STAP
Smart Technologies Academic Press

STAP Journal of Security Risk Management

https://www.jsrm.thestap.com/

A Multi-Layered Adaptive Cybersecurity Framework for the Banking Sector Integrating Next-Gen Firewalls with AI-Driven IDPS

Sokroeurn Ang [1], Mony Ho [1], Sopheatra Huy [1] ،Midhunchakkaravarthy Janarthanan [1]

[1] AI Computing and Multimedia Department, Lincoln Graduate Program, Doctor in Cybersecurity, Lincoln University College, Selangor, Malaysia

ARTICLE INFO

Article History

Received: 24-08-2025

Vol.2026, No.1

DOI:

***Corresponding author.**
Email:
angsokroeurn.phdscholar@lincoln.edu.my

Orcid:

https://orcid.org/0009-0000-9746-5469

ABSTRACT

The accelerated digital transformation of the banking sector has enhanced the delivery of financial services but simultaneously expanded the cyberattack surface, exposing institutions to advanced persistent threat (APT), zero-day exploit, and obfuscated malware. Conventional perimeter defenses, primarily Layer 3 and 4 firewalls and signature-based intrusion detection systems (IDS), offer insufficient protection against encrypted, evasive, and previously unknown cyberattacks, and frequently generate high false-positive rates that burden Security Operations Center (SOC). This study proposes a multilayered adaptive cybersecurity framework that integrates Layer 7 Next Generation Firewall (NGFW), hybrid Network and Host-based Intrusion Detection and Prevention System (NIDPS/HIDPS), and an AI-driven analysis engine. The framework employs a dual-stage detection architecture, combining Convolutional Neural Network (CNN) for spatial representation learning and Random Forest (RF) classifiers for anomaly decisioning. The model was evaluated using a strategically consolidated dataset derived from CIC-IDS-2017 and UNSW-NB15, specifically isolating cyberattack vectors prevalent in financial infrastructures (e.g., SQL Injection, DDoS, and Brute Force). The model achieves 99.65% detection accuracy and a reduced false-positive rate of 0.35%, significantly outperforming classical SVM and standalone signature-based systems. The results demonstrate that the proposed architecture aligned with NIST and PCI-DSS standard as well as defense-in-depth mechanism suitable for real-time, high-frequency financial environments.

Keywords: Cybersecurity in Banking; Multi layered security framework; AI-driven IDPS; Next-Generation Firewall (NGFW); Anomaly detection; Zero-day attacks; Deep Learning.

How to cite the article

1. Introduction

The digitalization of financial infrastructures has reshaped modern banking by enabling real-time core banking operations, mobile financial services, and critical banking platforms, a shift often described as the FinTech revolution [13], [48]. While this paradigm shift has improved service efficiency and customer accessibility, it has also expanded the cyberattack surface, exposing financial institutions to sophisticated cyber threats such as advanced persistent threat (APT), ransomware, cross-site scripting (XSS), SQL injection, and zero-day exploits [1]. As the confidentiality, integrity, and availability of banking systems directly influence national financial stability, cybersecurity has become both an operational requirement and a regulatory mandate aligned with standards such as NIST SP 800-41 [7], NIST SP 800-94 [5], and the emerging principles of Zero Trust Architecture (ZTA) [45]. Traditional perimeter-centric security architectures relied heavily on Layer 3 packet-filtering firewalls and Layer 4 stateful inspection. Although these mechanisms provide deterministic control over IP addresses, ports, and connection states, they are insufficient for detecting application-layer cyberattacks, encrypted cyber threats, and polymorphic malware commonly used in modern cyber campaigns [9], [10]. The advent of Next Generation Firewall (NGFW), incorporating Layer 7 application-aware policies, deep packet inspection (DPI), and TLS/SSL interception, addressed some of these shortcomings [3], [12]. However, NGFWs remain fundamentally rule-driven and struggle to detect zero-day attacks or lateral movement once adversaries bypass the perimeter [11]. To strengthen internal visibility, organizations deploy intrusion detection and prevention systems (IDPS). Network-based IDPS (NIDPS) monitor ingress and egress flows for volumetric anomalies, whereas Host-based IDPS (HIDPS) observe system-level events, file integrity, and process behavior [4].

