Minimax Theory and its Applications

Volume 11 (2026), No. 3s, 368 to 374

A Hybrid Ai and Mathematical Modelling Approach for Adaptive Network Security And Intrusion Prevention

Sudheer Nidamanuri[1], Dr M Praneesh[2], N Radhika Amareshwari[3], Dr. CH. Bhavani[4], Dr Madhulika Yarlagadda[5], P.K.Hemalatha[6], Omar Almomani[7], A.Smithakranthi[8]

[1]Assistant professor, Department of CSE-(CyS,DS) and AI&DS, Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering and Technology, Hyderabad, Telangana,500090.
Email:nidamanuri.sudheer@gmail.com, Orcid:0000-0002-8945-3414
[2]Assistant Professor, Department of Computer Science with Data Analytics, Sri Ramakrishna College of Arts & Science, Coimbatore, Tamilnadu, India. Email: raja.praneesh@gmail.com, Orcid id : 0000-0003-3691-1343.
[3]Senior Assistant Professor, Department of CSE -Cyber security, Geethanjali College of Engineering and Technology, Keesara Mandal, Cheeryal Village, Hyderabad, Telangana 501303
Email: radhika.amareshwari@gmail.com, Orcid:0009-0000-7523-4475
[4]Associate Professor, Department of Computer Science and Engineering, CVR College of Engineering, Hyderabad, Telengana, India. Email: vbhavani118@gmail.com, orcid- 0000-0002-1018-342
[5]Associate Professor, CSE Department, Amity School of engineering and Technology, Amity University, Hyderabad. Email:madhulika.yarlagadda@gmail.com
[6]Assistant professor, Department of mathematics, Vel Tech Rangarajan Dr Sagunthala R&D Institute of Science and Technology, Avadi. Chennai, India, Email: pkhemalathamsc@gmail.com
[7]Department of Networks and Cybersecurity , Hourani Center for Applied Scientific Research, Al-Ahliyya Amman University, Amman, Jordan. Email: o.almomani@ammanu.edu.jo, orcid.org/0000-0003-3160-6542
[8]Department of Computer Science and Engineering, Koneru Lakshmaiah education foundation, Green fields, Guntur, A.P-522302, India, Email: asmithakranthi@kluniversity.in

Abstract
The nature of attacks on modern communication networks is becoming more complex, making static and rule-based intrusions systems less effective in providing protection. Approach of Artificial Intelligence and Mathematical modelling proposed in this study for Adaptive Network security and Intrusion Prevention. It integrates artificial intelligence (AI) based traffic classification with mathematical threat detection algorithms to detect malicious traffic and establish appropriate security measures. The primary inputs are five network parameters: packet rate, average packet size, connection frequency, failed connection ratio and traffic anomaly index. The AI part determines the probability of intrusion and category of attack, while the mathematical model calculates a hybrid threat score of attack probability, attack severity, attack frequency, anomaly level and network vulnerability. The system determines adaptive actions to trigger, based on the computed score (blocking, monitoring, isolation, rate limiting). The accuracy, precision, recall, F1-score, false-positive rate, prevention success rate and response latency are used for performance evaluation and it allows for interpretable and adaptive decisions about intrusion prevention in various networks.

Keywords: Adaptive Network Security; Artificial Intelligence; Intrusion Detection; Intrusion Prevention; Mathematical Modelling; Threat Risk Assessment

1.Introduction

Today's communication networks enable cloud applications, industrial systems, financial services and IoT applications. They have also been proliferating quickly, exposing them to greater risks of cyberattacks like denial-of-service attacks, network scanning, unauthorized access, malware propagation and coordinated intrusion attempts. Typically, network-security solutions use a fixed threshold, a precompiled signature list and traditional rules. These can deal with attacks that they are aware of, but they will not help when network conditions change or when new attack patterns are encountered. However, legitimate traffic could exhibit abnormal behavior and cause unwanted blocking of static prevention mechanisms.

