Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 2 : 2024
ISSN :**1906-9685**

Journal of Nonlinear Analysis and Optimization : Theory & Applications
Editors-in-Chief :

SECURE DATA SHARING IN CLOUD STORAGE FOR BIG DATA APPLICATION

Gudivada Eepsitha Jahnavi PG STUDENT(M.Tech) ,DEPT OF Computer Science & Engineering

Email:eepsithajahnavig@gmail.com

Boddeda Ganesh, Associate. Prof, DEPT OF Computer Science & Engineering
Email:komal1234.ganesh@gmail.com

Avanthi Institute Of Engineering & Technology (Narsipatnam),Anakapalli (Ap)

ABSTRACT:

A cloud-based massive data sharing system uses a cloud service provider's storage capacity to share data with authorized users. The issue of data confidentiality may arise when cloud providers, in contrast to traditional solutions, store shared data in massive data centers outside of the data owner's trust zone. A secret sharing group key management protocol (SSGK) is presented in this article to guard against unauthorized access to shared data and the communication process. Unlike other attempts, SSGK uses a secret sharing method to disseminate the group key and a group key to encrypt the shared data. Comprehensive security and performance assessments demonstrate that our method greatly lowers data security and privacy concerns. sharing in cloud storage while also saving around 12% of storage space.

Keyword:-Cloud,AES,BigData,SSGK

I INTRODUCTION

Cloud Computing [1], Business Intelligence [2], Data Mining [3], Industrial Information Integration Engineering (IIIE) [4], and Internet-of-Things [5] are developing big data technologies that have ushered in a new age for future Enterprise Systems (ES) [6]. Cloud computing is a novel computing architecture in which all resources on the Internet constitute a cloud resource pool and can be dynamically assigned to various applications and services. When compared to traditional distribution systems, it saves a significant amount of money while providing excellent flexibility, scalability, and efficiency for job execution. The various corporate investments in creating and maintaining a supercomputing or grid computing environment for smart applications may be substantially minimised by employing Cloud Computing services. Despite these benefits, when storing personally identifiable information in the cloud, security needs skyrocket [7], [8]. Thisraises regulatory compliance concerns since sensitive data is being migrated from the federate domain to the distribute domain. To reap the benefits of big data technology, security and privacy concerns must beaddressed first. creating a security system for cloud storage is a difficult undertaking. Because shareddata on the cloud is outside the control zone of legitimate participants, the problem of making the shared data available on demand by legitimate users should be resolved. Furthermore, as the number of parties, devices, and apps participating in the cloud grows, so does the number of access points, making appropriate access control increasingly challenging. Finally, shared cloud data is subject to being deleted or improperly changed by the cloud provider ornetwork intruders. It is challenging to protect shared data from unwanted deletion, alteration, and falsification.

Traditionally, there are two distinct approaches for promoting the security of a sharing system. One example is accesscontrol [11], in which only authorised users listed in the access control table have access to shared data. The alternative technique is group key management which involves using a group key to secure shared data. Although access control ensures that data is only accessible by authorised users, it does not protect against cloud provider attacks.The group key is often handled by an independent third party in existing group key sharing systems. Such techniques arebased on the assumption that the third party is always truthful. However, this assumptionis not always correct, particularly in the context of cloud storage.

To solve the security issue of sharing dataon cloud storage, the article proposes a secret sharing group key management protocol, and our protocol employs the following methods to identify or prevent fraud. To begin, symmetric encryption techniques are used to encrypt the shared data in order to make it accessible on demand by legal users. When one data owner wishes to share data with others, the data owner distributes the decryption key to the lawful sharers. Second, the key used to decode the shared data determines who has access to the shared data. Asymmetric encryption techniques are used to encrypt the interactive communication, allowing only authorised participants to decode thekey. Third, if illegal users get access to shared data, this protocol employs a secret sharing method to assign keys to genuine participants. By incorporating a security mechanism into traditional service-oriented clouds, we may create a securityaware cloud and ensure the privacy of data sharing on cloud storage. Building a security mechanism on cloud storage may help tospeed cloud implementation in mission- critical business scenarios.

II. LITERATURE SURVEY

1. "In cloud computing, an efficient and secure identity-based encryption method with equality test," Xinyi Huang et al. [1] proposed an Identity-based (ID-based) ring signature that avoids the need for certificate verification. The security level of ring signature is enhanced by offering a forward secure ID-based ring signature technique. In this technique, if a user's secret key is hacked, all prior produced signatures are included, and the user remains legitimate. If a single user's secret key is stolen, it is difficult to request that all data owners reauthenticate their data. It is very crucial in any large-scale data sharing system, because it is highly efficient and does not require any pairing processes. The user secret key is a single integer, but the key update process necessitates exponentiation. This approach is beneficial, particularly for those who want authentication and user privacy.

2. "A scalable attributed-set-based access control in cloud computing with both sharing and full-fledged delegation of accessrights," In cloud computing, Huang Qinlong et al. [2] proposed an attribute-based secure data sharing method with Efficient revocation (EABDS). This suggested approach encrypts data with Data encryption key (DEK) using symmetric encryption method and then encrypts DEK using Ciphertext policy attribute-based encryption to ensure data confidentiality and achieve fine-grained access control (CP-ABE). The homomorphic encryption approach is used to solve the key escrow problem by generating attribute secret keys of users by attribute authority with the help of a keyserver. By creating the attribute secret keys alone, this homomorphic encryption approach prevents the attribute authority from accessing the contents. The EABDS

method provides instantaneous attribute revocation, which ensures forward and backward security while requiring less computation from users. The advantages of this approach are that it is more safe and efficient.