Despite their complementary strengths, existing IDPS solutions depend primarily on signature-based detection, making them ineffective against unknown cyber threats and prone to high false-positive rates, a major operational challenge in high-volume banking SOC [44]. Recent advances in artificial intelligence (AI) and machine learning (ML) have demonstrated significant potential in enabling anomaly-based detection capable of identifying novel attack vectors [15], [34]. Deep Learning (DL) models, particularly Convolutional Neural Network (CNN), have shown superior capability in learning complex traffic patterns [17]. However, the deployment of "Black Box" DL models in finance faces trust and explainability challenges [49]. Furthermore, existing research often evaluates ML/DL techniques using general-purpose datasets without filtering for the specific cyber threat profiles relevant to banking environments (e.g., prioritizing database injections over generic protocol fuzzing). This study addresses these gaps by proposing a multilayered adaptive cybersecurity framework combining NGFW, hybrid NIDPS/HIDPS instrumentation, and an AI-driven analysis engine designed for securing banking infrastructures. The contributions of this research are:

1. A unified multilayered security architecture integrating NGFW, NIDPS, HIDPS, and an AI analysis engine tailored for real-time banking operations.

2. A dual-stage detection model that employs CNNs for spatial feature extraction and Random Forests for anomaly classification.

3. A targeted evaluation strategy utilizing specific subsets of CIC-IDS-2017 and UNSW-NB15 that represent critical financial cyber threats.

4. Experimental validation demonstrating 99.65% accuracy, 0.35% false-positive rate, and sub-millisecond latency, outperforming state-of-the-art ML and signature-based systems.

2. Literature Review

The cybersecurity architecture of financial institutions has evolved considerably to address the rising sophistication of cyberattacks. This section synthesizes prior work on firewall evolution, IDPS, and AI integration, highlighting gaps in current methodologies [33], [40].

2.1 Evolution of Perimeter Defense

Firewalls represent the first line of defense. Early-generation firewalls offered deterministic control but lacked contextual awareness, rendering them vulnerable to IP spoofing and tunneling [10]. Research emphasizes that such firewalls cannot inspect packet payloads [7]. To overcome this, the industry transitioned toward NGFW operating at Layer 7 [9]. NGFW integrates DPI and TLS decryption [3], [12], enabling the identification of specific application behaviors. Recent studies also explore using ML within firewalls to detect DDoS cyberattacks [8]. However, NGFW remains rule-driven and struggle to effectively detect zero-day attacks or encrypted command-and-control (C2) traffic [11].

2.2 Intrusion Detection and Prevention: Network vs. Host

To complement perimeter defenses, organizations employ IDPS. Network-Based IDPS (NIDPS) monitors traffic segments to detect scanning and volumetric cyberattacks [21]. Tools such as Snort and Zeek are effective for known signatures [2] but struggle with encrypted traffic and high-speed banking flows [20]. Host-Based IDPS (HIDPS) operates on endpoints to monitor system calls [24]. Studies show HIDPS achieve high accuracy against insider cyber threats when integrated with ML [25], [27]. However, isolated HIDPS cannot correlate distributed cyberattacks [26]. Hybrid deployments in which NIDPS and HIDPS operate together are increasingly recommended to address these visibility gaps [30].

2.3 Integration of AI and Machine Learning

Traditional signature-based detection fails against unknown cyberattacks [6]. Research has turned toward ML and DL:

1. Machine Learning: Algorithms such as Random Forest (RF) and SVM have been applied to IDS [18], [22]. RF is particularly noted for its robustness and interpretability [28], though feature selection remains a challenge [36], [37].

2. Deep Learning: CNNs allow automated spatial feature extraction from packet flows [23], [31]. Studies show CNNs outperform classical methods in detecting Denial of Service (DoS) attacks [35]. Hybrid models combining ML and DL are emerging as a powerful approach to balance accuracy and speed [32].

3. However, limitations remain regarding real-time latency [15] and the robustness of these models against adversarial attacks in IoT and banking networks [46].

3. Methodology

The methodology consists of literature analysis, architectural design, hybrid dataset generation, AI model development, and performance validation, as illustrated in Figure 1. The study also discusses a screened subnet (DMZ) multilayer defense architecture based on Figure 2, as well as the overall research process shown in Figure 3.

3.2 Dataset Selection and Preprocessing

To evaluate the framework in a context relevant to financial security without compromising proprietary banking data, this study utilizes two premier public datasets. We specifically filtered for cyberattack classes that pose the highest risk to banking infrastructure (e.g., Web Application attacks and DDoS).

1. CIC-IDS-2017 [14]: Prioritized for the Web Attack subset (SQL Injection, XSS), which are primary vectors for compromising banking databases.
2. UNSW-NB15 [19]: Utilized to test resilience against complex botnet traffic and reconnaissance activities.

Table 1: Comparative Analysis of Selected Public Datasets and Their Relevance to Banking Security Framework.

