






SN-81A3FE0F8B95

Submission

-  My Files
-  My Files
-  University

Document Details

Submission ID

trn:oid:::28592:81360536

Submission Date

Feb 7, 2025, 2:20 PM GMT+5:30

Download Date

Feb 7, 2025, 2:21 PM GMT+5:30

File Name

752491.docx

File Size

26.1 KB

5 Pages

2,169 Words

14,316 Characters



0% detected as AI

The percentage indicates the combined amount of likely AI-generated text as well as likely AI-generated text that was also likely AI-paraphrased.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Detection Groups

- 
1 AI-generated only 0%
 Likely AI-generated text from a large-language model.
- 
2 AI-generated text that was AI-paraphrased 0%
 Likely AI-generated text that was likely revised using an AI-paraphrase tool or word spinner.

Disclaimer

Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (it may misidentify writing that is likely AI generated as AI generated and AI paraphrased or likely AI generated and AI paraphrased writing as only AI generated) so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

Frequently Asked Questions

How should I interpret Turnitin's AI writing percentage and false positives?

The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI-paraphrase tool or word spinner.

False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).

The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

What does 'qualifying text' mean?

Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.



AI-Powered Insider Threat Detection Using Behavioral Analytics and Multi-Device Correlation

Student's Name
Institutional Affiliation
Professor's Name
Course Name
Submission Date

Abstract- *Inside threats bring forth concrete security dilemmas for organizations that frequently cause data compromises alongside intellectual property theft that leads to marginalized financial losses. The complexity of spotting insider threats comes from their origin inside organization members who possess authorized access to organization systems. Traditional intrusion detection systems constructed from security rules cannot follow employee behavioral changes because they generate many incorrect alerts. An AI-powered detector of insider threats presents itself through behavioral analytics, which combines multi-device correlation to generate improved detection accuracy.*

Endpoints are monitored by machine learning algorithms throughout time in order to build a behavior baseline that evolves. Multiple supervised and unsupervised learning models combine to detect anomalies through Support Vector Machines (SVM), Random Forests, Neural Networks, and Isolation Forests. Two correlation techniques unite user activities across multiple devices in order to create enhanced contextual investigation benefits. Experimental findings based on the CERT Insider Threat Dataset prove that the proposed system detects threats at a 92% rate with only 3% false alarm frequency.

Feature engineering obtains automation through the Deep Feature Synthesis method that performs systematic pattern extraction from raw data input. The detection process delves into Principal Component Analysis (PCA) to achieve dimensionality reduction, where the most meaningful features help detection by minimizing redundant elements. These techniques help the system optimize large user activity processing while achieving better performance and spending less on computing dimensions. Through its research, this study expands AI-based cybersecurity methods and develops an adjustable and scalable system to fight internal threats. Future investigations will implement the framework in actual enterprise security systems, combine it with current defense infrastructure, and enhance its ability to detect changing attack types. The implementation of artificial intelligence-based behavioral analytics systems enables organizations to actively build more secure cybersecurity infrastructure.

Introduction

Internal threats that involve data breach incidents alongside intellectual property theft and system destruction constitute the main source of cybersecurity breaches. The authorized status of insiders who initiate attacks makes their detection very challenging. The traditional rule-based security systems prove inadequate in detecting new attack patterns, which causes both missed important incidents and many false-positive alerts [1]. The currently

developed machine learning models have gradually helped organizations to accurately and quickly detect internal security threats by critically analyzing the notion of human nature and monitoring any incident of abnormal system activities. Artificial intelligence technology portrays a robust framework that encompasses multi-device correlation integrated with behavioral tracking systems to increase detection precision. The system applies a combination of rules of supervised and

unsupervised learning approaches to adapt against new threats without producing excess false alerts.

Related Work

Research on insider threat detection continues intensively because it directly affects organizational security measures. Authentication systems and static rule-based access controls are unfit for detecting evolving insider threats because they prove inadequate for this purpose [2]. The early detection systems analyzed log files as their main approach while tracking user login times, monitoring file access frequencies, and detecting privilege elevation incidents. The detection methods fail because they produce numerous inaccurate alerts while simultaneously missing alerts of new security risks.

Insider threat detection has become more achievable through machine learning because this technology uses behavioral analytics to create user profiles for anomaly detection. Multiple supervised learning models use classified datasets to identify and categorize insider practices according to various studies. Deep learning algorithms that comprise autoencoders and neural networks processed insider activities to reach a detection accuracy level at 91% [3]. Supervised models face a significant drawback because they require extensive labeled data which enterprise environments usually lack in sufficient amounts. The unbalanced nature of insider threats reduces the number of obtainable malicious cases needed for successful training efforts.

