Enhanced Multi-Layer Authentication for Intrusion Detection and Secure Data Access in Cloud Shared Storage

Mrs. J.P. Kakad[1], Sheetal Gayke[2], Shraddha Vishe[3], Shraddha Barahate[4], Sonam Shinde[5]

Matoshri College of Engineering & Research Centre, Eklahare, Nashik

Abstract

This abstract introduces the critical need for secure shared storage systems in organizations within today's digital age. While these systems significantly enhance productivity through seamless access and collaboration, they also expose sensitive data to potential security threats. To mitigate unauthorized access and enhance data protection, the implementation of an Intrusion Detection and Prevention System (IDPS) is proposed. This solution provides real-time monitoring, detection, and prevention of unauthorized activities, ensuring that shared storage systems remain secure and resilient in the face of evolving cybersecurity threats. By adopting IDPS, organizations can maintain the delicate balance between accessibility and security, protecting critical information without hindering collaboration.

Keywords: Shared Storage, Security, Intrusion Detection and Prevention System (IDPS), Data Protection, Cybersecurity, Real-Time Monitoring

INTRODUCTION

In today's digital era, organizations rely heavily on shared storage systems to facilitate collaboration and improve operational efficiency. These systems enable seamless data access and sharing across teams, departments, and locations, empowering employees to work together effectively. However, with this convenience comes the risk of unauthorized access, data breaches, and cyberattacks, which can compromise sensitive information and disrupt operations. As organizations handle increasing amounts of confidential data, ensuring the security of shared storage systems becomes a top priority.

To address the growing security concerns, the implementation of robust security measures is essential. One of the most effective solutions is the use of an Intrusion Detection and Prevention System (IDPS). An IDPS monitors network traffic in real-time, detects potential security threats, and prevents unauthorized access by taking proactive measures. It not only protects against external attacks but also safeguards against internal misuse of data. By adopting an IDPS, organizations can enhance the security of their shared storage systems while maintaining the flexibility and accessibility required for efficient collaboration.

LITERATURE SURVEY

[1] Cloud Intrusion Detection Method Based on Stacked Contractive Auto-Encoder and Support Vector Machine, IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 10, NO. 3, JULY-SEPTEMBER 2022

[2] Cloud-Based Intrusion Detection Approach Using Machine Learning Techniques, BIG DATA MINING AND ANALYTICS ISSN 2096-0654 05/10 /2023

METHODOLOGY

- This phase involves evaluating the shared storage system's vulnerabilities and defining security needs based on the type of data, user access levels, and regulatory requirements.
- The system monitors network traffic for signs of potential threats such as unauthorized access or abnormal data flows using techniques like signature and anomaly-based detection.
- Monitors server activities such as file access, system calls, and user actions to detect suspicious behaviours at the server level, ensuring security directly within the system.
- Machine learning models analyze data to identify evolving threats, allowing the IDPS to adapt to new attack vectors and provide proactive defense against unknown threats.

PROPOSED SYSTEM

The proposed system for enhancing security in shared storage environments through an Intrusion Detection and Prevention System (IDPS) involves a comprehensive architecture that integrates real-time monitoring, user authentication, and data protection strategies. The IDPS will continuously track user activities and access patterns, employing both anomaly detection and signature-based methods to identify suspicious behavior, such as unauthorized access attempts and unusual file transfers. To strengthen security, the system will incorporate multi-factor authentication (MFA) and role-based access control (RBAC), ensuring users can only access data necessary for their roles. Additionally, the system will implement data encryption for both stored and transmitted information, alongside regular backup procedures to safeguard data availability in case of breaches. Alerts will be configured for varying severity levels, accompanied by a clear incident response plan outlining investigation and communication protocols. Integration with existing shared storage solutions will be facilitated through APIs, while audit logs will maintain a detailed record of access and modifications for compliance and analysis. User training and awareness programs will be established to educate employees about security best practices, including phishing recognition. Finally, the system will undergo regular assessments and updates, ensuring it remains effective against evolving cybersecurity threats while balancing accessibility and protection of sensitive data.