AI is significant in network security because it can detect complex and nonlinear patterns in network traffic. Machine-learning and deep-learning techniques can classify normal and malicious traffic, and determine the intrusion probabilities. But AI-driven security systems come with challenges in terms of interpretability and control of responses. Although high confidence of prediction does not always reflect high severity of attack or best prevention action. This can make security decisions hard to defend and might constrain response effectiveness.

A complementary approach is provided by mathematical modelling which quantitatively represents the attack probability, attack severity, attack frequency, anomaly level, and network vulnerability. Combined with AI predictions, these factors can be used to build security decisions that take into account both detection confidence and operational risk. This encourages the proposed hybrid approach that encompasses AI-driven intrusion classification, mathematical threat modelling and adaptive response selection. A significant research challenge is the lack of integration of intelligent detection, quantitative risk assessment and dynamic intrusion-prevention decisions into a coherent framework.

The five major contributions are the following: First, a combination of artificial intelligence and mathematical solutions to network security is created. Second, a multiclass intrusion classification is implemented by an AI model. Thirdly, mathematical modelling involves assessing attack risk in terms of probability, severity, frequency, anomaly level, and vulnerability. Fourth, an adaptive mechanism selects prevention actions based on the threat level calculated. Finally, the proposed framework is compared with a rule-based, a machine learning and an AI-only framework in terms of the detection, prevention and computational performance

2.Litrerature Review

Traditional intrusion detection and prevention systems mainly rely on signature-based and rule-driven methods to identify malicious network activities (Wu & Banzhaf, 2010; Bhuyan et al., 2013). These methods determine if the traffic is anomalous based on patterns that have been pre-provisioned, and are useful against known attacks. The problem with their reliance on existing signatures is that they cannot detect new or modified attacks. The anomaly-based systems have been designed to detect abnormality in network traffic and can have high false positive rates in case of normal network traffic patterns changing (Shiravi et al., 2012; Pajouh et al., 2016).

Machine-learning-based intrusion detection has the ability to detect complex relationships between network traffic features, thereby enhancing security (Mishra et al., 2018). Various techniques have been employed for the discrimination of normal and malicious traffic, including support vector machines, decision trees, random forests and artificial neural networks. The deep-learning algorithms such as convolutional neural network, recurrent neural network, autoencoder, and long short-term memory network are also included in feature learning and multiclass attack classification (Vinayakumar et al., 2019; Aldweesh et al., 2020; Ferrag et al., 2020). However, these models tend to be limited to just classification, and offer little information about the risk of detected attacks.

Mathematical and probabilistic cyber-security models offer quantitative approaches to assess the probability or threat level, impact or severity of the threat, and vulnerability (Wang et al., 2020). Risk-scoring models and optimization techniques aid in making more interpretable security decisions. The idea is extended by adaptive intrusion-prevention mechanisms, which dynamically select some of the actions (such as traffic monitoring, rate limiting, access restriction, blocking, or isolation). Hybrid AI based methods on the other hand, integrate intelligent detection capabilities with decision making mechanisms to enhance adaptability in a changing network environment (Wazid & Das, 2016).

However, there are very few existing works focusing on integration between adaptive prevention, mathematical threat evaluation, and AI prediction, and the existing works focus more on intrusion classification accuracy (Aldweesh et al., 2020; Mishra et al., 2018). Complex pattern can be detected by AI models, the risk can be quantified and calculated by mathematical model and transparent decision making can be achieved (Vinayakumar et al., 2019; Wang et al., 2020). A single framework is needed to link intrusion classification, quantitative threat assessment and adaptive response selection. To overcome this limitation, the proposed solution connects AI-based multiclass detection, mathematical risk modelling, and threat-level-based intrusion prevention all under one roof as an adaptive network-security solution.

