International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Cybersecurity Risk Detection and Assessment of Availability and Confidentiality Attacks in Stock Markets

Ms. Malathy S[1] and Dr. R. Anandhi[2]

[1]Research Scholar (Full–Time) ,PG & Research Department of Computer Science,
Dwaraka Doss Goverdhan Doss Vaishnav College, Chennai, India
[2]Assistant Professor, PG & Research Department of Computer Science
Dwaraka Doss Goverdhan Doss Vaishnav College , Chennai, India
[1]malathy10112001@gmail.com

Abstract
The computerization of stock markets has greatly improved trading efficiency but, at the same time, brought exposures to cyberattacks. This paper discusses two most important categories of cyberattacks in stock markets: Availability Attacks and Confidentiality Attacks. Whereas availability attacks cause an impairment in the normal functioning of markets, confidentiality attacks compromise sensitive financial information. This research assesses the trend of these attacks through mathematical modeling and experimental verification with AI-based detection methods. A model for risk assessment is envisioned in order to measure and prioritize threats by their severity to effectively develop mitigation strategies. The results ensure investor confidence and business resilience by identifying the strengths and weaknesses of different detection methods.

Keywords: Cybersecurity, Stock Markets, Availability Attacks, Confidentiality Attacks, Anomaly Detection, Risk Assessment

1. Introduction

The use of digital technologies in stock trading platforms has changed how markets operate. It enables high-frequency trades, real-time analytics, and smooth transactions.[1]However, this shift also exposes stock markets to different cyber threats that can affect data integrity, availability, and confidentiality. Robust cybersecurity structures in financial environments are more essential now than ever.Whereas earlier research has written about Authentication Attacks (Group A), this paper deals with:

- **Availability Attacks (Group B)** – Threats that interfere with trading activity[2] [3].
- **Confidentiality Attacks (Group C)** – Attacks that violate sensitive financial information[4][5].

A summary of all cyber threat groups is provided in Table 1.

Table 1: Classification of Stock Market Cyber Threats

Focus Area	Properties	Threats
Group A - Authentication Attacks		
Identity and Financial Frauds	Unauthorized access and impersonation	• SIM Swapping
		• Account Takeovers
		• Credential Stuffing
		• Phishing Attacks
Group B - Availability Attacks		
Market Disruption and System Manipulation	Disrupting stock market operations	• Ransomware Attacks
		• Exchange System Hacks
		• Algorithmic Trading Disruption
		• Distributed Denial-of-Service (DDoS) Attacks
Group C - Confidentiality Attacks		
Data Breach and Theft	Unauthorized access to sensitive data	• API Exploits
		• Brokerage and Exchange Data Breaches
		• Insider Trading via Data Breach
Group D - Integrity Attacks		
AI and Algorithmic Manipulation	Manipulating AI-based trading and market behavior	• Algorithmic Trading Exploits
		• Deepfake Financial News
		• Sentiment Manipulation Bots
		• Spoofing and Layering

2. Literature Review

Previous research explained in table 2 has looked into how vulnerable financial systems are to cyber threats. Several studies proposed methods for detecting fraud and anomalies using machine learning.[6] However, most of these lacked specific threat categories and dynamic risk evaluations designed for stock markets.Additionally, few comparisons of AI, anomaly detection, and behavioral analysis methods have been examined.

Table 2. Summary of the Literature Review

Author / Source	Year	Focus Area	Methodology	Key Contributions	Identified Gaps
Anderson, R. (Security Engineering)	2020	Security architecture for distributed systems	System design principles, case studies	Emphasized the importance of dependable system design in financial networks	Lacked AI-based threat detection focus
Tankard, C.	2011	Advanced Persistent Threats (APTs)	Threat monitoring and mitigation strategies	Provided insight into long-term and stealthy threats to systems	No specific focus on financial or

Author / Source	Year	Focus Area	Methodology	Key Contributions	Identified Gaps
					stock trading systems
Kshetri, N.	2019	Cybersecurity in global finance	Policy and international relations perspective	Discussed geopolitical dimensions of cybersecurity threats	Did not address technical detection techniques
Conti et al. (Cyber Threat Intelligence)	2018	Threat intelligence techniques	Signature-based and behavioral analysis	Reviewed threat intelligence applications in enterprise networks	Limited application to high-frequency trading systems
SEC Investor Bulletin	Ongoing	Online account protection	Regulatory advisories and user guidelines	Outlined best practices for investor account security	Lacked technical modeling or detection mechanisms
NIST SP 800-30	2012	Risk assessment methodology	Quantitative and qualitative frameworks	Established foundational principles for cybersecurity risk evaluation	Generic in scope; not specialized for stock market scenarios
Liu, F. et al. (ACM Computing Surveys)	2021	Insider threat detection	Comparative analysis of detection methods (rule-based, ML, etc.)	Reviewed techniques like behavior profiling and ML for insider threats	Focused only on insider threats, not broader stock market attacks

