INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 4, April 2026 | ISSN: 2456-4184 | IJNRD.ORG

Insider Threat Detection System

[1] Kajal Kumawat, [2]Priya Konar, [3]Vatsal Mishra, [4]Vedant Palav, [5] Dr. Preeti Gupta

[1,2,3,4] U.G. Student, Department of Information Technology, K.C College Of Engineering, Maharashtra.

[5]Associate Professor, Department of Information Technology, K.C College Of Engineering, Maharashtra.

ABSTRACT : ***Insider threats represent a critical challenge to modern organizations, as individuals with authorized access may deliberately or unintentionally compromise sensitive information. The proposed system, Insider Threat Detection System, is designed to identify and mitigate such risks using behavior-driven monitoring techniques along with enhanced authentication mechanisms. The system tracks user activities in real time, including access to confidential files, usage of external storage devices, and data transfer actions, to detect anomalies or suspicious patterns. To strengthen security during high-risk operations, Time-Based One-Time Password (TOTP) authentication integrated with Google Authenticator is employed, ensuring that only verified users can perform sensitive tasks. A zero-trust security model is adopted, where access permissions are determined based on contextual factors such as user role, time of access, and behavioral patterns rather than implicit trust. When irregular behavior is detected, the system can automatically enforce protective measures such as restricting access, encrypting critical data, and notifying administrators through a live monitoring dashboard. Furthermore, role-based access control is implemented to clearly define privileges for administrators and regular users, thereby limiting unauthorized interactions with protected resources. Administrators are equipped with real-time alerts and detailed activity logs, allowing prompt action against potential threats. Overall, the system aims to reduce the risk of internal data breaches while maintaining operational efficiency. By integrating continuous monitoring, behavioral analysis, and multi-factor authentication, the proposed solution provides a proactive framework for enhancing internal cybersecurity within organizations.***

KEY WORDS: ***Insider Threat Detection, Cybersecurity Monitoring, Role-Based Access Control (RBAC), Time-based One-Time Password (TOTP), Multi-Factor Authentication (MFA), Secure Access Control, Real-Time Threat Detection, Security Logging and Auditing***

INTRODUCTION

In the modern digital era, organizations increasingly depend on interconnected systems and data-driven operations, making information security a major priority. Although external cyberattacks receive significant attention, many security incidents actually originate from within the organization. These incidents, known as insider threats, occur when individuals with legitimate access—such as employees, contractors, or system administrators—misuse their privileges, whether intentionally or accidentally. Such threats are particularly dangerous because they can evade traditional security controls and result in serious consequences, including data leaks, loss of intellectual property, and disruption of business operations.

As organizations handle larger volumes of sensitive data and rely on technologies like cloud platforms, internal networks, and portable storage devices, monitoring user activities becomes increasingly complex. Traditional security approaches are largely designed to protect against external intrusions and often fail to identify suspicious behavior from trusted users. This limitation highlights the need for advanced solutions that can observe internal activities, evaluate user behavior patterns, and detect anomalies as they occur. Early identification of such threats is crucial to reducing the risk of data exposure and preventing long-term damage to organizational resources.

To overcome these challenges, the proposed *Insider Threat Detection System* offers a proactive approach to internal security by focusing on behavioral analysis and controlled access. The system continuously tracks user actions, including file interactions, use of external devices, and execution of sensitive operations, while enforcing strong authentication for critical tasks. By combining role-based access control, continuous monitoring, and multi-factor authentication, the system aims to improve security without affecting the normal workflow of authorized users. This integrated approach enables organizations to better protect their data and maintain the confidentiality, integrity, and availability of critical information assets.

II. LITERATURE SURVEY

Real-Time Monitoring Systems for Insider Threat Prevention

The research focuses on real-time monitoring of user activities to prevent insider threats proactively. It highlights the importance of immediate alerts and automated response mechanisms.

