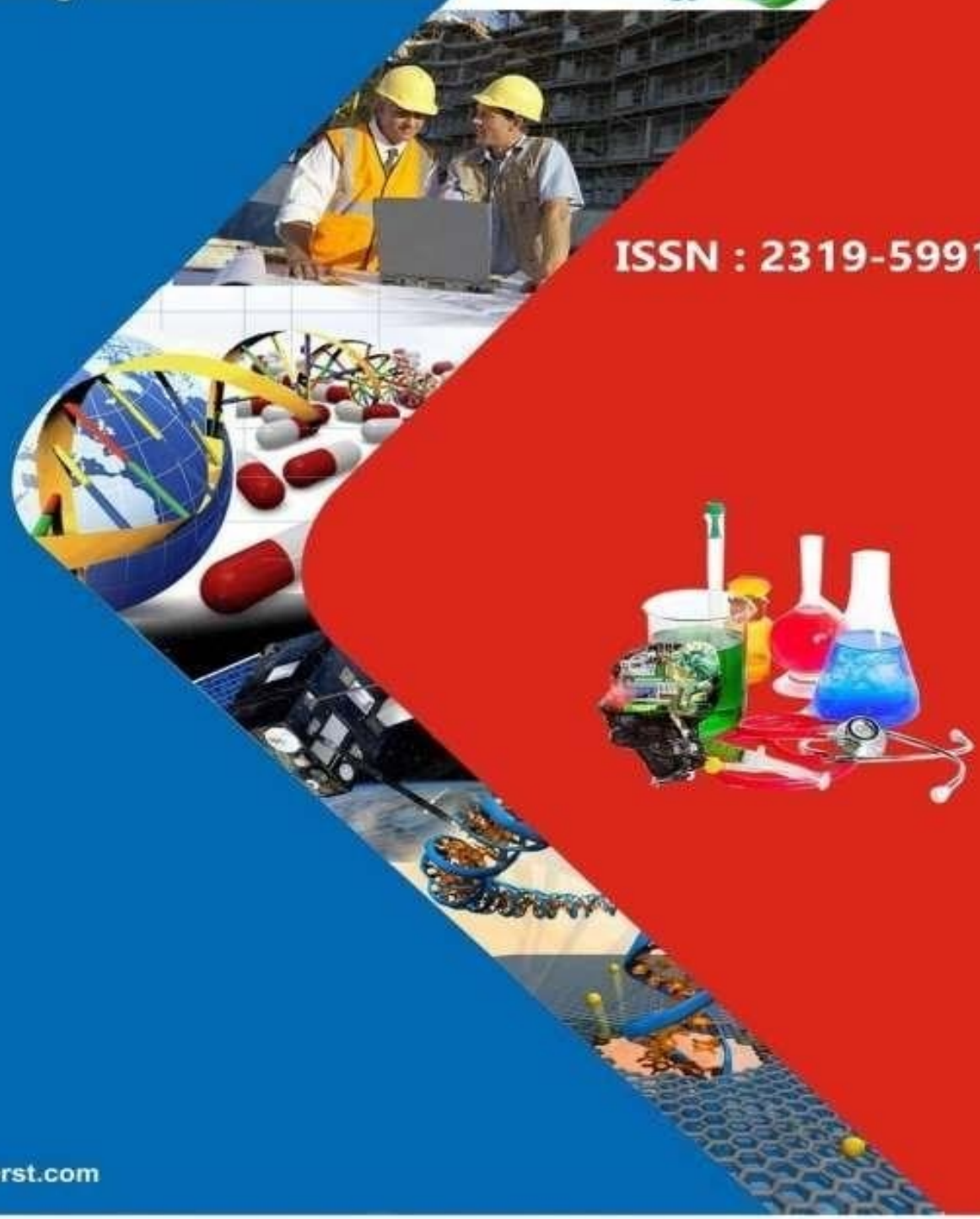
International Journal of Engineering Research and Science & Technology

IJERST

ISSN : 2319-5991



www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 2, 2025

ML POWERED INSIDER THREAT DETECTION IN ORGANISATION

Kantheti Teena Dhanasri, 21PD1A0539, Department of CSE, West Godavari Institute Of Science and Engineering, Andhra Pradesh, India.

Eerlagadda Srivalli, 21PD1A0522, Department of CSE, West Godavari Institute Of Science and Engineering, Andhra Pradesh, India.

Ippili Sai, 21PD1A0531, Department of CSE, West Godavari Institute Of Science and Engineering, Andhra Pradesh, India.