Unsupervised learning aspect address the problem of sparse labeled information through anomaly detection operations apart from pre-defined attack signatures. The cybersecurity field makes extensive use of Isolation Forest together with One-Class Support Vector Machines (OCSVM) to monitor abnormal user actions and discover internal threats without requiring specific attack signatures [4]. Security risks are identified through these models since they create normal activity reference points to detect

substantial deviations. Their main disadvantage is their high number of incorrect false-positive results because they falsely detect normal employee actions like working different hours or using alternate devices or remote access as suspicious. The challenge of cutting down false positive detections acts as an obstacle to transform unsupervised models into highly dependable solutions for insider threat detection.

Research has proved that innovations that unite supervised learning techniques with unsupervised learning methods achieve both precise detection outcomes and decreased numbers of false alarms. The combination of Convolutional Neural Networks with Recurrent Neural Networks functions as a user behavior sequence modeling framework that brings superior detection capabilities to classic ML models, according to research findings in [5]. The combination of Random Forest and XGBoost in ensemble learning architecture achieved a 99.3% precision level for detecting insider threats, as reported in this research [6]. The combined framework uses both labeled and unlabeled information yet demands high processing power, which limits operational implementation for real-time enterprise deployment.

Insider threat detection research suffers from an essential weakness due to the absence of correlations between multiple devices in its analysis. Research about insider threat detection examines primarily one endpoint using desktop activity logs while dismissing analytic connections between multiple devices such as mobile phones, VPNs, and cloud applications. The detection of coordinated attacks becomes limited since multiple devices used by an insider create more challenging investigation areas. The proposed multi-device behavioral analysis method in this research improves sophisticated intrusion detection capabilities by collecting data from every device in use.

The innovative development of ML-based insider threat detection faces three primary issues regarding dataset imbalance management, false positive reduction, and multi-device activity correlation. The study fills the research gaps by building a security monitoring framework that combines supervised learning with anomaly detection and multi-device correlation.

Methodology

System Architecture

The system operates with six key components that unite to perform effective insider threat detection. Data collection functions as the first element where organizations acquire raw data from multiple system sources, including endpoints, servers, and cloud resources, for complete user behavior tracking. The preprocessing stage receives collected data for filtering out duplicated or anomalous records, which enables normalized activity log normalization across various information sources [7]. The process of behavioral profiling utilizes historical activity data to create a dynamic behavior baseline between users.

Most of the systems utilize anomaly procedures to detect anomalies through powerful models such as Long Short-Term Memory Networks and Isolation Forest algorithms to analyze statistical outliers and temporal patterns, making all activities faster and also capturing real-time threats. The detection accuracy gets boosted by Multi-Device Correlation, which merges activities from various devices to track coordinated threats that remain hidden when monitoring individual endpoints. The final module performs Risk Scoring and alerts management that assigns threat level scores to anomalies through impact severity evaluation and triggers immediate notifications for critical incidents toward quicker response [8]. A complete security approach in this system enables accurate threat detection and minimizes unneeded

alerts, which results in a secure cybersecurity protection method.

Machine Learning Pipeline

The machine learning pipeline arranges its functions in three fundamental phases. Feature Engineering deploys Deep Feature Synthesis (DFS) to produce behavioral features from automatically extracted information about login actions, file access behavior, and device activity patterns, which provides complete profiling capabilities [9]. The Model Training stage uses CERT Insider Threat data to train diverse ML models through supervised and unsupervised methods that employ labeled and anomalous data, respectively [10]. The evaluation uses accuracy, precision, recall, and F1-score to determine how well the model detects insider threats.

Multi-Device Correlation

The detection of security risks becomes more precise when multiple devices are cross-referenced since this method integrates all user interactions across systems. The discovery of an employee using corporate sensible files on a laptop with parallel mobile device login creates a security concern point. The system achieves better insider threat mitigation by analyzing the relationship between these security events that occur simultaneously.

Experimental Results

Dataset and Experimental Setup

The system received testing through the CERT Insider Threat Dataset, which is an established standard for cybersecurity research. A total of 30 million records representing user activity data are included in this dataset, which contains logs for system accesses as well as documentation transfers email interactions and internet browsing records. A dedicated evaluation required selecting 900 users, 75 of whom were marked as insider threats following pre-established attack cases. The dataset provides an excellent foundation for performing thorough testing of machine learning systems designed for threat detection.

Evaluation Metrics and Performance

The model received assessments through four measurements: accuracy, precision, recall, and F1-score. Table 1 presents the performance evaluation data comparing different ML models.

Model	Accur acy	Precisi on	Rec all	F1- sco re
SVM	97%	98%	97%	96 %
Rando m Forest	96%	95%	94%	93 %
Neutra l Netwo rk	96%	94%	94%	95 %
AdaBo ost	94%	93%	91%	92 %
Isolati on Forest	92%	90%	89%	88 %
OCSV M	87%	86%	84%	83 %

The SVM model reached superior performance by detecting every insider threat without generating excessive false-positive results.