Insider Threat Detection Using Time-Based Access Control

This study emphasizes time-based access control to restrict user actions based on working hours. It helps detect suspicious access attempts during unusual time periods

Multi-Factor Authentication and Insider Threat Prevention

The research shows that integrating multi-factor authentication reduces insider misuse of credentials and enhances internal security.

Context-Aware Insider Threat Detection Systems

This paper introduces context-aware analysis by considering time, location, and user role to detect insider threats. Context data collection may raise privacy concerns.

User Behavior Profiling for Insider Threat Detection

This paper develops user behavior profiles to identify deviations from normal activity patterns. It improves the detection of insider threats through profiling.

III. EXISTING SYSTEM

Current organizational security frameworks mainly depend on fundamental authentication methods, typically involving usernames and passwords, along with basic role-based access control mechanisms. While these measures offer a preliminary level of protection, they are insufficient to address insider threats, as they rely heavily on trust once access is granted. Individuals with valid credentials can often interact with sensitive data without additional verification, increasing the likelihood of internal misuse and data exposure.

Moreover, traditional systems lack the capability to continuously observe and evaluate user activities. Actions such as unauthorized file access, irregular use of external storage devices, and unusual behavioral patterns frequently remain undetected due to the absence of real-time monitoring and intelligent analysis. Although activity logs may be generated, they are often reviewed retrospectively rather than being analyzed instantly, which delays threat identification and limits timely response.

Another limitation of existing solutions is the lack of advanced authentication techniques for high-risk operations. Mechanisms like Time-Based One-Time Passwords (TOTP) are generally not implemented, making systems more vulnerable to risks such as credential sharing and replay attacks. Additionally, the absence of action-specific authentication and secure, well-structured logging reduces the effectiveness of the overall security infrastructure. These shortcomings highlight the necessity for a more advanced and proactive approach to insider threat detection and prevention.

➤ **Key Limitation:**

- **Dependence on Manual Configuration and User Setup:** The effectiveness of the system depends on proper user creation, TOTP configuration, and administrative control. Any misconfiguration or improper setup can reduce the system's effectiveness and create potential security gaps..

IV. PROPOSED SYSTEM

The proposed solution introduces a comprehensive framework for detecting and preventing insider threats by applying multiple layers of security controls within an organization. It combines Role-Based Access Control (RBAC) with Time-Based One-Time Password (TOTP) authentication to ensure that access to sensitive information is strictly limited to verified users. Unlike conventional approaches, the system applies authentication at the action level, meaning that critical tasks—such as accessing confidential data or enabling external storage devices—require additional verification. This significantly lowers the chances of unauthorized usage and misuse of credentials.

A key feature of the system is its ability to perform continuous monitoring and maintain detailed logs of user activities. It observes actions such as file access, system operations, and connections of external devices through an event-driven process. When irregular or suspicious behavior is identified—such as attempts to access restricted files, interaction with potentially harmful links, or unauthorized use of USB devices—the system immediately generates alerts and initiates appropriate security measures. These responses may include restricting user permissions or temporarily locking the system to prevent further risk. This real-time detection capability enables organizations to respond quickly and reduce potential damage caused by insider threats.

In addition, the system strengthens authentication by implementing unique, user-specific TOTP codes that are valid for a single use, eliminating the possibility of reuse or sharing. It also supports detailed auditing and logging functionalities, allowing administrators to monitor activities and perform in-depth analysis when required. The inclusion of advanced features such as phishing detection and secure data handling techniques, including steganography, further enhances the overall security framework. Altogether, this proposed system delivers a more intelligent, reliable, and proactive approach to safeguarding organizational data against internal threats compared to traditional methods.

