In contrast to existing arrangements, our own needs at any rate t assemble directors to attempt to recover a follow key, forestalling abuse of single-authority power and guaranteeing non-frameability. Here, we propose another security safeguarding public examining plan for numerous bunch supervisors in shared distributed storage, in light of a model for information (in a bunch) imparted to different bunch administrators. This recommended plot not just offers staggered security insurance (counting personality protection, detectability, and non-frameability), yet it additionally considers bunch client renouncement. 2) To screen all information block changes in mists, we create an information structure dependent on a paired tree. At the point when the current information block is defiled, bunch individuals will finish the information changes the paired tree to track down the latest right information block. 3) We utilize an approved verify method to approve TPAs's test messages. Subsequently, just TPAs affirmed by bunch clients can pass the verification and challenge the cloud, forestalling malignant difficulties.

III. EXISTING METHODOLOGIES

The second pattern is a many-to-many pattern, which defines a situation in which a significant number of customers in a common group must allow admittance to their information simultaneously.

IV. IDENTITY BASED ENCRYPTION

Integrating identity-based encryption in revocable storage (RS-IBE) in existing work adds forward/in reverse security of ciphertext by simultaneously implementing extra functionalities of client denial and ciphertext update.

IBE

Identity Based Encryption successfully addresses the problem of encryption key management (IBE). Any string can be used as a public key in IBE to encrypt data without using certificates. In identity-based systems, anyone can create a public key by using a realized personality esteem, for example, an ASCII string. A dependable

Fig 3.1 Existing System Architecture

The second pattern is a many-to-many pattern, which defines a situation in which a significant number of customers in a common group must allow admittance to their information simultaneously.
outsider, the Private Key Generator (PKG), is responsible for generating the corresponding private keys. Before creating a matching master private key, the PKG creates a ace public key. If they have the ace public key, any client will produce a public key that relates to the personality ID by joining it with the character esteem. The user who is authorised to apply for Identity ID contacts the PKG, which uses the master key to create a personal key for Identity ID. Users can now encrypt messages without having to first distribute keys to individual contributors. Because of technical limitations, pre-distribution of authenticated keys is difficult or impossible. However, in order to decrypt or sign messages, the approved individual must receive the optimum personal key from the PKG.

**RS-IBE**

The non-revocable data sharing system should guarantee confidentiality and backward secrecy. Furthermore, forward secrecy is guaranteed by the technique for unscrambling and re-scrambling all common information. However, this creates new challenges. It's worth mentioning that the decryption and reencryption processes require the use of users' secret keys, exposing the entire information sharing framework to new attacks. When all is said in done, a mysterious key's impact ought to be restricted to the most widely recognized unscrambling, and it is not recommended to use a secret key to regularly replace cypher textual content. Another point to consider is efficiency. To maintain the cypher text of the shared data up to date, the data supplier must download, decrypt, reencrypt, and upload it on a regular basis. This process is uncomfortable and unwanted for cloud users with limited computation and storage capacity because it has a high communication and computing cost.

**V. SECURE GROUP DATA SHARING WITH USER REVOCATION**

To facilitate data sharing, it is vital that only authorised users have access to data stored in the Cloud. Figure 4.1 depicts secure group partaking in the cloud. When the proprietor of a group wishes to share data with others, he or she gives the secret key for data encryption to all group members. The encrypted data can then be retrieved from the Cloud by any member of the institution and decrypted using the secret key, obviating the need for the group owner's intervention. This procedure has the disadvantage of being incredibly inefficient. When a member of the institution's access rights are returned to the group owner, that member must no longer have admittance to the relating information. Because the data access key is now in the hands of an unauthorised member of the organisation. As a result, the group owner must re-encrypt the data to change the key. The group owner would appropriate the new key to the group's existing clients at the point when the information is re-scrambled, which is inefficient computation.

This proposal also focuses on defining data access misbehaviour in the cloud using a data auditing scheme. Data sharing, which allows other users to share data, is one of the most prevalent cloud storage features. others with their information. The organisation specialises in distant information honesty examining. The proprietor must first create marks for information obstructs prior to transferring them to the cloud. These marks are utilized to check that the cloud claims these information blocks during the uprightness evaluating stage. There was likewise a bunch. The proprietor transfers these information squares to the cloud, alongside their relating marks. To be successful Due to the shortcomings of the existing auditing scheme, it is recommended that an efficient integrity auditing be conducted with the assistance of an outsider inspector.
VI. METHODOLOGY

AES Encryption

The block cipher is another name for the AES cypher. On AES, no successful attacks have been reported. AES has the advantages of being simple to implement on eight-bit processors and powerful on 32-bit structure processors. Multiple rounds of AES encryption are used. Sub-byte, shift row, mix column, and upload round key are all important steps in each round. The substitution of bytes using a lookup-up table is known as sub-byte. The moving of rows in accordance with the byte duration is known as shift row. The Galois topic matrix is multiplied by the mix column. Finally, the output matrix of the mix column is XORed with the round key in the upload round key step. The numerous rounds available

Algorithm Procedure

The set of regulations begins with an Add round key diploma observed via the usage of 9 rounds of 4 degrees a tenth round of three ranges This holds true for both encryption and decryption, with the exception that each degree of spherical the decryption set of policies is the inverse of its encryption set of rules counterpart. The following are the four ranges:

1. Fill in the blanks with bytes.
2. Rearrange the rows
3. Combine the columns
4. Include a round key

In reality, the Mix Columns stage is not included in the 10th spherical. The following are the first nine rounds of the decryption algorithm:

1. Rows with an inverse shift
2. Substitute bytes in the opposite direction
3. Add Round Key in the Inverse
4. Columns with Inverse Mix

The Inverse Mix Columns degree is left out of the tenth round once more. Each of these levels will now be taken into account in greater depth.

