SEMARAK ILMU
PUBLISHING
202103268166(003316878-P)

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage: https://jaraset.com/
ISSN: 2462-1943

SEMARAK ILMU
Journal of
ADVANCED RESEARCH IN APPLIED SCIENCES AND ENGINEERING TECHNOLOGY
ISSN 2462 - 1943

SECURING DATA IN THE CLOUD: A SYSTEMATIC REVIEW OF TECHNIQUES FOR SECURE DATA STORAGE AND SHARING FOR ENHANCED DATA PROTECTION

Tarunesh Verma [1*], Dr. Meghna Dubey [2]

[1] Research Scholar, Department of Computer Science and Engineering, Mewar University, Rajasthan, India
[2] *Associate Professor, Department of Computer Science and Engineering, Mewar University, Rajasthan, India*

ARTICLE INFO

Article history:
Received: 22-08-2024
Received in revised form: 18-09-2024
Accepted: 28-09-2024
Available online: 12-11-2024

Keywords:

Cloud computing, data privacy and security, data protection, data storage, data sharing.

ABSTRACT

The landscape of data security in cloud settings is critically examined in this systematic study, which focuses on methods for safe data exchange and storage for increased data protection. The cloud environment supports many advantages, but it also has a number of drawbacks. When it comes to cloud computing and information security, data protection is the main worry. Various approaches have been devised to tackle this problem. Nevertheless, a thorough examination of the current solutions is lacking, therefore it becomes necessary to investigate, categories, and evaluate the substantial body of prior research in order to determine if these solutions may be used in order to satisfy the criteria. This article provides a thorough analysis and comparative research of the most popular methods for safe data exchange and protection in cloud environments. It also draws attention to new trends, weaknesses in existing approaches, and possible future paths in the pursuit of improved data security. Researchers, practitioners, and policymakers are intended to get a greater understanding of the dynamic field of safe data management in cloud computing by means of the synthesized information offered here.

Introduction

Since data defines each company's individuality, it is often seen as the most important asset in an organization. It serves as the primary source of knowledge, information, and eventually wisdom for making wise choices and taking appropriate action. It might include making a building more energy-efficient, increasing income for a business, curing a sickness, fulfilling goals, and enhancing performance [1].

Moreover, every organization that wants to improve performance must have access to data analysis, sharing, and storage [2]. But as data continues its fast expansion, businesses are under tremendous pressure to store the vast amounts of data locally [3]. Due to a lack of resources, it is now more difficult to study the data. Due to the cloud's numerous benefits, including on-demand service, scalability, dependability, flexibility, measurable services, disaster recovery, accessibility, and many more, the majority of enterprises have moved to it for these services [4]. The concept of cloud computing offers enormous memory space and cheap, high processing power. It gives cloud customers a great deal of ease by enabling them to access the desired services on several platforms at any time and from any place. Users may save costs and increase productivity to manage projects and form partnerships by moving their local data management system to the cloud and using cloud-based services.

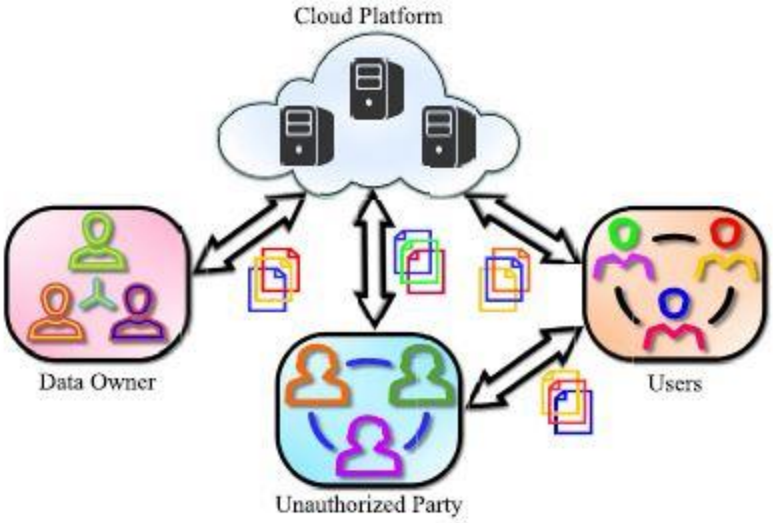

Figure 01: Block diagram of sharing environment.