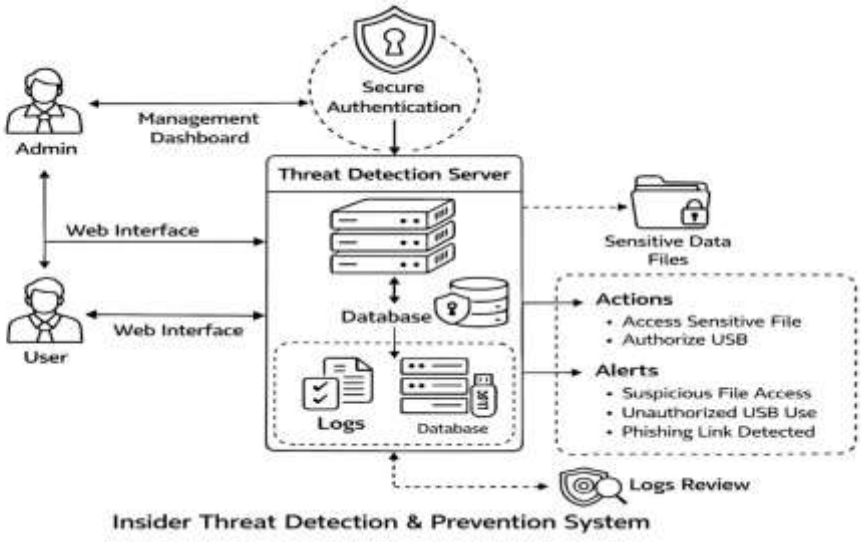

Figure 4.1: Block Diagram for Proposed System

V. RESULTS:-

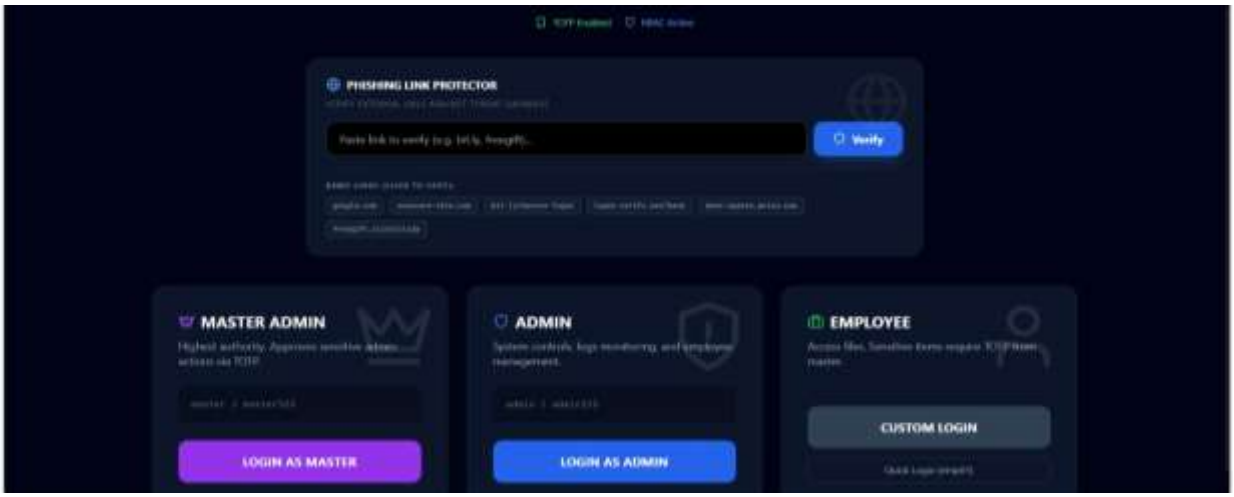

Fig 5.1 Login Page

The login page serves as the entry point to the system, allowing users to access it using valid credentials. It verifies usernames and passwords to ensure only authorized users can log in. The system also applies role-based access control to assign permissions based on user roles, enhancing overall security.