3. Proposed Methodology

3.1 Network Security Architecture and Input Modelling

The framework proposed combines all of these elements: network traffic preprocessing, AI-based intrusion detection, mathematical threat assessment, adaptive security decisions, and intrusion prevention. In the first stage, network traffic is fed into feature extraction and normalization as seen in Figure 1. Once the normalization of the inputs is performed, the AI model is employed to classify whether an intrusion has been detected and to estimate the probability of an attack. Mathematical modelling determines the threat detected, and produces a hybrid risk score to decide on security action (monitor, rate limit, block or isolate).

Five primary network parameters are considered, as summarized in Table 1: packet rate P_r, average packet size P_s, connection frequency C_f, failed connection ratio F_r, and traffic anomaly index A_i. The input vector is

$$X = [P_r, P_s, C_f, F_r, A_i] \quad , _____ \quad (1)$$

Min-max normalization is applied as

$$x_i^{'} = \frac{x_i - x_i^{\min}}{x_i^{\max} - x_i^{\min}} \quad , _____ \quad (2)$$

and the normalized feature vector is

$$X^{'} = [P_r^{'}, P_s^{'}, C_f^{'}, F_r^{'}, A_i^{'}] \quad , _____ \quad (3)$$

This normalized vector is used for subsequent intrusion detection and threat assessment.

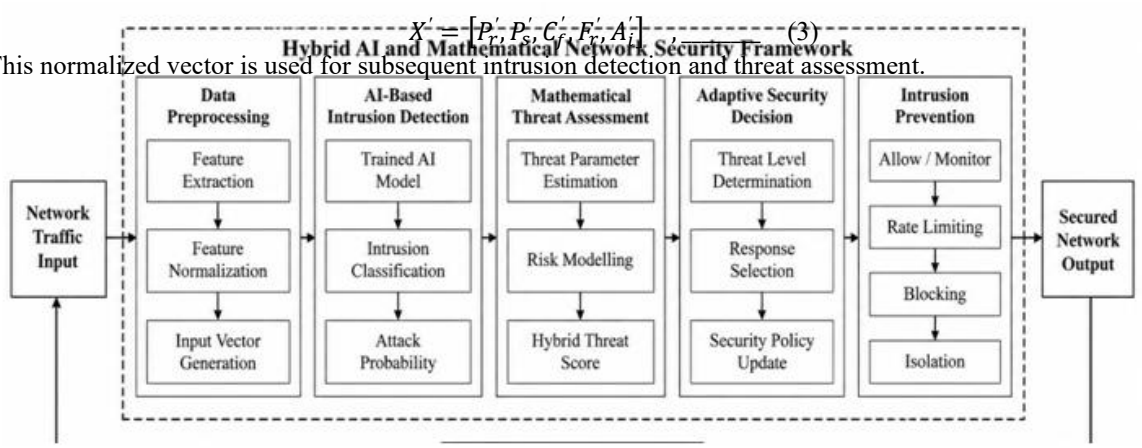


Fig. 1. Overall Architecture of the Proposed Hybrid AI and Mathematical Network Security Framework

Table 1. Network Traffic Input Parameters and Numerical Ranges

Parameter	Symbol	Range	Unit
Packet Rate	P_r	0–1000	packets/s
Average Packet Size	P_s	64–1500	bytes
Connection Frequency	C_f	0–500	connections/s
Failed Connection Ratio	F_r	0–1	ratio
Traffic Anomaly Index	A_i	0–1	index

3.2 AI-Based Intrusion Detection and Classification

The normalized network traffic vector obtained from the preprocessing stage is supplied to the AI-based intrusion detection model. The proposed classifier has five input features, two hidden layers of 32 and 16 neurons, respectively, as shown in Figure 2. The hidden layers use ReLU activation and a five-class Softmax layer sets the probability of each traffic category.

