www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 06, Issue 07, July 2026, pp : 1717-1722

e-ISSN : 2583-1062
Impact Factor : 7.001

AI-BASED INSIDER BEHAVIOR ANALYSIS USING BEHAVIORAL ANALYTICS AND TRUST SCORE EVALUATION

Gowtham S[1], Deepesh G[2], Dr. Chandrakanth G Pujari[3]

[1,2]Student Of MCA, Department Of MCA, Dr. Ambedkar Institute Of Technology, Bengaluru, India.

[3]Guide, Department Of MCA, Dr. Ambedkar Institute Of Technology, Bengaluru, India.

DOI: https://www.doi.org/10.58257/IJPREMS54416

ABSTRACT

The increasing reliance on digital collaboration platforms has improved organizational productivity but has also increased the risk of security incidents caused by trusted employees. Unlike external attacks, insider-related risks often arise from authorized users whose activities appear legitimate, making abnormal behavior difficult to identify using conventional security mechanisms. Traditional access control and authentication methods primarily verify user identity but provide limited capability to continuously evaluate employee behavior after system access is granted.

This paper presents an **AI-Based Insider Behavior Analysis** system that integrates secure file sharing with behavioral analytics to strengthen organizational security. The proposed system continuously monitors employee activities such as file-sharing behavior, camera permission status, policy violations, and mobile phone detection using the YOLOv8 object detection model. Behavioral events are analyzed to generate a dynamic trust score that reflects the reliability of individual users based on their observed activities. Before sensitive files are accessed or shared, administrators can review the generated trust score and behavioral summary to support informed security decisions.

The system also provides a centralized behavioral analytics dashboard that visualizes employee activities, identifies abnormal behavioral patterns, and facilitates communication between administrators and employees through an integrated messaging module for incident clarification and resolution. By combining artificial intelligence, behavioral monitoring, trust-based evaluation, and secure collaboration within a unified framework, the proposed system offers an effective and practical approach for improving organizational security while supporting responsible access to confidential information.

Keywords: Behavioral Analytics, Insider Behavior Analysis, Artificial Intelligence, Trust Score, Secure File Sharing, YOLOv8, User Behavior Monitoring, Organizational Security.

1. INTRODUCTION

The rapid growth of digital technologies has transformed the way organizations store, manage, and share confidential information. Cloud-based platforms and secure file-sharing systems have improved collaboration by enabling employees to access organizational resources from different locations. However, these advancements have also increased the possibility of security risks originating from authorized users who already possess legitimate access to sensitive organizational data. Unlike external cyberattacks, insider-related incidents are often difficult to identify because user activities initially appear legitimate.

Traditional security mechanisms such as authentication, access control, and encryption primarily focus on preventing unauthorized access to organizational systems. Although these techniques effectively protect against external threats, they provide limited capability to evaluate user behavior after successful authentication. Employees may unintentionally violate security policies or misuse organizational resources, making continuous behavior monitoring essential for maintaining information security.

This research presents an **AI-Based Insider Behavior Analysis** system that integrates secure file sharing with behavioral analytics to monitor employee activities and improve organizational security. The proposed system continuously analyzes user behavior, including file-sharing activities, camera permission status, policy compliance, and mobile phone detection using the YOLOv8 object detection model. Based on these behavioral events, the system generates a dynamic trust score that reflects the overall reliability of each employee and assists administrators in making informed security decisions before sensitive information is accessed or shared.

To support effective security management, the system provides a centralized behavioral analytics dashboard that enables administrators to monitor employee activities, review trust scores, identify unusual behavioral patterns, and communicate directly with employees through an integrated messaging module whenever suspicious activities require

clarification. This approach promotes proactive security management while maintaining secure collaboration among authorized users.

The proposed framework combines artificial intelligence, behavioral analytics, trust score evaluation, and secure file-sharing mechanisms into a unified platform for analyzing insider behavior. By continuously evaluating employee activities instead of relying solely on traditional access control mechanisms, the system provides an effective approach for strengthening organizational security and protecting confidential information.

