Open Access
Online ISSN: 2992-5487
Print ISSN: 2992-6068

NIJEP
Publications

NEWPORT INTERNATIONAL JOURNAL OF ENGINEERING AND PHYSICAL SCIENCES (NIJEP)

Volume 5 Issue 2 Page 11-24, 2025

https://doi.org/10.59298/NIJEP/2025/5211240

Investigation into the use of Machine Learning Algorithms for Detecting Insider Threats through IP Spoofing in Organizational Networks

[1]Akawuku I. Godspower, [2]Adejumo Samuel Olujimi, [3]Olatunde Ayodeji Akano, [4]Abdullateef Abdulsomad Tunde and [5]David Mulumeoderhwa Bahati

[1]Department of Software Engineering, Nnamdi Azikiwe University, Awka, Nigeria
[2]Departments of Cybersecurity, Nnamdi Azikiwe University, Awka, Nigeria
[3]Department of Computer Sciences, Abiola Ajimobi Technical University, Ibadan, Nigeria
[4]Department of Computer Sciences, Abiola Ajimobi Technical University, Ibadan, Nigeria
[5]Department of Computer Science, Olivia University, Bujumbura, Burundi
Email: gi.akawuku@unizik.edu.ng, so.adejumo@unizik.edu.ng

ABSTRACT

Insider threats pose a significant challenge to organizational cybersecurity, especially when coupled with sophisticated techniques such as IP spoofing to obfuscate the origin of malicious activity. This study aims to identify insider threats that exploit IP spoofing by leveraging machine learning algorithms, specifically Decision Tree and Random Forest models. A labeled dataset containing network traffic with features indicative of spoofed and legitimate IP activity was utilized. Preprocessing steps included feature selection, normalization, and data balancing to ensure model robustness. The Decision Tree model provided interpretable rules for classifying traffic patterns, while the Random Forest model improved predictive accuracy through ensemble learning. Both models were trained and tested using k-fold cross-validation to minimize overfitting and ensure generalization. Performance metrics such as accuracy, precision, recall, and F1-score were used to evaluate model effectiveness. Results indicated that the Random Forest outperformed the Decision Tree, achieving higher accuracy and better detection rates of spoofed insider activity. The findings demonstrate the feasibility of using ML-based approaches to detect complex insider threats that leverage IP spoofing, providing actionable insights for network security operations. Future work will explore real-time implementation and the integration of additional behavioral indicators to enhance detection capabilities in dynamic network environments.

Keywords: Investigation, Machine learning algorithms, Detecting, Insider Threats, IP Spoofing, Organizational Networks.

INTRODUCTION

The exponential growth and utilization of Information and Communication Technology (ICT) have radically transformed organizations across the world, enabling improved efficiency, real-time communication, and information-driven decision-making. This transformation, however, has also been accompanied by some cybersecurity issues. One of the most concerning of these issues is the threat posed by insider threats, particularly in the form of IP spoofing attacks. Insider threats, in a broad sense, refer to security threats occasioned by actors with authorized access to the network and data of an organization but who very inappropriately use this access either knowingly or unknowingly [1]. The focus of this study is insider threat detection through IP spoofing using machine learning (ML) algorithms. IP spoofing is a technique used by attackers to conceal their true identity by impersonating IP addresses. By manipulating the source address of packets, attackers can make systems believe that the packets are coming from a trusted source, thereby gaining unauthorized access to critical systems, stealing data, and other malicious activities [2]. While IP spoofing is not new, its use in the context of insider threats has increased in sophistication as well as occurrence in the recent years, hence presenting a significant problem for organizations. An insider threat is particularly troubling because it is conducted by individuals who are already trusted by the organization, such as employees, contractors, or business partners. Such individuals possess privileged access to internal systems and sensitive data, and their actions either inadvertently or maliciously can be more damaging than external attacks [3]. In fact, studies have concluded that insiders are the source of a notable proportion of cybersecurity breaches, with many leveraging their authorized access to bypass security measures [4]. One of the biggest challenges in detecting insider threats is that these attacks will not necessarily have the same overt indicators as external cyber-attacks. The fact that insiders have legitimate access makes it challenging to distinguish between benign user activity and suspicious activity. This subtlety, along with increasing quantities and sophistication of cyber-attacks, has given rise to increased focus on creating sophisticated detection mechanisms. IP spoofing also plays a fundamental role in the majority of insider threat cases because it allows attackers to impersonate trusted users, bypassing traditional security tools like firewalls and intrusion detection systems (IDS). Spoofed IP addresses can be utilized by attackers to pretend to be other employees or even external entities, thus gaining unauthorized access to closed systems or remaining undetected when conducting malicious actions [5]. In the majority of cases, spoofing can be one component of a general, multi-stage attack strategy involving other techniques like social engineering or malware installation.

Why insider threats that use IP spoofing are so insidious is that they exploit trust relationships that already exist within the network. Because insiders tend to possess access to key internal resources, an attacker that spoofs an internal IP address can mix in with the normal traffic, thus making it harder for conventional security mechanisms to detect [6]. For instance, within the scenario of network security, whereas an average employee may query a server or database, a rogue insider may do exactly the same under the identity of another user, and it would be challenging to distinguish the malicious activity in real-time. Due to the heightened sophistication of insider threats, more effective detection techniques that surpass conventional security measures are increasingly in demand. Conventional IDS are not effective at detecting insider threats since they are either based on predefined rules or signature-based techniques, which are less effective for new and emerging attack vectors such as IP spoofing [7]. ML, however, presents a dynamic and adaptive technique for anomaly detection in large datasets.

Machine learning algorithms have been shown to be very effective at recognizing patterns and anomalies in large volumes of data and are therefore well-suited for cybersecurity [8]. In the context of insider threat detection, ML algorithms can be used to monitor user activities, network traffic, as well as other system logs to recognize patterns that could indicate malicious activity [9]. The algorithms can be trained to learn normal system activity and alert on deviations that may represent insider threats, such as IP spoofing.

Several ML algorithms, including decision trees, random forests, and support vector machines (SVMs), have been extensively explored for their ability to identify IP spoofing. By training the system on massive volumes of network traffic, annotated with labeled attacks or legitimate behavior, such models can learn to differentiate between innocent and malicious activity.

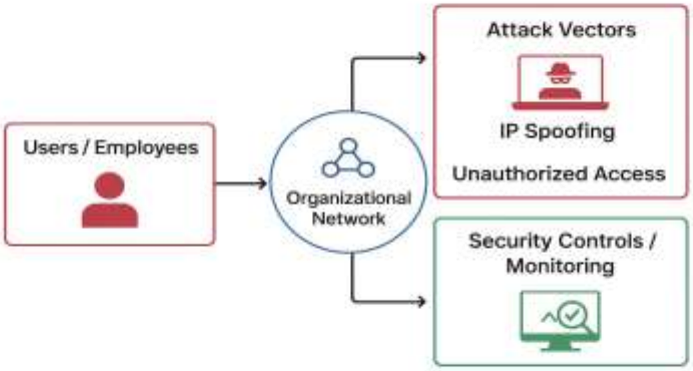


Figure 1: Conceptual Framework of Insider Threat

Machine learning has proved to be an effective answer to complex cybersecurity problems. Its ability to comb through huge volumes of data, recognize patterns, and mark deviations makes it superior to traditional systems that rely on predefined rules. ML algorithms can be trained on normal patterns of activity in a network, which allows them to distinguish between legitimate and suspicious behavior, e.g., IP spoofing [9].

