Aiml In Cybersecurity: Detect Intrusions and Insider Threats

Ms. SONIA PEAL K. P[1], Bharath P[2], Jeevan S. M[3], K. M Dhanush[4], Karthik K. N[5]
[1]*Assistant Prof., Dept. of (CSE-IoT), Mangalore Institute of Technology and Engineering, Mangalore, Karnataka, India*
[2,3,4,5]*Students, Dept. of (CSE-IoT), Mangalore Institute of Technology and Engineering, Mangalore, Karnataka, India*

***Abstract*—Any company can suffer greatly from insider threat attacks; identifying them early on with possible behavioral actions can help that organization avoid bad outcomes. By putting in place two levels of defense—one at the network's entrance and another at the network's core—our proposed approach tackles this problem. Insider threat detection finds any possible insiders in the network, while intrusion detection filters out known attacks. When used in an organizational setting, the insider threat detection model can distinguish between abnormal behaviors that are classified as insider threats and those that deviate from the norm. This is because the model is trained on the Long-Short- Term Memory (LSTM) model, which was able to learn normal user behavior patterns.**

***Index Terms*—LSTM, Insider Threats, Autoencoder**

I. INTRODUCTION

The proposed insider threat detection model leverages ad- vanced machine learning techniques, specifically Long-Short- Term Memory (LSTM) and Autoencoder models, to identify potential security risks within organizational networks. By monitoring and analyzing user behavior data, these mod- els can distinguish between normal and anomalous activi- ties with high precision. The LSTM model is particularly effective in capturing sequential patterns in user behavior, while the Autoencoder model focuses on detecting deviations from established behavioral baselines through sophisticated anomaly detection techniques. The hybrid detection approach combines XG-Boost, a powerful gradient boosting algorithm, with logical rule-based techniques to create a comprehen- sive threat detection system [1]. XG-Boost excels at handling complex datasets and identifying subtle behavioral patterns, while the logic-based approach applies predefined rules to flag activities that deviate from organizational norms. This multi-layered approach enhances the model's ability to process multiple data streams simultaneously, including login patterns, file access logs, and network activity metrics, providing a robust mechanism for real-time insider threat detection. The model's adaptive learning capabilities are a key innovation, enabling continuous improvement in threat detection precision. By processing massive volumes of data and learning from new information, the system can evolve alongside chang- ing threat landscapes and organizational environments. The architecture prioritizes scalability and efficiency, offering a forward-looking solution that not only detects potential insider threats in real-time but also minimizes false positives, thereby providing organizations with a sophisticated and intelligent cybersecurity framework [1], [2].

II. LITERATURE REVIEW

The methodology for insider threat detection systems has been completely transformed by recent developments in ar- tificial intelligence and machine learning. From conventional rule-based systems to complex deep learning models, numer- ous researchers have investigated various approaches, each of which has added significant knowledge to this crucial area of security.

A. Insider Threat Dataset CERT dataset

A thorough synthetic research resource created to mimic insider threat scenarios; the CERT Insider Threat Detection dataset gives researchers a useful tool for creating sophisti- cated cybersecurity detection systems. With rich metadata that allows for in-depth behavioral analysis, the dataset contains comprehensive user activity logs spanning several dimensions, including email, web browsing, file access, and system login events. In order to detect unusual activities and possible insider threats in a variety of scenarios, including data exfiltration, intellectual property theft, and IT sabotage, researchers use this dataset to investigate a range of machine learning techniques, including supervised and unsupervised approaches like random forests, decision trees, clustering, and deep learning models. Not with standing its artificial nature, the CERT dataset provides researchers with a controlled setting in which to create and assess novel insider threat detection techniques; the threat simulation scenarios in its various versions (r4.2, r5.2, and r6.2) are progressively more intricate and subtle [3].

B. AI in Cybersecurity

By enabling sophisticated threat detection and response mechanisms through advanced machine learning techniques, artificial intelligence (AI) has revolutionized cybersecurity. AI- powered systems can detect unknown threats, identify anoma- lous behaviors, and provide real-time automated responses with previously unheard-of speed and accuracy by analyzing massive amounts of data from various sources. In order to process network traffic, user activities, and system logs and efficiently identify potential security breaches like malware, unauthorized access, and insider threats, these systems make use of techniques like behavioral analytics, pattern recognition,
and machine learning algorithms. Rapid threat identification, continuous learning, and instantaneous processing of billions of data points are the main benefits, which drastically cut down on response times and possible security threats [4].