2. LITERATURE REVIEW

2.1 Study by Das et al. (2024)

Das et al. proposed a User and Entity Behavior Analytics (UEBA) framework that applies machine learning techniques to monitor employee activities and identify abnormal behavioral patterns. The study demonstrated that behavioral analytics can improve the early identification of suspicious user activities by analyzing deviations from normal behavior. However, the proposed approach primarily focused on behavioral monitoring and did not incorporate trust score evaluation or secure organizational file-sharing mechanisms.

2.2 Study by Rashid et al. (2022)

Rashid et al. developed a deep learning-based model for analyzing employee behavior using organizational activity logs. The system successfully identified abnormal behavioral patterns by learning from historical user data, thereby improving the accuracy of insider behavior analysis. Despite its effectiveness, the framework depended heavily on large training datasets and did not provide real-time behavioral evaluation or intelligent trust assessment for organizational users.

2.3 Study by Alneyadi et al. (2021)

Alneyadi et al. investigated secure access control and authentication mechanisms for protecting organizational information. Their work emphasized controlled access and secure document management to reduce unauthorized data exposure. Although the proposed solution strengthened access security, it offered limited support for continuous behavioral analytics, trust score generation, and administrator-assisted behavior evaluation after user authentication.

2.4 Research Gap

Existing research demonstrates the importance of behavioral analytics, machine learning, and secure access control in improving organizational security. However, most existing approaches focus on either user behavior analysis or secure file management independently. Limited attention has been given to integrating behavioral analytics, dynamic trust score evaluation, secure file sharing, AI-based device monitoring, and administrator-employee communication within a single framework. To address the identified research gap, this work proposes an AI-Based Insider Behavior Analysis framework that continuously observes employee activities, evaluates user trust through dynamic scoring, incorporates AI-driven mobile phone detection, and assists administrators with behavior assessment and communication. By integrating these capabilities into a single platform, the framework enhances the secure management of confidential organizational data.

3. PROPOSED METHODOLOGY

3.1 System Architecture

The proposed AI-Based Insider Behavior Analysis system follows a layered architecture consisting of the User Layer, Frontend, Backend, AI Behavior Analysis Module, Database, and Administrator Dashboard. Employees and administrators interact with the system through a React.js-based web interface. The backend, developed using Node.js and Express.js, manages user authentication, authorization, file management, activity logging, user administration, and secure communication with the AI module. Every user action, including file upload, download, sharing, preview, login, and other activities, is recorded and forwarded for behavioral analysis. The frontend also provides access to behavioral analytics, trust score information, and administrator communication features through a centralized interface.

The AI Behavior Analysis module, implemented using Python Flask, continuously evaluates employee activities by combining behavioral analytics with YOLOv8-based mobile phone detection during sensitive operations such as file preview or access. Behavioral records generated from employee interactions are evaluated by the proposed framework to derive an adaptive trust score, allowing the system to continuously reassess user reliability based on observed activities rather than relying solely on static access privileges. All user information, activity logs, behavioral records,

trust scores, and messages are securely stored in MongoDB. The Administrator Dashboard retrieves this information to present behavioral analytics, user activity reports, trust score summaries, alerts, and communication history, enabling administrators to monitor employee behavior, investigate unusual activities, and make informed decisions for protecting organizational information.