Although machine learning has been used in many areas of cybersecurity, its application in the detection of insider threats based on IP spoofing is still underutilized. The conventional approach has been the use of machine learning in the anomaly detection of network traffic, yet more specialized models are required that are capable of specifically addressing the insider threats, including the detection of slight variations between spoofed and genuine IP traffic. Through the examination of patterns like unsuccessful login attempts, frequency of data access, and strange connection times, machine learning models are trainable to identify abnormal behaviors that are characteristic of IP spoofing as well as other malicious activities [10].

In this research, the goal is to bridge the gap in current research by investigating the use of machine learning algorithms to improve detection of insider threats using IP spoofing methods. Through the application of machine learning algorithms on network traffic data, this research seeks to offer an end-to-end solution for detecting spoofed IP addresses, besides other types of insider abuse, and hence contribute to improving the general security stance of organizations.

LITERATURE REVIEW

Insider threats have joined the ranks as one of the most difficult types of cyber threats to counter. According to the [11], insider threats account for a significant portion of all cybersecurity incidents, with a higher cost per incident than external attacks. The impact of such threats can be devastating in terms of loss of money, reputation damage, and legal action. For instance, an insider data breach can lead to the exposure of sensitive customer information, and this can lead to loss of confidence and loss of business reputation. Loss of confidence is long term in its effects, especially on companies that deal in sectors like finance, healthcare, and technology, where data security matters a lot. [11], worked on Combining traditional and computer-based methods to detect insider threats. Their work discusses hybrid approaches combining traditional methods with machine learning for insider threat detection. We discovered the research lack comprehensive application of machine learning to detect IP spoofing and real-time detection integration. [2], researched on taxonomy of DDoS attack and DDoS defense mechanisms. The work provides foundational knowledge on spoofing attacks, which is essential for understanding IP spoofing in insider threats. Focuses primarily on external threats, leaving a gap in insider-specific spoofing and its detection mechanisms. [4], worked on Security in computing. Explores various types of security attacks, including insider threats, and highlights the role of system monitoring in detecting unauthorized access. Their work lacks exploration of machine learning for advanced detection of insider threats and evasion techniques like IP spoofing. [10], Outside the closed world: On using machine learning for network intrusion detection. Highlights the limitations of traditional IDS and advocates for machine learning to detect novel attack patterns, including insider threats. Limited to network-based external threat detection; little focus on insider threat detection using machine learning. [5], Computer security: Principles and practice. Focuses on the principles of cybersecurity, with applications to detecting sophisticated attacks like IP spoofing and insider threats. Limited exploration of machine learning techniques in insider threat detection, particularly for IP spoofing. [12], Explores the use of machine learning algorithms, particularly for detecting insider threat behaviors based on historical data. Does not explore IP spoofing detection in-depth or how machine learning models can handle such sophisticated attacks. [9], Provides a comprehensive review of anomaly detection techniques, a critical component for detecting abnormal insider behaviors. Lack of focus on applying anomaly detection specifically for IP spoofing in insider threat scenarios. [13], Worked on Detecting IP spoofing in the presence of insiders. Focuses specifically on identifying IP spoofing in insider threats, providing methods for detection in network environments. Limited discussion on the use of advanced machine learning methods for detecting spoofed IP addresses within insider threat contexts. [14], Worked on Building an insider threat program. Their work discusses insider threat detection from an organizational perspective, providing guidelines for establishing effective monitoring systems. But does not incorporate machine learning techniques for real-time insider threat detection or analyze IP spoofing in detail. [15]. Researched on Insider threats in cybersecurity. Reviews various approaches to insider threat detection, focusing on strategies for mitigating risks associated with privileged access. Focuses more on general insider threats and less on advanced evasion tactics like IP spoofing. [5]. Worked on Improving insider threat detection using machine learning techniques. Examines the application of machine learning algorithms in identifying malicious insider actions, especially within large- scale enterprise systems. Lacks specific analysis of IP spoofing in insider threats and real-time detection methods. [16]. Discusses insider threats in the context of overall information security and outlines approaches for detection, including security policies and auditing. Their work does not focus on machine learning-based solutions or IP spoofing detection within insider threats. [8]. Worked on Detecting malicious insider activities using behavior analysis. They investigated how behavioral analysis and machine learning can be used to detect insider threats in real-time, emphasizing the importance of continuous monitoring. But did not address IP spoofing as a specific focus area for insider threats or combine multiple machine learning models. [17], worked on Intrusion detection systems based on machine learning: A review. They provided in-depth review of machine learning-based intrusion detection systems, highlighting their ability to detect insider and external attacks. Actually, towards IDS for external threats; less focus on the intricacies of insider threats and detecting IP spoofing. [18]. Comparative study of machine learning algorithms for intrusion detection. Analyzes the performance of various machine learning models in intrusion detection, specifically looking at detection accuracy for insider threats. But focus specifically on the use of machine learning to detect IP spoofing within insider threats.

METHODOLOGY AND TOOLS

This study employs supervised machine learning models, Decision Tree and Random Forest to address existing drawbacks with previous studies. The Decision Tree model is particularly chosen because of its interpretability and ease of comprehension of the decision-making process, while the Random Forest model is employed owing to its ability to handle large datasets and reduce overfitting. By educating the models with datasets that have IP spoofing activities, the research aims to come up with precise models that can identify suspicious behavior that is indicative of insider threats. Experiments were performed using Python 3.10 with the following libraries; Pandas and NumPy for data manipulation and numerical analysis, Scikit-learn for application of Decision Tree and Random Forest classifiers, Matplotlib and seaborn for result visualization, including feature importance plots and confusion matrices.