RESULT

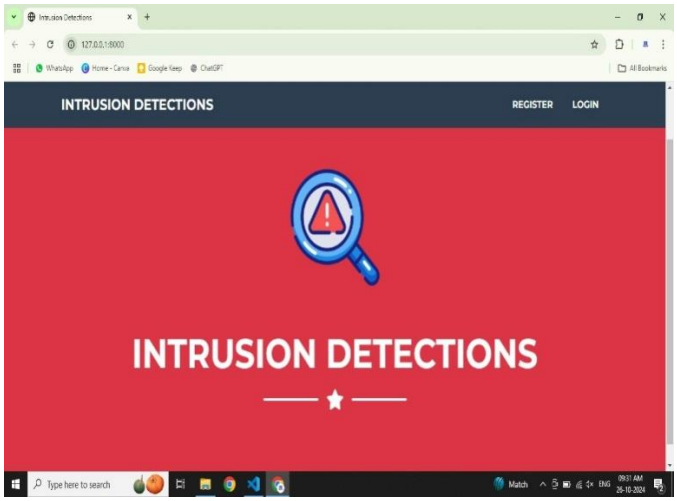

Fig: Home page

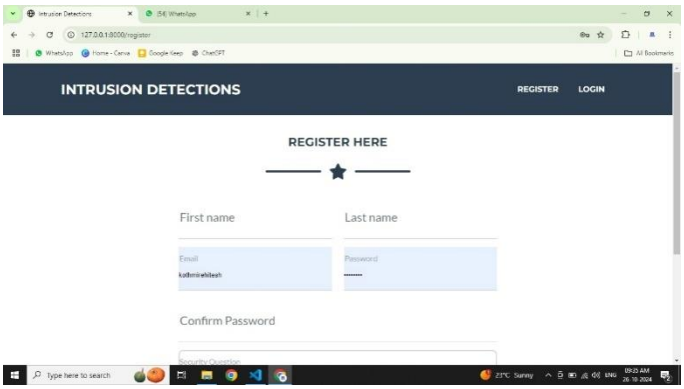

Fig: Register page

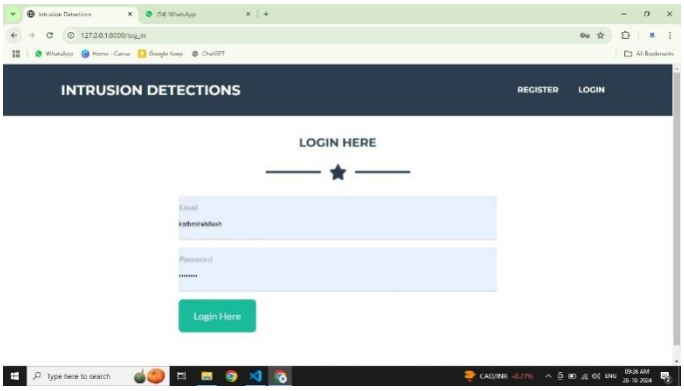

Fig: Login page

CONCLUSION

The Intrusion Detection and Prevention System (IDPS) successfully enhances data security in shared storage environments through its multi-layered authentication and real-time monitoring features. The integration of machine learning further strengthens threat detection and adaptation. Overall, the system provides robust protection against unauthorized access and evolving threats, demonstrating significant improvements over traditional security methods. Future work will focus on continuous updates and refinements to maintain and enhance its effectiveness.

REFERENCES

[1] Cloud Intrusion Detection Method Based on Stacked Contractive Auto-Encoder and Support Vector Machine, IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 10, NO. 3, JULY-SEPTEMBER 2022

[2] Cloud-Based Intrusion Detection Approach Using Machine Learning Techniques,BIG DATA MINING AND ANALYTICS ISSN 2096-0654 05/10 /2023

[3] W. Wang, "Cloud Intrusion Detection Method Based on Stacked Contractive Auto-Encoder and Support Vector Machine," IEEE Transactions on Cloud Computing, vol. 10, no. 3, pp. 640-652, July-Sept. 2022.

[4] H. Attou and A. Guezzaz, "Cloud-Based Intrusion Detection Approach Using Machine Learning Techniques," Big Data Mining and Analytics, vol. 6, no. 3, pp. 311-320, Sept. 2023, doi: 10.26599/BDMA.2022.9020038.

[5] A. M. Abdallah, "Cloud Network Anomaly Detection Using Machine and Deep Learning Techniques—Recent Research Advancements," IEEE Access, vol. 12, pp. 12345-12360, 2024.

[6] R. Kumar and M. Gaur, "A Hybrid Intrusion Detection System for Cloud Computing Based on Deep Learning and Ensemble Methods," Journal of Cloud Computing: Advances, Systems and Applications, vol. 11, no. 2, pp. 175-189, May 2023.