3. Methodology

A. Dataset Description

This research uses a dataset of 10,000 records that have the following features:

- Type of Attack - Specifies the type or class of cyberattack contained in the record.
- Likelihood - Reports the estimated probability or chance of the attack materializing
- Effect - Refers to the potential severity or impact of the attack in case of occurrence.
- Risk Score - A number that shows the overall risk level, usually based on probability and impact.
- AI Detection Results - Displays the output from an AI model regarding whether the activity is malicious or normal.

- Anomaly Detection Flags - A binary indicator that shows whether the record reflects abnormal or suspicious behavior.
- Behavior Analysis Outputs - Offers insights from behavioral analytics, highlighting deviations or unusual patterns in system or user activity.

B. Threat Modeling and Mathematical Representations

This section explains the major cyber threats under Group B and Group C that pose risks to stock trading systems. [7]

Group B: Availability Attacks

1. Ransomware Attacks - Malicious code encrypts trade information or system access, and a ransom must be paid to decrypt it. This can halt market operations. Ransomware attacks encrypt critical stock market data and demand payment for decryption.

Mathematical Model: The chance of a successful ransomware attack depends on encryption speed and system strength:

$$P(R)=1-e-\lambda T$$

where:

- λ = Rate of encryption spread across the system.
- **T** = Time elapsed before detection and response.

A higher λ means faster encryption, which raises the likelihood of a successful attack. Early detection aims to reduce T, which makes ransomware threats less effective.

2. Exchange System Hacks - Stock exchanges get hacked by criminals who manipulate stock prices, steal financial data, or disrupt trading activity[8].Cybercriminals take advantage of weaknesses in trading platforms to gain unauthorized access.

Mathematical Model: Risk evaluation is based on access patterns:

$$R_{hack} = \sum_{i=1}^{N} W_i . F_i \qquad (1)$$

where:

- **W_i** = Weight of an access anomaly.
- **F_i** = Extracted behavioral features

3. Algorithmic Trading Disruption - Hackers exploits the gap in trading algorithms, leading to manipulated stock behavior and financial loss.Manipulative trading activities upset market stability by affecting asset prices.

Mathematical Model: Unusual acceleration of price is identified by:

$A_t = \frac{P_{t+1} - P_t}{\Delta T}$ (2)

If A_t > θ, the system identifies possible market manipulation.

4. Distributed Denial-of-Service (DDoS) Attacks - Traffic overloading in trading systems, leading to business suspension and delayed trade executions.DDoS attacks overwhelm stock market systems with overwhelming volumes of traffic, rendering them useless.[9]

Mathematical Model: We model the probability of a DDoS attack as:

$$P(\text{DDoS}) = \frac{T_{obs} - T_{avg}}{T_{std}} \quad (3)$$

where:

- T_{avg} = Average traffic for a given time.
- T_{std} = Normal traffic pattern standard deviation.
- T_{obs} = Observed traffic volume.

Group C: Confidentiality Attacks

1. API Exploits - The vulnerabilities of the Financial API are used for unauthorized access, stealing secret information, or altering transactions.Hackers use vulnerable APIs used by trading platforms and brokerage companies to gain access to confidential financial data.

Mathematical Model: Access risk assessment through entropy-based detection:

$$H(A) = \sum_{i=1}^{N} P(a_i) \log P(a_i) \quad (4)$$

where :

- $H(A)$= entropy of API requests. High entropy identifies abnormal behavior.

2. Brokerage and Exchange Data Breaches - Hackers attack stock exchanges and brokerage houses to access information of investors, resulting in identity theft and financial fraud. Cyber thieves breach the systems of brokerage and steal data of investors, resulting in financial fraud and identity theft.

Mathematical Model: Estimating breach probability based on statistical probability:

$$P(Breach) = 1 - e^{-\lambda t} \quad (5)$$

where:

- λ = historical breach frequency, t = time since last attack.