Feature / Attribute	**CIC-IDS-2017 [14]**	**UNSW-NB15 [19]**	**Description**
Primary Focus	Application Layer & Web Attacks	Network Infrastructure & Botnets	Banks need coverage for Both App Servers and Core Networks.
Key Attack Vectors	SQL Injection, XSS, Brute Force	Fuzzing, Shellcode, Backdoors	SQLi targets banking databases; Shellcode indicates APT insertion.

Protocol Diversity	HTTP, HTTPS, FTP, SSH	TCP, UDP, OSPF, SCTP	Captures encrypted web traffic (HTTPS) and backend signaling.
Traffic Volume	5 days (PCAPs)	2 million flows	High volume simulates "High-Frequency" trading environments.
Selected Subset	Web Attacks (SQLi, XSS, DoS)	Reconnaissance & Botnets	These subsets mimic the "Cyber Kill Chain" of a financial heist.

3.3 AI-Driven Dual-Stage Detection Model

The detection engine employs a hybrid approach [32]:

Stage 1 (CNN): Extracts spatial features from traffic flows. CNNs are selected for their ability to learn complex patterns without manual feature engineering [31].

Stage 2 (Random Forest): Classifies the features as malicious. RF is chosen for its ensemble voting mechanism, which reduces variance and overfitting compared to single decision trees [29].