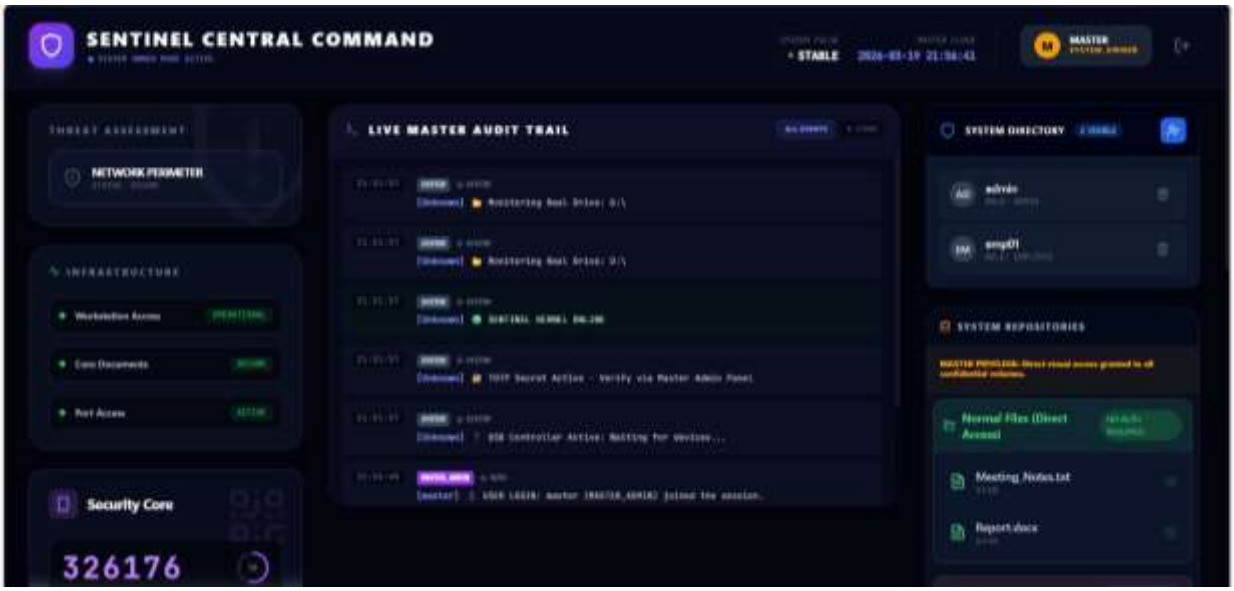

Fig 5.2 Master Admin Dashboard

The Master Admin dashboard offers full control over the system, enabling management of users and overall operations. It provides detailed activity logs and system-level insights for effective supervision. This interface supports centralized control and helps in identifying and analyzing potential insider threats.