BENEFITS OF RBAC

It's dependable: Users' access to information can be easily controlled by organizations based on their positions.

It increases operational performance: Many transactions are automated thanks to RBAC, and workers don't waste time using applications and services that aren't required to complete their tasks

Because only a few individuals within an organization have access to sensitive data, it reduces the risk of security breaches and data leakage.

Scalability: As a business expands and hires more employees, the number of positions does not have to change. This makes things easier for HR and IT departments, which would otherwise have to deal with a slew of administrative tasks.

Improved security compliance: Having RBAC in place means that an organization meets the requirements for privacy and confidentiality.
VII. EXPERIMENTAL RESULTS
Experimental result shows the overall performance of the proposed system. Here Role based access control for data sharing and auditing schemes are implemented using PHP as front end and MySQL as back end software. This will helps to improve file security.

New Doctor Registration

Above figure shows the process of new doctor registration. Doctors are considered as group owner and they could register and get permission from cloud to access and share data through cloud.

Patient Registration
This figure shows the process of entering patient details. Central Authority has permission to add patient details and allocate patients to the specified doctors. Patients are considered as group members.

**File Upload**

Above figure shows the process of file uploading. In this process group owner can upload file to share. Uploaded files get encrypted and stored on server.

**Key Verification and File Download**
This figure shows the process of file downloading and key verification. After verification of shared secret keys, group members can get files in decrypted format.

**User Revocation**

This figure shows the user revocation process. Central Authority has permission to remove members from the group.

**Performance Measurement**
From the execution of the two calculations, the time intricacy for creating verification and checking information blocks (50; 100; 200; 400; 500) is calculated. The computational variance for a huge number of files could not be calculated due to the device's setup constraints. The graph below depicts the average time it takes to generate proofs.

<table>
<thead>
<tr>
<th>Number of Blocks</th>
<th>Proof Generation Time (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Existing</td>
</tr>
<tr>
<td>100</td>
<td>1.2</td>
</tr>
<tr>
<td>200</td>
<td>2.3</td>
</tr>
<tr>
<td>300</td>
<td>3.4</td>
</tr>
<tr>
<td>400</td>
<td>4.5</td>
</tr>
<tr>
<td>500</td>
<td>5.5</td>
</tr>
</tbody>
</table>

**Verifiction Time:**

The mean of 20 trails based on the execution of the suggested algorithm is used to calculate the time complexity of proof confirmation of information blocks (50; 100; 200; 400; 500). The computational variance for a huge number of files could not be calculated due to the device's setup constraints. The graph below shows the average proof verification time.

<table>
<thead>
<tr>
<th>Number of Blocks</th>
<th>Existing(ms)</th>
<th>Proposed(ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>0.25</td>
<td>0.42</td>
</tr>
<tr>
<td>200</td>
<td>0.5</td>
<td>0.75</td>
</tr>
<tr>
<td>300</td>
<td>0.8</td>
<td>1.2</td>
</tr>
<tr>
<td>400</td>
<td>1.025</td>
<td>1.5</td>
</tr>
<tr>
<td>500</td>
<td>1.65</td>
<td>1.9</td>
</tr>
</tbody>
</table>
Audit Time Analysis for Different File Sizes:

The auditing time may differ based on the file size. The below table show the various file sizes in MB and auditing time taken for different file size in milliseconds. The graph shows the auditing time variation based on different file sizes.

<table>
<thead>
<tr>
<th>File Size (MB)</th>
<th>Auditing Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1049.66</td>
</tr>
<tr>
<td>2</td>
<td>1523.36</td>
</tr>
<tr>
<td>3</td>
<td>1573.84</td>
</tr>
<tr>
<td>4</td>
<td>1643.11</td>
</tr>
<tr>
<td>5</td>
<td>1732.45</td>
</tr>
</tbody>
</table>

VIII. CONCLUSION

As data sharing requests continue to increase, cloud data sharing will become available in the future. A review of secure data sharing in a cloud computing environment was submitted as part of the proposed work. The data is outsourced by the group owner to save money. The group owner does not have authority over their information in light of the fact that the cloud specialist organization is an outsider. The issue with cloud-based information sharing is protection and security concerns. AES encryption, Group data sharing, and User revocation are just some of the approaches outlined in this paper to help protection and secure information sharing. The study finds that a safe enemy of impact information sharing plan for gatherings is more efficient, facilitates access control mechanisms, and ensures data confidentiality in group sharing. In addition, the proposed mechanisms support batch auditing, as well as effective integrity auditing of shared data. TPA would not gain any insight into the information content put away on the cloud worker during the fruitful inspecting measure, which not only relieves the cloud user of the time-consuming auditing task, but also eliminates the fear of their outsourced data being leaked.

REFERENCES