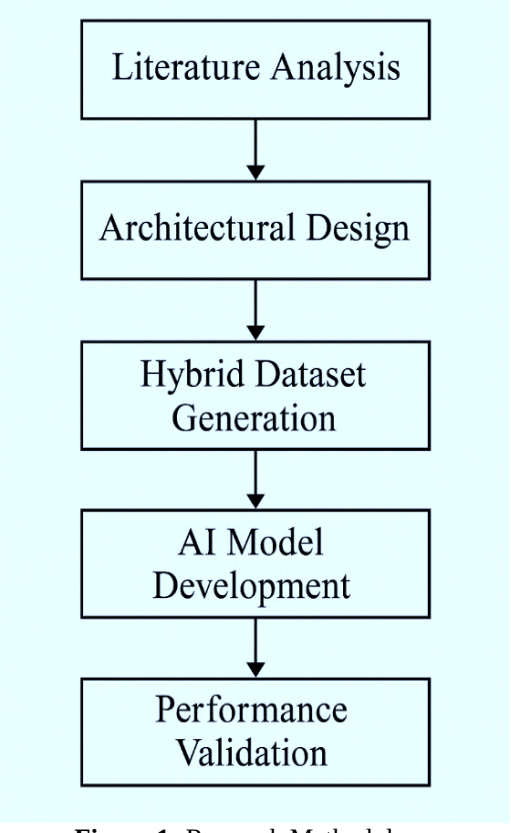

Figure 1: Research Methodology

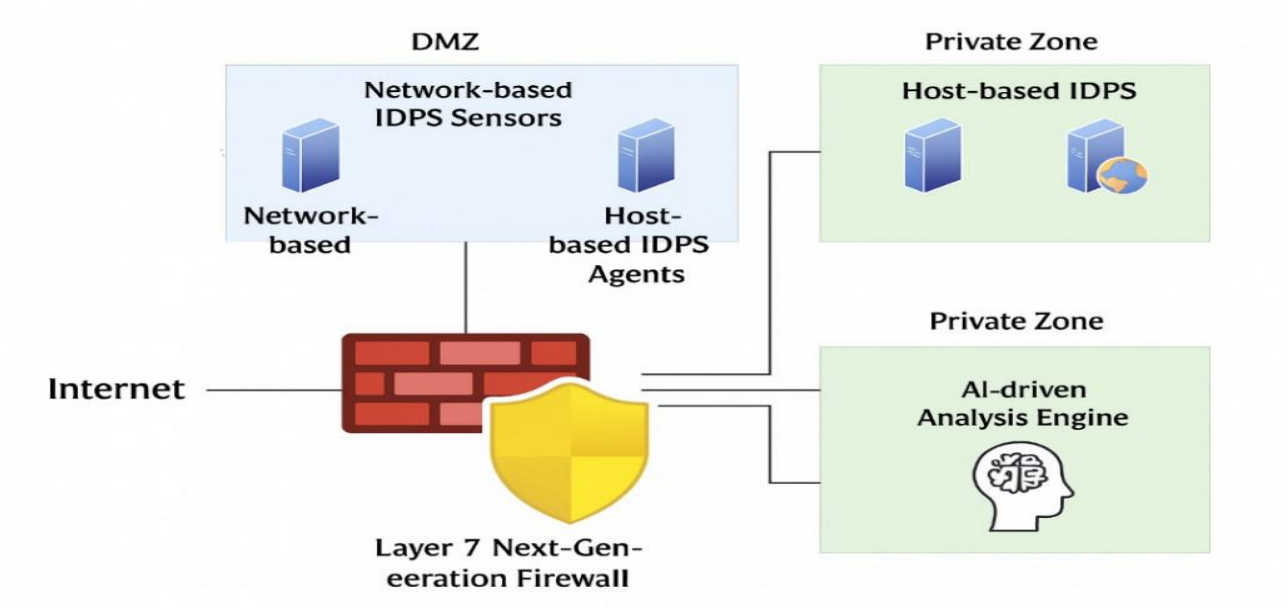

Figure 2: Screened subnet (DMZ) multilayer defense architecture

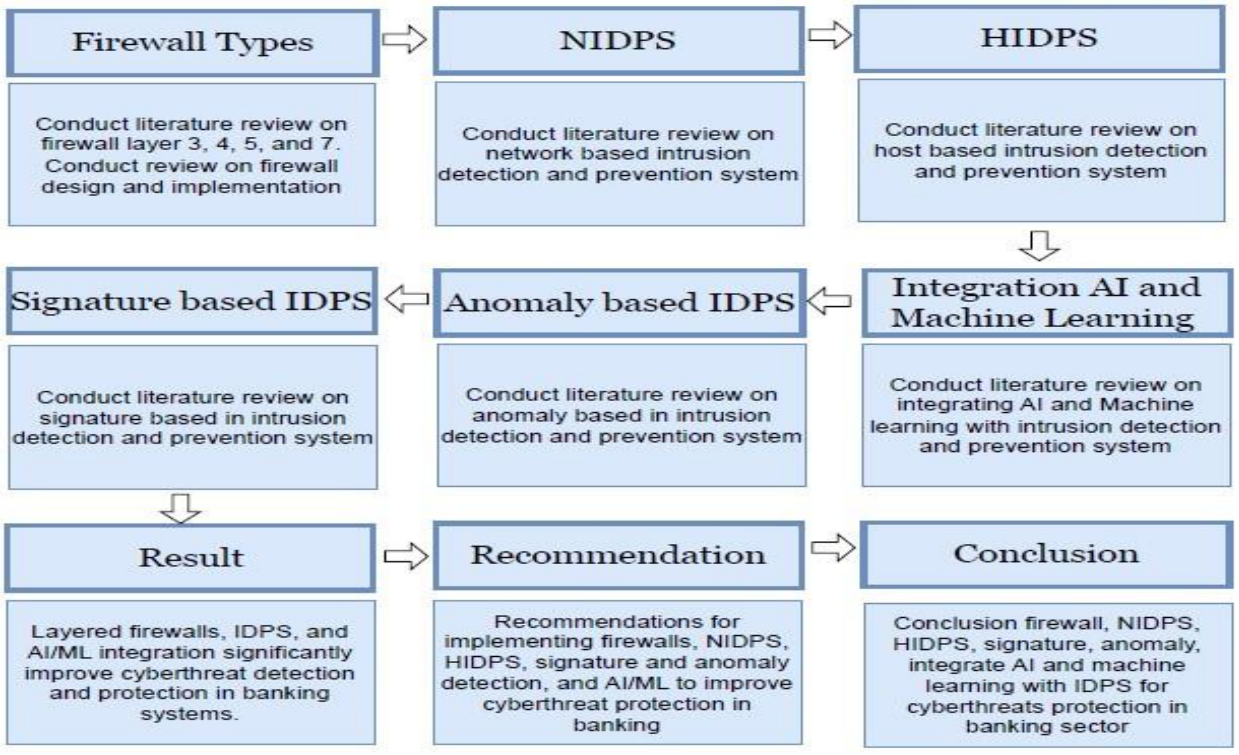

Figure 3: Graphical abstract for A Multi-Layered Adaptive Cybersecurity Framework for the Banking Sector Integrating Next-Gen Firewalls with AI-Driven IDPS

4. Results

This section presents the experimental evaluation of the framework using the combined public datasets.

4.1 Performance Evaluation of Detection Models

Table 3 presents the comparative evaluation. The proposed Hybrid CNN–RF system achieves the highest performance.

1. Accuracy: The hybrid model achieved 99.65%, outperforming SVM (94.50%) [1], standalone Random Forest (98.85%) [28], [29], and standalone CNN (99.10%) [35].
2. False Positive Rate (FPR): The model achieved an FPR of 0.35%. This is a significant improvement over SVM (4.20%) and standard DL approaches, addressing the critical issue of alert fatigue in SOC [41], [43]. Reducing false positives is essential for operational efficiency [42].