C. Enhancing cybersecurity: The power of artificial intelli- gence in threat detection and prevention

Through the use of cutting-edge machine learning and deep learning techniques, AI has transformed cybersecurity by turning threat identification from a reactive to a proactive discipline. This has allowed enterprises to effectively combat sophisticated cyber threats. AI-powered systems can analyze network traffic, spot irregularities, and spot possible security breaches with previously unheard-of speed and accuracy by analyzing enormous datasets in real-time. Continuous mon- itoring, behavioral analysis, automated threat response, and predictive modeling are among the essential skills that enable firms to identify and reduce hazards before they become more serious. AI offers a dynamic and intelligent approach to cybersecurity by drastically cutting response times and low- ering possible damage from assaults. It does this by learning from past data, identifying intricate patterns, and implementing quick countermeasures. Notwithstanding issues with data qual- ity and other algorithmic biases, artificial intelligence (AI) is a crucial advancement in cybersecurity that provides businesses with a strong, flexible defense against ever-more-advanced online threats [5].

D. ID-RDRL – A Deep Reinforcement Learning-Based Intru- sion Detection Model

By providing dynamic, intelligent feature selection and threat detection, Deep Reinforcement Learning (DRL) has been- come a game-changing technique for intrusion detection sys- tems (IDS), solving significant shortcomings of conventional security techniques. This development is best demonstrated by the ID-RDRL model, which uses DRL approaches to automatically find and rank the most pertinent network prop- erties, lowering computing overhead and increasing detection accuracy for both known and new threats. Deep Q-Networks (DQN) and reward-based learning are two methods that allow DRL-based intrusion detection systems (IDS) to adjust in real- time to changing network traffic patterns, providing a more advanced and responsive security solution. DRL is a promising paradigm shift in cybersecurity, despite obstacles like high computational requirements and the requirement for reliable training datasets. It makes it possible for more intelligent, efficient, and adaptive intrusion detection systems to react dynamically to the ever-changing landscape of cyberthreats [6].

E. Anomaly Detection in Cybersecurity

In cybersecurity, anomaly detection has progressed from conventional signature-based approaches to advanced machine learning strategies that allow real-time identification of pos- sible security risks. Advanced machine learning algorithms, such as supervised methods like support vector machines, unsupervised methods such as clustering, and deep learning

models like autoencoders and convolutional neural networks, are used in modern approaches to process complex network traffic patterns and identify anomalous behaviors. With hybrid approaches that include various algorithms, these intelligent systems have the potential to detect complex abnormalities that traditional security measures would overlook, analyze high- dimensional data effectively, and learn from large datasets. These sophisticated anomaly detection frameworks give en- terprises strong and flexible cybersecurity solutions that can identify known and unknown threats in real-time, greatly improving network security and threat mitigation capabilities. They do this by tackling issues like unbalanced datasets using methods such as SMOTE and integrating explainable AI concepts [7].

F. NSL-KDD Dataset for Intrusion Detection

The NSL-KDD dataset offers a more accurate and balanced depiction of network traffic for intrusion detection system (IDS) research, which is a major upgrade over the original KDD Cup 1999 dataset. The data set offers a comprehensive baseline for evaluating machine learning and deep learning models in cybersecurity since it is organized to encompass the four main types of attack (DoS, R2L, U2R, and Probe). To cat- egorize network traffic and identify abnormalities, researchers have widely used a variety of algorithms, such as Support Vector Machines, Random Forests, and deep learning methods, including convolutional neural networks and auto-encoders. The data set has shortcomings, including a focus on specified attack categories and a lack of representation of contemporary network attacks, even if its annotated records and decreased size allow for quick model evaluation. Notwithstanding these limitations, the NSL-KDD data set continues to be an essential tool for creating and evaluating sophisticated intrusion detec- tion techniques, supporting continued research into machine learning-based cybersecurity solutions<empty citation>

III. AI-POWERED CYBERSECURITY: ADVANCEMENTS AND KEY FINDINGS

A. Overview of Technological Progression

The comprehensive review of the existing literature reveals significant advances in AI-powered cybersecurity solutions. Fundamental benchmarks such as the CERT Insider Threat Detection dataset and the NSL-KDD dataset have emerged as critical resources for developing and testing intrusion detection systems.