For several applications, a variety of approaches for data security in cloud environments have been investigated and developed. Generally, data security is accomplished by discovering leakers and blocking leaks; however, this article focuses on finding the malevolent entity responsible for leaks and preventing leaks, as shown in below figure. The primary strategies to stop data leaks are based on machine learning, encryption, access control, and differential privacy; leaker identification is mostly accomplished via probabilistic methods and watermarking [7].

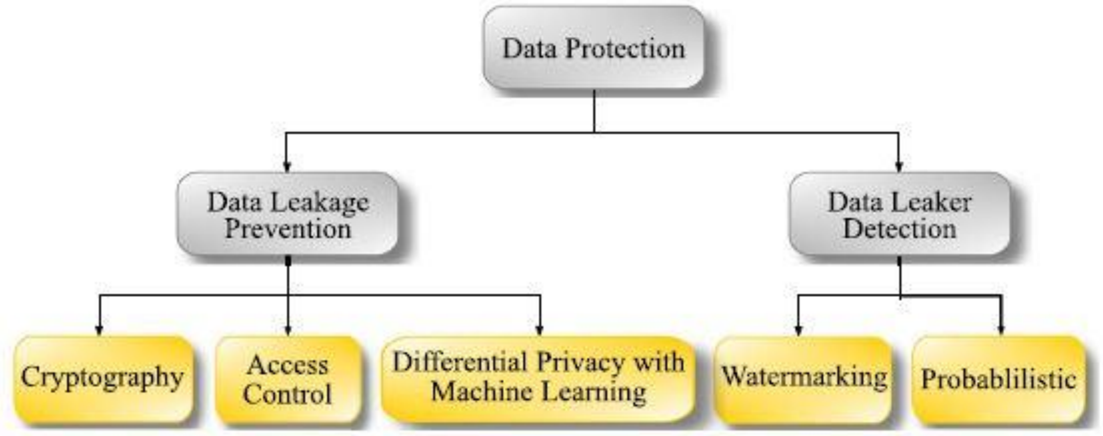

Figure 02: Major classification of data protection techniques.

Literature Review

This technology made it easier to outsource decryption, revoke attributes, and update policies as user characteristics changed. The severe tests are used to evaluate the performance of the suggested method, which is evaluated in terms of processing power and storage overhead but falls short in terms of privacy protection. Li et al. [6] propose a lightweight data sharing strategy (LDSS) for mobile cloud computing. By using the CP-ABE system, LDSS improved the structure of the access control tree and stimulated the mechanism suitable for mobile cloud settings. In this method, a significant amount of computing is moved from mobile devices to external proxy servers. When users in mobile cloud environments communicate data, the overhead on the side of the mobile device in LDSS is minimized.

A Privilege-based Multilevel Organizational Data-sharing (P-MOD) approach was presented in [2] by Zaghloul et al. A privilege-based access structure is included into P-MOD's attribute-based encryption technique to enhance its ability to handle and share large data sets efficiently. The experimental research shows that for a hierarchical organization with several levels to execute encryption and decryption and generate keys, P-MOD is more efficient than both CP-ABE and FH-CP-ABE [5] systems. Additionally, the P-MOD scheme minimizes the cumulative amount of operations when compared to the hierarchical systems FH-CP-ABE, HABE, and HABE [3].

In order to enhance the effectiveness of the policy in a cloud setting, Li et al. [8] proposed a Linear Secret Sharing approach (LSSS) matrix access structure that is based on an efficient CP-ABE approach. This system updates the dynamically. The plan's goals are to fend against chosen plaintext assaults (CPAs) and lower the proxy cloud service provider's (PCSP) storage use, communication costs, and data owner's processing expenses. In terms of managing policy changes and updates effectively, the suggested system has performed better than Policy Update CP-ABE [8], according to theoretical analysis and experimental simulation. Zhang et al. [9] provide a privacy-preserving scheme of the hidden access policy CP-ABE (HP-CP-ABE) schemes with an efficient authority verification in order to guarantee data confidentiality and safeguard user privacy. This method designs an authority detection system to confirm that the user is authorized and to finish the decryption procedure. Through this method, a constant-sized private key that is unaffected by the quantity of user characteristics was produced.