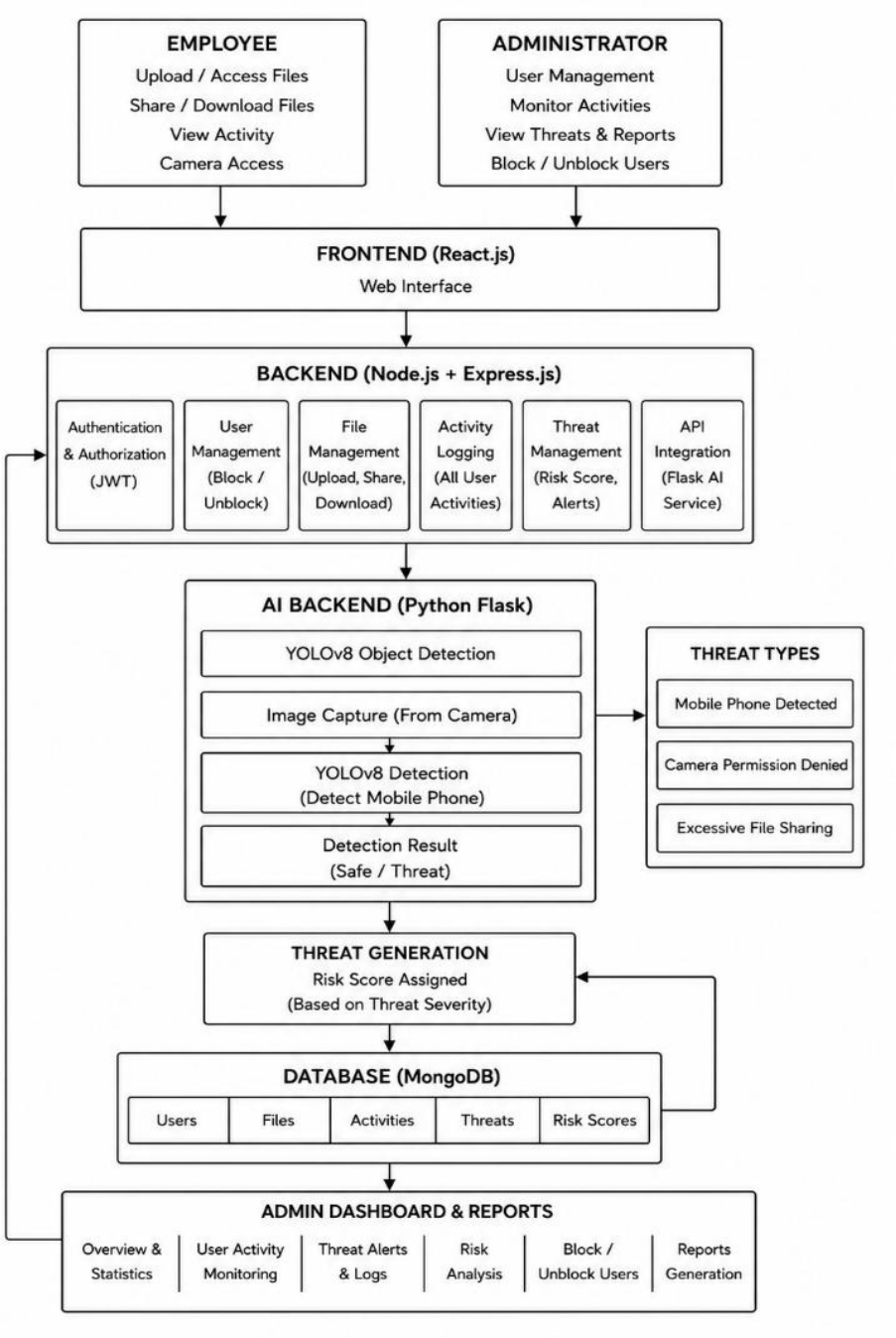


Fig. 1. System Architecture of the Proposed AI-Based Insider Behavior Analysis

3.2 User Authentication and Access Control

The proposed system employs a role-based authentication mechanism to verify user credentials and provide access according to assigned responsibilities. The administrator creates employee accounts by entering the required employee information. Once registration is completed, the system automatically generates an initial password and securely sends the login credentials to the employee's registered email address. Employees authenticate using JWT-based authentication, while role-based authorization ensures that employees and administrators can access only the functionalities permitted for their respective roles.

