



Article Title: **Secure Data Storage and Sharing Techniques: A Review**

Secure Data Storage and Sharing Techniques: A Review

Akila Rahini R¹, Sukanya S T²

¹Department of Master of Computer Application, Narayanaguru College of Engineering,
Anna University, Chennai.

²Assistant Professor, Department of Master of Computer Application, Narayanaguru College
of Engineering, Anna University.

ABSTRACT

A large number of researchers, academia, government sectors, and business enterprises are adopting the cloud environment due to the least upfront capital investment, maximum scalability, and several other features of it. Despite the multiple features supported by the cloud environment, it also suffers several challenges. Data protection is the primary concern in the area of information security and cloud computing. Numerous solutions have been developed to address this challenge. However, there is a lack of comprehensive analysis among the existing solutions and a necessity emerges to explore, classify, and analyze the significant existing work for investigating the applicability of these solutions to meet the requirements. This paper presents a comparative and systematic study, and in-depth analysis of leading techniques for secure sharing and protecting the data in the cloud environment. The discussion about each dedicated technique includes: functioning for protecting the data, potential and revolutionary solutions in the domain, the core and adequate information including workflow, achievements, scope, gaps, future directions, etc. about each solution. Furthermore, a comprehensive and comparative analysis of the discussed techniques is presented. Afterward, the applicability of the techniques is discussed as per the requirements and the research gaps along with future directions are reported in the field. The authors believe that this article's contribution will operate as a catalyst for the potential researchers to carry out the research work in the area. In this paper investigating various methods used in the existing work for the secure data storage.

Keywords: Cloud Computing, Data Storage, Cryptography, Watermarking, Risk Based Security.

1 Introduction

Data is acknowledged as the most vital asset of an organization because it defines the uniqueness of every enterprise. It is the main foundation of information, knowledge, and ultimately the wisdom for correct decisions and actions. It might be helping to cure a disease, boost a company's revenue, make a building more efficient or be responsible for achieving the targets, and improving the performance. Furthermore, storage, analysis, and sharing of data are the essential services required by any organization to upgrade its performance. However, with the explosive evolution of data, enormous pressure emerges on the enterprises for storing the voluminous data locally. Also, it has become difficult to explore the data due to limited



Article Title: Secure Data Storage and Sharing Techniques: A Review

resources. Most businesses have shifted to the cloud for these services due to its several advantages such as on-demand service, scalability, reliability, elasticity, measured services, disaster recovery, accessibility, and many others. Cloud computing is a paradigm that enables huge memory space and massive computation capacity at a low cost. It allows users to obtain the intended services across multiple platforms irrespective of location and time and consequently conveys an extensive convenience to the cloud users.

By migrating the local data management system into cloud storage and using cloud-based services, users can accomplish cost savings and productivity enhancements to manage projects and establish collaborations. Therefore, individuals and organizations are shifting increasingly to the cloud for their multiple services. With the growing expansion of cloud computing technologies, it is not difficult to imagine that almost all the businesses will be switched to the cloud in the foreseeable future. Despite the multiple features offered by cloud computing, it encounters several impediments that may obstruct its fast growth, if not tackled appropriately. Consider a real implementation, where an enterprise permits its staff or departments to store and share the data through the cloud. By exploiting the cloud, the enterprise can be completely released from the burden of maintaining and storing the data locally.

Nevertheless, it also endures various security threats, which are the leading concerns of cloud users. Firstly, outsourcing the data to the cloud servers signifies that the data is out of the users' control resulting in discomfort to the users because the outsourced data may comprehend sensitive and valuable information. Secondly, data sharing is frequently put into operation in a hostile and open environment, and the cloud server turned out to be a target of attacks. In the worst condition, users' data may be revealed by the cloud server itself for illegal profit. Furthermore, the data need to be shared among distinct relevant stakeholders, for instance, business partners, employees, customers, etc., interior or exterior of the organization's premises for upgrading the performance of the business. However, the recipient party can maltreat this data and disclose it purposefully or inattentively to some unauthorized third party. A sharing environment where the data owners need to share the organization's valuable data to the cloud platform due to the limited storage and computational capacity of the enterprises and the multiple benefits of clouds. Furthermore, the cloud data is shared with multiple users as per different requirements for its utility purpose. However, the recipient party may leak the data after obtaining it. The data can be leaked by the involved parties or may steal by the unauthorized party through illegal access. Data leakage or loss may induce a severe threat to the organization's confidentiality. It can diminish the value of shareholders, decline the firm's rank and status, and destruct the enterprise's goodwill and reputation.

As the data is an important asset of an organization, thus it is essential to keep this asset secure. There arises a necessity for solutions that can protect the data efficiently in the sharing environment. A number of models for data protection in the cloud environment have been explored and developed for many applications. Typically, data protection is achieved through leakage prevention and leaker detection and this article concentrates on achieving efficient



Article Title: Secure Data Storage and Sharing Techniques: A Review

protection by preventing leakage and detecting the malicious entity responsible for leakage as depicted. The major approaches for preventing data leakage are tailored by utilizing cryptography, access control mechanisms, and differential privacy with machine learning techniques while leaker detection is mainly achieved through watermarking and probabilistic techniques.

