Enterprise User Risk Detection Using Behavioral Analytics and Deep Learning

Venkata Vamsi Krishna Bezawada
MSc in Data Science, South East Technological University Carlow
Supervisor: Milu Philip

Introduction

- Insider threats originate from individuals within an organization who misuse legitimate access
- They are difficult to detect because their behavior often appears normal
- Traditional rule-based systems fail to detect subtle and evolving threats
- Insider threat detection involves challenges such as class imbalance (rare malicious events), integration of multi-source behavioral data, and the need for explainable models
- This project uses behavioral analytics and deep learning to detect anomalous user activity

Research Objectives

To develop a system that can:

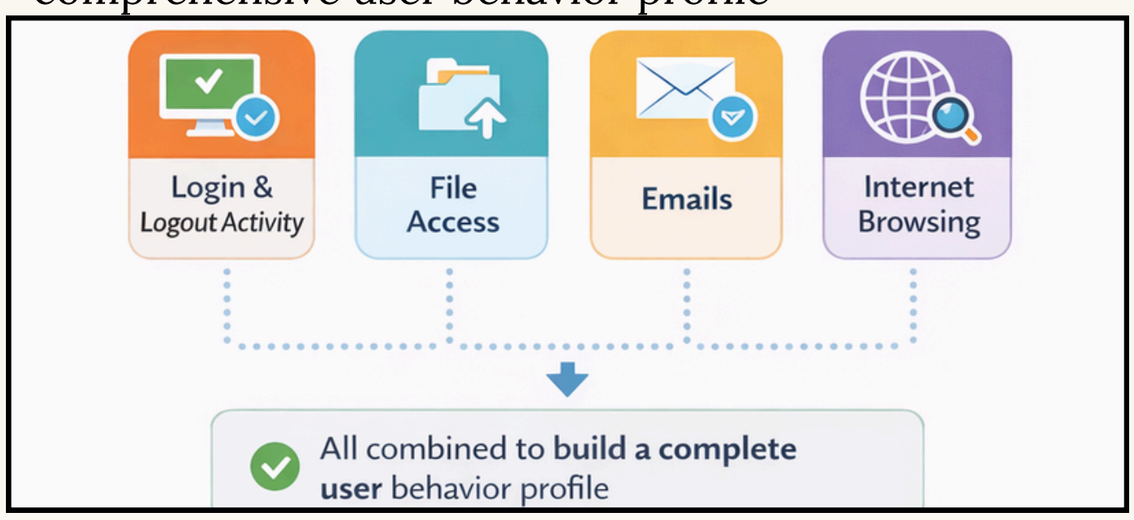
- Detect risky user behavior
- Identify potential insider threats
- Analyze user activity patterns over time
- Support early detection and response

Key Idea

- Every user has a unique behavioral pattern
- Suspicious activity is identified as a deviation from normal behavior over time
- The system learns baseline behavior using historical data
- Sequential activity patterns are analyzed to detect anomalies
- Each user is assigned a risk score based on detected deviations

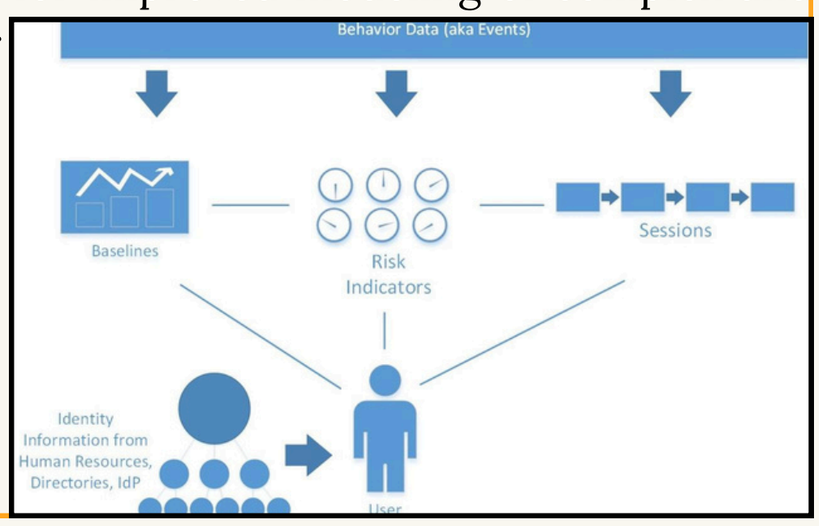
Data Used

- Employee login activity
- File access
- Emails
- Internet usage
- Data from multiple sources is combined to build a comprehensive user behavior profile



Method

1. Collect and preprocess multi-source user activity data
2. Build baseline behavioral profiles for each user
3. Use LSTM-based models to learn sequential activity patterns
4. Apply Autoencoder-based anomaly detection to identify deviations
5. Extend with Transformer and Graph Neural Network (GNN) approaches for improved modeling of complex and relational behavior
6. Generate a risk score based on anomaly detection results
7. Flag high-risk users for further analysis



Literature Review

- LSTM and Transformer-based models are used to learn sequential user behavior and detect anomalies
- Graph Neural Networks (GNNs) model relationships between users and resources for improved detection
- Insider threat detection faces extreme class imbalance, with rare malicious events
- SMOTE, undersampling, and focal loss are used to address imbalance, though their effectiveness remains limited
- SHAP-based explainable AI is used for interpreting model predictions, but its real-world use is limited
- Multi-modal data fusion improves detection by combining multiple behavioral data sources

Tools

Next Steps

- Evaluate models on standardized datasets (e.g., CERT)
- Improve handling of class imbalance and rare events
- Integrate SHAP for model explainability
- Explore real-world deployment and scalability
- Perform validation in operational environments
- Validate performance using Precision, Recall, and F1-score

References

- Adeduro, A., et al. (n.d.). Proactive insider threat detection framework: An explainable AI and behavioral analytics-driven approach.
- Aljumaily, H., et al. (2025). Enhancing user and entity behavior analytics in SIEM systems using AI-powered anomaly detection: A data-driven simulation approach. International Journal of Multidisciplinary Research and Analysis, 1(2). https://doi.org/10.33971/ijmrai.1.2.11
- Ali, M., et al. (2025). Real-time detection of insider threats using behavioral analytics and deep evidential clustering.