IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 6, April 2023

Secure Role Based Access Control Data Sharing Approach and Cloud Environment

Om Shama[1], Usama Baig[2], Raman Chandak[3]
Students, Department of Computer Engineering [1]
Professor, Department of Computer Engineering[2,3]
Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India

Abstract: *the primary objective of cloud storage is to maintain data integrity, which involves implementing measures to prevent unauthorized access and ensuring that data can be regenerated if mishandled. To achieve this, a proxy server will be assigned the task of protecting and restoring data in case of unauthorized modifications. Users' data will be stored in both public and private areas of the cloud, with only public data being accessible to users and private data being kept more secure. Cloud storage offers users various redundancy configurations to balance performance and fault tolerance, with data availability being critical in distributed storage systems, especially when node failures are common in real-life scenarios. In this research, a proposed aes 128 encryption algorithm and role-based access control (rbac) scheme are explored to provide secure data storage and sharing, as well as a secure user access policy. Additionally, a backup server approach is used as a proxy storage server for ad hoc data recovery for all distributed data servers. The experiment's analysis is proposed in both public and private cloud environments, utilizing keywords such as rbac, elgamal encryption scheme, proxy key generation, advanced encryption standard (aes), and more.*

Keywords: Cloud

I. INTRODUCTION

The current system allows users to act as both Data Owners and Data Consumers, and authorities are assumed to have strong computational abilities while being monitored by government offices due to the presence of personally identifiable information in some attributes. To address access control in public cloud storage, a threshold multi-authority CP-ABE scheme called TMACS has been proposed. TMACS enables multiple authorities to manage a uniform attribute set by using (t; n) threshold secret sharing to share the master key among them. Legal users can generate their secret key by interacting with any t authorities, making TMACS both verifiable secure and robust. A hybrid multi-authority scheme that combines traditional methods with TMACS has also been constructed to handle attributes coming from different authorities while maintaining security and system-level robustness.

An attribute revocation mechanism has been proposed for multi-authority data access control in Cloud storage systems. It achieves both forward and backward security, but a bidirectional re-encryption method used in cipher text updating introduces security vulnerabilities. An attack method has been proposed, showing that a revoked user can still decrypt new cipher texts that require the new version secret keys to decrypt.

To address data privacy and user identity privacy in existing access control schemes, a semi-anonymous privilege control scheme called Anony Control has been introduced. AnonyControl decentralizes the central authority to limit identity leakage and achieves semi-anonymity. The file access control has also been generalized to privilege control, allowing for the management of privileges for all operations on cloud data. AnonyControl-F has been fully introduced to prevent identity leakage and achieve full anonymity. Both AnonyControl and Anon Control-F are secure under the decisional bilinear Diffie-Hellman assumption, and their feasibility has been exhibited through performance evaluation.

Cipher-text Policy Attribute-based Encryption (CP-ABE) is a suitable technology for data access control in cloud storage due to the direct control it provides data owners over access policies. However, applying existing CP-ABE schemes to data access control for cloud storage systems is difficult due to the attribute revocation problem. To address

DOI: 10.48175/IJARSCT-9425

this, an expressive, efficient, and revocable data access control scheme has been designed for multi-authority cloud storage systems. It proposes a revocable multi-authority CP-ABE scheme and applies it as the underlying technique for the data access control scheme.

To address the challenge of sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud, a secure multi-owner data sharing scheme called Mona has been proposed. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. The storage is divided into N disjoint sets controlled by each authority, with each authority only aware of part of the attributes. A Data Owner outsources encrypted data files to the Cloud Servers, who merely store them. Newly joined Data Consumers request private keys from all the authorities, and they do not know which attributes are controlled by which authorities. The authorities jointly create a corresponding private key and send it to the Data Consumers. While all Data Consumers can download any of the encrypted data files, only those whose private keys satisfy the privilege tree Tp can execute the operation associated with privilege p. The server executes an operation p only if the user's credentials are verified through the privilege tree Tp.

II. PROPOSED SYSTEM

In the proposed system, there are five entities: data owner, user, third-party auditor (TPA), cloud server, and attacker (untrusted entity). The data owner uploads a data file to the cloud server using a cryptographic algorithm, and once the file is stored in the database, the owner receives a notification about successful storage. The data owner has full access to the specific data file and can share it with any user who requests it. However, the user cannot access the file without a key, which is granted by the TPA if the user is trusted.

The shared user can access the file anytime through the cloud server, and if the data owner revokes access, the user cannot access the file. The system is also designed to prevent SQL injection attacks. The data owner can also share and revoke the file to individual users, and the system generates a new proxy key when access is revoked. In case an untrusted user alters or hacks the file, the system can recover the file and give access to the user.