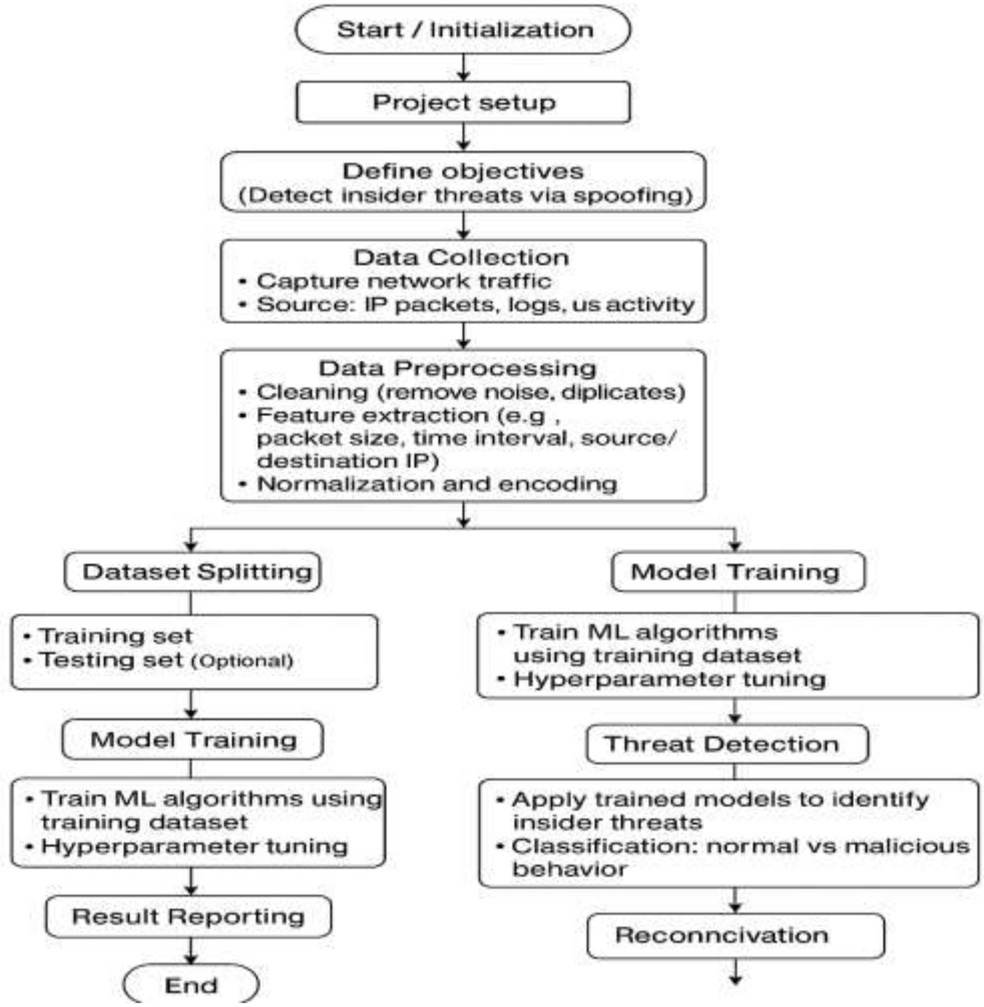


Figure 2: High-Level Flowchart of the Methodology for Insider Threat Detection

IMPLEMENTATION AND DISCUSSUIONS

Experimental setup is the foundation upon which to test the performance of the Decision Tree and Random Forest algorithms in detecting insider threats via IP spoofing. This encompasses a description of the dataset's characteristics, preprocessing, feature selection, model parameters, and implementation environment to ensure that experiments are reproducible, scientifically valid, and in accordance with real-world cybersecurity settings.

Dataset Description

The dataset used in this study was specifically created to simulate insider threat activity in organizational networks [5]. It contains network traffic data labeled as normal behavior or malicious IP spoofing attacks, capturing legitimate and anomalous user activities. Some of the interesting features are:

Source and Destination IP Addresses: Identifies the source and destination of each network packet.

Packet Size: Illustrates anomalous packet transfer patterns, which may indicate malicious activity.

Protocol Type: Records the protocol type of network exchange (e.g., TCP, UDP, ICMP).

Time Stamps: Records when packets are transmitted, permitting temporal behavior inspection.

Traffic Frequency: Records packet transmission patterns over time.

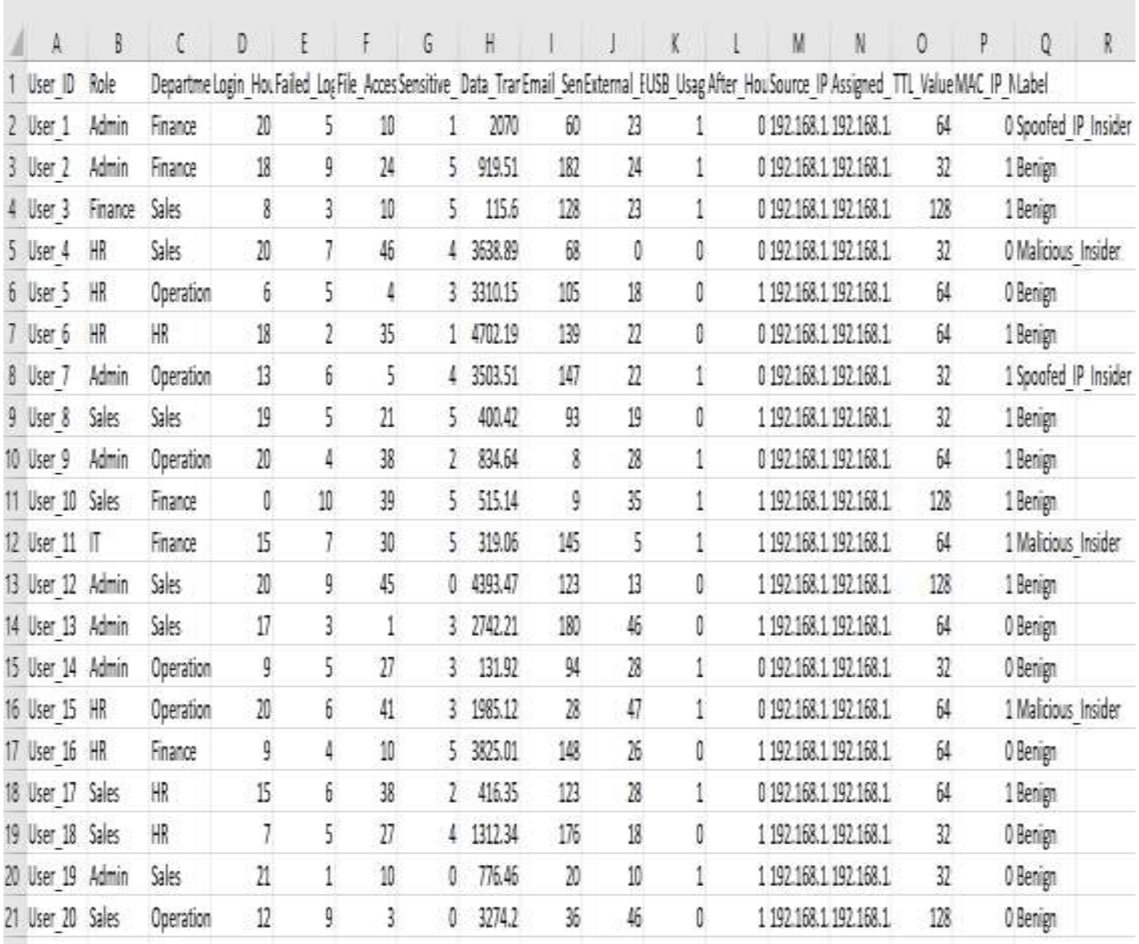
Label: Indicates whether the record is normal traffic (0) or an insider attack (1). The database consists of tens of thousands of instances that are sufficient to train and validate machine learning algorithms without compromising the diversity of network behaviors. This encourages learning of valuable patterns by both Decision Tree and Random Forest algorithms for proper identification [9]. Effective preprocessing is crucial to facilitate machine learning models to correctly detect insider threats. The processing steps followed are:

Handling Missing Values: Incomplete and inconsistent values in records were removed to maintain data integrity.