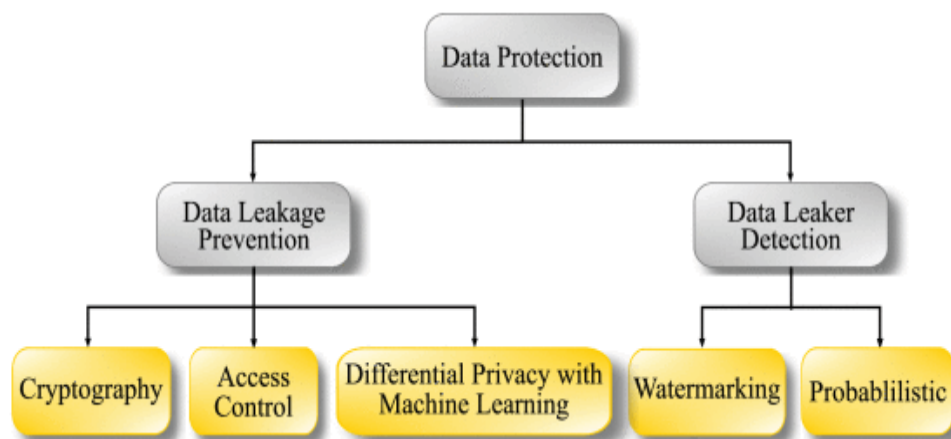


Figure 1: *Data Protection*

2 Related Works

[1] Online Information Leaker Identification Scheme for Secure Data Sharing. In 2020, A.K. Singh and I. Gupta, demonstrated on this paper proposes a novel scheme for the leaker identification that deals with the dynamic scenario by handling the requests of the users in an online custom. A distribution strategy is introduced having less risk associated with exposing the data and furthermore improves the likelihood of identifying the leaker when the information is revealed by the malicious user. The observed results signify an improvement for average probability, average success rate, and detection rate respectively compared to the prior work. Also, the proposed framework significantly minimizes the possibility of data leakage and synchronously achieves.

[2] A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing. In 2018. R. Li, C. Shen, H. He, X. Gu, Z. Xu and C.-Z. Xu, demonstrated on the popularity of cloud computing, mobile devices can store/retrieve personal data from anywhere at any time. Consequently, the data security problem in mobile cloud becomes more and more severe and prevents further development of mobile cloud. There are substantial studies that have been conducted to improve the cloud security. However, most of them are not applicable for mobile cloud since mobile devices only have limited computing resources and power. Solutions with low computational overhead are in great need for mobile cloud applications. In this paper, propose a lightweight data sharing scheme (LDSS) for mobile cloud computing. It adopts CP-ABE, an access control technology used in normal cloud environment, but changes the



Article Title: Secure Data Storage and Sharing Techniques: A Review

structure of access control tree to make it suitable for mobile cloud environments. LDSS moves a large portion of the computational intensive access control tree transformation in CP-ABE from mobile devices to external proxy servers. Furthermore, to reduce the user revocation cost, it introduces attribute description fields to implement lazy-revocation, which is a thorny issue in program based CP-ABE systems. The experimental results show that LDSS can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments.

[3] Layer-Based Privacy and Security Architecture for Cloud Data Sharing. In 2019, I. Gupta, N. Singh and A. K. Singh, demonstrated on the management of data while maintaining its utility and preservation of security scheme is a matter of concern for the cloud owner. In order to minimize the overhead at cloud service provider of applying security over each document and then send it to the client, we propose a layered architecture. This approach maintains security of the sensitive document and privacy of its data sensitivity. To make a balance between data security and utility, the proposed approach categorizes the data according to its sensitivity. Perseverance of various categorization requires different algorithmic schemes. We set up a cloud distributed environment where data is categorized into four levels of sensitivity; public, confidential, secret, top secret and a different approach has been used to preserve the security at each level. At the most sensitive layers i.e. secret and top secret data, we made a provision to detect the faulty node that is responsible for data leakage. Finally, experimental analysis is carried out to analyze the performance of the layered approach. The experimental results show that time taken (in ms) in processing 200 documents of size 20 MB is 437, 2239, 3142, 3900 for public, confidential, secret and top secret data respectively when the documents are distributed among distinct users, which proves the practicality of the proposed approach.