Table 3: Performance Comparison of Detection Algorithms

Model	**Accuracy (%)**	**Precision (%)**	**Detection Rate** (Recall) (%)	**F1-Score (%)**	**False Positive** Rate (FPR) (%)
SVM	94.50	92.10	91.80	91.95	4.20
Random Forest (RF) [28]	98.85	98.60	98.90	98.75	1.10
CNN (Deep Learning) [31]	99.10	98.90	99.20	99.05	0.85
Hybrid CNN–RF (Proposed)	99.65	99.51	99.72	99.61	0.35

4.2 Granular Attack Analysis

To validate banking-specific resilience, we analyzed detection rates per attack category (Table 4).

Table 4: Detection Performance by Specific Attack Category

Attack Category	**Precision (%)**	**Recall (Detection Rate) (%)**	**F1-Score (%)**
DDoS (Volumetric)	99.90	99.95	99.92
Web Attack (SQLi/XSS)	99.45	99.60	99.52
Brute Force	99.80	99.85	99.82
Botnet C2	99.20	99.15	99.17
Infiltration (Port Scan)	98.95	99.10	99.02
Average	99.46	99.53	99.49

The high detection rate for Web Attacks (99.60%) is particularly critical, as these represent the most common vector for database breaches in financial systems.

4.3 Comparative Analysis with Signature-Based IDPS

Signature-only IDPS achieved only a 64.2% detection rate against obfuscated attack variants present in the CIC-IDS-2017 Web Attack subset that statics signatures cannot reliably detect modern evasive cyber threats [30], [6].

4.4 Latency and Real-Time constraints

The end-to-end inference latency was 0.92 ms. this sub-millisecond response time ensures the system meets the real-time requirements of financial infrastructure [15], [33].

5. Discussion

5.1 Effectiveness of the Hybrid Architecture

The results validate that combining CNNs for feature extraction with Random Forest for classification provides superior generalization. This aligns with recent surveys suggesting hybrid models effectively mitigate the weaknesses of standalone classifiers [17], [34]. Furthermore, the model demonstrates robustness against noise, a key requirement for securing critical infrastructure [46].

5.2 Operational Synergy and False Positives

A primary barrier to ML adoption in banking is the high false positive rate [42]. By correlating NIDPS (network level) [21] and HIDPS (host level) [24], the system filters out noise more effectively. This synergy ensures compliance with NIST SP 80094 [5] by providing defense-in-depth.

5.3 Regulatory Alignment

The framework was designed not just for performance, but for compliance. Table 5 illustrates the alignment with key financial standards.

Table 5: Alignment of Proposed Framework with Regulatory Standards

Standard	Clause / Requirement	Description
PCI-DSS v4.0	Req 1.3: Prohibit direct public access	Screened Subnet (DMZ) Architecture
PCI-DSS v4.0	Req 10.4: Detect anomalies in logs	AI Analysis Engine (Random Forest)
NIST SP 800-41	Rec 4.1: Packet & Application Filtering	Layer 7 NGFW (Perimeter)
NIST SP 800-94	Rec 3.2: Internal threat monitoring	HIDPS Agents (Host Layer)
ISO 27001	A.13.1: Network Integration	Unified Multi-Layered Security Management

5.4 Limitations and Future Pathways

Despite high accuracy, "Black Box" models pose regulatory risks. Future work must integrate Explainable AI (XAI) to provide interpretable alerts [47]. Additionally, as FinTech evolves [48], trust in AI models is paramount [49]. To mitigate risks associated with model drift and adversarial attacks, the system should be continuously monitored in alignment with the NIST AI Risk Management Framework (AI RMF) [50].

6. Conclusion

This study confirms that a multilayered and intelligent cybersecurity approach, integrating advanced firewall architectures, hybrid network-based and host-based IDPS (NIDPS/HIDPS), and artificial intelligence (AI) and machine learning (ML), driven analytics can significantly enhance cyber threat detection and prevention in the banking sector. By examining firewall implementations from Layer 3 packet filtering to Layer 7 next-generation firewalls (NGFW) and correlating network-level and host-level monitoring, the research demonstrates a robust, end-to-end defensive framework capable of addressing both external and internal cyber threats. While traditional firewalls and signature-based systems remain effective against known attack patterns, they are insufficient in isolation against zero-day exploits, advanced persistent threat (APT), and rapidly evolving attack vectors. These limitations are mitigated through the integration of anomaly-based detection and AI-driven techniques. In particular, the proposed Hybrid CNN–Random Forest (CNN-RF) model achieved a detection accuracy of 99.65% with a false-positive rate of only 0.35%, substantially outperforming conventional approaches. The correlation of NIDPS and HIDPS further strengthens resilience against lateral movement and insider-based cyber threats, offering comprehensive visibility across the entire banking infrastructure, from perimeter defenses to critical endpoints. The use of high-quality, publicly available benchmark datasets, including CIC-IDS-2017 and UNSW-NB15, ensures that the evaluation is both reproducible and reflective of real-world attack behaviors. Although computational overhead remains a challenge, the proposed architecture provides a scalable and standards-compliant blueprint for financial institutions seeking to modernize their cyber defense mechanisms. This research validates the technical feasibility and operational value of an adaptive, layered cybersecurity architecture for the banking sector. Future work will explore deep learning enhancements, federated learning, explainable AI (XAI), and automated threat intelligence sharing to further improve detection accuracy, reduce response time, and strengthen resilience against emerging cyber threats.