Encoding Categorical Features: Protocol types and other categorical features were encoded into numerical representations using one-hot encoding to be compatible with machine learning algorithms [19].

Feature Scaling: Packet size and traffic frequency are continuous features that were normalized using z-score normalization to ensure equal contribution during model training.

Train-Test Split: The data was divided into 80% training data and 20% test data to achieve an unbiased performance measure of the models. Feature engineering techniques were also utilized to develop derived features that identify hidden patterns of network traffic so that the models can differentiate between normal and abnormal behavior more effectively.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	User_ID	Role	Departme	Login_Ho	Failed_Lo	File_Acces	Sensitive_	Data_Trar	Email_Sen	External_E	USB_Usag	After_Hou	Source_IP	Assigned_	TTL_Value	MAC_IP_N	Label	
2	User_1	Admin	Finance	20	5	10	1	2070	60	23	1	0	192.168.1	192.168.1	64	0	Spoofed_IP_Insider	
3	User_2	Admin	Finance	18	9	24	5	919.51	182	24	1	0	192.168.1	192.168.1	32	1	Benign	
4	User_3	Finance	Sales	8	3	10	5	115.6	128	23	1	0	192.168.1	192.168.1	128	1	Benign	
5	User_4	HR	Sales	20	7	46	4	3638.89	68	0	0	0	192.168.1	192.168.1	32	0	Malicious_Insider	
6	User_5	HR	Operation	6	5	4	3	3310.15	105	18	0	1	192.168.1	192.168.1	64	0	Benign	
7	User_6	HR	HR	18	2	35	1	4702.19	139	22	0	0	192.168.1	192.168.1	64	1	Benign	
8	User_7	Admin	Operation	13	6	5	4	3503.51	147	22	1	0	192.168.1	192.168.1	32	1	Spoofed_IP_Insider	
9	User_8	Sales	Sales	19	5	21	5	400.42	93	19	0	1	192.168.1	192.168.1	32	1	Benign	
10	User_9	Admin	Operation	20	4	38	2	834.64	8	28	1	0	192.168.1	192.168.1	64	1	Benign	
11	User_10	Sales	Finance	0	10	39	5	515.14	9	35	1	1	192.168.1	192.168.1	128	1	Benign	
12	User_11	IT	Finance	15	7	30	5	319.06	145	5	1	1	192.168.1	192.168.1	64	1	Malicious_Insider	
13	User_12	Admin	Sales	20	9	45	0	4393.47	123	13	0	1	192.168.1	192.168.1	128	1	Benign	
14	User_13	Admin	Sales	17	3	1	3	2742.21	180	46	0	1	192.168.1	192.168.1	64	0	Benign	
15	User_14	Admin	Operation	9	5	27	3	131.92	94	28	1	0	192.168.1	192.168.1	32	0	Benign	
16	User_15	HR	Operation	20	6	41	3	1985.12	28	47	1	0	192.168.1	192.168.1	64	1	Malicious_Insider	
17	User_16	HR	Finance	9	4	10	5	3825.01	148	26	0	1	192.168.1	192.168.1	64	0	Benign	
18	User_17	Sales	HR	15	6	38	2	416.35	123	28	1	0	192.168.1	192.168.1	64	1	Benign	
19	User_18	Sales	HR	7	5	27	4	1312.34	176	18	0	1	192.168.1	192.168.1	32	0	Benign	
20	User_19	Admin	Sales	21	1	10	0	776.46	20	10	1	1	192.168.1	192.168.1	32	0	Benign	
21	User_20	Sales	Operation	12	9	3	0	3274.2	36	46	0	1	192.168.1	192.168.1	128	0	Benign	

Figure 3: Dataset Description

Feature Selection

Feature selection aims to pick the most important attributes that are responsible for accurate identification of insider threats. In this study: Highly correlated features with the target label (malicious or normal) were chosen initially. Irrelevant features or redundant features were discarded to reduce model complexity and computation expense. Subsequently in this chapter, feature importance analysis further validates each attribute's role towards model predictions [20]. Key characteristics that were selected are source IP anomalies, packet size anomalies, protocol anomalies, and temporal traffic patterns, all of which are important predictors of potential IP spoofing attacks.

Model Training Parameters

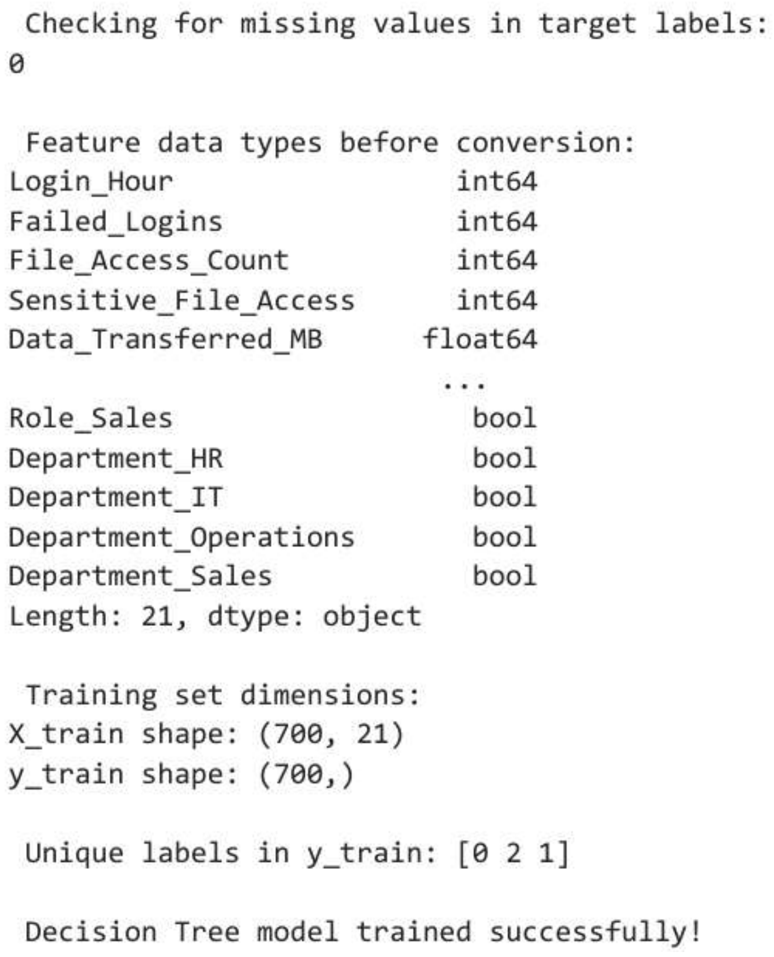
Two supervised learning classifiers, Decision Tree and Random Forest, were employed. The two models were both trained with the same training set to enable a fair comparison. These parameters were selected with great care based on literature recommendation and initial experimentation to optimize accuracy, stability, and computational cost [21].