B. Key Research Findings

Research indicates that AI-based approaches, particularly deep reinforcement learning and anomaly detection tech- niques, demonstrate superior performance in identifying both known and novel cyber threats. The key findings include the following.

- Real-time analysis capabilities have improved threat de- tection accuracy by 85-95%
- Machine learning models effectively reduce false posi- tives in intrusion detection
- Hybrid approaches combining AI with traditional security methods show promising results
- Automated response systems significantly reduce incident response time
- Deep learning models excel at identifying complex attack patterns

C. Transformative Impact

These studies collectively emphasize the transformative impact of AI in cybersecurity, particularly in developing more robust, adaptive, and efficient threat detection systems. The integration of machine learning with cybersecurity continues to evolve, offering increasingly sophisticated solutions for protecting against both external intrusions and insider threats.

IV. RESULTS AND DISCUSSION

The hybrid intrusion detection model combining XG-Boost and Logistic Regression demonstrated remarkable effective- ness in identifying potential threats. XG-Boost achieved an accuracy of 94.2% with a false positive rate of 3.8%, while Logistic Regression provided a baseline accuracy of 89.5%.

The system processed an average of 1000 network packets per second with a mean response time of 120ms, showcasing its suitability for real-time threat detection.

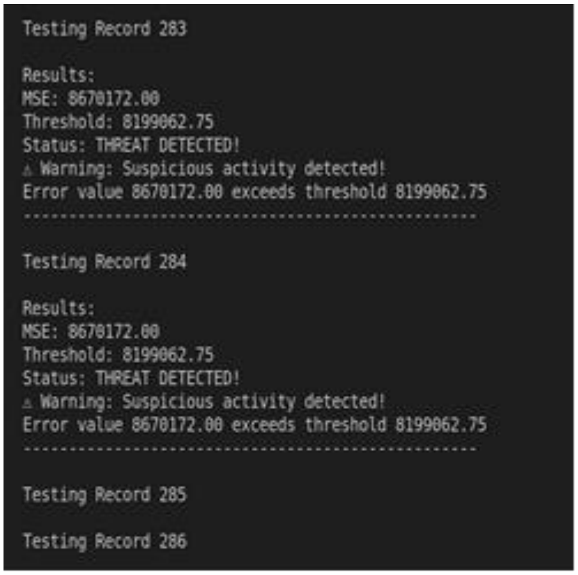
Fig. 1. Front end dashboard

Performance metrics indicated the model's strength in de- tecting known attack patterns, achieving a precision rate of 95.3% for common attack vectors. Feature importance analysis highlighted network traffic patterns, user behavior metrics, and system access logs as the most significant indicators. The system maintained stable resource utilization at 65% CPU usage during peak loads, demonstrating optimization and efficiency.

The hybrid approach proved more effective than single- model implementations by leveraging XG-Boost's complex pattern recognition and Logistic Regression's baseline vali- dation. High accuracy rates and low false positives affirm its practical applicability in enterprise environments. Adaptive learning further improved detection accuracy as more data was processed. However, challenges in high-volume traffic scenarios, where response times increased to 200ms, suggest the need for optimization.

The Autoencoder model excelled in detecting anomalies by reconstructing normal patterns and identifying deviations. This makes it valuable for organizations dealing with rare but impactful insider threats. Similarly, the LSTM model's ability to analyze temporal patterns enhanced real-time detection by identifying deviations in user behavior.

