OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

PROTECTING DATA FOR ACCESSING PUBLIC CLOUD STORAGE WITH DIFFERENT ATTRIBUTE AUTHORITIES

SHAIKH AFSHAN JABEEN MD ABDUL SHKOOR[1], ASST.PROF. V. S. KARWANDE[2]

ME Student, Department of Computer Science & Engineering, EESGOI , India[1]

HOD, Assistant Professor, Department of Computer Science and Engineering, EESGOI, India [2]

Abstract: ***Protecting data and managing data access in a public cloud storage system is a difficult task. Cipher text Policy Attribute-Based Encryption (CP-ABE) is a promising technique for providing versatile, fine-grained, and secure data access control for cloud storage with honest-but-suspicious cloud servers. When a CP-ABE scheme is used in a large-scale cloud storage system, however, numerous works have been proposed in which the single attribute authority must conduct the time-consuming user legitimacy verification and hidden key distribution, resulting in a single-point performance bottleneck. Clients can be trapped in line for a long time to receive their mystery keys, resulting in the framework's inefficiency. Despite the fact that multi authority access control proposals have been proposed, these plans are still unable to overcome the drawbacks of single-point bottleneck and low performance, due to the way each authority still deals with a disjoint characteristic set independently. In this paper, a novel heterogeneous architecture is proposed to solve the problem of a single point performance bottleneck and provide a more robust access control scheme with auditing capabilities. Multiple attribute authorities are used in this system to spread the burden of user legitimacy verification. Meanwhile, a CA (Central Authority) is implemented in this scheme to produce hidden keys for validity checked users, and each of our scheme's authorities manages the entire attribute collection individually. This system increases key generation efficiency while still meeting security requirements.***

Keywords: *CA (Central Authority); Cipher text Policy Attribute-Based Encryption (CP-ABE); attribute authorities (AAs); Location-aware attribute-based access control system (LABAC).*

I INTRODUCTION

The Cloud storage is an important service in Cloud computing technology because it frees users from document/data management issues and allows them to monitor and access their data remotely through a link. However, safeguarding data and managing data access is a difficult task, prompting a number of studies to suggest CP-ABE schemes for providing versatile, fine-grained, and reliable data access control for cloud storage. When a CP-ABE scheme with single attribute authority is used in a large-scale cloud storage system, it must conduct the time-consuming user legitimacy verification and secret key distribution, which results in a single-point performance bottleneck. Despite the fact that multi authority access control proposals have been proposed, these plans are still unable to overcome the drawbacks of single-point bottleneck and low reliability, as each authority maintains a disjoint attribute collection separately. To address this issue, a novel heterogeneous architecture has been proposed to eliminate the problem of a single point performance bottleneck and provide a more effective access control scheme with an auditing mechanism. This scheme used multiple attribute authorities to distribute the burden of user legitimacy verification and a CA (Central Authority) to produce secret keys for legitimacy checked users, with each authority managing the entire attribute collection separately. This scheme can be made more reliable by providing verification to the data owner and his or her file, by providing a log to learn about the user, and by monitoring CAs. actions with an observer. If a difference is detected, the observer produces a report and replaces the CA, who was selected from among the AAs, with a new AA to serve as CA. In cloud storage, data access control is a difficult problem to address. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is a possible cryptographic technique for addressing the above issue, allowing data access control to be enforced based on users' permanent characteristics. However, in some cases, access policies are linked to both temporary and permanent requirements for users (such as access time and location). CP-ABE is incapable of coping successfully with such circumstances. In this paper, we look at a scenario in which a user's access privilege is based on their attributes as well as their location. We propose a cloud-based location-aware attribute-based access control system (LABAC) to meet this data access control requirement. LABAC is the only organization that combines CP-ABE with location trapdoors to create access policies. In this way, data owners can combine both user attributes and locations in a flexible way to implement fine-grained data control. The fact that LABAC does not need any additional revocation mechanisms to revoke location-aware access privileges when the user's location change is a competitive advantage. A study of security and performance is provided, demonstrating the security and efficiency of LABAC in realistic implementations.