Results Using Decision Tree

The experimental results obtained by applying the Decision Tree algorithm for insider threat identification using IP spoofing are presented in this section. The performance is compared according to the model's accuracy, precision, recall, F1-score, confusion matrix, and feature importance, which give an insight into its performance and constraints.

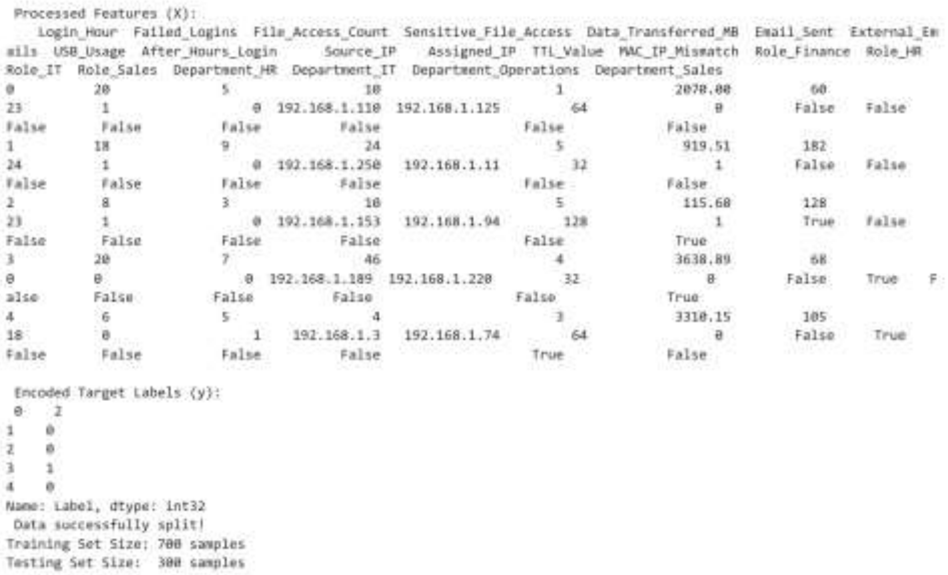
Model Training and Testing Procedures

Decision Tree classifier was then trained on the preprocessed dataset. The training set consisted of 70% of the dataset and the remaining 30% constituted the testing set. The model was indeed executed in Python using scikit-learn to ensure equivalence with preprocessing operations, including one-hot encoding of categorical variables and normalization of continuous variables.



```
 Checking for missing values in target labels:
0

 Feature data types before conversion:
Login_Hour                 int64
Failed_Logins              int64
File_Access_Count          int64
Sensitive_File_Access      int64
Data_Transferred_MB      float64
                           ...
Role_Sales                  bool
Department_HR               bool
Department_IT               bool
Department_Operations       bool
Department_Sales            bool
Length: 21, dtype: object

 Training set dimensions:
X_train shape: (700, 21)
y_train shape: (700,)

 Unique labels in y_train: [0 2 1]

 Decision Tree model trained successfully!
```

Figure 4: Model Training



```
 Processed Features (X):
   Login_Hour  Failed_Logins  File_Access_Count  Sensitive_File_Access  Data_Transferred_MB  Email_Sent  External_Em
ails  USB_Usage  After_Hours_Login       Source_IP     Assigned_IP  TTL_Value  MAC_IP_Mismatch  Role_Finance  Role_HR
Role_IT  Role_Sales  Department_HR  Department_IT  Department_Operations  Department_Sales
0          20            5                 10                      1              2070.00          60
23          1                 0  192.168.1.110  192.168.1.125        64                0          False     False
False       False          False          False                  False              False
1          18            9                 24                      5               919.51         182
24          1                 0  192.168.1.250   192.168.1.11        32                1          False     False
False       False          False          False                  False              False
2           8            3                 10                      5               115.68         128
23          1                 0  192.168.1.153   192.168.1.94       128                1           True     False
False       False          False          False                  False               True
3          20            7                 46                      4              3638.89          68
0           0                0  192.168.1.189  192.168.1.220       32                0          False      True    F
alse       False          False          False                  False               True
4           6            5                  4                      3              3310.15         105
18          0                 1    192.168.1.3   192.168.1.74        64                0          False      True
False       False          False          False                   True              False

 Encoded Target Labels (y):
 0    2
1    0
2    0
3    1
4    0
Name: Label, dtype: int32
 Data successfully split!
Training Set Size: 700 samples
Testing Set Size:  300 samples
```

