Data Breaches in Cloud Storage: Risks and Prevention Strategies

Review Paper - Inam Ul Haq - BITF22M017

Project Idea

The project aims to investigate why data breaches continue to occur in cloud storage despite advancements in security. It focuses on identifying technical, architectural, and human-driven weaknesses across AWS, Azure, and GCP.

Project Summary

Cloud storage has become a core component of modern computing, yet misconfigurations and identity-related failures continue to expose sensitive data. Through systematic analysis of major breaches (Capital One, BlueBleed, Sennheiser, Pfizer), this project evaluates how cloud environments are compromised and the role of IAM, network controls, logging, and automation in preventing such attacks. The paper compares native cloud security architectures, examines CSPM tools (Prowler, ScoutSuite, Wiz), and highlights emerging AI-based offensive and defensive techniques.

What Has Been Done

I have conducted a Systematic Literature Review (2015–2025) of research papers. I have analyzed four major real-world cloud breaches. Also, I have compared the security architectures of AWS, Azure, and GCP, evaluated leading CSPM and CNAPP security tools and assessed modern frameworks including Zero Trust Architecture and AI-driven threat detection.

Conclusion

Cloud breaches are less about cloud providers and more about configuration complexity, identity misuse and lack of continuous monitoring. Preventing such incidents requires adopting Zero Trust principles, automated misconfiguration scanning through CSPM tools and AI-enhanced anomaly detection. As attack speed increases in the AI era, organizations must prioritize automation, simplification and lifecycle management to build secure, resilient cloud environments.