Rather than allowing continued use of the password assigned during registration, the application requires every employee to define a new confidential password before accessing organizational features. This approach minimizes

the security risks associated with temporary login credentials and ensures that only the respective employee knows the account password. This process minimizes the risks associated with default credentials and improves account protection. In addition, administrators can activate, block, or unblock employee accounts whenever unusual behavior or policy violations are observed. Restricting access to blocked accounts helps prevent unauthorized system usage and contributes to maintaining a secure organizational environment.

3.3 Secure File Sharing and Activity Monitoring Module

The secure file-sharing module enables employees to upload, preview, download, and share confidential documents while ensuring that access is limited to authorized recipients. Before sharing a file, users specify the intended recipient and appropriate access permissions, allowing confidential information to remain accessible only to approved employees. This controlled sharing mechanism improves data confidentiality and minimizes unauthorized disclosure of organizational documents.

Along with secure file management, the system continuously records user activities, including file uploads, downloads, previews, sharing operations, and login events. These activity records provide the behavioral information required for continuous user analysis and support the identification of abnormal usage patterns. Together, secure document handling and systematic recording of user interactions provide meaningful behavioral evidence that supports employee behavior analysis, trust score evaluation, and informed administrative decision-making.

3.4 AI-Based Behavior Analysis and Trust Score Module

The AI-Based Behavior Analysis module continuously evaluates employee activities using artificial intelligence and behavioral analytics. When employees interact with confidential documents, the application temporarily activates the device camera to capture images. These images are then examined by the YOLOv8 object detection model to identify the presence of mobile phones, providing additional behavioral evidence for subsequent trust score evaluation. In addition to object detection, the module examines behavioral events such as frequent file sharing, repeated login attempts, camera permission status, and policy compliance to understand employee behavior.

The collected behavioral information is evaluated to compute an adaptive trust score that changes according to recent user activities and observed behavioral patterns. Rather than relying solely on static access permissions, the trust score provides administrators with an additional measure for assessing user reliability before confidential operations are performed. This continuous evaluation supports intelligent behavior analysis while improving organizational security.

3.5 Behavioral Analytics and Administrator Dashboard

The Behavioral Analytics module consolidates user activity records, trust score information, and behavioral observations into a centralized administrator dashboard. The dashboard presents employee activity logs, behavioral summaries, trust score trends, and alerts that help administrators monitor user behavior throughout the organization. Historical behavioral records enable administrators to compare recent activities with previous patterns, supporting more accurate evaluations of employee behavior.

Instead of treating every activity as suspicious, the system provides behavioral insights that assist administrators in identifying deviations from normal user behavior. These analytical reports support informed decision-making and help administrators respond appropriately while reducing unnecessary interruptions for legitimate users.

3.6 Administrator Communication and Decision Support Module

The Administrator Communication and Decision Support module allows administrators to review employee behavior, trust scores, and activity records through a centralized dashboard. When unusual behavior is observed, administrators can communicate with employees using the integrated messaging feature before making decisions. Based on the behavioral analysis and employee response, appropriate actions such as maintaining access, issuing warnings, or temporarily restricting user access can be taken.

4. RESULTS AND DISCUSSION

4.1 Employee Account Creation Interface

Figure 2 illustrates the employee account creation interface used by the administrator. During registration, the administrator enters the employee's details, including employee ID, department, contact information, and work schedule. After successful registration, the system automatically generates login credentials and securely sends them to the employee's registered email address, simplifying the onboarding process while ensuring secure account creation.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
www.ijprems.com
editor@ijprems.com
Vol. 06, Issue 07, July 2026, pp : 1717-1722
e-ISSN : 2583-1062
Impact Factor : 7.001