II LITERATURE SURVEY

As big data systems are rapidly expanding in cloud computing, privacy has become a major concern. In different ways, the advantages of implementing these new technologies have enhanced or modified service models and improved application efficiency. However, the rapidly increasing amount of data sizes has created a slew of problems in practice. One of the serious problems during data processing and delivery is the execution time of data encryption. Many existing applications forego data encryption in order to achieve a standard of efficiency that balances privacy concerns. We focus on privacy in this paper and suggest a novel data encryption strategy called Dynamic Data Encryption Strategy (D2ES). Under time constraints, our proposed solution aims to selectively encrypt data and use privacy classification methods. Using a selective encryption technique within the necessary execution time parameters, this approach is designed to optimize the privacy security scope. In our tests, the efficiency of D2ES was evaluated, providing proof of the privacy enhancement [1].

Cloud Computing is the long-awaited vision of computing as a utility, in which users can store their data securely in the cloud and access high-quality software and services on demand from a shared pool of configurable computing resources. Users can be relieved of the responsibility of local data storage and maintenance by outsourcing their data. However, since users no longer have physical control of potentially large amounts of outsourced data, data integrity security in Cloud Computing is a difficult and potentially dangerous challenge, especially for users with limited computing resources and capabilities. As a result, allowing public auditability for cloud data storage protection is crucial so that consumers can rely on an external audit party to verify the integrity of outsourced data when necessary. The following two basic conditions must be fulfilled in order to safely implement an appropriate third party auditor (TPA): 1) TPA should be able to effectively audit cloud data storage without requiring a local copy of the data and without imposing any unnecessary on-line burden on the cloud customer; 2) The third-party auditing process should not introduce any new vulnerabilities that compromise user data privacy. We use and combine the public key based holomorphic authenticator with random masking in this paper to create a privacy-preserving public cloud data auditing scheme that meets all of the above requirements. We explore the technique of bilinear aggregate signature to extend our key result into a multi-user environment, where TPA can perform multiple auditing tasks simultaneously, to facilitate efficient handling of multiple auditing tasks. The proposed schemes are probably safe and highly effective, according to extensive security and performance analysis[2].

Various privacy-preserving approaches to ensure privacy and protection of electronic health records (EHRs) in the cloud have been described in a systematic and thorough analysis of security and privacy-preserving issues in e-health solutions. In order to develop a robust security model for EHR, this paper highlights the research challenges and directions in cyber security. We performed a comprehensive review of the IEEE, Science Direct, Google Scholar, PubMed, and ACM databases for papers on EHR approaches published between 2000 and 2018, and summarized them in terms of architecture styles and evaluation strategies. Several papers were surveyed, examined, and evaluated, and the following tasks were identified: 1) EHR security and privacy; 2) e-health data in the cloud security and privacy requirements; 3) EHR cloud architecture; and 4) various EHR cryptographic and non-cryptographic approaches. In e-Health applications, big data offers a wealth of information and expertise. There are important privacy and protection issues that need to be addressed right away. The emphasis of research should be on how to be more effective. EHR protection protocols are comprehensive, and strategies to protect the privacy and confidentiality of EHR data are being investigated. Details about patients must be kept confidential. [4].

Cloud storage is a common technology that allows you to store and view data over the Internet rather than on your local machine's hard drive. Cloud computing allows users to store data without worrying about its accuracy or reliability. However, storing data in the cloud raises some security concerns. Data owners lose physical ownership of their data when they outsource it to the cloud. Certain Cloud Service Providers (CSPs) could be deceptive with the data of cloud customers, stealing data from the cloud and selling it to third parties for profit. As a result, while outsourcing data to the cloud is cost-effective and reduces the complexity of long-term storage and maintenance, cloud servers have the least guarantee of data confidentiality, privacy, protection, and availability. A variety of solutions have been suggested to resolve cloud security problems. The integrity verification strategy for outsourced data is the subject of this article. The proposed scheme incorporates an encrypting method with a technique for maintaining data integrity. The encrypting scheme used here is ElGamal, a public key cryptographic algorithm, and the SHA-256 hash function is used to ensure data storage accuracy on an untrusted server[5].