Kukkala Ravikanth, 21PD1A0546, Department of CSE, West Godavari Institute Of Science and Engineering, Andhra Pradesh, India.

Kanteti Jaswanth, 22PD5A0507, Department of CSE, West Godavari Institute Of Science and Engineering, Andhra Pradesh, India.

Dr. M.Aravind Kumar, Professor, Department of ECE, West Godavari Institute Of Science and Engineering, Andhra Pradesh, India.

M.Chilakaiah, Assistant Professor, Department of ECE, West Godavari Institute Of Science and Engineering, Andhra Pradesh, India.

ABSTRACT

Insider threats pose a significant challenge to organizational security by exploiting legitimate access to sensitive data and systems. Traditional security measures often fail to detect these threats, highlighting the need for advanced solutions. This study explores the use of machine learning models—Convolutional Neural Networks (CNN), Random Forest (RF), and Decision Trees (DT)—to detect insider threats by analyzing historical behavioral data, such as login activity, data access, and communication logs. While CNNs excel at identifying complex patterns, RF and DT models provide strong classification accuracy and transparency. The models' effectiveness is evaluated using metrics like accuracy, precision, recall, and F1-score, ensuring an optimal balance between detection and false positives. Integrating machine learning with cybersecurity practices enhances threat detection and strengthens organizational security.

INTRODUCTION

Insider threats, stemming from individuals with legitimate access to internal systems and sensitive data, present a significant security risk to organizations, as they exploit existing privileges for malicious activities like data theft, fraud, espionage, and sabotage. Unlike external threats, insider attacks blend with normal user behavior, making detection challenging for traditional security systems. As reliance on digital infrastructure increases, the consequences of such threats have become more severe, urging cybersecurity teams to prioritize early detection. Machine learning (ML) offers a promising solution by analyzing historical user behavior to identify unusual patterns and emerging threats. This study explores the use of Convolutional Neural Networks (CNN), Random Forest (RF), and Decision Trees (DT) to detect insider threats, aiming to develop a proactive system that balances high detection rates with minimal false positives, enhancing organizational security and mitigating potential damage.

LITERATURE SURVEY

Insider threats pose a significant challenge in cybersecurity, originating from authorized users with legitimate access to organizational data and systems. Traditional security methods, such as rule-based systems and access control mechanisms, struggle to detect

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

these threats due to their subtlety and insiders' ability to bypass conventional controls. Early approaches, like rule-based anomaly detection, had high false positive rates and struggled to adapt to evolving attack strategies (Schatz et al., 2017). Similarly, role-based access control (RBAC) mechanisms were found inadequate for identifying subtle behavioral changes in malicious insiders (Probst et al., 2019). These methods, while structured, lack the flexibility to address emerging or unpredictable insider threat patterns, highlighting the need for more adaptive solutions.

EXISTING METHOD

Existing methods for detecting insider threats typically employ statistical analysis, rule-based systems, and machine learning algorithms, with many studies leveraging anomaly detection techniques like Support Vector Machines (SVM), Random Forests, and neural networks to identify malicious user behaviors. These approaches often analyze user activities, system logs, and network traffic to spot abnormal behavior. Dimensionality reduction techniques such as Principal Component Analysis (PCA) help manage high-dimensional data, while feature extraction methods like Deep Feature Synthesis generate meaningful insights from raw data. Oversampling techniques like SMOTE address class imbalances, enhancing model recall and accuracy. Despite the success of traditional methods, newer ensemble and deep learning models are advancing detection accuracy and reliability in identifying complex insider threats.

PROPOSED METHOD

The proposed method utilizes machine learning techniques to detect insider threats by analyzing historical user behavior data, such as login times, file access logs, and communication patterns. It employs three models—Convolutional Neural Networks (CNN), Random Forest (RF), and Decision Trees (DT)—each chosen for their strengths in classification and pattern recognition. Feature engineering extracts key characteristics like unusual access times and unauthorized file access, while CNN detects complex data patterns, and RF and DT offer more interpretable decision-making. Hyperparameter tuning optimizes performance, and evaluation metrics such as accuracy, precision, recall, and F1-score ensure effective threat detection with minimal false positives. By integrating these models into real-time monitoring, the method strengthens internal security measures by proactively identifying and mitigating insider threats.