[4] SELI: Statistical Evaluation Based Leaker Identification Stochastic Scheme for Secure Data Sharing. In 2020, I. Gupta and A. K. Singh, demonstrated on a data leakage has become a critical challenge for any organisation, especially when the third party is involved with legitimate permissions to access its confidential data. This study provides a statistical evaluation-based leaker identification (SELI) scheme to identify the malicious entity when the data is leaked by any agent at some unauthorized place. A new distribution strategy for object and agent selection which enriches the guilty agent recognition is introduced. The three algorithms named SELI-first come first serve, SELI-round Robin (SELI-RR) and SELI-shortest request first (SELI-SRF) are presented for the agent selection. Furthermore, the spurious data objects are added while distributing the data sets among the agents to uniquely identify the leaker. The SELI scheme estimates the guilty entity based on the allocated data among the agents using biograph. The proposed solution achieves an improvement and average probability and average success rate respectively in case of SELI-SRF and case of SELI-RR for detection rate compared to the prior work. In addition to this, the SELI scheme proved its efficiency by securing recall and specificity.



Article Title: Secure Data Storage and Sharing Techniques: A Review

[6] Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing.

In 2020, L. Zhang, Y. Cui and Y, demonstrated on a Mu Data sharing is a convenient and economic service supplied by cloud computing. Data contents privacy also emerges from it since the data is outsourced to some cloud servers. To protect the valuable and sensitive information, various techniques are used to enhance access control on the shared data. In these techniques, Ciphertext-policy attribute-based encryption (CP-ABE) can make it more convenient and secure. Traditional CP-ABE focuses on data confidentiality merely, while the user's personal privacy protection is an important issue at present. CP-ABE with hidden access policy ensures data confidentiality and guarantees that user's privacy is not revealed as well. However, most of the existing schemes are inefficient in communication overhead and computation cost. Moreover, most of those works take no consideration on authority verification or the problem of privacy leakage in authority verification phase. To tackle the problems mentioned above, a privacy preserving CP-ABE scheme with efficient authority verification is introduced in this paper. Additionally, the secret keys of it achieve constant size. Meanwhile, the proposed scheme achieves the selective security under the decisional n -BDHE problem and decisional linear assumption. The computational results confirm the merits of the presented scheme.

3 Conclusion

In this paper, the different strategies for the recognizing secure data storage is studied. It is investigated that no technique alone is efficient in ensuring the absolute security of the data from every directly or indirectly engaged party in the system. The robust solution can be developed by integrating the techniques for providing complete security to the system in the sharing environment. Moreover, with the set of highlights of addressed remarkable solutions, it is deemed that the exposed analysis will act as a milestone for the potential researchers working in the area as well as other emerging applications demanding secure data storage and sharing for its protection.

References

1. Ashutosh Kumar Singh; Ishu Gupta, Year: 2020, "Online information leaker identification scheme for secure data sharing", Multimedia Tools and Applications, Vol: 79, no: 41, pp. 31165 – 31182.
2. Ruixuan Li; Chenglin Shen, Heng He, Xiwu Gu, Zhiyong Xu, and Cheng-Zhong Xu, Year: 2018, "A lightweight secure data sharing scheme for mobile cloud computing", IEEE Transaction on Cloud Computing, Vol: 6, no: 2, pp. 344 – 357.
3. Ishu Gupta; Niharika Singh; Ashutosh Kumar Singh, Year: 2019, "Layer-based privacy and security architecture for cloud data sharing", Communication. Software System, Vol: 15, no: 2, pp. 173 – 185.
4. Leyou Zhang; Yilei Cui; Yi Mu, Year: 2020, "Improving security and privacy attribute based data sharing in cloud computing", IEEE Transaction on System, Vol: 14, no: 1, pp. 387 – 397.



Article Title: Secure Data Storage and Sharing Techniques: A Review

5. Ishu Gupta; Ashutosh Kumar Singh, Year: 2020, "SELI: Statistical evaluation based leaker identification stochastic scheme for secure data sharing", IET Communication, Vol: 14, no: 20, pp. 3607 – 3618.
6. Ehab Zaghloul; Kai Zhou; Jian Ren, Year: 2020, "P-MOD: Secure privilege-based multilevel organizational data-sharing in cloud computing", IEEE Transaction on Big Data, Vol: 6, no: 4, pp. 804 – 815.
7. Wenting Shen; Jing Qin; Jia Yu; Rong Hao; Jiankun Hu, Year: 2019, "Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage", IEEE Transaction on Forensics Security, Vol: 14, no: 2, pp. 331 – 346.
8. Xiaokui Shu; Danfeng Yao; Elisa Bertino, Year: 2015, "Privacy-preserving detection of sensitive data exposure", IEEE Transaction on Forensics Sector, Vol: 10, no: 5, pp. 1092 – 1103.
9. Panagiotis Papadimitriou; Hector Garcia-Molina, Year: 2011, "Data leakage detection", IEEE Transaction on Knowledge Data Engineering, Vol: 23, no: 1, pp. 51 – 63.
10. Neeraj Kumar; Vijay Katta; Himanshu Mishra; Hitendra Garg, Year: 2014, "Detection of data leakage in cloud computing environment", International Conference on Computational Intelligence and Communication Networks, Vol: 10, no: 4, pp. 803 – 807.