3. Insider Trading Through Data Breach – Data breach provides unauthorized access to financial privileged information in a manner that insiders or intruders get the opportunity to utilize insider information in a manner in which they execute illegal trade.Intruders utilize stolen insider information to execute illegal trades and reap unjust market benefits.[10]

Mathematical Model: For modeling the probability of an insider attack based on suspicious transactions:

$$P(Insider) = \frac{N_s}{N_t} \cdot \left(\frac{v_s}{v_t}\right) \qquad (6)$$

where:
• N_s = Number of suspicious transactions by an entity.
• N_t = Total transactions by entities.
• v_s = Volume of all suspicious transactions.
• v_t = Overall trading volume.

A high value of P(Insider) suggests a possible insider trading activity.These threats point to the relevance of robust cybersecurity controls that secure stock trading sites.

C. AI-Based Threat Detection Framework

Our model incorporates:
- Supervised machine learning algorithms (Random Forest, XGBoost) for predictive threat categorization.[11]
- Unsupervised anomaly detection methods (Autoencoders, Isolation Forests).
- Reinforcement learning for improving cybersecurity response mechanisms.

D. Risk Score Calculation

Risk Score is a figure applied to measure the potential effect of attacks on cybersecurity.[12] It measures the severity of various kinds of attacks in terms of probability of occurrence and effects they have.
To measure quantitatively the risk for each attack, we consider the Risk Score as:

$$R(A_i) = P(A_i) \times I(A_i) \qquad (7)$$

where:
• $R(A_i)$ = Risk Score of an attack.
• $P(A_i)$ = Probability of occurrence of the attack.
• $I(A_i)$ = Impact score, which is measured in terms of cost loss, system downtime, and investor confidence loss.
The model delivers an organizational capability to rank the mitigation interventions based on the severity of cyber threats and the application of corresponding security interventions.[13]

4. Results and Discussion

A. Comparison of Attack Frequency

Figure 1 represents the occurrence of various cyberattacks on stock exchanges and concludes with the most prevalent threats. The x-axis is the range of various types of cyberattacks, and the y-axis is their estimated frequency. [14] Higher bars express higher attack frequencies, which reflect areas that need higher applications of cybersecurity. This analysis can be utilized to prioritize measures against risks in order to improve market stability and security.

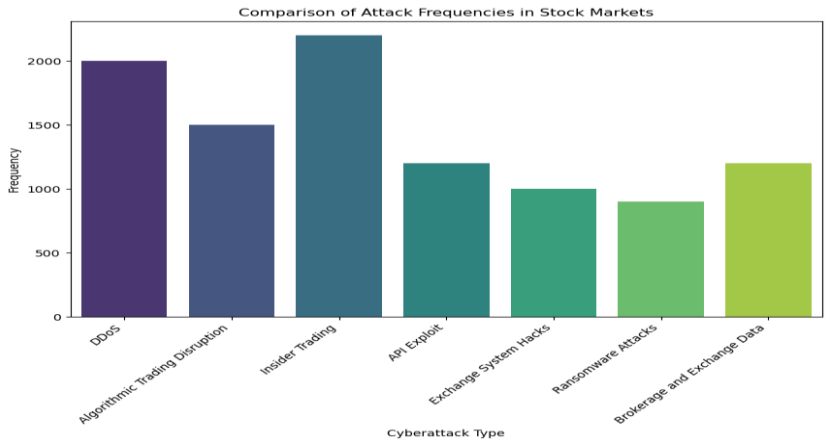

Figure 1 Cyberattack Frequency Distribution in Stock Markets

B. Experimental Validation of Detection Techniques

We compared the performance of AI-based detection, anomaly detection, and behavior analysis methods as indicated in Table 2.

Table 2 : Performance Comparison of Cyberattack Detection Methods

Detection Method	Precision	Recall	F1-Score
AI-Based Detection	0.795594	0.824350	0.809717
Anomaly Detection	0.702329	0.684883	0.693496
Behavior Analysis	0.591500	1.000000	0.743324

- AI-driven detection recorded the best F1-score performance and is thus the most effective method to identify cyber threats in stock markets.
- Behavior analysis recorded perfect recall but may be prone to false positives.
- Anomaly detection was also consistent but with a slightly elevated false positive rate

C. Confusion Matrix for Detection Techniques

The AI detection model, which was built with a Random Forest Classifier, was tested with a confusion matrix, presented in Figure 2 A confusion matrix gives a breakdown of the classification performance of the model.