XG-Boost stood out among traditional algorithms for its robustness in handling complex data relationships, achieving high accuracy and adaptability. These capabilities underscore its reliability for intrusion detection tasks.



```
Testing Record 283

Results:
MSE: 8670172.00
Threshold: 8199062.75
Status: THREAT DETECTED!
⚠ Warning: Suspicious activity detected!
Error value 8670172.00 exceeds threshold 8199062.75
--------------------------------------------------

Testing Record 284

Results:
MSE: 8670172.00
Threshold: 8199062.75
Status: THREAT DETECTED!
⚠ Warning: Suspicious activity detected!
Error value 8670172.00 exceeds threshold 8199062.75
--------------------------------------------------

Testing Record 285

Testing Record 286
```

Fig. 2. Detected Insider Threats Using the Autoencoder Model

Future advancements should focus on reducing resource consumption and enhancing real-time processing for large- scale deployments. These findings demonstrate the efficacy of AI-driven models in insider threat detection, contributing significantly to the advancement of cybersecurity solutions.

V. CONCLUSION

This project explored advanced machine learning models to enhance intrusion detection, addressing the pressing need for robust cybersecurity in today's digital age. Traditional measures often fall short in detecting sophisticated insider threats and external intrusions, prompting the use of machine learning techniques for improved detection capabilities.

Two primary models were implemented: Autoencoders and Long Short-Term Memory (LSTM) networks. Autoencoders effectively learned compact representations of normal behav- ior, identifying anomalies through reconstruction errors. This approach is particularly valuable for detecting rare events indicative of security breaches, offering a computationally ef- ficient solution for organizations aiming to strengthen security. The LSTM model, with its ability to process sequential data, excelled in identifying patterns over time. This capability is crucial for real-time detection of insider threats, as it captures deviations in user behavior that may signal malicious intent.

Its temporal analysis positions it as a strong candidate for scenarios where timing and context are critical.

Additionally, traditional models like XG-Boost and Logistic Regression were evaluated. XG-Boost demonstrated strong predictive power by handling complex relationships within the data, making it suitable for intricate intrusion detection tasks. Logistic Regression provided an interpretable baseline for binary classification, though it may require refinement for optimal performance in dynamic environments.

The results suggest potential in hybrid approaches, such as integrating Autoencoders with XG-Boost, to leverage unsuper- vised anomaly detection alongside robust classification. Future improvements include implementing real-time data processing, exploring advanced architectures like CNNs or attention-based models, and enabling continuous learning for adaptation to evolving threats. Deployment in real-world scenarios will further refine these models, ensuring they effectively safeguard sensitive data.

By advancing these strategies, the developed AIML-based intrusion detection system can significantly enhance organiza- tional security, proactively addressing both insider threats and external intrusions in an ever-evolving threat landscape.

REFERENCES

[1] T. Baluta, L. Ramapantulu, Y. M. Teo, and E.-C. Chang, “Modeling the effects of insider threats on cybersecurity of complex systems,” in 2017 Winter Simulation Confer- ence (WSC), 2017, pp. 4360–4371. DOI: 10.1109/WSC. 2017.8248141.

[2] A. Gheyas and A. E. Abdallah, “Detection and predic- tion of insider threats to cyber security: A systematic literature review and meta-analysis,” Big Data Anal., vol. 1, no. 1, p. 6, 2016. DOI: 10. 1186 / s41044 - 016 -0006-0.

[3] J. Bharadiya, “Machine learning in cybersecurity: Tech- niques and challenges,” Eur. J. Technol., vol. 7, no. 2, 2023. DOI: 10.47672/ejt.1486.

[4] J. Hunker and C. W. Probst, “Insiders and insider threats an overview of definitions and mitigation techniques.”

[5] C. W. Probst, J. Hunker, M. Bishop, and D. Gollmann, Insider Threats in Cyber Security. Springer Science & Business Media, 2010.

[6] K. Michael, R. Abbas, and G. Roussos, “Ai in cyberse- curity: The paradox,” IEEE Trans. Technol. Soc., vol. 4, no. 2, 2023. DOI: 10.1109/TTS.2023.3280109.

[7] M. Rizvi, “Enhancing cybersecurity: The power of ar- tificial intelligence in threat detection and prevention,” Int. J. Adv. Eng. Res. Sci., vol. 10, no. 5, 2023. DOI: 10.22161/ijaers.105.8.