

## **Data Leakage Detection in Cloud Computing Platforms**

***Synopsis Report of the (Minor Project - 2)***

Mentor – Dr. Keshav Sinha

|  |  |  |  |
| --- | --- | --- | --- |
| S. No | Students Name | Roll Number | Sap Id |
| 1. | Anishka Sinha | R2142211008 | 500094103 |
| 2. | Vishaka Joshi | R2142210856 | 500094135 |
| 3. | Priyanshu Singh | R2142210604 | 500094151 |
| 4. | Akshay Saini | R2142210604 | 500094151 |

Project Title: Data Leakage Detection System for Cloud Computing Platforms

1. Introduction

Data security is paramount in today's digital age, especially with the increasing reliance on cloud computing platforms. Unauthorized access to sensitive information poses significant risks to businesses and organizations. The Data Leakage Detection System aims to address these concerns by developing a mechanism to detect and prevent data leaks during critical processes such as web dashboard logins and virtual machine transfers.

2. Project Overview

The Data Leakage Detection System utilizes packet recording mechanisms during authentication and migration procedures within cloud computing environments. By analyzing management and communication packets in real-time, instances of data leakage are identified and mitigated. The project focuses on creating a cloud testbed environment using OpenStack and VMware VCenter software for demonstration purposes.

3. Objectives

- Develop a mechanism for detecting data leaks in cloud computing platforms.

- Record packets during authentication and migration processes to identify instances of data leakage.

- Conduct threat simulation experiments to validate the effectiveness of the detection mechanism.

- Create a cloud testbed environment utilizing OpenStack and VMware VCenter software for demonstration.

4. Scope

The scope of the project includes:

- Detection of data leaks during web dashboard logins and virtual machine transfers.

- Analysis of management and communication packets for real-time detection.

- Creation of a cloud testbed environment using OpenStack and VMware VCenter software.

5. Functional Requirements

- Packet recording mechanism during authentication and migration processes.

- Real-time analysis of management and communication packets.

- Threat simulation experiments to validate detection mechanisms.

- Creation of a cloud testbed environment for demonstration.

6. Non-Functional Requirements

- Performance: The system should have minimal impact on network performance during packet recording and analysis.

- Security: The system should adhere to industry standards for data security and encryption.

- Usability: The user interface should be intuitive and user-friendly for administrators to configure and manage.

- Reliability: The system should be reliable and able to detect data leaks accurately without false positives.

7. SWOT Analysis

- Strengths:

- Utilization of packet recording mechanisms for real-time detection.

- Integration with OpenStack and VMware VCenter software for demonstration.

- Focus on empirical validation through threat simulation experiments.

- Weaknesses:

- Dependency on network infrastructure for packet recording and analysis.

- Complexity in configuring and managing the system.

- Potential performance impact during packet recording and analysis.

- Opportunities:

- Integration with additional cloud platforms for broader coverage.

- Collaboration with industry partners for real-world validation and deployment.

- Expansion of features to include predictive analytics for proactive data leak prevention.

- Threats:

- Rapidly evolving cloud computing technologies may require frequent updates and adaptations.

- Competition from existing data leakage detection solutions.

- Regulatory compliance requirements may impact system design and implementation.

8. Conclusion

The Data Leakage Detection System presents a comprehensive approach to address the critical issue of data leakage in cloud computing platforms. By leveraging packet recording mechanisms and real-time analysis, the system aims to detect and prevent data leaks during crucial processes. The project's focus is on empirical validation and demonstration using OpenStack and VMware VCenter software to ensure the effectiveness and practicality of the proposed solution.

9. References

- [1] "An improved data leakage detection system in a cloud computing environment," ResearchGate, [Online]. Available: https://www.researchgate.net/publication/354308045\_An\_improved\_data\_leakage\_detection\_system\_in\_a\_cloud\_computing\_environment

- [2] "Data Leakage Detection in Cloud Computing Platform," ResearchGate, [Online]. Available: https://www.researchgate.net/publication/335190617\_Data\_Leakage\_Detection\_in\_Cloud\_Computing\_Platform

- [3] "Data Leakage Detection in Cloud Computing Platforms: A Comprehensive Review," Springer, [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-13577-4\_9

- [4] "Empirical Study on Data Leakage Detection System in Cloud Computing Environments," arXiv, [Online]. Available: https://arxiv.org/pdf/2202.11965.pdf

10. Appendix

The Object-Oriented Analysis and Design (OOAD) methodology was selected for this research work. It provides a structured approach to analyzing and designing systems, treating different system components as objects with associated properties and behaviors. This methodology facilitates the development of a graphical framework model during the software development lifecycle.

Preventing data leakage in cloud environments requires a comprehensive approach that encompasses both technical solutions and organizational policies. Here is a methodology outlining steps you can take:

1. Data Classification: Start by classifying your data based on its sensitivity.

2. Risk Assessment: Conduct a thorough risk assessment to identify potential vulnerabilities and threats to your data.

3. Access Controls: Implement strong access controls to restrict access to sensitive data.

4. Encryption: Encrypt data both in transit and at rest.

5. Data Loss Prevention (DLP): Deploy DLP solutions that monitor and control the movement of data within the cloud environment.