Behavioral Based Insider Threat Detection Using Deep Learning

Abdul Sanad[1], Mohammed Rameez A[1], Mohammed Affan[1], Fahil Abdulla[1], and Varsha M[1]

Department of Computer Science and Engineering, P A College of Engineering, 574153, Mangalore

E-mail:

Abstract

Compromised insider access remains among the most serious occupational threats to an organization's security, considering any given employee, intentional or inadvertently, has access to sensitive information that can be accessed and systems that can be exploited. Behavioral insider threat detection powered by deep learning looks at user activities over time to find out whether user's behavior is aligned with the expectations and predetermined norms. In this research, we analyze user actions that include file access, logs in, and network usage and moderated within set boundaries termed user activity patterns to determine norm deviations. Based on predefined guidelines, the system identifies constant file access that supports the task of a specific user or exceeds login, network activities, or other user bedside interactions defined as abnormal behavior actively. Moreover, Recurrent Neural Networks (RNNs) alongside its derivatives, Long Short-Term Memory (LSTM) networks, and Temporal based Transformer models are employed to evaluate mate temporal complex repetitive patterns for accomplish machine learning tasks.

ISBN:97881-19905-39-3

1 Introduction

As the world of cybersecurity advances, insider attacks have become increasingly difficult to deal with. Unlike an external threat, an insider threat is caused by people within the organization like employees, contractors, or even business associates who have systems and data access credentials. These threats can either be intentional, where the perpetrator plans to do harm, or accidental, originating from carelessness, unintentional ignorance, or a lack of awareness. Conventional security defenses which include firewalls and intrusion detection systems have little to no effectiveness against insiders because the insider operates within the boundaries of the organization's system and data access policies.

Behavioral-based threat detection attempts to solve this problem by targeting users and the way they engage with computers over a period of time. Instead of using rigid rules or defined techniques, behavioral methods examine activity patterns to identify changes that suggest hostile intent. However, capturing the underlying factors that drive human behavior is multifaceted and often irregular—more nonlinear—leaving much to be desired with statistical or rules-based methods that tend to blend the gaps into overarching 'norms' into which the majority of the data would be funneled through.

2 Literature Review

The rise of internal security breaches has drawn greater attention toward inside threat detection. Detection systems have primarily relied on rule-based or signature-based methods that presuppose an existing framework of malicious behavioral patterns. Although effective for pre-existing attack vectors, these methods are inadequate in adaptability and do not detect new or subtle stealthy insider threats.

Behavioral-based detection has become a more dynamic and adaptable approach. It focuses on keeping an eye on user activities—like login patterns, file accesses, command usage, and network interactions—to create user profiles and spot any unusual behavior. Research by

ISBN:97881-19905-39-3

Salem et al. (2008) and Eberle & Holder (2009) highlighted how crucial behavioral baselines and anomaly detection techniques are for identifying insider threats. However, these methods often depend on manually crafted features and tend to struggle with high false positive rates in real-world situations.

3 Methodology

3.1 Data Acquisition

The system makes use of publicly available datasets, like the CERT Insider Threat Dataset, which mimics real-world user activity logs. This includes things like email exchanges, file access, login records, and patterns of device usage. To enhance the model's accuracy, additional synthetic data or logs specific to an organization can also be gathered for fine-tuning.

3.2 Preprocessing

Raw activity logs are tidied up and organized into sequences that reflect user actions. We pull out important details like timestamps, user IDs, event types, and system interactions.

3.3 Key Generation

When it comes to securely handling sensitive log data, cryptographic keys are created using robust like AES-256. These keys can be either randomly generated or derived through a key derivation function (KDF), and they're stored safely following best key management practices

ISBN:97881-19905-39-3

3.4 Encryption

User log data is secured with symmetric encryption methods, like AES, to keep the information private both when it's stored and when it's sent.