To further enhance the system's security, a new primitive called identity-based remote data integrity checking is proposed, which ensures secure cloud storage. The security model of this primitive is based on two important properties: soundness and perfect data privacy. A new construction of this primitive is provided, which achieves both soundness and perfect data privacy. The proposed protocol is efficient and practical, as demonstrated by both numerical analysis and implementation

III. LITERATURE SURVEY

Title Author and Year	Proposed System	Findings	Drawbacks
Wei Li, KaipingXue TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage [1]	System proposed a access control systems for public cloud storage, brings a single-point bottleneck on both security and performance against the single authority for any specific attribute. First design multi-authority access control architecture to deal with the problem. By introducing the combining of (t, n) threshold secret sharing and multi-authority CP-ABE scheme, then proposes and realizes a robust and verifiable multi-authority access control system in public cloud storage, in which multiple authorities jointly manage a uniform attribute set. Further by efficiently combining the traditional multi-	**1:**Provide security of Access Policy 2: Security against collision as well as injection attack 3: Data confidentiality guarantee 4: Soundness and completeness 5: Security against Compromising Aas	**1:** Bottleneck issue generate when user request’s very high. 2: multiple resources required for all authorities.

DOI: 10.48175/IJARSCT-9425

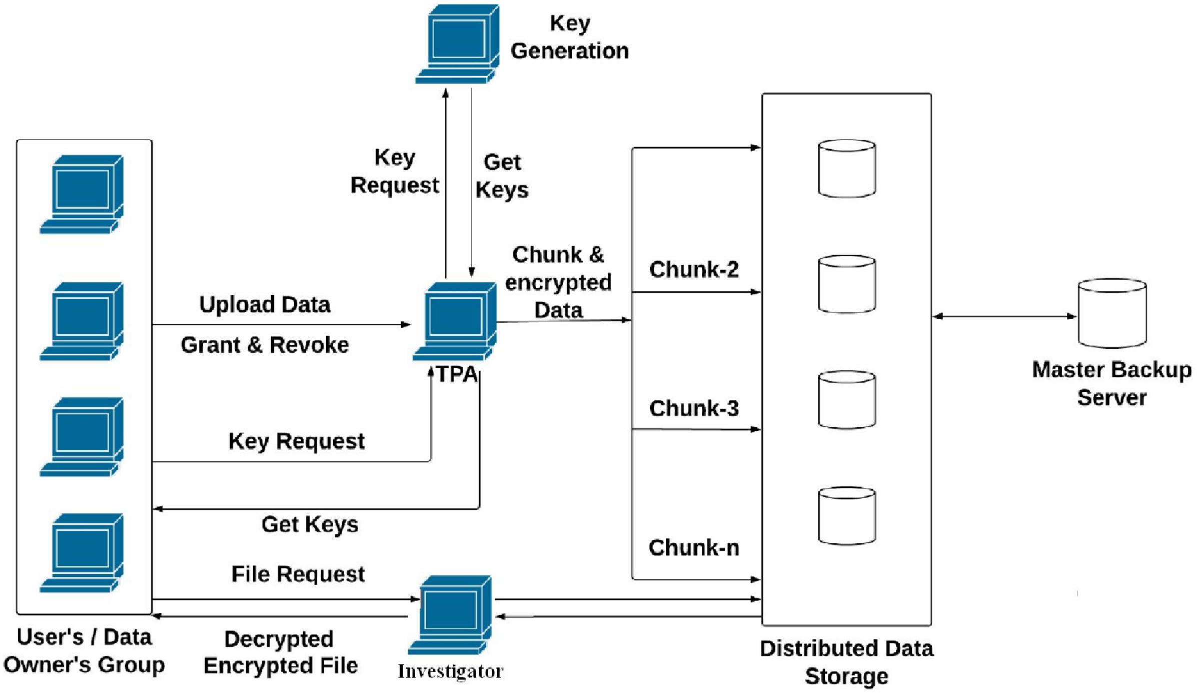
	authority scheme with this scheme, construct a hybrid one, which can satisfy the scenario of attributes coming from different authorities as well as achieving security and system-level robustness. Cloud storage is an important service of cloud computing		
L. Zhou, V. Varadharajan, and M. Hitchens Achieving secure role-based access control on encrypted data in cloud storage [2]	Proposed a role-based encryption (RBE) scheme that integrates the cryptographic techniques with RBAC. The RBE scheme allows RBAC policies to be enforced for the encrypted data stored in public clouds. Based on the proposed scheme, system also present a secure RBE-based hybrid cloud storage architecture that allows an organization to store data securely in a public cloud, while maintaining the sensitive information related to the organization's structure in a private cloud. System describes a practical implementation of the proposed RBE-based architecture and discusses the performance results. They also demonstrate that users only need to keep a single key for decryption, and system operations are efficient regardless of the complexity of the role hierarchy and user membership in the system.	**1:** System architecture provides public as well private cloud which can provide resources on ad hoc basis. **2:** administrator first define the policy for authenticate users, and he can change also that will provide more flexibility for system	**1:** No provide for key management server or not allocate any resource for key server. 2: Very expensive for private cloud resources.
Jung, et al. a semi-anonymous attribute-based privilege control scheme [3]	AnonyControl and a fully anonymous attribute-based privilege control scheme AnonyControl-F to address the user privacy problem in a cloud storage server. The proposed scheme was able to protect user's privacy against each single authority. Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F. The scheme was tolerant against authority compromise and compromising of up to (N −2) authorities did not bring the whole system down. The author provides detailed information about security and feasibility of the scheme. Also implements the real toolkit of a multi-authority-based encryption scheme AnonyControl and AnonyControl.	**1:** System generates a key from multiple authorities' base on different attributes it will provide highest security to encrypted data. **2:** Authorities (t,n) any T authority from n provide a keys to end user once request has generated	**1:** Multiple resources required. **2:** Sometime increase time complexity to checking keys from all authorities when specific authority is busy.
E. Goh, H. Shacham, N.	System presents SiRiUS, a secure file system designed to be layered over	1: Minimal Client Software. A SiRiUS user	**1:** A serious problem with this