Confusion Matrix Analysis

1. **Accuracy (A)**

$$A = \frac{TP+TN}{TP+TN+FP+FN} \quad (8)$$

2. **Precision (P)**

$$P = \frac{TP}{TP+FP} \quad (9)$$

3. **Recall (R)** (a.k.a. Sensitivity or True Positive Rate)

$$R = \frac{TP}{TP+FN} \quad (10)$$

4. **F1-Score (F1)** (harmonic mean of precision and recall)

$$F_1 = 2 \times \frac{P \times R}{P+R} \quad (11)$$

5. **False Positive Rate (FPR)**

$$FPR = \frac{FP}{FP+TN} \quad (12)$$

6. **Detection Latency (DL)**

Time (in seconds) to detect fraud from input instance to classification result.

- $T_{arrive,i}$ **:** The time at which the transaction (or data instance) arrives in the system.
- $T_{detect,i}$ **:** The time at which the system detects the fraud.

$$L_i = T_{detect,i} - T_{arrive,i} \quad (13)$$

This represents the delay between arrival and detection.

7. Average Detection Latency (for n transactions):

In order to calculate the average detection latency for all fraud instances:

$$D^L = \frac{1}{n}\sum_{i=1}^{n}\left(T_{detect,i} - T_{arrive,i}\right) \quad (14)$$

Figure 2 represents the Confusion matrix has four important elements:

- **True Positives (TP)** = 1300 → Accurately classified attack instances.
- **True Negatives (TN)** = 89 → Accurately classified non-attack instances.
- **False Positives (FP)** = 334 → Misclassified normal instances as attacks (false alarms).
- **False Negatives (FN)** = 277 → Misclassified attack instances as normal (missed detections)

Total test sample size utilized for evaluation is:
Total Samples=TP+TN+FP+FN=1300+89+334+277=2000

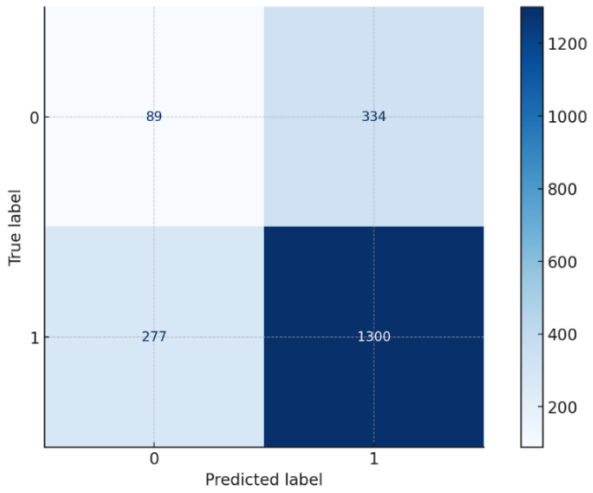

Figure 2 AI-Based Detection Confusion Matrix

• The detection system with AI showed excellent recall (82.41%), which implies an excellent capability to identify attacks.
• A false positive rate of 334 cases does imply some over-classification of normal activity as attacks.
• There could be scope for further optimization of the selection of features and hyperparameters to improve classification accuracy and minimize false positives.

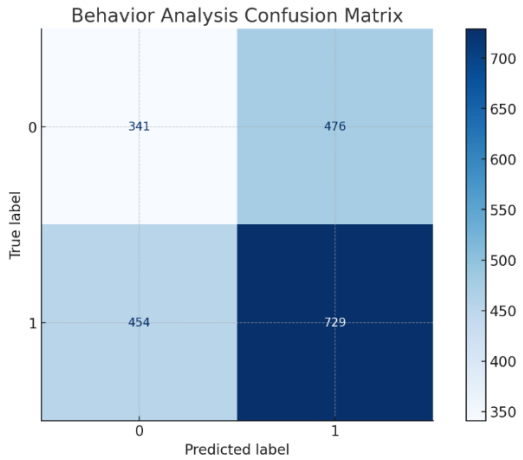

Figure 3 Behavior Analysis Confusion Matrix

The confusion matrix illustrated in figure 3 depicts the performance of a Behavior Analysis-Based Intrusion Detection Model on a test set. The matrix assesses the effectiveness of the model to differentiate between normal and attack behaviors, giving an idea of its classification accuracy. [15]

Components of a Confusion Matrix

A confusion matrix comprises four major values:

- **True Positives (TP) =** 729 → Identifies correctly attack behaviors.
- **True Negatives (TN)** = 341 → Identifies correctly normal behaviors.
- **False Positives (FP)** = 476 → Normal behavior incorrectly labeled as attacks.
- **False Negatives (FN)** = 454 → Attack behavior incorrectly identified as normal.