SOFTWARE REQUIREMENTS:

1. OPERATING SYSTEM: **WINDOWS**
2. VERSION : Python 3.6.6
3. PROGRAMMING LANGUAGE**:** PYTHON
4. DEVELOPMENT IDE **:** JUPYTER NOTEBOOK

HARDWARE REQUIREMENTS

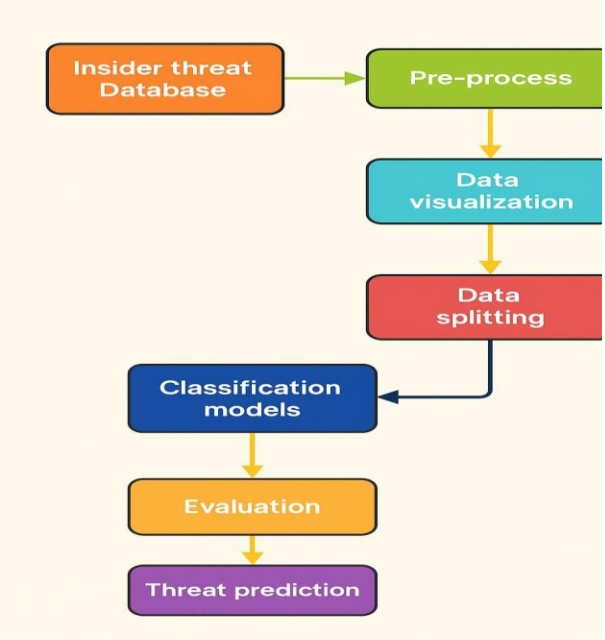
1. PROCESSOR :AMD RYZEN
2. SPEED : 2.3GHZ
3. RAM :800 GB

ARCHITECTURE DIAGRAM

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 2, 2025



The ML-powered Insider Threat Detection system in an organization works by continuously monitoring and analyzing user behavior, network activity, and access patterns using machine learning algorithms to identify anomalies that deviate from established norms. It leverages supervised and unsupervised learning models trained on historical data, including login times, file access, email usage, and device interactions, to flag potential insider threats such as data theft, sabotage, or policy violations. Real-time alerts are generated when suspicious activity is detected, allowing security teams to investigate and respond proactively. The system continuously evolves by learning from new data, improving its accuracy in distinguishing between normal and malicious behavior.

CONCLUSION

Insider threats, stemming from individuals with legitimate system access, pose a major challenge to organizations as they often bypass traditional security measures. This study investigates the use of machine learning models—Convolutional Neural Networks (CNN), Random Forest (RF), and Decision Trees (DT)—for detecting such threats through behavioral analysis. By leveraging features like login activity, file access, and communication logs, these models can effectively differentiate between normal and malicious user behavior. CNNs capture complex patterns in sequential data, while RF and DT offer strong classification with interpretability. The research highlights the importance of balancing accuracy and false positives to ensure practical deployment, showing that ML integration into cybersecurity systems enables real-time threat detection and proactive risk mitigation, reinforcing the need for continuous model refinement against evolving insider tactics.

FUTURE SCOPE

As insider threats grow increasingly sophisticated, future research in ML-based detection can focus on enhancing model accuracy and reducing false positives through the optimization of deep learning architectures like LSTM and Transformers, as well as by developing hybrid models that combine multiple techniques. Advancements in real-time detection and adaptive learning are also crucial, involving the creation of systems capable of live monitoring and self-adaptation using reinforcement learning to keep pace with evolving threat patterns. Additionally, integrating ML models with advanced cybersecurity systems such as SIEM, IDS, behavioral biometrics, and access control mechanisms will foster a more robust, multi-layered defense strategy.

REFERENCES

1. Patel, S., & Patel, D. (2017). *A comprehensive survey on insider threat detection techniques in cloud computing*. *International Journal of Computer Applications*, **159**(5), 27–33.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 2, 2025

2. Soni, H., & Nasser, A. (2019). *Machine learning-based anomaly detection for insider threat mitigation*. *Journal of Computer Security*, **27**(6), 723–742.
3. Gao, J., & Liu, S. (2018). *A review of machine learning approaches for detecting insider threats*. *Computational Intelligence and Neuroscience*, **2018**, Article ID 2037592.
4. Zhang, L., & Wang, Y. (2020). *Survey on machine learning methods for insider threat detection*. *International Journal of Security and Its Applications*, **14**(4), 1–14.
5. Gupta, A., & Singh, J. (2021). *Design of an intelligent insider threat detection system using machine learning*. *Journal of Cybersecurity and Privacy*, **1**(3), 234–253.
6. Chandramohan, S., & Sangeetha, D. (2021). *Network traffic anomaly detection for insider threat identification using machine learning*. *International Journal of Computer Science and Information Security*, **19**(1), 85–92.