Discussion

The findings show that AI-based insider hazard tracking is conducted better than classical boundary-based practices because it incorporates refined habits inspection with united device analysis. Traditional security methods using static rule systems lose effectiveness when new user behavior patterns emerge because the proposed system reacts automatically to changing patterns for detecting hidden threats, which static detection approaches miss. Through the integration of DFS with PCA, the detection process becomes more efficient because the system removes unnecessary data features without compromising accuracy outcomes [11]. The optimized system enhances its ability to analyze enormous amounts of user activity data in real-time through this modification, which improves both

detection precision and response speed against insider threats.

The security benefits come with multiple challenges that organizations must overcome. The frequent requirement for model updates is the main challenge because patterns change and attackers develop new techniques. The high level of employee monitoring invokes privacy issues that force organizations to balance their security needs with ethical standards [12]. Upcoming scientific inquiries will inspect privacy-respecting technologies while applying the system to authentic enterprise locations and embedding it into established cybersecurity infrastructure to enable broad usage and practical implementation.

Conclusion

An AI framework uses behavioral analytics and multi-device correlation to help security monitoring through its developed method for insider threat detection. The system utilizes endpoint analysis of user activity patterns to find unusual behavior while maintaining high accuracy since it produces few false alerts. High-level detection precision leads to early identification of security risks, which minimizes attacks on data systems and unauthorized system access. Extended enterprise-wide deployment of this system necessitates additional improvements aimed at better connectivity with current cybersecurity architectural systems. Moving forward, research will investigate actual deployment methods while focusing on ways to increase scalability and privacy-centered methods to maintain efficiency in ethical insider threat identification.

REFERENCES

- [1] I. H. Sarker, H. Janicke, M. A. Ferrag, and A. Abuadbbba, "Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions towards automation, intelligence and transparent cybersecurity modeling for critical infrastructures," Internet of

- Things, vol. 25, p. 101110, Feb. 2024, <https://doi.org/10.1016/j.iot.2024.101110>
- [2] B. B. Sarhan and N. Altwaijry, "Insider threat detection using Machine learning approach," *Applied Sciences*, vol. 13, no. 1, p. 259, Dec. 2022, <https://doi.org/10.3390/app13010259>
- [3] B. B. Sarhan and N. Altwaijry, "Insider threat detection using Machine learning approach," *Applied Sciences*, vol. 13, no. 1, p. 259, Dec. 2022, <https://doi.org/10.3390/app13010259>
- [4] S. F. Gerard, V. Adedoyin, and J. O. Agbaje, "An Empirical Internet Protocol Network Intrusion Detection using Isolation Forest and One-Class Support Vector Machines," Jan. 01, 2023, <https://scholarworks.montana.edu/handle/1/18188>
- [5] M. A. Khan, "HCRNNIDS: Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System," *Processes*, vol. 9, no. 5, p. 834, May 2021, <https://doi.org/10.3390/pr9050834>
- [6] W. F. Urmi et al., "A stacked ensemble approach to detect cyber attacks based on feature selection techniques," *International Journal of Cognitive Computing in Engineering*, vol. 5, pp. 316–331, Jan. 2024, <https://doi.org/10.1016/j.ijcce.2024.07.005>
- [7] S. Cofre-Martel, E. L. Droguett, and M. Modarres, "Big Machinery Data Preprocessing Methodology for Data-Driven Models in Prognostics and Health Management," *Sensors*, vol. 21, no. 20, p. 6841, Oct. 2021, <https://doi.org/10.3390/s21206841>
- [8] A. Collen and N. A. Nijdam, "Can I sleep safely in my smarthome? A novel framework on Automating dynamic risk assessment in IoT environments," *Electronics*, vol. 11, no. 7, p. 1123, Apr. 2022, <https://doi.org/10.3390/electronics11071123>
- [9] J. Ng, "Machine learning to accelerate insider attack detection - ProQuest." <https://search.proquest.com/openview/1d8f546a3c024828d5047b9826c9b8d9/1?pq-origsite=gscholar&cbl=18750&diss=y>
- [10] C. W. Probst, J. Hunker, D. Gollmann, and M. Bishop, *Insider Threats in Cyber Security*. Boston, MA, USA: Springer, 2010.
- [11] B. B. Sarhan and N. Altwaijry, "Insider threat detection using Machine learning approach," *Applied Sciences*, vol. 13, no. 1, p. 259, Dec. 2022, <https://doi.org/10.3390/app13010259>
- [12] S. Segkouli, D. Giakoumis, K. Votis, A. Triantafyllidis, I. Paliokas, and D. Tzovaras, "Smart Workplaces for older adults: coping 'ethically' with technology pervasiveness," *Universal Access in the Information Society*, vol. 22, no. 1, pp. 37–49, Jul. 2021, <https://doi.org/10.1007/s10209-021-00829-9>