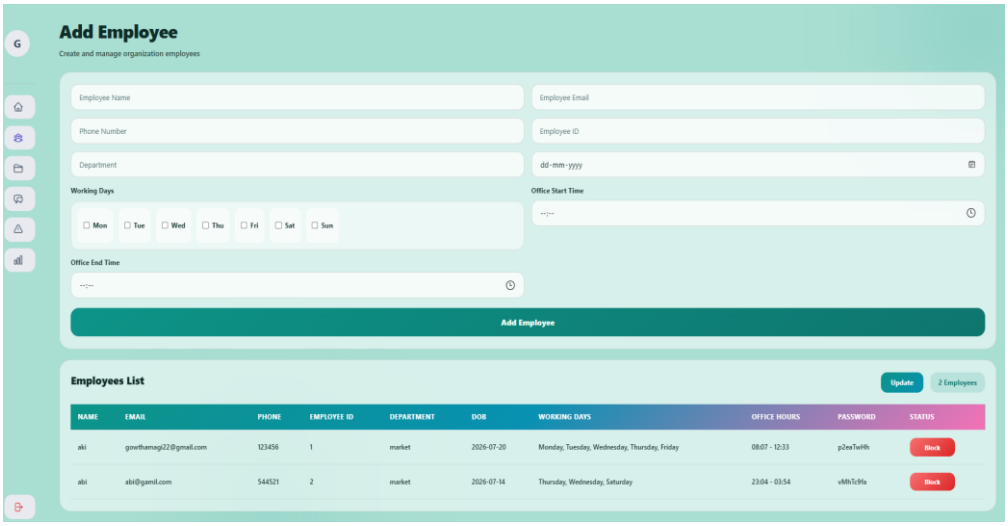


Fig. 2. Employee Account Creation Interface

4.2 My Files Interface

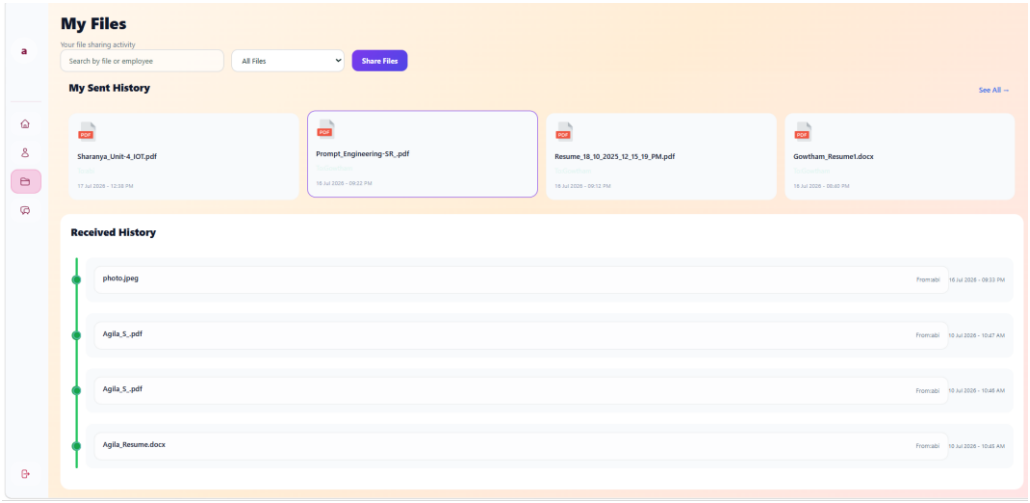


Fig. 3. My Files Interface

Figure 3 illustrates the My Files interface, where employees can securely manage their uploaded and shared documents. The interface allows users to upload, preview, download, and share files with authorized recipients while maintaining controlled access. All document-related activities are recorded to support behavioral analysis and administrative monitoring.

4.3 Behavioral Analytics Dashboard



Fig. 4. Behavioral Analytics Dashboard

Figure 4 presents the Behavioral Analytics Dashboard, which provides administrators with an overview of employee activities, behavioral observations, and dynamically generated trust scores. The dashboard summarizes user interactions, highlights behavioral patterns, and enables administrators to review employee behavior for informed security-related decision-making.4.4 Threat Monitoring Interface.