Modadugu, and D. Boneh, proposed Sirius: Securing remote untrusted storage **[4]**	insecure network and P2P file systems such as NFS, CIFS, OceanStore, and Yahoo! Briefcase. SiRiUS assumes the network storage is untrusted and provides its own read-write cryptographic access control for file level sharing. Key management and revocation is simple with minimal out-of-band communication. File system freshness guarantees are supported by SiRiUS using hash tree constructions.	should need to run only a user-level daemon. Usersshould not be required to upgrade or patch the client OS kernel. 2: Performance. SiRiUS should not perform unreasonably worse than its underlying file system.	legacy network file system is that their access control mechanisms are insecure and easily defeated. 2: File name collusion problem should be occurring because of multiple distributed keys.
Kan Yang and Xiao huaJiafirst key-policy attribute-based encryption (KP-ABE) schemes allowing for non-monotonic access structures [5]	In this work first show that a certain class of identity-based broadcast encryption schemes generically yields monotonic KP-ABE systems in the selective set model. Then describe a new efficient identity-based revocation mechanism that, when combined with a particular instantiation of our general monotonic construction, gives rise to the first truly expressive KP-ABE realization with constant-size cipher- texts. The downside of these new constructions is that private keys have quadratic size in the number of attributes.	**1:** No middle warerequired it will reduce the network load of system. **2:** single key algorithm used it will reduce.	**1:** Single keys base algorithm used for data encryption, the security can be leak sometime. 2: There can be possible SQL injection base as well collusion base attack due to less security
K. Ren, C. Wang, and Q. Wang “Security Challenges for the Public Cloud” 2012 [6]	This paper they introduce a detailed analysis of the cloud computing security issues and challenges focusing on the cloud-computing types and the service delivery types.	1) The continued in flux ofmobile devices and personal devices is creating more security challenges. 2) Extension of sensitive application to pointsoutside the enterprise perimeter, including across the Internet, is creating new challenges.	In this work they only detailed analysis of the cloud computing security issues and challenges they don’t solve any issues of cloud computing security problems.
B. Wang, B. Li, and H. Li, “Panda: Public Auditing for Shared Data with EfficientUser Revocation in the Cloud” 2015 [7]	In this paper, they propose a novel public auditing mechanism for the integrity of shared data with efficient user revocation in mind.	1) It follows protocols and does not pollute data integrity actively as a malicious adversary. 2) Cloud data can be efficiently shared among a large number of users, and the public verifier is able to handle a large number of auditing tasks simultaneously and	1) Straightforward method may cost the existing user a huge amount of communication and computation resources. 2)The number of re-signed blocks is quite large or the membership of the