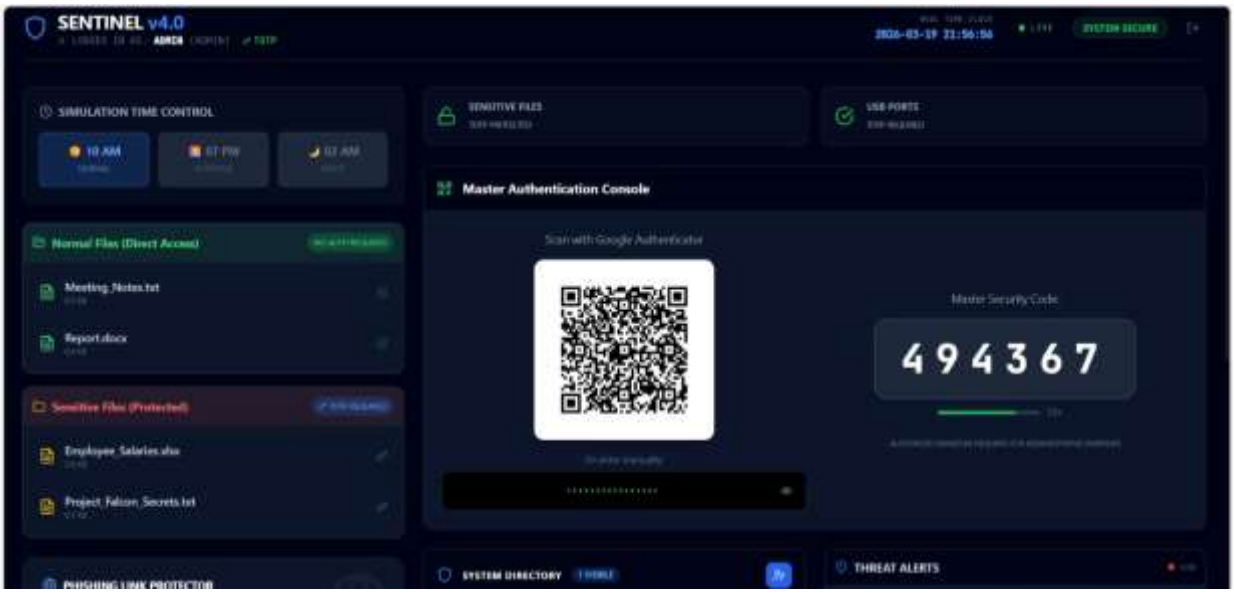

Fig 5.3 Admin Dashboard

The Admin dashboard enables administrators to oversee employee activities and review logs within their permitted scope. It presents user actions in an organized manner while limiting access to higher-level controls, ensuring secure and controlled system management.

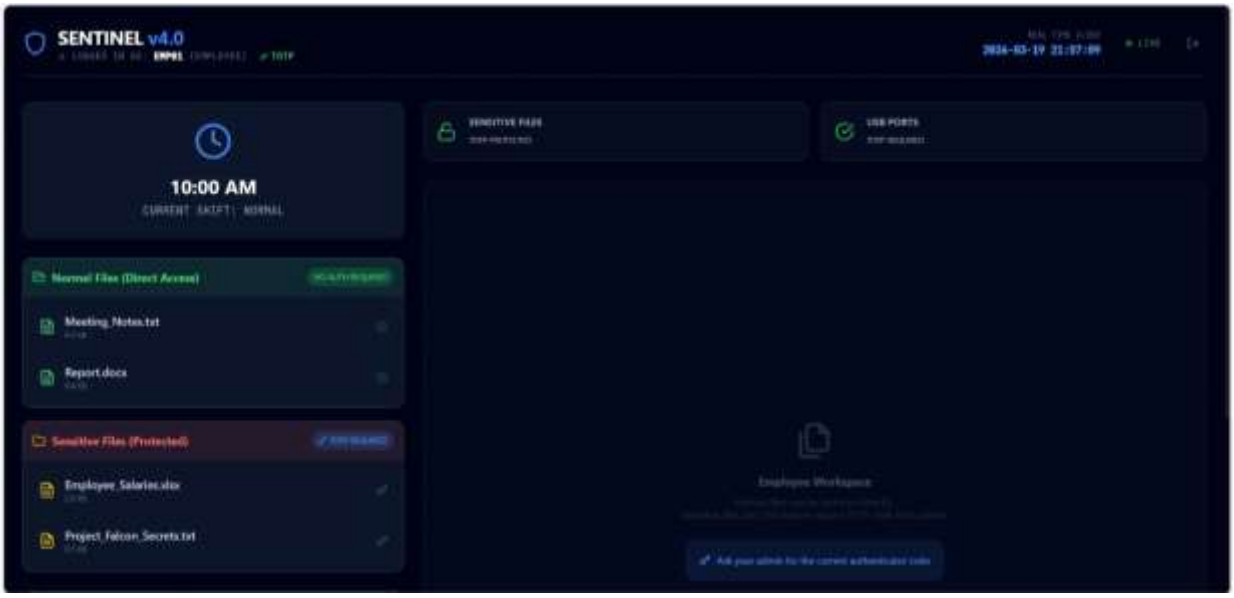

Fig 5.4 Employee Dashboard

The Employee dashboard offers a restricted interface tailored to individual user roles for performing assigned tasks. It ensures access only to authorized features, maintaining system security. All user actions are recorded to support monitoring and detect any suspicious behavior.