The hidden-layer operations are expressed as

$$h_1 = \text{ReLU}(W_1 X^{'} + b_1) \quad , _____ \quad (4)$$
$$h_2 = \text{ReLU}(W_2 h_1 + b_2) \quad , _____ \quad (5)$$

The Softmax probability for intrusion class $C_k$is

$$P(C_k \mid X) = \frac{e^{z_k}}{\sum_{j=1}^{K} e^{z_j}} \quad , _____ \quad (6)$$

and the predicted class is determined as

$$\hat{C} = \arg\max_{k} P(C_k \mid X) \quad ,_____ \quad (7)$$

The five output classes are C_0: Normal, C_1: DoS/DDoS, C_2: Probe/Scanning, C_3: Unauthorized Access, and C_4: Malware/Suspicious Traffic. The predicted intrusion class and attack probability are subsequently provided to the mathematical threat-assessment stage.

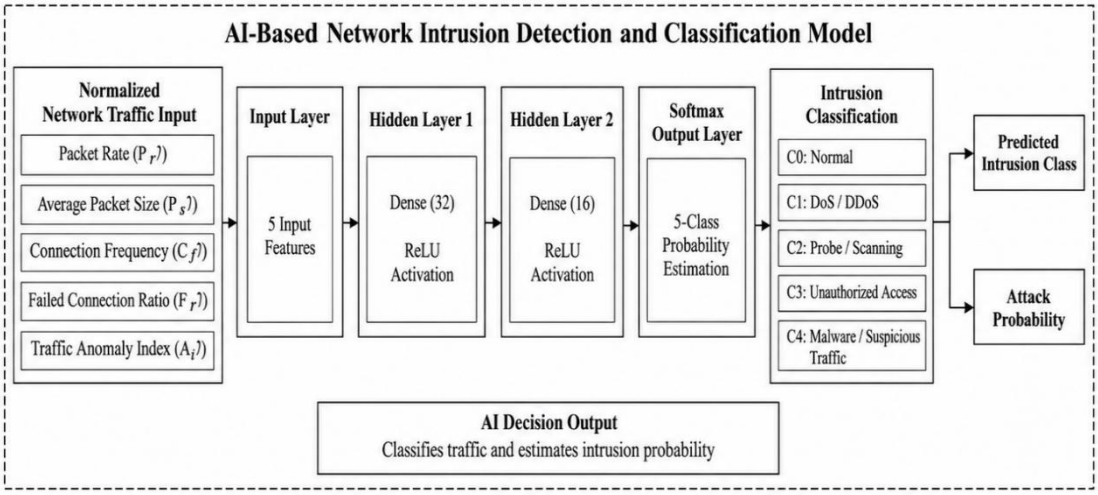


Fig. 2. AI-Based Network Intrusion Detection and Classification Model

3.3 Mathematical Threat-Risk Modelling

The mathematical threat-risk model translates the AI output into an understandable security rating for adaptive intrusion prevention. This model takes into account attack probability, attack severity, attack frequency, traffic anomaly level and network vulnerability. Table 2 gives a summary of the variables and weighting factors for the mathematical assessment.

Table 2. Mathematical Threat Variables, Definitions and Weighting Parameters

Variable	Symbol	Definition	Suggested Weight
Attack Probability	P_a	Probability that the observed traffic is malicious	0.35
Attack Severity	S_a	Estimated impact level of the detected attack	0.25
Attack Frequency	F_a	Frequency or repetition level of malicious activity	0.20
Traffic Anomaly Index	A_i	Degree of deviation from normal network behavior	0.20
Network Vulnerability	V_n	Exposure level of the affected network resource	Used in risk model

The attack probability is calculated by the highest probability in the malicious traffic classes:

$$P_a = \max_{k \neq 0} P(C_k \mid X) \quad ,_____ \quad (8)$$

A normalized threat intensity is then determined based on attack probability, severity, frequency, and anomaly data:

$$T = w_1 P_a + w_2 S_a + w_3 F_a + w_4 A_i \quad ,_____ \quad (9)$$

where the weighting coefficients satisfy

$$\sum_{i=1}^{4} w_i = 1 \quad ,_____ \quad (10)$$

with $w_1 = 0.35$, $w_2 = 0.25$, $w_3 = 0.20$, and $w_4 = 0.20$.