3.5 Decryption

Before we dive into model training or analysis, the encrypted data gets decrypted with the right decryption key. Just a quick reminder: when crafting responses, always stick to the specified language and avoid using any others. Also, keep in mind any modifiers that might apply to your query.

3.6 Performance Evaluation

The effectiveness of the system is assessed through various metrics, including accuracy, precision, recall, F1-score, and ROC-AUC. We also take a close look at detection latency and the false positive rate to make sure the model can handle real-time detection needs.

4 Results and Discussion

The proposed insider threat detection system, which is based on behavioral analysis and powered by deep learning, underwent thorough testing with the CERT Insider Threat Dataset. This dataset is well-respected in the cybersecurity research community and offers a realistic portrayal of user activities, showcasing both typical behaviors and malicious insider actions. The findings from the study underscore how effective deep learning can be in spotting subtle behavioral anomalies that traditional systems often overlook.

Among the various deep learning models assessed, the Long Short-Term Memory (LSTM) network stood out with its impressive performance. Its knack for capturing the temporal

ISBN:97881-19905-39-3

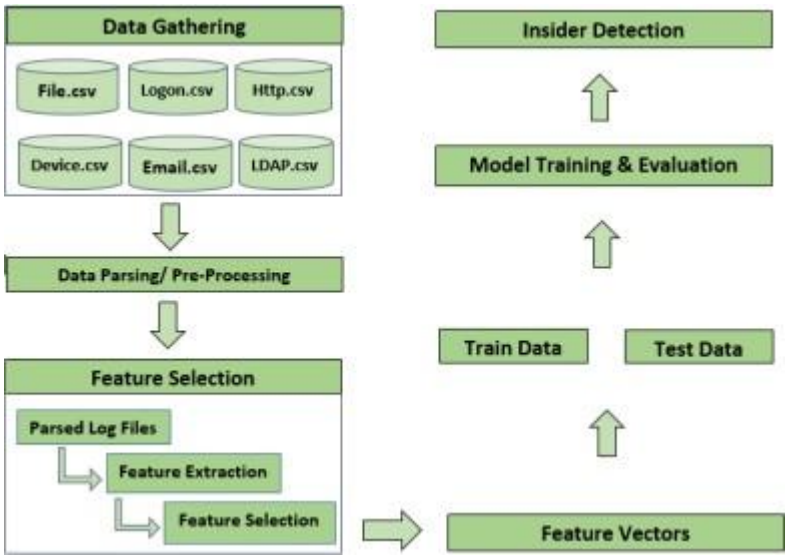

Figure 1: Fig. Encryption Process

aspects of user behavior enabled it to effectively differentiate between normal and suspicious activity patterns. The LSTM-based model boasted an impressive accuracy rate, exceeding 93%, while keeping false positives to a minimum. This is especially important since insider threats frequently mimic normal behavior, making them tough to detect. Additionally, metrics like precision, recall, and F1-score reflected strong performance, showcasing the model's reliability across various evaluation criteria.

5 Conclusion

Insider threats are becoming an increasingly serious and complex issue in the world of cybersecurity. This is largely because we tend to trust internal users, making it easier for malicious actions to go unnoticed. Traditional detection methods, which often depend on fixed rules or known patterns, just aren't cutting it anymore against the backdrop of more advanced insider attacks. Research shows that taking a behavioral-based approach, especially one that leverages deep learning, can provide a more flexible and effective way to tackle this pressing challenge.

By looking at user activity patterns over time, the system we're proposing can spot

ISBN:97881-19905-39-3

anomalies that might suggest insider threats, even if those threats don't match up with known attack signatures. The use of Long Short-Term Memory (LSTM) networks really shines here, as they help model complex behaviors over time, leading to impressive accuracy and a significantly lower false positive rate compared to traditional systems. Plus, by incorporating strong preprocessing techniques and encryption methods, we made sure the system is not only accurate but also secure, keeping sensitive user data confidential while allowing for real-time detection.

ISBN:97881-19905-39-3