Cloud computing has advanced dramatically in recent years. Cloud storage technology is receiving more attention and better development as the amount of unstructured data grows at an exponential rate. However, under the new storage system, all of a user's data is stored solely on cloud servers. In other words, consumers lose control of their data and risk privacy breaches. Traditional privacy security systems typically rely on encryption technology, but these approaches are unable to withstand an attack from inside a cloud server. We propose a three-layer storage architecture based on fog computing to solve this issue. The proposed architecture would take full advantage of cloud storage while still safeguarding data privacy. Furthermore, the Hash-Solomon code algorithm is intended to break data into multiple sections. Then, to preserve privacy, we can store a small portion of the data on a local machine and on a fog server. Furthermore, this algorithm can calculate the distribution proportion stored in the cloud, fog, and local machine, respectively, using computational intelligence. The viability of our scheme has been validated through theoretical safety review and experimental evaluation, making it a valuable complement to existing cloud storage schemes[6].

Data owners are being increasingly inspired in the evolving cloud computing model to outsource their complex data management systems from local sites to the commercial public cloud for greater flexibility and cost savings. Sensitive data must be encrypted before being outsourced to protect users' privacy, which makes efficient data use a difficult job. We identify and solve the problem of privacy-preserving query over encrypted graph-structured data in cloud computing (PPGQ) for the first time in this paper, as well as provide a set of strict privacy criteria for such a safe cloud data utilization system to become a reality. The concept of "filtering-and-verification" is extended to our work. To provide feature-related details about each encrypted data graph, we first create a feature-based index, and then use the powerful inner product as the pruning method to carry out the filtering procedure. We propose a safe inner product computation technique and then develop it to meet various privacy requirements under the known-background threat model to meet the challenge of supporting graph query without privacy breaches [7].

III. SYSTEMS ARCHITECTURE

Data owner encrypts the data with symmetric key algorithm. we formulates the access policy over an attribute set and then encrypts the symmetric key under the policy according to the public keys obtained by CA. Data owner is verified for its legitimacy during registration and data is also verified before uploading.

User The data user (consumer) is assigned a global user identity Uid by CA. It can get any interested encrypted data from the cloud and the user can decrypt the encrypted data if and only if its attribute set satisfy the access policy. Central Authority (CA) It is the administrator of the entire system. It helps in system construction by setting up system parameters and generating public key for attribute of universal attribute set. It generates unique ids for AAs and users after registration. It generates secrete keys for legitimacy verified users. It has capacity to trace which AA has maliciously verified a user. Attribute Authorities (AAs) The attribute authorities (AAs) manages the whole attribute set individually so it can perform legitimacy verification of any user independently. AAs verify users legitimate attributes and generates intermediate key to assist CA to generate secret keys. Cloud Server Cloud servers provide public platform for data owners to store and share their encrypted data. Encrypted data can be freely downloaded by any user.

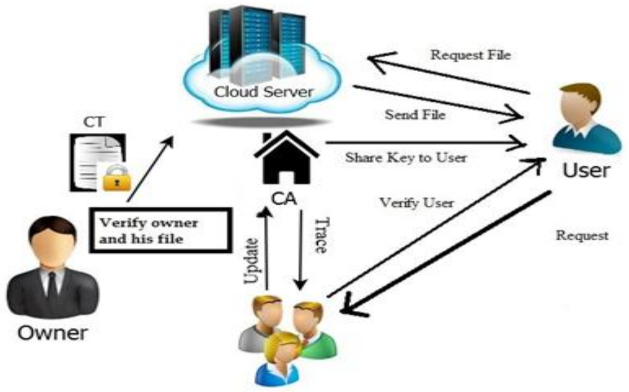
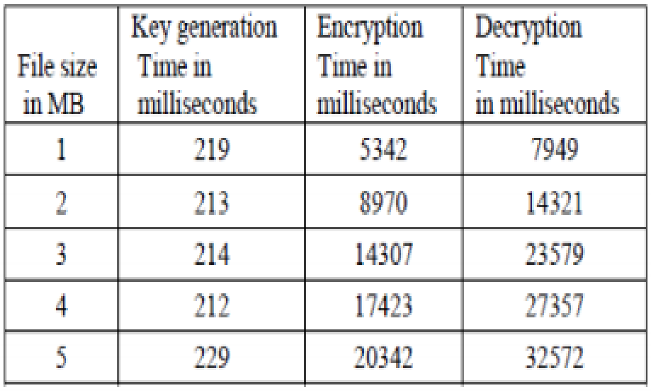