The network security risk is determined by:

$$R = P_a S_a V_n \quad , _____ \quad (11)$$

where V_n denotes the normalized level of vulnerability of the affected network-side resource. At last, the threat intensity and mathematical risk are combined to get the hybrid threat score:

$$H = \alpha T + (1 - \alpha) R \quad , _____ \quad (12)$$

where H represents the final hybrid threat score and $0 \leq \alpha \leq 1$. The calculated score is subsequently used by the adaptive security mechanism to select the right intrusion prevention action.

3.4 Adaptive Intrusion Prevention Decision Model

The hybrid threat score is used to determine the required security response. The AI output along with attack severity, frequency, anomaly level and network vulnerability result in an estimation of threat intensity, risk score and final hybrid threat score H as shown in Figure 3 below. The adaptive prevention decision is determined as

$$A(H) = \begin{cases} A_0, & 0 \leq H < 0.20 \\ A_1, & 0.20 \leq H < 0.40 \\ A_2, & 0.40 \leq H < 0.60 \\ A_3, & 0.60 \leq H < 0.80 \\ A_4, & H \geq 0.80 \end{cases} \quad , _____ \quad (13)$$

where A_0 to A_4 represent increasingly stronger security responses. The corresponding threat levels and prevention actions are summarized in Table 3. Normal traffic is allowed, low-risk traffic is monitored, moderate threats result in rate limiting, high threats result in temporary blocking, critical threats result in blocking and isolation. Security policy is updated by a feedback mechanism depending on the selected answer.

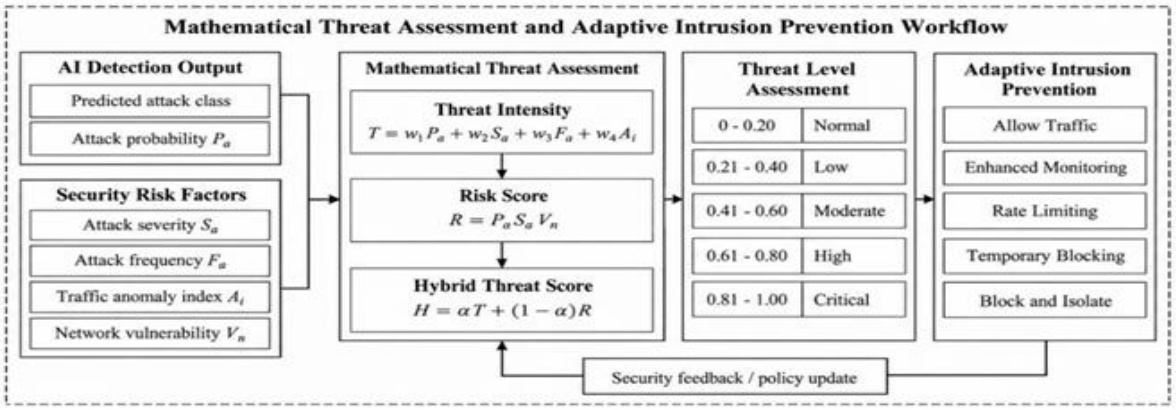


Fig. 3. Mathematical Threat Assessment and Adaptive Intrusion Prevention Workflow

Table 3. Hybrid Threat Levels and Corresponding Adaptive Prevention Actions

Hybrid Threat Score	Threat Level	Adaptive Prevention Action
0.00–0.20	Normal	Allow Traffic
0.21–0.40	Low	Enhanced Monitoring
0.41–0.60	Moderate	Rate Limiting
0.61–0.80	High	Temporary Blocking
0.81–1.00	Critical	Block and Isolate