4.4 Administrator–Employee Messaging Interface

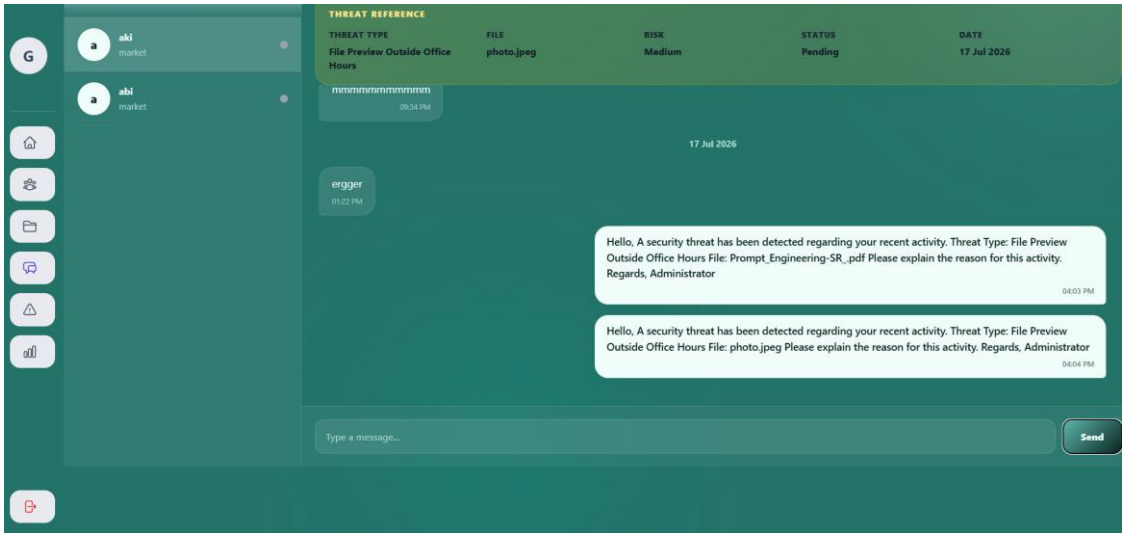


Fig. 5. Administrator–Employee Messaging Interface

Figure 5 illustrates the messaging interface that enables communication between administrators and employees. When unusual behavioral patterns require clarification, administrators can initiate conversations directly through the system. This feature supports transparent communication, helps resolve concerns, and assists administrators in making appropriate decisions based on employee responses and behavioral records.

5. CONCLUSION

This paper presented an AI-Based Insider Behavior Analysis framework that combines behavioral analytics, secure file management, and trust score evaluation to improve organizational security. The proposed system continuously monitors employee activities, analyzes behavioral patterns, and incorporates YOLOv8-based mobile phone detection during confidential operations to provide additional behavioral insights. By generating adaptive trust scores and presenting behavioral information through an administrator dashboard, the framework supports informed decision-making without relying solely on traditional access control mechanisms. The integrated communication feature further enables administrators to clarify unusual activities before taking corrective actions. Overall, the proposed framework combines behavioral analytics, adaptive trust score evaluation, and secure document management to provide administrators with meaningful insights for informed decision-making while promoting a safer organizational environment.

6. REFERENCES

[1] J. R. C. Nurse, S. Creese, and D. De Roure, "Security Risk Assessment in Internet of Things Systems," IT Professional, vol. 19, no. 5, pp. 20–26, Sept.–Oct. 2017.

[2] A. Tuor, S. Kaplan, B. Hutchinson, N. Nichols, and S. Robinson, "Deep Learning for Unsupervised Insider Threat Detection in Structured Cybersecurity Data Streams," AAAI Workshops, 2017.

[3] G. Jocher, A. Chaurasia, and J. Qiu, YOLOv8: Ultralytics Object Detection Model, Ultralytics, 2023.

[4] D. Merkel, "Docker: Lightweight Linux Containers for Consistent Development and Deployment," Linux Journal, no. 239, pp. 2–7, 2014.

[5] M. Grinberg, Flask Web Development: Developing Web Applications with Python, 2nd ed., O'Reilly Media, 2018.