

Assignment2

Data Leakage in Cloud Storage

Lecturer

Dr. Mohammed Anbar

Student

Ahmed Mohammed Ahmed Alnahari

251003035

Problem Statement

Data leakage in cloud storage is a significant security challenge, particularly due to misconfigurations, weak authentication mechanisms, and insider threats (Zuo et al., 2019; Montano et al., 2022). And As cloud adoption grows, so does the risk of unauthorized access and data exposure, leading to financial and reputational damage for businesses (Ulybyshev et al., 2018). While encryption, access control, and behavioral monitoring have been proposed as countermeasures (Braghin et al., 2022; Khan et al., 2018), and these solutions often suffer from performance trade-offs, implementation complexity, and insider attack vulnerabilities (Wang et al., 2021).

Problem Domain

Data leakage in cloud storage remains a significant security challenge, affecting both **individuals and organizations** due to misconfigurations, weak authentication mechanisms, and insider threats (Zuo et al., 2019; Montano et al., 2022).

Need for Research

There is a pressing need to develop a multi-layered security framework that integrates encryption, machine learning, real-time behavioral analytics, and access control mechanisms to prevent cloud data leakage proactively.

Research Objectives

The primary goal of this research is to develop an integrated security framework to minimize data leakage risks in cloud storage by combining proactive monitoring, real-time threat detection, and access control mechanisms.

The following objectives will guide this research :

1. To identify the primary causes of data leakage in cloud storage, including misconfiguration, authentication flaws, and insider threats.
2. To evaluate the effectiveness of existing data leakage prevention methods, such as encryption, access control, and privacy-preserving computation.
3. To analyze the trade-offs between security, performance, and usability in cloud security models.
4. To propose an advanced security framework that integrates proactive monitoring, real-time anomaly detection, and adaptive access control mechanisms for enhanced cloud data protection.

Literature Review

Importance of the Problem:

Cloud service providers host vast amounts of sensitive information, including personal and corporate data. A single breach can expose millions of records, leading to severe regulatory penalties (British Airways breach, 2018; Capital One breach, 2019). Current security measures remain fragmented and reactive, often addressing threats after they occur rather than preventing them proactively (Montano et al., 2022). This research is crucial for developing more efficient, proactive, and adaptive security strategies that mitigate data leakage risks effectively.

Problem Description:

The increasing reliance on cloud storage has expanded the risk of unauthorized access, data breaches, and financial losses, making it a critical issue for data security and privacy (Ulybyshev et al., 2018).

Misconfigured cloud storage settings and weak authentication protocols have led to high-profile breaches exposing millions of records (British Airways breach, 2018; Capital One breach, 2019).

Existing Solutions:

- Automated scanning tools (e.g., LeakScope) to detect misconfigured cloud storage (Zuo et al., 2019).
- Encryption-based access control mechanisms to secure sensitive data (Ulybyshev et al., 2018; Braghin et al., 2022).
- Privacy-preserving computational techniques, such as sparse matrices, to obfuscate sensitive data in cloud operations (Khan et al., 2018).
- Existing cloud security mechanisms, including encryption, access control, and behavioral monitoring, have been deployed to mitigate risks (Braghin et al., 2022; Khan et al., 2018).

References

- Zuo, C., Lin, Z., & Zhang, Y. (2019). Why Does Your Data Leak? Uncovering the Data Leakage in Cloud from Mobile Apps. IEEE Security & Privacy Conference. <https://yinqian.org/papers/sp19.pdf>
- Ulybyshev, D., Bhargava, B., & Oqab-Alsalem, A. (2018). Secure Data Exchange and Data Leakage Detection in an Untrusted Cloud. ICACCT (Springer CCIS).
https://www.cs.purdue.edu/homes/bb/Papers2018/LeakageDetection/Ulybyshev2018_Chapter_SecureDataExchangeAndDataLeakage-%20FromRealSpringerJournal.pdf
- Montano, I. H., Aranda, J. J. G., Diaz, J. R., Cardín, S. M., de la Torre Díez, I., & Rodrigues, J. J. P. C. (2022). Survey of Techniques on Data Leakage Protection and Methods to Address the Insider Threat. Cluster Computing (Springer).
https://www.researchgate.net/publication/362010417_Survey_of_Techniques_on_Data_Leakage_Protection_and_Methods_to_address_the_Insider_threat/link/62d8314e45865722d7791f97/download
- Braghin, S., Simioni, M., & Sinn, M. (2022). DLPFS: The Data Leakage Prevention FileSystem. Cloud Security & Privacy Workshop.
<https://arxiv.org/pdf/2108.13785>
- Khan, K., Shaheen, M., & Wang, Y. (2018). Using Sparse Matrices to Prevent Information Leakage in Cloud Computing. IEEE FiCloud Conference.
<https://qspace.qu.edu.qa/handle/10576/13165#:~:text=Cloud%20computing%20represents%20the%20promise,protocols%20ensure%20no%20information%20leakage>