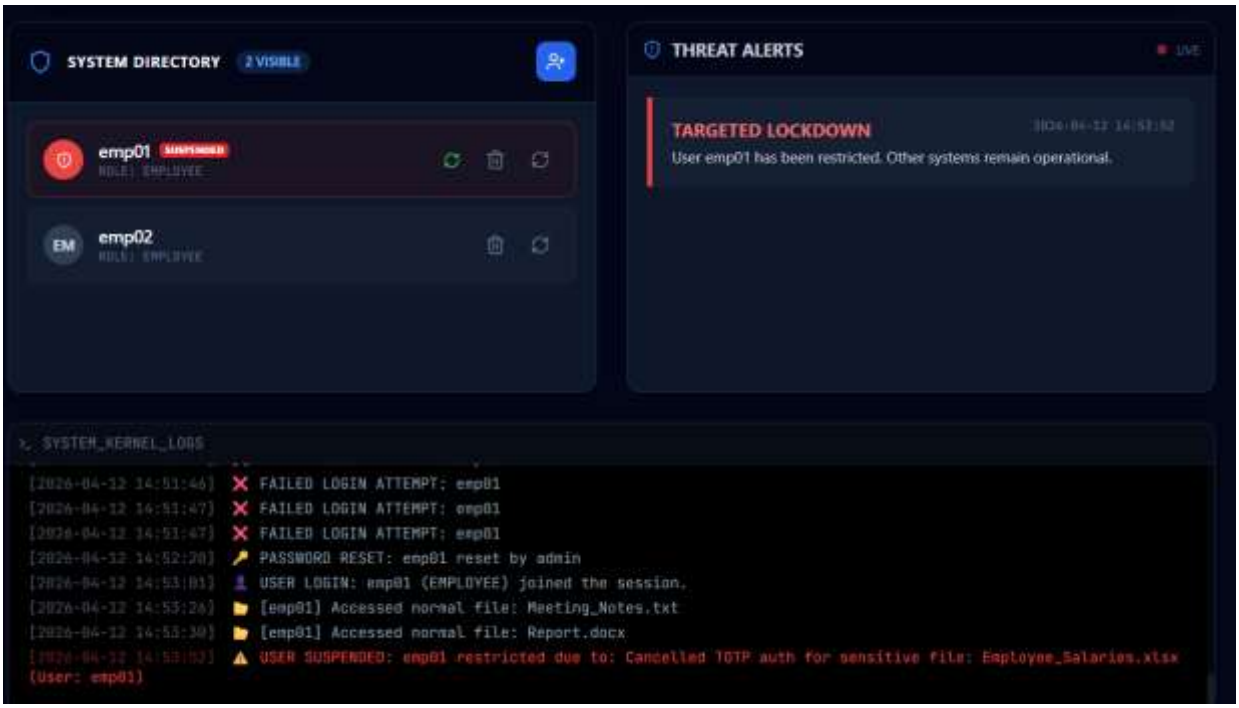

Fig 5.5 Threat Detection Page And Logs Generation

This page presents detailed system logs along with identified threats for administrative review. It organizes information based on severity levels to highlight suspicious activities. Administrators can use these insights to evaluate risks and take appropriate security measures.