III PROPOSED SYSTEM

SSGK proposes an efficient solution to the safe challenges of data sharing on cloud storage without relying on any trusted third party. Aside from employing a symmetric encryption method [11] to encrypt the shared data, an asymmetric algorithm [12] and a secret sharing scheme are employed toprevent unwanted users from obtaining the key needed to decode the shared data. Both Blakley and Shamir separately proposed secret sharing systems in 1979 as a way for safeguarding cryptographic keys. A dealerdivides a secret into n shares and distributes them to n shareholders in a secret sharing system. This secret may be reconstructed using any t shares. Chor et al. expanded the concept of original secret sharing and introduced the concept of verified secret sharing (VSS). The verifiability attribute means that shareholders may check to see if their shares are consistent.

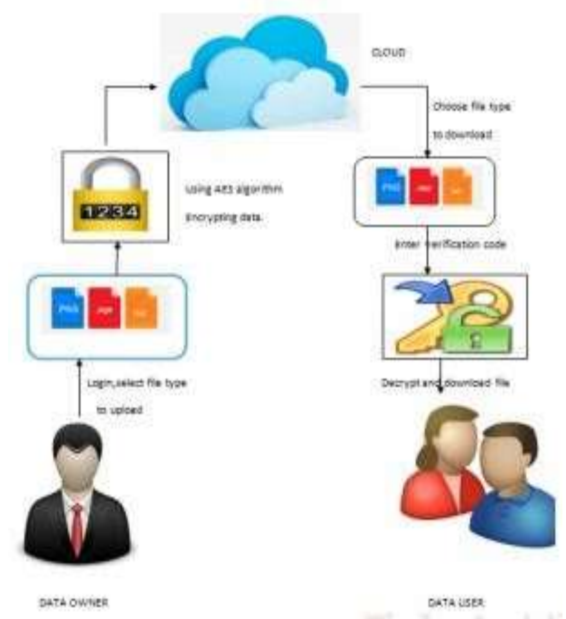

Fig 1:System Architecture

IV IMPLEMENTATION

4.1 The cloud service provider

offers a public platform for data owners to store andexchange encrypted data. Owners' data access is not controlled by the cloud provider. Any user can freely download the encrypted data.

4.2 The data owner

establishes the access policy and encrypts its data using a symmetric encryption method and a group key. A sharing group is made up of group members who met the access policy. Theowner then employs a secret sharing mechanism to deliver the encryption key to the sharing group.

4.3 Members of the group

Each member of the group, including the data owner, is issued a unique and a pair of keys.Members of the group can easily obtainany encrypted material from the public cloud that they are interested in. However, the user can only decrypt the data if and only if the data owner provides the data decryption key.

V Results

SECURE DATA SHARING IN CLOUD STORAGE FOR BIG DATA APPLICATION

Fig 2:-home page

VI CONCLUSION

In this work, we present a unique group key management mechanism for cloud storage data sharing. We employ RSA and verified secret sharing in SSGK to give the data owner fine-grained control over the outsourced data without depending on a third party. Furthermore, we provide a comprehensive analysis of various attacks and related countermeasures, demonstrating that GKMP is secure even under weaker assumptions. Furthermore, we show that our protocol has reduced storage and processing complexity. Our scheme's security mechanism ensures the anonymity of grid data in cloud storage. Encryption encrypts transmission on the public channel; a validated security system restricts access to grid data to authorised parties. Our approach is more practical due to its improved storage and calculation speed. Each member of the group, including the data owner, is issued a unique and a pair of keys.Members of the group can easily obtain any encrypted material from the public cloud that they are interested in. However, the user can only decrypt the data if and only if the data owner provides the data decryption key.

The issue of forward and backward security in group key management may need changes to our protocol. Future study will focus on developing an efficient dynamic mechanism of group members.

VI REFERENCES

[1] J. Sen (2011a). A Stable Mechanism for Protecting Web Servers against Distributed Denial of Service Attacks. International Journal of Network Security and Applications, Vol. 3, No. 2, March 2011, pp.162-179.

[2] J. Sen (2011b). A Novel Detection Mechanism for Distributed Denial of Service Attacks Proceedings of the First International Conference on Computer Science and Information Technology (CCSIT'11), Springer CICS Vol 133, Part III, January 2011, Bangalore, India, pp. 247-257.

J. Sen, J. Sen, J. Sen, J. Sen, J. Sen, J (2010a). An Intrusion Detection System Based on Agents for Local Area Networks. International Journal of Communication Networks and Information Security (IJCNIS), August 2010, Vol. 2, No. 2, pp. 128-140.

[4] J. Sen (2010b). Clustered Wireless Ad Hoc Network Intrusion Detection Architecture Proceedings of the 2nd IEEE International Conference on Intelligence in Communication Systems and Networks (CICSyN'10), July

2010, Liverpool, UK, pp.202-207.

[5] J. Sen (2010c). A Fault-Tolerant and Robust Distributed Intrusion Detection System. Proceedings of the First International Conference on Parallel, Distributed, and Grid Computing (PDGC'10), pp. 123-128, Waknaghat, India, October 2010.

[6] J. Sen (2010d). A Framework for Distributed Trust Management for Detecting Malicious Packet Dropping Nodes in a Mobile Ad Hoc Network. International Journal of Network Security and its Applications (IJNSA), Vol. 2, No. 4, October 2010, pp. 92-104.

[7] J. Sen (2010e). A Framework for Distributed Trust and Reputation in Mobile Ad Hoc Networks. Proceedings of the First International Workshop on Trust Management in Peer-to-Peer Systems (IWTMP2PS), July 2010, Chennai, India, pp. 538-547. Vol. 89 of Springer CCIS.