		efficiently.	group is frequently changing.
J. Yuan and S. Yu, “Public Integrity Auditing for DynamicData Sharing With Multiuser Modification” 2015 [8]	In this paper, authors propose a novel integrity auditing scheme for cloud data sharing services characterized by multiuser modification, public auditing, high error detection probability, efficient user revocation as well as practical computational/ communication auditing performance.	1) We explore on the secure and efficient shared data integrate auditing for multi-user operation for cipher-text DB. 2) By incorporating the primitives of victor commitment, asymmetric group key agreement and group signature, we propose an efficient data auditing scheme while at the same time providing some new features, such as traceability and countability. 3) We provide the security and efficiency analysis of our scheme, and the analysis results show that our scheme is secure and efficient.	1) In the Wang et al. scheme, the user revocation problem is not considered and the auditing cost is linear to the group size and data size. 2) However, the scheme assumed that the private and authenticated channels exist between each pair of entities and there is no collusion among them. Also, the auditing cost of the scheme is linear to the group size.
Y. Zhu, H.G. Ahn, H. Hu, S.S. Yau, H.J. An, and C.J. Hu, **“Dynamic Audit Services for Outsourced Storages in Clouds”.**[9]	In this paper, authors propose a dynamic audit service for verifying the integrity of an untrusted and outsourced storage.In addition, they propose a method based on probabilistic query and periodic verification for improving the performance of audit services.	In this work, they introduce a dynamic audit service for integrity verification of untrusted and outsourced storages.Public auditability, Dynamic operations, Timely detection, Effective forensic, Lightweight.	Unfortunately, the traditional cryptographic technologies, based on hash functions and signature schemes, cannot support for data integrity verifycation without a local copy of data. In addition, it is evidently impractical for audit services to download the whole data for checking data validation due to the communication cost, especially for large-size files.

C. Wang, S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage". 2013 [10]	In this paper, authors propose a secure cloud storage system supporting privacy-preserving public auditing. They further extend their result to enable the TPA to perform audits for multiple users simultaneously and efficiently.	To the best of their knowledge, our scheme is the first to support scalable and efficient privacy preserving public storage auditing in Cloud. Specifically, their scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner.	Although outsourcing data to the cloud is economically attractive for long-term large-scale storage, it does not immediately offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the success of cloud architecture.

IV. SYSTEM ARCHITECTURE



V. GOALS AND OBJECTIVE

Our objective is to enhance the security of our cloud system by implementing various measures. Firstly, we aim to prevent collusion attacks, brute force attacks, and malicious queries that could compromise the confidentiality, integrity, and availability of the data. Additionally, we plan to establish a new verification and authentication protocol between the system authorities and a trusted third party to enhance the overall security posture.

To further improve the system's efficiency, we intend to optimize the time required for authentication and authorization processes. Another critical aspect of our security strategy is to mitigate the risk of malicious queries that could exploit system vulnerabilities. We will strive to ensure the highest level of security against external and internal attacks, such as collusion attacks and SQL injection attacks. One of our key strategies is to implement the AES encryption scheme in the proposed system architecture, which will provide strong protection for sensitive data stored in the cloud system

VI. LIST OF FUNCTIONALITIES

Data Owner:

- Data Owner uploads data and share data with others through the cloud storage.
- Data owner can share data files as well as download data files at his side.
- One more point in that Revocation; in revocation data owner can revoke any user with data file for permanently.

TPA (Third Party Auditor):

- The TPA is responsible for auditing the integrity of cloud data on behalf of group users.
- Third Party Auditor can accept or reject the users request for file access.
- The legal users are honest and will not leak any private information to others.
- User receives the requested file decrypted by TPA.

User:

- In that user can access the file through the cloud storage then he must request to TPA for data accessibility.
- When TPA grant access the request of users then and then only user can access the data or download the data.
- The legal group users are honest and will not leak any private information to others.

Cloud Server:

- Cloud server provides storage for user’s data.
- The cloud provides enormous storage space and computing resources for group users. Through cloud storage, group users can enjoy the data sharing service.
- It stores all the data in encrypted format and retrieves the data on TPA’s request.
- It is connectedto a WAN network.

Investigator:

- To analyse attacks on the system.
- TPA send push notification to investigator when he found hash value of file is changed and data is modified by attacker.:
- TPA encrypt the file and file content like name, data, creation data and generate the hash value in database. After encryption, he stores encrypted file in cloud server and proxy server.