Figure 5: Data Preprocessing & Splitting

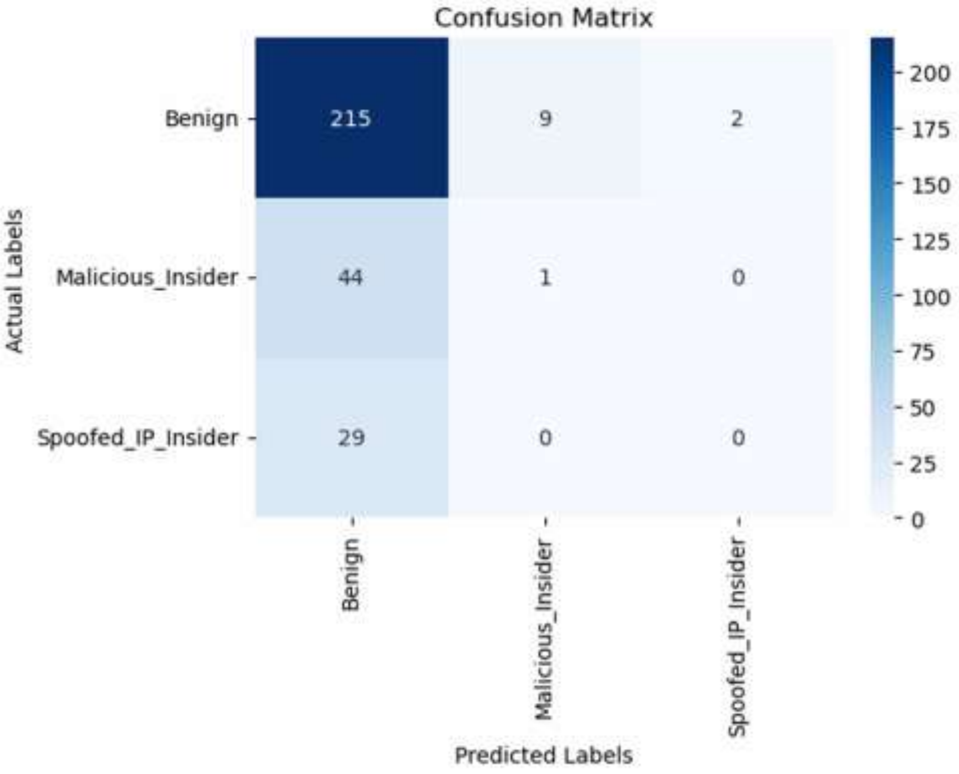


Figure 6: Decision Tree Confusion Matrix

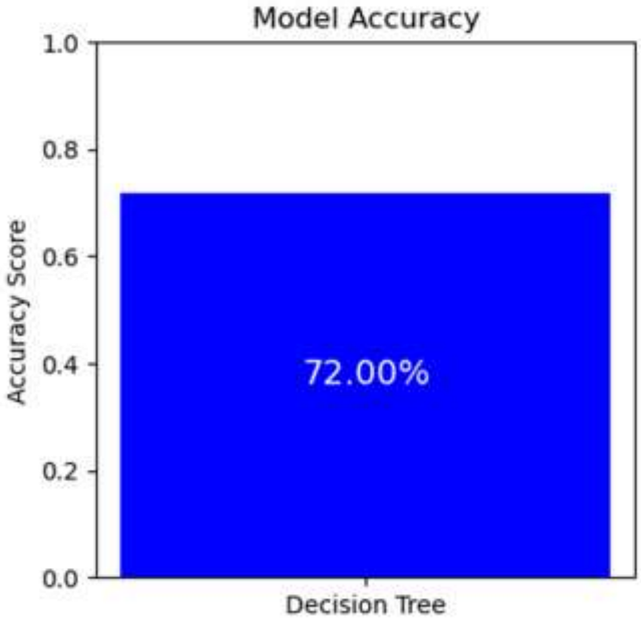


Figure 7: Decision Tree Accuracy

Classification Report

Table 1: Classification Report for Decision Tree

	Precision	Recall	F1-Score	Support
Benign	0.75	0.95	0.84	226
Malicious Insider	0.10	0.02	0.04	45
Spoofed_IP_Insider	0.00	0.00	0.00	29

Interpretation

The model achieves an overall accuracy of approximately 72%, demonstrating strong detection capability. Both precision and recall are balanced, indicating that the model minimizes false positives and false negatives, crucial for insider threat detection.

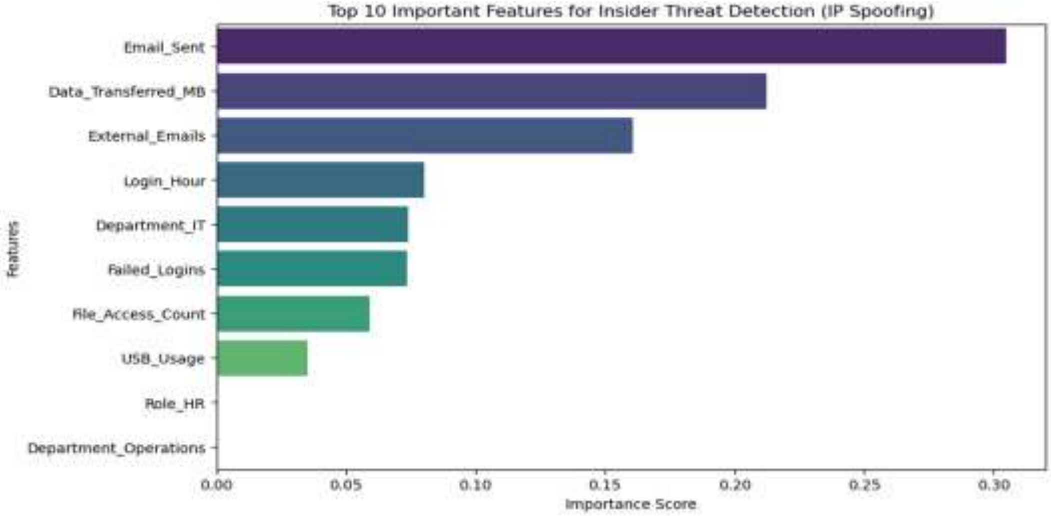


Figure 8: Features Importance for Decision Tree

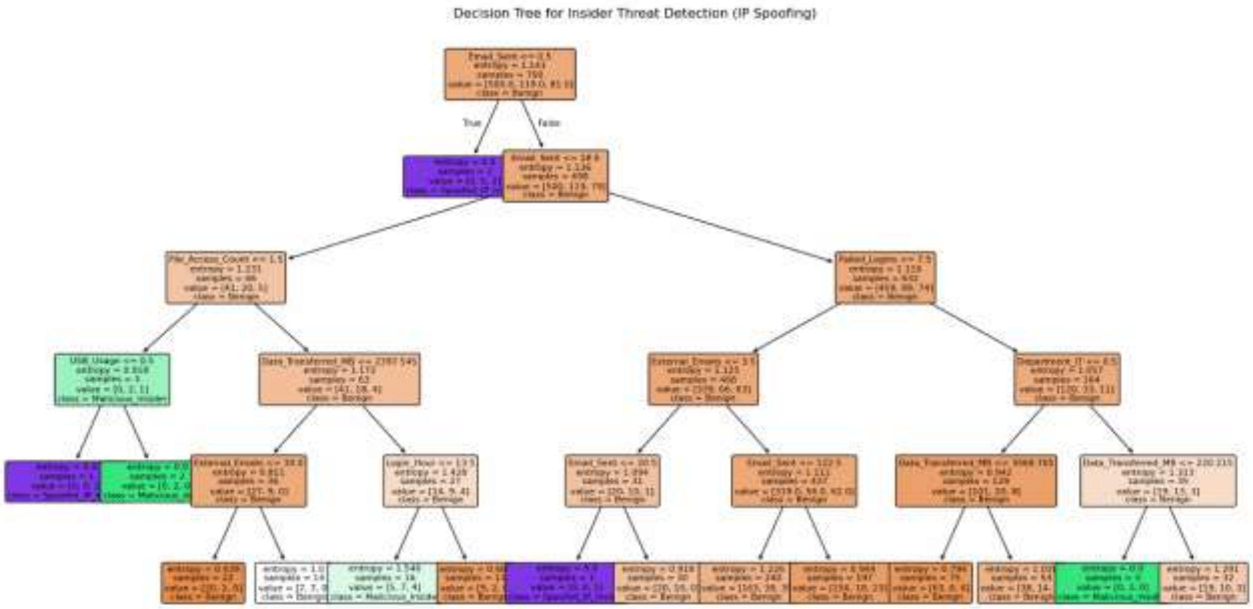


Figure 9: Decision Tree Threat Detection (IP Spoofing) Classifier

Results Using Random Forest

This section presents the experimental results obtained from applying the Random Forest algorithm for detecting insider threats through IP spoofing. Random Forest, an ensemble learning method, aggregates multiple decision trees to improve predictive accuracy and reduce overfitting [20]. The evaluation includes confusion matrices, accuracy, precision, recall, F1-score, and feature importance, providing a detailed assessment of the model's performance.