4. Results And Discussion

4.1 Intrusion Detection Performance

The intrusion detection performance of the proposed framework is evaluated using accuracy, precision, recall, F1-score, false positive rate, and prevention rate. The comparative results are summarized below in Tabular Form as Table 4. The proposed Hybrid AI–Mathematical Approach recorded the highest accuracy and precision of 97.6% and 97.1% respectively, and retained the same high recall and f1-scores of 96.8% and 96.9%

respectively. It has also the lowest false positive rate of 2.4% and the highest prevention rate of 96.2%. The proposed framework demonstrated the detection reliability which is more stable compared to the three other frameworks, Rule Based IDS, Conventional ML IDS and AI-Only IDS, when dealing with normal and attack traffic. The enhanced capabilities stem primarily from the combining of AI classification of intrusions with mathematical threat assessment and adaptive prevention to limit false alarms and increase the accuracy of identifying and managing malicious traffic.

Table 4. Comparative Intrusion Detection and Prevention Performance

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)	Prevention Rate (%)
Rule-Based IDS	88.4	87.6	85.9	86.7	7.8	82.5
Conventional ML IDS	92.1	91.5	90.8	91.1	5.6	87.9
AI-Only IDS	95.3	94.8	94.2	94.5	3.9	91.8
Proposed Hybrid AI–Mathematical Approach	97.6	97.1	96.8	96.9	2.4	96.2

4.2 Attack-Type Classification Analysis

The class-wise classification performance of the proposed AI model is presented in Figure 4. The model is able to separate normal traffic, DoS/DDoS, Probe/Scanning, Unauthorized Access and Malware/Suspicious Traffic. Normal traffic gets the best precision (98.4%), recall (98.1%) and F1-score (98.2%). The results of classification of DoS/DDoS are also excellent with accuracy of 97.9% and F1 score of 97.7%. Probe/Scanning has an F1-score of 96.6%, and Unauthorized Access has an F1-score of 95.9%. In case of Malware/Suspicious Traffic, the lowest performance comes in terms of precision (95.7%), recall (95.3%) and F1-score (95.5%), which means the host malware and suspicious traffic are comparatively harder to classify due to overlapping characteristics of traffic. In general, as can be seen in Figure 4, the classification accuracy of the proposed model does not drop significantly when used to classify network traffic in the different considered attack classes and network traffic classes.

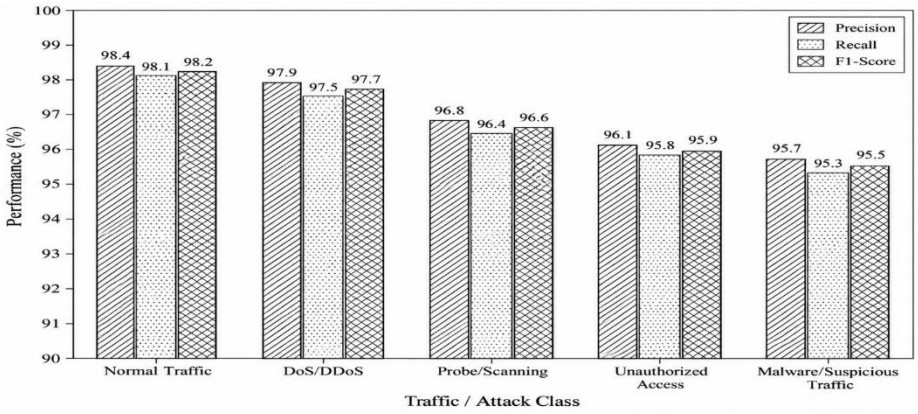


Fig. 4. Classification Performance across Different Network Traffic and Attack Classes

4.3 Mathematical Threat and Risk Assessment

The mathematical threat model analyzes various network scenarios in terms of attack probability, threat intensity, risk score, and hybrid threat score. The lowest are for normal traffic, the highest are for high rate and mild scanning. Severe attacks of DoS and DDoS, unauthorized access and combined severe attacks expose the largest risk as they increase the likelihood of an attack, severity, frequency, anomaly level and vulnerability. The model is able to distinguish between low and high-risk network states therefore facilitating more reliable adaptive security decisions.