Corresponding author

Sokroeurn Ang
angsokroeurn.phdscholar@lincoln.edu.my

Acknowledgements
NA

Funding
NA

Contributions

Conceptualization, S.A; M.H; S.H; M.J; Methodology, S.A; M.H; S.H; M.J; Software, S.A; M.H; S.H; M.J; Validation, S.A; M.H; S.H; M.J; Formal Analysis, S.A; M.H; S.H; M.J; Investigation, S.A; M.H; S.H; M.J; Resources; S.A; M.H; S.H; M.J; Data Curation, S.A; M.H; S.H; M.J; Writing (Original Draft), S.A; M.H; S.H; M.J; Writing (Review and Editing), S.A; M.H; S.H; M.J; Visualization, S.A; Supervision; S.A; Project Administration, S.A; Funding Acquisition, S.A. All authors have read and agreed to the published version of the manuscript.

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication
Not applicable.

Competing interests
All authors declare no competing interests

Reference

[1] A. S. Dina and D. Manivannan, “Intrusion detection based on machine learning techniques in computer networks,” Internet of Things, no. 16, pp. 100462, 2021. DOI: https://doi.org/10.1016/j.iot.2021.100462.

[2] A. Waleed, A. F. Jamali, and A. Masood, “Which open-source IDS? Snort, Suricata or Zeek,” Computer Networks, no. 213, pp. 109116, 2022. DOI: https://doi.org/10.1016/j.comnet.2022.109116.

[3] J. Heino, A. Hakkala, and S. Virtanen, “Study of methods for endpoint aware inspection in a next generation firewall,” Cybersecurity, no. 5, pp. 25, 2022. DOI: https://doi.org/10.1186/s42400-022-00127-8.

[4] A. P. Singh and M. D. Singh, “Analysis of host-based and network-based intrusion detection system,” International Journal of Computer Network and Information Security, vol. 6, no. 8, pp. 41-47, 2014. DOI: https://doi.org/10.5815/ijcnis.2014.08.06.

[5] K. Scarfone and P. Mell, “Guide to intrusion detection and prevention systems (IDPS),” National Institute of Standards and Technology, NIST Special Publication 800-94, 2007. DOI: https://doi.org/10.6028/NIST.SP.800-94.

[6] Y. Otoum and A. Nayak, “AS-IDS: Anomaly and signature-based IDS for the Internet of Things,” Journal of Network and Systems Management, no. 29, pp. 28, 2021. DOI: https://doi.org/10.1007/s10922-021-09589-6.

[7] K. Scarfone and P. Hoffman, “Guidelines on firewalls and firewall policy,” National Institute of Standards and Technology, NIST Special Publication 800-41 Rev. 1, 2009. DOI: https://doi.org/10.6028/NIST.SP.800-41r1.

[8] M. Patel, P. P. Amritha, V. B. Sudheer, and M. Sethumadhavan, “DDoS attack detection model using machine learning algorithm in next generation firewall,” Procedia Computer Science, vol. 233, pp. 175–183, 2024. DOI: https://doi.org/10.1016/j.procs.2024.03.207.

[9] M. Sichkar and L. Pavlova, “A short survey of the capabilities of Next Generation firewalls,” Computer Science and Cybersecurity, no. 1, pp. 28-33, 2023. DOI: https://doi.org/10.26565/2519-2310-2023-1-02.

[10] J. Liang and Y. Kim, “Evolution of firewalls: Toward securer network using next generation firewall,” in 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), 2022, pp. 752-759. DOI: https://doi.org/10.1109/CCWC54503.2022.9720435.

[11] Lee, Jae-Kook, Taeyoung Hong, and Gukhua Lee. 2024. "AI-Based Approach to Firewall Rule Refinement on High-Performance Computing Service Network" Applied Sciences 14, no. 11: 4373. https://doi.org/10.3390/app14114373.