Research Methodology

Access Control Based Models

The method made use of an attribute-based key management strategy that preserves user privacy while imposing attribute-based ACPs. To save overhead at the data owners and ensure data confidentiality from the cloud, the data owner encrypts their data coarsely, while the cloud encrypts data on top of the owner's encryption. A safe data sharing plan for the cloud's dynamic members is provided in [10]. Because their public keys have been verified, users may safely get their private keys. Even if revoked users work with the untreated cloud to protect the system against collusion attempts, they will not be able to access the original data. To allow dynamic groups, it is not necessary for previous users to update their private keys whenever a new user joins or when a person is removed.

For public cloud storage, [11] offers a threshold multi-authority CP-ABE access control system (TMACS) in which many authorities collaborate to maintain a common set of attributes. To handle the attributes set and achieve security and system-level robustness, a combination of the traditional multi-authority scheme and the TMACS scheme is used, in which multiple authorities within an authority set and attributes originating from different authority sets jointly maintain a subset of the entire attribute set.

In [12], Timed-Release Encryption (TRE) is embedded into Cipher text-Policy Attribute-based Encryption (CP-ABE) to provide a time and attribute factors combined access control on time sensitive data for public cloud storage (TAFC) technique. With the help of this scheme, data owners may flexibly provide access to various users at different times based on a well defined access policy that takes release time and attribute management into account.

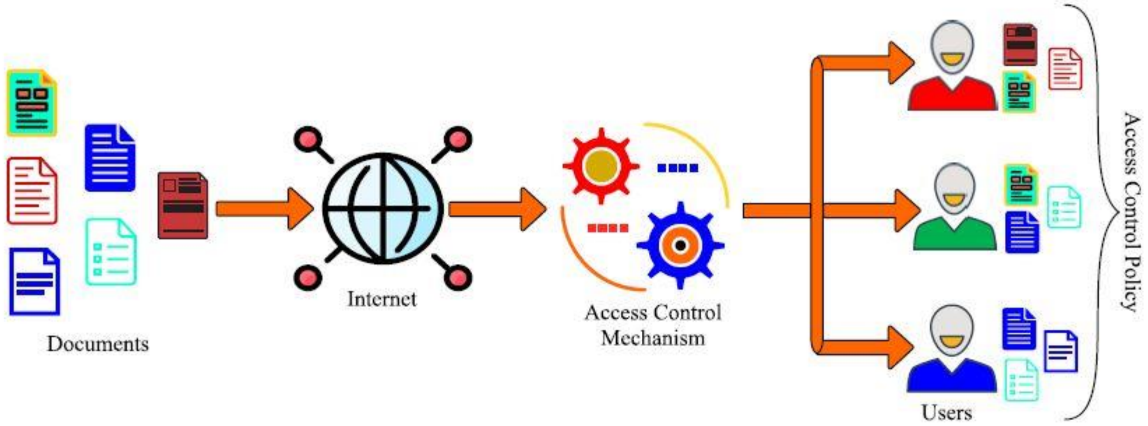

Figure 03: Schematic representation of access control based models.

Comparative and Comprehensive Analysis

The significant examined technique's advantages and disadvantages, resulting in a comparison of these approaches by taking into consideration certain criteria (CR). The observations listed below are as follows:

- Among the several strategies, namely Cryptography (CG), Access Control (AC), Differential Privacy using machine learning (DP), Watermarking (WM), and Probability (PB), only DP and CG are able to guarantee privacy (P), although other techniques guarantee security (S). Of all the strategies, it is claimed that only CG and DP maintain security and privacy.

- While data leaker detection (D) is confirmed by the WM and PB procedures, data leaking prevention (L) is obtained by CG, AC, and DP. It is significant because none of the five strategies provide simultaneous detection and prevention [12].
- Confidentiality (C), integrity (I), and accessibility (A) are the three characteristics that can be attained by CG, AC, and DP; WM and PB can only achieve integrity.
- CG and DP perform better for the data protection (DR) criteria than the other three techniques, AC, WM, and PB, because they fulfill the maximum security parameters. However, these two techniques do not allow for leakage detection, which is equally important for the other security parameters [13].

According to a comprehensive analysis, CG is in the forefront of the strategies for maintaining confidentiality, security, privacy, and leakage prevention. The best way to protect privacy without incurring transformation costs is via AC. DP is the best method for maintaining privacy while combining functionality. The best methods for ensuring data usefulness in conjunction with leak detection are watermarking and probability. Moreover, PB is the better leaker estimating approach without the influence of data modification, whereas WM is the best leaker detection technique for pinpointing the exact perpetrator. It is necessary to use an integration of the strategies for an efficient data security system, since no one technique can guarantee totally safe procedures [14].