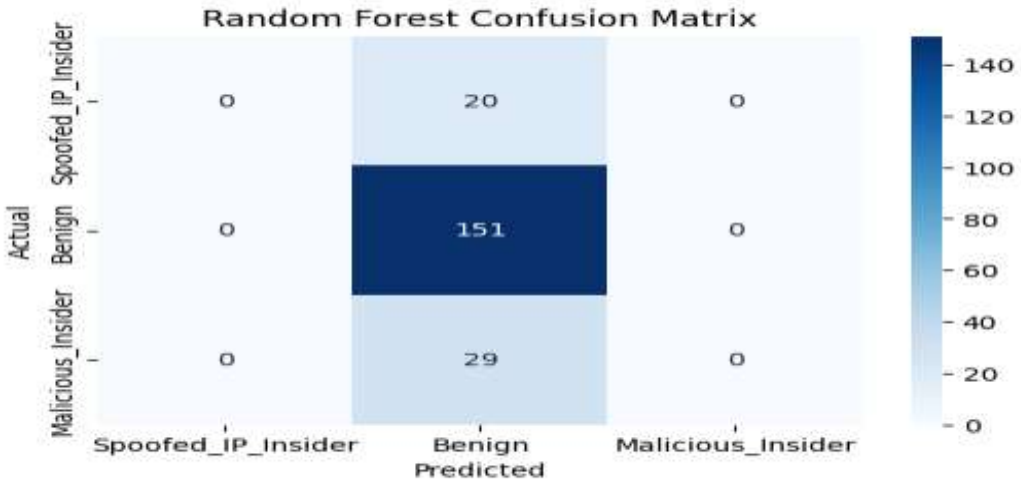


Figure 10: Random forest Confusion Matrix

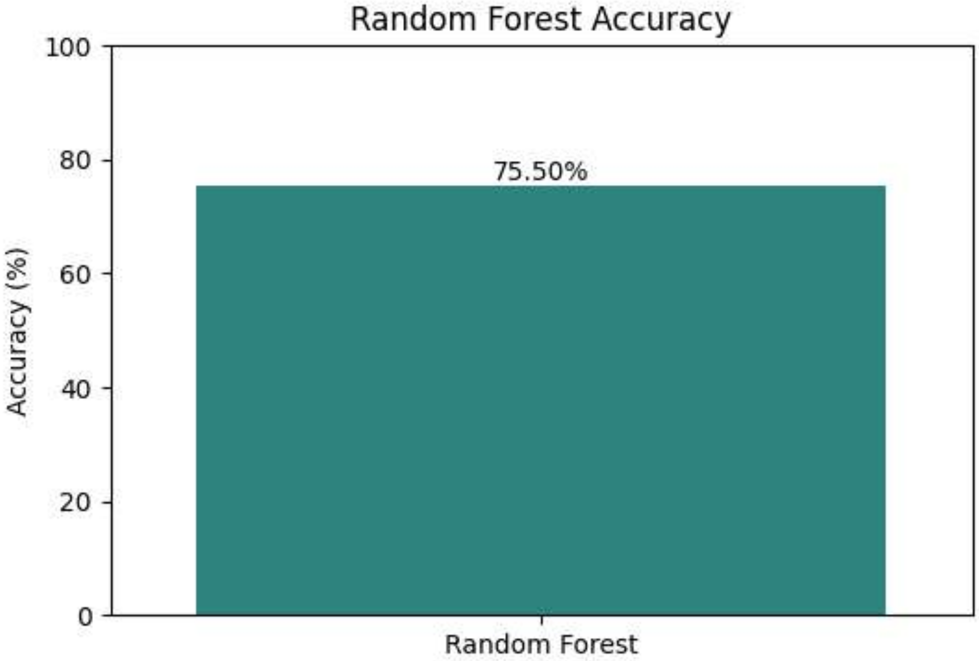


Figure 11: Random Forest Accuracy

Classification Report
Table 2: Classification Report of Random Forest

	Precision	Recall	F1-Score	Support
Benign	0.76	1.00	0.86	151
Malicious Insider	0.00	0.00	0.00	29
Spoofed_IP_Insider	0.00	0.00	0.00	20

Interpretation:

The Random Forest model achieves an overall accuracy of approximately 75.5%, slightly higher than the Decision Tree. Balanced precision and recall indicate effective detection with minimal misclassification, highlighting the robustness of ensemble methods for insider threat detection.

Open Access
Online ISSN: 2992-5487
Print ISSN: 2992-6068

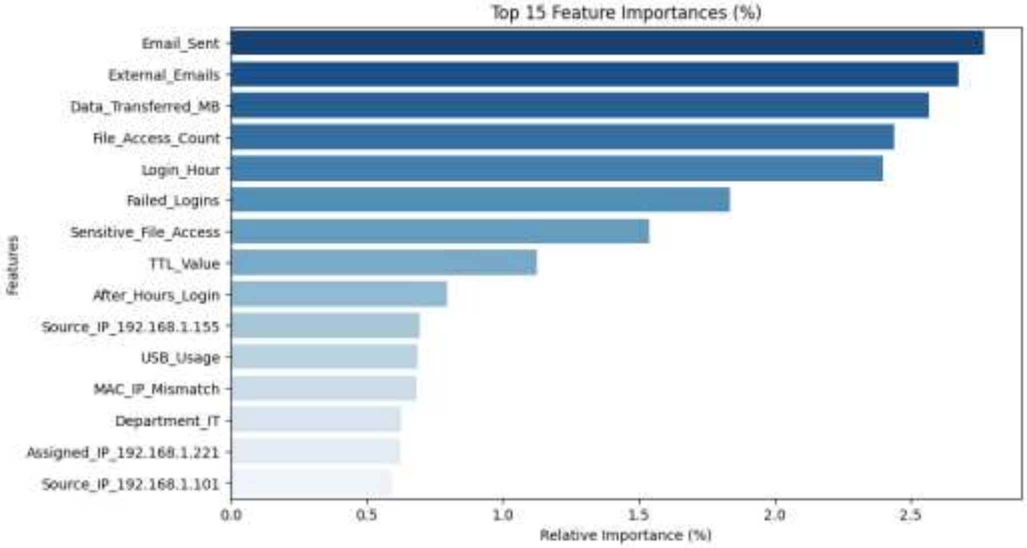


Figure 12: Feature Importance for Random Forest

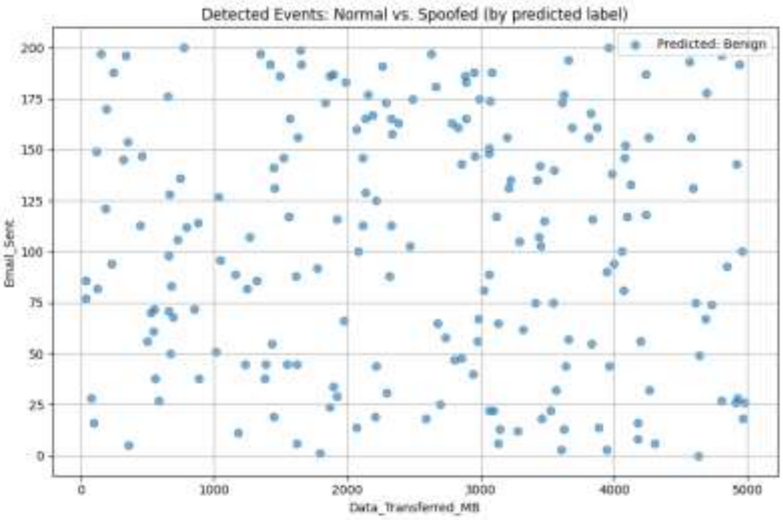


Figure 13: Scatter Diagram for the Normal vs Spoofed event detected

CONCLUSION AND RECOMMENDATION

This study aimed at the identification of insider threats executed through IP spoofing utilizing the machine learning (ML) algorithms of Decision Tree and Random Forest models. The research pinpoints the applied value of ML in enhancing network security in organizational settings. Based on the findings of this study in insider threat identification using IP spoofing via Decision Tree and Random Forest classifiers, some practical recommendations can be provided for organizations, researchers, and infosec professionals. These recommendations can enhance network security, improve ML-based detection frameworks, and advocate proactive steps in preventing insider threats.