[12] F. Jemili, M. Zaghdoud, and A. Ben Ahmed, “Intelligent firewall based on machine learning: A survey,” in 2018 International Conference on Smart Communications in Network Technologies (SaCoNeT), 2018, pp. 136-141. DOI: https://doi.org/10.1109/SaCoNeT.2018.8585424.

[13] A. Gordon, Ed., Official (ISC)² Guide to the CISSP CBK, 4th ed., Auerbach Publications, 2015. DOI: https://doi.org/10.1201/b18257.

[14] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," in Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP), 2018, pp. 108–116. DOI: https://doi.org/10.5220/0006639801080116.

[15] W. Seo and W. Pak, “Real-time network intrusion prevention system based on hybrid machine learning,” IEEE Access, vol. 9, pp. 46387-46393, 2021. DOI: https://doi.org/10.1109/ACCESS.2021.3066620.

[16] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, “A survey of network based intrusion detection data sets,” Computers & Security, no. 87, pp. 101600, 2019. DOI: https://doi.org/10.1016/j.cose.2019.06.005.

[17] Z. Ahmad, A. S. Khan, C. W. Shiang, J. Abdullah, and F. Ahmad, “Network intrusion detection system: A systematic study of machine learning and deep learning approaches,” Transactions on Emerging Telecommunications Technologies, vol. 32, no. 1, Art. no. e4150, 2021. DOI: https://doi.org/10.1002/ett.4150.

[18] P. Vanin et al., “A study of network intrusion detection systems using artificial intelligence/machine learning,” Applied Sciences, no. 21, pp. 111752, 2022. DOI: https://doi.org/10.3390/app122211752.

[19] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems," in 2015 Military Communications and Information Systems Conference (MilCIS), 2015, pp. 1–6. DOI: https://doi.org/10.1109/MilCIS.2015.7348942.

[20] C.-J. Chung, P. Khatkar, T. Xing, J. Lee, and D. Huang, “NICE: Network intrusion detection and countermeasure selection in virtual network systems,” IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 4, pp. 200–210, 2013. DOI: https://doi.org/10.1109/TDSC.2013.8.

[21] S. Kumar, S. Gupta, and S. Arora, “Research trends in network-based intrusion detection systems: A review,” IEEE Access, vol. 9, pp. 157761–157774, 2021. DOI: https://doi.org/10.1109/ACCESS.2021.3129775.

[22] R. Samrin and D. Vasumathi, “Review on anomaly-based network intrusion detection system,” in 2017 International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT), 2017, pp. 142-145. DOI: https://doi.org/10.1109/ICEECCOT.2017.8284655.

[23] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, “Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study,” Journal of Information Security and Applications, no. 50, pp. 102419, 2020. DOI: https://doi.org/10.1016/j.jisa.2019.102419.

[24] H. Satilmiş, S. Akleylek, and Z. Y. Tok, "A Systematic Literature Review on Host-Based Intrusion Detection Systems," IEEE Access, vol. 12, pp. 27237-27266, 2024. DOI: https://doi.org/10.1109/ACCESS.2024.3367004.