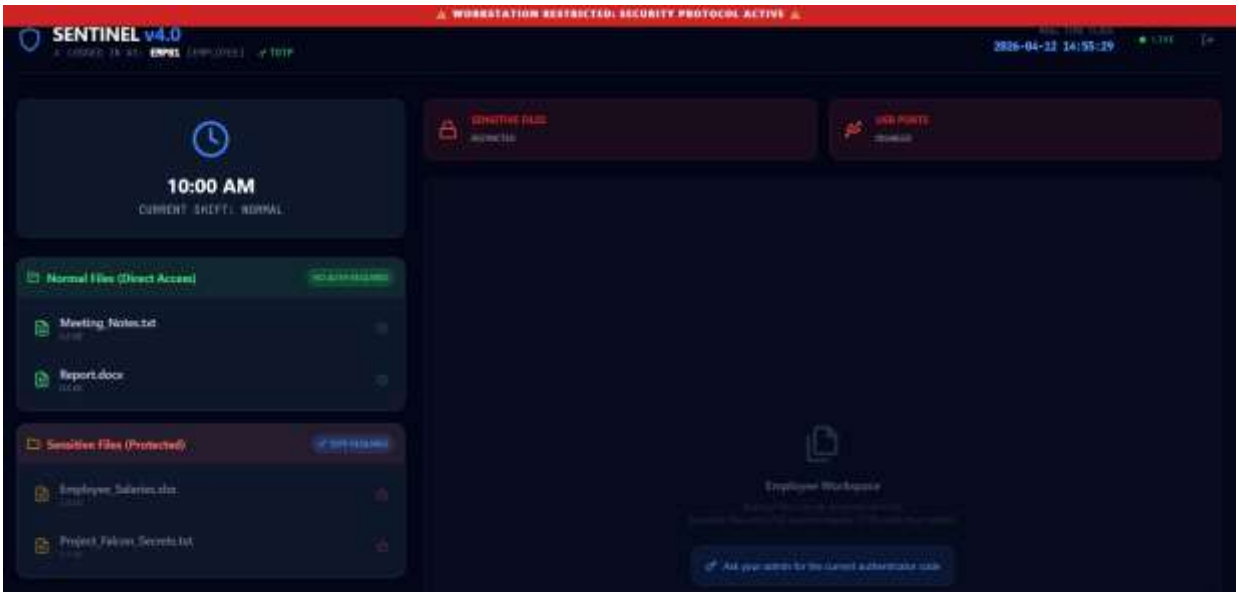

Fig 5.6 Lockdown State

This page indicates the system's response when suspicious activity is identified in a user account. During this state, access is limited to stop any further unauthorized actions. The lockdown feature helps contain potential threats and preserve overall system security.

VI. CONCLUSION

The Insider Threat Detection System presents a dependable and efficient solution for identifying and monitoring suspicious activities using a rule-based approach. It combines technologies such as React (Vite) for the frontend and Flask with Socket.IO for backend operations, ensuring a smooth and interactive user experience. By leveraging tools like Watchdog, WMI, and PyWin32, the system performs continuous real-time tracking of file activities and system processes.

The use of predefined rules enables fast detection of potential threats without relying on complex models, making the system lightweight and effective. Instant alert generation allows administrators to respond quickly to security incidents, while the intuitive dashboard simplifies log analysis and supports better decision-making.

VII. REFERENCES

1) Bishop, M., & Gates, C. (2008). Defining the insider threat. Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research, 1–3. ACM.

2) Greitzer, F. L., Kangas, L. J., Noonan, C. F., Dalton, A. C., & Hohimer, R. E. (2013). Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats. 2013 IEEE Security and Privacy Workshops, 46–53. IEEE.

3) Magklaras, G., & Furnell, S. (2005). A preliminary model of end user sophistication for insider threat prediction in IT systems. Computers & Security, 24(5), 371–380.

4) Liu, Y., & Chen, T. M. (2018). Behavioral modeling for insider threat detection. IEEE Systems Journal, 12(2), 1833–1842.

5) Eberle, W., Holder, L., & Cook, D. J. (2010). Insider threat detection using graph-based approaches. Journal of Applied Security Research, 6(1), 32–81.

6) Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes. Addison-Wesley Professional.

7) Salem, M. B., Hershkop, S., & Stolfo, S. J. (2008). A survey of insider attack detection research. In Insider Attack and Cyber Security (pp. 69–90). Springer.

8) Brdiczka, O., Liu, J., Price, B., Shen, J., Patil, A., Chow, R., & Bart, E. (2012). Proactive insider threat detection through graph learning and psychological context. 2012 IEEE Symposium on Security and Privacy Workshops, 142–149. IEEE.

9) Cole, E., Garman, J., & Friedberg, J. (2005). Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft. Syngress Publishing.

10) Legg, P. A., Buckley, O., Goldsmith, M., & Creese, S. (2015). Automated insider threat detection system using user and role-based profile assessment. IEEE Systems Journal 11(2), 12.