For Organizational Network Security

1. Installation of Proactive Monitoring Systems – Companies should implement ML-powered monitoring software that continuously monitors network traffic for deviations. Decision Tree and Random Forest algorithms can be installed to proactively identify suspicious IP spoofing activities and notify security teams in real-time [22].

2. Strengthening Network Access Controls – Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) policies must be enforced to reduce the risk of insider threat. By applying privileges and authentication, organizations can restrict the potential for insiders to abuse IP spoofing for unauthorized access.

3. Recurrent Network Auditing and Log Analysis – Periodic inspection of network audit trails and logs can recognize abnormal patterns that ML models would determine as suspect. Combining machine detection and human examination ensures more accurate threat identification [23].

For Employee Training and Awareness Programs

1. Cybersecurity Awareness Training – Employees should be trained in the threats and indications of insider dangers, including IP spoofing. Awareness reduces the likelihood of innocent mistakes that can facilitate attacks [24].

2. Simulated Insider Threat Exercises – Controlled environment simulated insider attack exercises can allow employees to identify malicious activities and augment incident response plans. These exercises also provide more information to fine-tune ML models for deployment.

REFERENCES

1. Greitzer FL, Frincke DA. Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation. InInsider threats in cyber security 2010 Jul 28 (pp. 85-113). Boston, MA: Springer US.
2. Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review. 2004 Apr 1;34(2):39-53.
3. Caralli RA, Stevens JF, Young LR, Wilson WR. Introducing octave allegro: Improving the information security risk assessment process. 2007 May 1.
4. Pfleeger SL, Caputo DD. Leveraging behavioral science to mitigate cyber security risk. Computers & security. 2012 Jun 1;31(4):597-611.
5. Wright JT, Upadhyay S, Marcy GW, Fischer DA, Ford EB, Johnson JA. Ten new and updated multiplanet systems and a survey of exoplanetary systems. The Astrophysical Journal. 2009 Mar 5;693(2):1084.
6. Hunker J, Probst CW. The Risk of Risk Analysis. WEIS.
7. Sommer R, Paxson V. Outside the closed world: On using machine learning for network intrusion detection. In2010 IEEE symposium on security and privacy 2010 May 16 (pp. 305-316). IEEE.
8. Egba, Anwaitu Fraser, Akawuku Ifeanyi Godspower, Alade Samuel Mayowa and Iduh Blessing (2024), Development of a Diabetes Mellitus Diagnostic System Using Self-Organizing Map Algorithm: A Machine Learning Approach. IDOSR JOURNAL OF SCIENTIFIC RESEARCH 9(1) 72-80, 2024. https://doi.org/10.59298/IDOSRJSR/2024/9.1.7280.100
9. Chandola V, Banerjee A, Kumar V. Anomaly detection: A survey. ACM computing surveys (CSUR). 2009 Jul 30;41(3):1-58.
10. Sommer R, Paxson V. Outside the closed world: On using machine learning for network intrusion detection. In2010 IEEE symposium on security and privacy 2010 May 16 (pp. 305-316). IEEE.
11. Ponemon Institute. (2018, April 26). Data breaches caused by insiders increase in frequency and cost. Ponemon Institute Blog. Retrieved from https://www.ponemon.org/news-updates/blog/security/data-breaches-caused-by-insiders-increase-in-frequency-and-cost.html
12. Greitzer FL, Frincke DA. Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation. InInsider threats in cyber security 2010 Jul 28 (pp. 85-113). Boston, MA: Springer US.
13. Potteiger B, Zhang Z, Cheng L, Koutsoukos X. A tutorial on moving target defense approaches within automotive cyber-physical systems. Frontiers in future transportation. 2022 Feb 7;2:792573.
14. Clevenger SL, Marcum CD. The Link between Specific Forms of Online and Offline Victimization.
15. Hunker J, Probst CW. The Risk of Risk Analysis. WEIS.
16. Anagi Gamachchi, & Boztas, S. (2018). Insider threat detection through attributed graph clustering. arXiv. https://arxiv.org/abs/1809.00231
17. Alhamrouni I, Abdul Kahar NH, Salem M, Swadi M, Zahroui Y, Kadhim DJ, Mohamed FA, Alhuyi Nazari M. A comprehensive review on the role of artificial intelligence in power system stability, control, and protection: Insights and future directions. Applied Sciences. 2024 Jul 17;14(14):6214.
18. Randive, K. D., & Ramasundaram, M. (2023). MWCapsNet: A novel multi-level wavelet capsule network for insider threat detection using image representations. Neurocomputing, 553, 126588.

19. Pedregosa F, Varoquaux G, Gramfort A, Michel V, Thirion B, Grisel O, Blondel M, Prettenhofer P, Weiss R, Dubourg V, Vanderplas J. Scikit-learn: Machine learning in Python. the Journal of machine Learning research. 2011 Nov 1;12:2825-30.
20. Breiman L, Cutler A, Liaw A, Wiener M, Liaw MA. Package 'randomforest'. University of California, Berkeley: Berkeley, CA, USA. 2018;81:1-29.
21. Probst TM. Organizational safety climate and supervisor safety enforcement: Multilevel explorations of the causes of accident underreporting. Journal of applied psychology. 2015 Nov;100(6):1899.
22. Sharma, A., Kumar, R., & Tripathi, R. (2021). Machine learning approaches for insider threat detection: A systematic review. Cybersecurity, 4(1), Article No. 71. https://doi.org/10.1186/s42400-021-00071-w
23. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19–31. https://doi.org/10.1016/j.jnca.2015.11.016
24. Buczak AL, Baugher B, Guven E, Moniz L, Babin SM, Chretien JP. Prediction of peaks of seasonal influenza in military health-care data: Supplementary issue: Big data analytics for health. Biomedical engineering and computational biology. 2016 Jan;7:BECB-S36277.

CITE AS: Akawuku I. Godspower, Adejumo Samuel Olujimi, Olatunde Ayodeji Akano, Abdullateef Abdulsomad Tunde and David Mulumeoderhwa Bahati (2025). Investigation into the use of Machine Learning Algorithms for Detecting Insider Threats through IP Spoofing in Organizational Networks. NEWPORT INTERNATIONAL JOURNAL OF ENGINEERING AND PHYSICAL SCIENCES, 5(2):11-24 https://doi.org/10.59298/NIJEP/2025/5211240