This discussion is essential to enhance the behavior-based detection mechanism in cybersecurity intrusion detection systems to better mitigate threats while reducing false alarms.

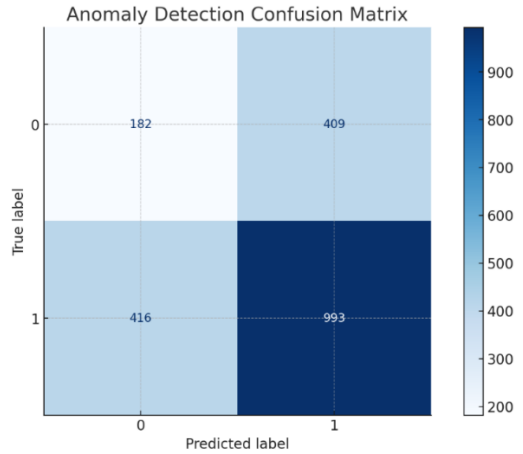

Figure 4 Anomaly Detection Confusion Matrix

The confusion matrix in Figure 4 depicts the performance of an Anomaly Detection Model in distinguishing between normal and anomalous instances. The confusion matrix facilitates understanding the accuracy, false positive rate, and efficiency of the model in detecting anomalies.

Confusion Matrix Breakdown

- **True Positives (TP) =** 993 → Correctly identified anomalies.
- **True Negatives (TN)** = 182 → Correctly identified normal instances.
- **False Positives (FP) =** 409 → Normal instances incorrectly classified as anomalies (false alarms).
- **False Negatives (FN)** = 416 → Normal instances incorrectly labeled as anomalies (false alarms).

The study is useful in anomaly detection problems like intrusion detection systems, fraud detection, and fault detection in industrial control systems, where it is essential to reduce false negatives in order to avoid security violations.[16]

D. Cybersecurity Risk Score & Heatmap Visualization Implementation

To validate the effectiveness of our risk score equation, we used the following Python-based model for risk analysis:

Risk Score Analysis for Cybersecurity Attacks

The heatmap displays the mean risk score for different types of attacks and aids in threat prioritization for cybersecurity risk management in igure 5.

1. Highest Risk Attacks:

a.Exchange System Hack, Insider Trading, and DDoS attacks had the highest relative risk scores 2.6

2.Moderate Risk Attacks:

a. Algorithmic Trading Disruption and API Exploits had a relative risk score of 2.5

3. Lowest Risk Attack:

a. Ransomware Attacks had the lowest relative risk score of 2.4, possibly due to the fact that more effective security measures were in place to mitigate them.

Comparing them helps the cybersecurity teams to concentrate on high-risk threats and build strong mitigation strategies

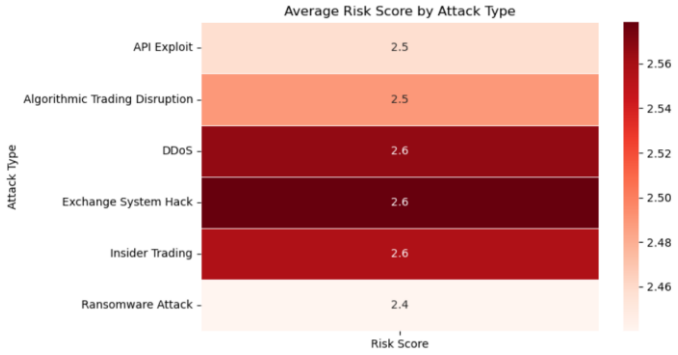

Figure 5 Average Risk Score

Performance Metrics Heatmap for Detection Methods

The second chart (Table 2) compares various cybersecurity detection methods using important performance metrics: Precision, Recall, and F1-Score. [17]

• AI-Based Detection is overall best with an F1-score of 0.81 and balanced precision-recall values.
• Anomaly Detection is comparatively less efficient with an F1-score of 0.69 and poor recall (0.68), which suggests potential detection failure.
• Behavior Analysis has good recall (1.0) but bad precision (0.59), which implies that it identifies a lot of actual threats and also generates false alarms.