Conclusions

In the fields of information security and cloud computing, data protection is a difficult problem. Many works are interpreted in an attempt to lessen this difficulty. Nonetheless, there is a lack of sufficient research on the current options. From this vantage point, the study provided a thorough analysis and examined the most cutting-edge methods pertaining to the functionality and pertinent solutions for safely sharing data in a cloud context. Each mentioned solution's future directions and research gaps are emphasised, along with the necessary and sufficient information needed to extract the method's core. In-depth examination and a comparative study of the procedures that are referred to are also carried out. Research indicates that no method can guarantee complete data security against all parties involved in the system, whether directly or indirectly. By combining the methods for offering total protection to the system in the shared environment, a strong solution may be created.

Furthermore, it is anticipated that the analysis that has been made public will serve as a benchmark for future studies in the field and other new applications that need safe data sharing and archiving in order to preserve it. This is because the study includes a selection of the most noteworthy solutions that have been addressed.

References

[1] A. K. Singh and I. Gupta, ``Online information leaker identification scheme for secure data sharing," Multimedia Tools Appl., vol. 79, no. 41, pp. 31165_31182, Nov. 2020.

[2] E. Zaghloul, K. Zhou, and J. Ren, ``P-MOD: Secure privilege-based multilevel organizational data-sharing in cloud computing," IEEE Trans. Big Data, vol. 6, no. 4, pp. 804_815, Dec. 2020.

[3] I. Gupta and A. K. Singh, ``GUIM-SMD: Guilty user identification model using summation matrix-based distribution," IET Inf. Secur., vol. 14, no. 6, pp. 773_782, Nov. 2020.

[4] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, ``Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage," IEEE Trans. Inf. Forensics Security, vol. 14, no. 2, pp. 331_346, Feb. 2019.

[5] I. Gupta and A. K. Singh, ``An integrated approach for data leaker detection in cloud environment," J. Inf. Sci. Eng., vol. 36, no. 5, pp. 993_1005, Sep. 2020.

[6] R. Li, C. Shen, H. He, X. Gu, Z. Xu, and C.-Z. Xu, ``A lightweight secure data sharing scheme for mobile cloud computing," IEEE Trans. Cloud Computer, vol. 6, no. 2, pp. 344_357, Apr. 2018.

[7] I. Gupta, N. Singh, and A. K. Singh, ``Layer-based privacy and security architecture for cloud data sharing," J. Commun. Softw. Syst., vol. 15, no. 2, pp. 173_185, Apr. 2019.

[8] J. Li, S. Wang, Y. Li, H. Wang, H. Wang, H. Wang, J. Chen, and Z. You, ``An efficient attribute-based encryption scheme with policy update and _le update in cloud computing,"IEEE Trans. Ind. Informat., vol. 15, no. 12, pp. 6500_6509, Dec. 2019.

[9] C. Suisse. (2017). 2018 Data Center Market Drivers: Enablers Boosting Enterprise Cloud Growth. Accessed: May 19, 2019. [Online].

[10] I. Gupta and A. K. Singh, ``A framework for malicious agent detection in cloud computing environment," Int. J. Adv. Sci. Technol., vol. 135, pp. 49_62, Feb. 2020.

[11] Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni, and K.-R. Choo, ``Fuzzy identity-based data integrity auditing for reliable cloud storage systems," IEEE Trans. Dependable Secure Computer., vol. 16, no. 1, pp. 72_83, Jan./Feb. 2019.

[12] I. Gupta and A. K. Singh, ``A probabilistic approach for guilty agent detection using bigraph after distribution of sample data," Proc. Computer. Sci., vol. 125, pp. 662_668, Jan. 2018.

[13] L. Zhang, Y. Cui, and Y. Mu, ``Improving security and privacy attribute based data sharing in cloud computing," IEEE Syst. J., vol. 14, no. 1, pp. 387_397, Mar. 2020.

[14] I. Gupta and A. K. Singh, ``Dynamic threshold based information leaker identification scheme," Inf. Process. Lett., vol. 147, pp. 69_73, Jul. 2019.