4.4 Adaptive Intrusion Prevention Performance

The adaptive prevention mechanism determines the actions based on the computed hybrid threat level. Normal traffic can resume, low risk defined as 'watchful waiting' is subject to monitoring, moderate risk is subject to 'rate limiting', high risk traffic is temporarily restricted and critical traffic is blocked and isolated. The results (Table 4) suggest that the proposed approach has a prevention success rate of 96.2%, a false-positive rate of 2.4%. This means that only highly suggestive attacks are being blocked, and not low risk attacks unnecessarily.

4.5 Comparative Discussion and Computational Performance

The proposed Hybrid AI – Mathematical Approach is better than the Rule Based IDS, Conventional ML IDS, and AI-Only IDS. From Table 4, it has 97.6% accuracy, 97.1% precision, 96.8% recall, 96.9% F1-score and prevention rate of 96.2%, and the false positive rate of 2.4%. The AI is used to identify traffic patterns, and the mathematical model transforms the AI's detection result into a meaningful threat score for adaptive response control. Though the framework is more flexible and transparent in terms of decisions, its foundation is dependent on weighting parameters and selection of the threshold, as well as evolving attack distributions.

5. Conclusion

This study developed a hybrid AI and mathematical modelling framework for adaptive network security and intrusion prevention. The idea will be based on AI-based multiclass intrusion detection and quantitative threat and risk estimation to facilitate a structured security decision-making process. The AI model categorizes network traffic as normal or multiple types of attacks; the mathematical component analyzes the probabilities of attacks, attack's severity, attack's frequency, anomaly level and network vulnerability and calculates an interpretable hybrid threat score. Adaptive prevention actions, such as normal traffic allowance, monitoring improvements, rate limiting, temporary blocking, and full isolation are directly proportional to the calculated threat score. This integration allows the framework to take more action on extreme attacks, and not over block any low risk or even legitimate traffic. The comparative evaluation revealed the increased detection accuracy, F1-score, prevention success rate and reduced false-positive rate when compared to rule-based, conventional machine-learning and AI-only methods. The overall framework combines both intelligent intrusion recognition and mathematically controlled response selection and it offers an adaptable and interpretable solution for network security applications. The framework can be expanded in future by integrating online learning, explainable AI, other categories of attacks, optimizing the thresholds, embedding in a distributed network environment, and real-time deployment.

References

1. Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, *189*, 105124.

2. Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2013). Network anomaly detection: methods, systems and tools. *Ieee communications surveys & tutorials*, *16*(1), 303-336.

3. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, *50*, 102419.

4. Mishra, P., Varadharajan, V., Tupakula, U., & Pilli, E. S. (2018). A detailed investigation and analysis of using machine learning techniques for intrusion detection. *IEEE communications surveys & tutorials*, *21*(1), 686-728.

5. Pajouh, H. H., Javidan, R., Khayami, R., Dehghantanha, A., & Choo, K. K. R. (2016). A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks. *IEEE Transactions on Emerging Topics in Computing*, *7*(2), 314-323.

6. Shiravi, A., Shiravi, H., Tavallaee, M., & Ghorbani, A. A. (2012). Toward developing a systematic approach to generate benchmark datasets for intrusion detection. *computers & security*, *31*(3), 357-374.

7. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE access*, *7*, 41525-41550.

8. Wang, Z., Chen, L., Song, S., Cong, P. X., & Ruan, Q. (2020). Automatic cyber security risk assessment based on fuzzy fractional ordinary differential equations. *Alexandria Engineering Journal*, *59*(4), 2725-2731.

9. Wazid, M., & Das, A. K. (2016). An efficient hybrid anomaly detection scheme using K-means clustering for wireless sensor networks. *Wireless Personal Communications*, *90*(4), 1971-2000.

10. Wu, S. X., & Banzhaf, W. (2010). The use of computational intelligence in intrusion detection systems: A review. *Applied soft computing*, *10*(1), 1-35.