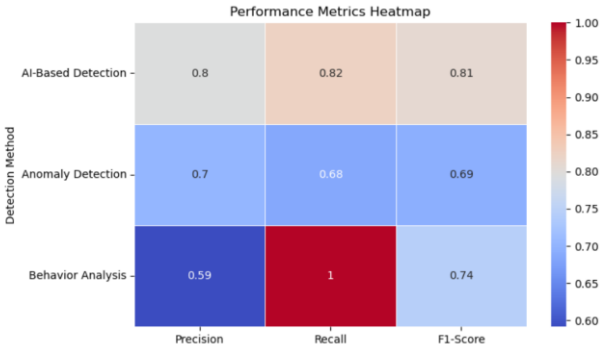

Figure 6 Performance Metrics Heatmap

The Performance Metrics Heatmap figure 6 depicts these findings identify the strength and limitation of each detection approach in cyber security use.

5. Conclusion

This research aimed at examining two significant cyber threat types in stock markets: Availability Attacks (Group B) and Confidentiality Attacks (Group C). By considering the frequency of attacks and computed risk rankings, Availability Attacks—namely Exchange System Hacks and DDoS attacks—were designated as most common and greatest risk, as they have the capability of shutting down trading functions and causing market instability. Confidentiality Attacks like Insider Trading and API Exploits also reflected high impact, mainly targeting sensitive financial information. Among the detection techniques reviewed, AI-based detection algorithms performed best, having the highest F1-score with a good trade-off between precision and recall and hence are most effective for threat identification in stock trading scenarios.

Future Work

Subsequent studies will focus on Group D: Integrity Attacks with algorithmic manipulation and AI-driven deception strategies like spoofing, deepfake financial news, and sentiment manipulation. Such attacks need sophisticated detection because they are discreet and behavior-induced. The research aims to create effective prevention and detection methods specifically for Group D, utilizing hybrid deep learning models, graph-based behavior analysis, and real-time data stream incorporation. Furthermore, there is room for cooperation with regulatory organizations to comply with the financial data protection

regulations and investigate post-quantum cryptographic methods for future-proofing trading platforms' cybersecurity.

References

1. R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020.
2. A. Kshetri, "Cybersecurity and International Relations," Computer, vol. 52, no. 3, pp. 84-87, 2019.
3. D. Ghelani, "Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review," Authorea, Sept. 22, 2022, DOI: 10.22541/au.166385207.73483369/v1.
4. Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments," Energy Reports, vol. 7, pp. 8176-8186, 2021.
5. I. Kumar, "Emerging threats in cybersecurity: a review article," International Journal of Applied and Natural Sciences, vol. 1, no. 1, pp. 1-8, 2023.
6. C. Tankard, "Advanced Persistent Threats and How to Monitor and Deter Them," Network Security, 2011.
7. M. Conti, A. Dehghantanha, et al., “Cyber Threat Intelligence: Methods and Techniques,” Elsevier, 2018.
8. SEC Investor Bulletin: Protecting Your Online Investment Accounts, U.S. Securities and Exchange Commission.
9. NIST Special Publication 800-30, "Guide for Conducting Risk Assessments", 2012.
10. F. Liu, P. Wang, et al., “Insider Threat Detection Techniques: A Review,” ACM Computing Surveys, 2021.
11. V. Kumar, J. Srivastava, and A. Lazarevic, Eds., Managing Cyber Threats: Issues, Approaches, and Challenges. Boston, MA, USA: Springer, 2005.
12. M. S. Abu, S. R. Selamat, A. Ariffin, and R. Yusof, "Cyber threat intelligence–issue and challenges," Indonesian Journal of Electrical Engineering and Computer Science, vol. 10, no. 1, pp. 371-379, 2018.
13. M. Ulsch, Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks. Hoboken, NJ, USA: John Wiley & Sons, 2014.
14. Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," Electronics, vol. 12, no. 6, p. 1333, 2023.
15. R. Prasad and V. Rohokale, "Cyber threats and attack overview," in Cyber Security: The Lifeline of Information and Communication Technology. Cham, Switzerland: Springer International Publishing, 2019, pp. 15-31.
16. B. Dash, M. F. Ansari, P. Sharma, and A. Ali, "Threats and opportunities with AI-based cyber security intrusion detection: a review," International Journal of Software Engineering & Applications (IJSEA), vol. 13, no. 5, 2022.
17. S. K. A. Ramesh, "AI-enhanced cyber threat detection," International Journal of Computer Trends and Technology (IJCTT), vol. 72, no. 6, pp. 64-71, 2024.