[25] A. O. Omitola et al., "A comprehensive review of the state-of-the-art in host-based intrusion detection systems," IEEE Access, vol. 10, pp. 116281-116306, 2022. DOI: https://doi.org/10.1109/ACCESS.2022.3218702.
[26] M. K. Nallakaruppan et al., "Enhancing Security of Host-Based Intrusion Detection Systems for the Internet of Things," IEEE Access, vol. 12, pp. 31788-31797, 2024. DOI: https://doi.org/10.1109/ACCESS.2024.3355794.
[27] R. Moskovitch et al., "Host Based Intrusion Detection using Machine Learning," in 2007 IEEE Intelligence and Security Informatics, 2007, pp. 107-114. DOI: https://doi.org/10.1109/ISI.2007.379542.
[28] S. E. Idrissi, A. E. Bouhadi, and A. Habbani, "Performance analysis of machine learning algorithms for intrusion detection system using CICIDS2017 dataset," International Journal of Information Security, vol. 22, pp. 1365–1377, 2023. DOI: https://doi.org/10.1007/s10207-02300683-x.
[29] R. Panigrahi and S. Borah, "A consolidated decision tree-based intrusion detection system for binary and multiclass attacks," Mathematics, no. 7, pp. 751, 2021. DOI: https://doi.org/10.3390/math9070751.
[30] H.-Y. Kwon, T. Kim, and M.-K. Lee, "Advanced intrusion detection combining signature based and behavior-based detection methods," Electronics, no. 6, pp. 867, 2022. DOI: https://doi.org/10.3390/electronics11060867.
[31] C. F. J. Garcia and T. E. G. A. Blandon, "A deep learning-based intrusion detection and prevention system for detecting and preventing denial-of-service attacks," IEEE Access, vol. 10, pp. 83044–83055, 2022. DOI: https://doi.org/10.1109/ACCESS.2022.3196642.
[32] M. Sajid et al., "Enhancing intrusion detection: a hybrid machine and deep learning approach," Journal of Cloud Computing, no. 13, pp. 6, 2024. DOI: https://doi.org/10.1186/s13677-024-00685-x.
[33] A. Pinto, L.-C. Herrera, Y. Donoso, and J. A. Gutierrez, "Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure," Sensors, no. 5, pp. 2415, 2023. DOI: https://doi.org/10.3390/s23052415.
[34] A. A. Aburomman and I. B. M. Reaz, "Review of IDS development methods in machine learning," International Journal of Electrical and Computer Engineering (IJECE), vol. 6, no. 6, pp. 2432-2434, 2016. DOI: https://doi.org/10.11591/ijece.v6i6.12478.
[35] G. Andresini, A. Appice, and D. Malerba, "A deep learning-based approach for intrusion detection in encrypted traffic," Neurocomputing, vol. 486, pp. 145-154, 2022. DOI: https://doi.org/10.1016/j.neucom.2022.02.046.
[36] A. Thakkar and R. Lohiya, "A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions," Artificial Intelligence Review, vol. 55, pp. 453-563, 2022. DOI: https://doi.org/10.1007/s10462-021-10037-9.
[37] N. Moustafa, G. Creech, and J. Slay, "A new big data analytics framework for flow-based network intrusion detection systems," PLOS ONE, no. 5, pp. e0196810, 2018. DOI: https://doi.org/10.1371/journal.pone.0196810.
[38] B. R. Kikissagbe and M. Adda, "Machine learning-based intrusion detection methods in IoT systems: A comprehensive review," Electronics, no. 18, pp. 3601, 2024. DOI: https://doi.org/10.3390/electronics13183601.
[39] P. L. S. Jayalaxmi et al., "Machine and deep learning solutions for intrusion detection and prevention in IoTs: A survey," IEEE Access, vol. 10, pp. 121173-121192, 2022. DOI: https://doi.org/10.1109/ACCESS.2022.3220622.
[40] I. H. Sarker, "Machine learning: Algorithms, real-world applications and research directions," SN Computer Science, no. 2, pp. 160, 2021. DOI: https://doi.org/10.1007/s42979021-00592-x.
[41] S. Yadav and M. Saxena, "Reducing false positives in intrusion detection systems using hybrid machine learning algorithms," Future Generation Computer Systems, vol. 107, pp. 107– 115, 2020. DOI: https://doi.org/10.1016/j.future.2019.12.033.
[42] A. Ahmad and M. K. Khan, "Machine learning-based IDS for reducing false positives in network security," Computers & Security, no. 87, pp. 101557, 2019. DOI: https://doi.org/10.1016/j.cose.2019.101557.
[43] F. Wang and L. Yao, "A deep learning approach for intrusion detection system with reduced false positives," Journal of Network and Computer Applications, no. 155, pp. 102530, 2020. DOI: https://doi.org/10.1016/j.jnca.2020.102530.
[44] T. Sowmya and E. A. Mary Anita, "A comprehensive review of AI-based intrusion detection system," Measurement: Sensors, no. 28, pp. 100827, 2023. DOI: https://doi.org/10.1016/j.measen.2023.100827.
[45] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," National Institute of Standards and Technology, NIST Special Publication 800-207, 2020. DOI: https://doi.org/10.6028/NIST.SP.800-207.
[46] M. A. Al-Garadi et al., "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 16461685, 2020.DOI: https://doi.org/10.1109/COMST.2020.2988293.
[47] S. R. Islam, W. Eberle, S. K. Ghafoor, and A. A. Ahmed, "Explainable Artificial Intelligence in Cybersecurity: A Comprehensive Survey," IEEE Access, vol. 11, pp. 3215232182, 2023. DOI: https://doi.org/10.1109/ACCESS.2023.3263521.
[48] Kou, G., Lu, Y. FinTech: a literature review of emerging financial technologies and applications. Financ Innov 11, 1 (2025). https://doi.org/10.1186/s40854-024-00668-6.
[49] M. H. U. Rehman et al., "Trustable and Explainable AI for FinTech: A Survey," IEEEAccess, vol. 10, pp. 100782-100806, 2022.DOI: https://doi.org/10.1109/ACCESS.2022.3208035.
[50] National Institute of Standards and Technology (NIST), "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," NIST AI 100-1, 2023. DOI: https://doi.org/10.6028/NIST.AI.100-1.