VI. METHODOLOGY

This work involves the use of advanced encryption techniques to enable secure data access control. Specifically, the proposed approach includes a multi-Authority scheme where all data records are encrypted by multiple authorities, and a multi-Client scheme where search capabilities are encrypted under an access policy before being sent to the clients. In addition, the Fine-Grained Access Control Attribute-based encryption (ABE) protocol is utilized to provide precise access control for encrypted data based on the client's attributes. This protocol ensures that only clients with attributes that satisfy the access policy can decrypt the encrypted messages that are encrypted under certain policies. Overall, this approach enables efficient and secure data access control while minimizing negotiation and maximizing privacy protection

VII. CONCLUSION

In this work the system proposes a secure Role Base Access Control (RBAC) data sharing scheme for untrusted

DOI: 10.48175/IJARSCT-9425

environment in the cloud. In our scheme, the users can securely get their private keys from middleware authorities, TPA provides secure communication between multi users. Also, our scheme canprovide secure revocation for untrusted users. The proxy key generation has also been proposed in this work. When data owner revokes any specific end user system automatically expired the existing keys and generates new keys for all shared users. The system can achieve the highest level of security as well as privacy through such approaches.

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

ACKNOWLEDGMENT

The Present World Of Competition There Is A Race Of Existence In Which Those Are Having Will To Come Forward Succeed. Project Is Like A Bridge Between Theoretical And Practical Work. With This Will We Joined This Project. First, We Would Like To Thank The Supreme Power The Almighty God Who Is Obviously The One Has Always Guided Us To Work On The Right Path Of Life.

We Sincerely Thank Prof. R.H. Borhade Sir Head Of The Department Of Computer Science of Smt Kashibai Navale College Of Engineering, For All The Facilities Provided To Us In The Pursuit Of This Project.

We Are Indebted To Our Project Guide Prof. D.N. Bhaturkar, Department Of Computer Science Of Smt. Kashibai Navale College Of Engineering. We Feel It's A Pleasure To Be Indebted To Our Guide For His Valuable Support, Advice And Encouragement And We Thank Him For His Superb And Constant Guidance Towards This Project.

We Are Deeply Grateful To All The Staff Members Of The CS Department, For Supporting Us In All Aspects.

We Acknowledge Our Deep Sense Of Gratitude To Our Loving Parents For Being A Constant Source Of Inspiration And Motivation.

REFERENCES

[1]. Wei Li, Kaiping Xue, Yingjie Xue, And Jianan Hong, "TACS: A Robust And Verifiable Threshold Multiauthority Access Control System In Public Cloud Storage, IEEE Transactions On Parallel And Distributed Systems, VOL.24, No. 06, October 2017.

[2]. Taeho Jung, Xiang-yang Li, Zhiguo Wan, And Meng Wan, "Control Cloud Data Access Privilege And Anonymity With Fully Anonymous Attribute-based Encryption", IEEE Transactions On Information Forensics And Security, VOL. 10, No. O1, January 2017.

[3]. S. Kamara And K. Lauter, "Cryptographic Cloud Storage," In Proceedings Of The 14th Financial Cryptography And Data Security. Springer, 2010, Pp. 136-149.

[4]. B. Wang, B. Li, And H. Li, "Panda: Public Auditing For Shared Data With Efficient User Revocation InThe Cloud, IEEE Transactions On Services Computing, Vol. 8, No. 1, Pp. 92-106, 2015.

[5]. I. Yuan And S. Yu, "Public Integrity Auditing For Dynamic Data Sharing With Multiuser Modification," IEEE Transactions On Information Forensics And Security, Vol. 10, No. 8, Pp. 1717 - 1726, Aug. 2015.

[6]. Y. Zhu, H.G. Ahn, H. Hu, S.S. Yau, H.J. An, And C.J.Hu, "Dynamic Audit Services For Outsourced Storages In Clouds," IEEE Transactions On Services Computing, Vol.6, No. 2, Pp. 409-428, 2013.

[7]. C. Wang, S. Chow, Q. Wang, K. Ren, And W. Lou, "Privacy-preserving Public Auditing For Secure Cloud Storage," IEEE Transactions On Computers, Vol. 62, No.2, Pp. 362-375, 2013.

[8]. N. AttraPadung, B. Libert, And E. Pana_eu, "Expressive Key Policy Attribute-based Encryption With Constantsize Cipher Texts." In Proceedings Of The 14th International Conference On Practice And Theory In Public Key Cryptography. Springer, 2011, Pp. 90-108.

[9]. T. Jung, X. Li, Z. Wan, And M. Wan, "Privacy Preserving Cloud Data Access WithMultiauthorities," In Roceedings Of The 32nd Ibe International ConterenceOn Computer Communications. Bbs. 2013. Do 2625-2633.

DOI: 10.48175/IJARSCT-9425