Figure No 3.1: System Architecture

IV EXPERIMENTAL RESULTS

Performance Analysis as shown in Table 4.1. The framework is implemented using the ABE algorithm, and its efficiency is assessed. The device determined how long it would take to generate a key. The average time required for ten users is 30 milliseconds. The device is in the process of distributing and managing hidden keys. Following the completion of the system's implementation, the system will be evaluated on its output in terms of Uploading and downloading time for various file sizes. The time it takes to distribute keys and share files.



File size in MB	Key generation Time in milliseconds	Encryption Time in milliseconds	Decryption Time in milliseconds
1	219	5342	7949
2	213	8970	14321
3	214	14307	23579
4	212	17423	27357
5	229	20342	32572

Table No 4.1: Performance Analysis

V CONCLUSION

A new heterogeneous architecture has been proposed to remove the single point output bottleneck and improve the efficiency of existing CP-ABE schemes. The proposed scheme provides fine-grained, stable, and efficient access control with one-CA/multi-AAs for public cloud storage by essentially reformulating the CP-ABE cryptographic technique into this novel system. Multiple AAs are used in this scheme to share the burden of time-consuming legitimacy verification and to be on standby for fulfilling new user requests. An auditing tool has been suggested for tracing an attribute authority's potential misbehavior. To ensure that this scheme is safe and effective, it was subjected to a rigorous security and performance review. The scheme will effectively resist individual and colluded malicious users, as well as honest-but-curious cloud servers, according to the security review.

REFERENCES

[1]. Keke Gai, Meikang Qiu, Hui Zhao “Privacy-Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing,” IEEE TRANSACTIONS ON BIG DATA, 2016.

[2] Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,” IEEE INFOCOM 2010.

3] Keke Gai, Meikang Qiu, Hui Zhao, Jian Xiong, “Privacy-Aware Adaptive Data Encryption Strategy of Big Data in Cloud Computing,” IEEE 3rd International Conference on Cyber Security and Cloud Computing, 2016.

[4] Shekha Chenthara , Khandakar Ahmed, Hua Wang , And Frank Whittaker, “Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing,” IEEE Translations and content mining are permitted for academic research only, 2019.

[5] Sarah Shaikh, Deepali Vora, “Secure Cloud Auditing over Encrypted Data,” International Conference on Advanced Computer Science, 2013.

[6] Tian Wang , Jiyuan Zhou, Xinlei Chen , Guojun Wang , Anfeng Liu , Yang Liu, “A Three-Layer Privacy Preserving Cloud Storage Scheme Based on Computational Intelligence in Fog Computing,” IEEE Transactions On Emerging Topics in Computational Intelligence, Vol. 2, No. 1, February 2018.

[7] Ning Cao, Zhenyu Yang, Cong Wang, Kui Ren, Wenjing Lou, “Privacy-Preserving Query over Encrypted Graph-Structured Data in Cloud Computing,” International Conference on Distributed Computing Systems, 2011.

[8] Zhangjie Fu, Kui Ren, Enabling personalized search over encrypted outsourced data with efficiency improvement 2015 IEEE.

[9] Zhangjie Fu, Xingming Sun and Sai Ji, Towards efficient content-aware search over encrypted outsourced data in cloud IEEE INFOCOM 2016.

[10] Jianan Hong, Kaiping Xue TAFC: Time and attribute factors combined access control on time sensitive data in public cloud 2015 IEEE.

[11] Yingjie Xue, Jianan Hong, Wei Li and Kaiping Xue, LABAC: A location-aware attribute-based access control scheme for cloud storage 2016 IEEE.

[12] Wei Li, Kaiping Xue, Yingjie Xue, and Jianan Hong TMACS: A robust and verifiable threshold multi-authority access control system in public cloud stor age 2015 IEEE.