https://doi.org/10.65025/ICAIC26081d

Protection of Computer Systems and Networks Through Hybrid Algorithms for Network Intrusion Detection and Prevention

Vladimir Đokić[1*] , Dragana Đokić[1]
vladimirdjokic@unionnikolatesla.edu.rs, draganadjokic@unionnikolatesla.edu.rs,

[1]Faculty of Informatics and Computer science, University Union—Nikola Tesla, Belgrade, Serbia

https://orcid.org/0009-0004-9678-6999 (V. Đokić)
https://orcid.org/0000-0002-9206-2764 (D. Đokić)

Abstract

The rapid growth of networked digital infrastructure has correspondingly expanded the threat surface accessible to hostile actors, rendering comprehensive intrusion detection and prevention capabilities a strategic necessity for any organization. This paper examines the application of hybrid algorithms — combining rule-based, statistical, and machine learning approaches — within firewall, intrusion detection system (IDS), and intrusion prevention system (IPS) architectures. Through a comparative analysis of detection methodologies and empirical performance data, the study demonstrates that hybrid approaches consistently outperform single-method systems, achieving detection rates of 94–99 percent while reducing false positive rates to below 4 percent. The paper provides a structured taxonomy of network attack categories, analyzes the complementary strengths of signature-based and anomaly-based detection, and evaluates the integration of deep learning classifiers into contemporary network security systems. The findings indicate that layered hybrid architectures represent the current operational standard for comprehensive network protection.

Keywords: network security, hybrid algorithms, firewall, intrusion detection system, intrusion prevention system, anomaly detection, machine learning, deep learning, network intrusion.

Introduction

Contemporary organizations manage increasingly complex and geographically distributed digital infrastructures that are subject to a growing volume and diversity of cyber threats. As business-critical operations continue shifting toward networked platforms — spanning cloud deployments, operational technology, and mobile endpoints — the set of exploitable entry points available to adversaries has grown proportionally, elevating the potential consequences of insufficient perimeter security to a level that can undermine an organization's ability to sustain operations.

Network security architectures have traditionally relied on three primary defensive mechanisms: firewalls, whose function is to regulate inbound and outbound traffic flows according to defined security rules at the network perimeter; intrusion detection systems (IDS), which perform continuous inspection of network traffic streams in search of behavioral indicators linked to adversarial activity; and intrusion prevention systems (IPS), which extend IDS by taking active countermeasures — terminating suspect connections or discarding hostile packets — rather than confining their role to

alert generation. While these mechanisms have proven effective against known attack patterns, the increasing sophistication of modern threats — including zero-day exploits, advanced persistent threats (APTs), and polymorphic malware — has brought to light the inherent shortcomings of defenses that depend solely on pre-compiled attack signatures or immutable filtering policies.

The relationship between information system security and organizational resilience has been extensively studied in the context of emergency planning and business continuity. As Đokić V. (2025) argues in his doctoral research on electronic sensor shields of computer systems in emergency situations:

> *"The security of information systems is crucial in the digital age, and private companies — both small and large — must implement measures combining physical, IT, and mobile container protection to create a secure data network capable of withstanding the increasingly frequent attacks on information systems that are occurring today" (Đokić V., 2025, p. 3).*

This perspective is directly applicable to the network security domain: the layered logic of combining physical, procedural, and algorithmic protections that underpins the electronic sensor shield concept maps directly onto the hybrid algorithmic architectures examined in this paper. Moreover, the software dimension of organizational security extends beyond purely technical countermeasures. As Đokić D. (2026) demonstrates in her research on encapsulated software tools in contemporary teaching, the adoption of any integrated software solution — including security platforms — requires structured attention to implementation conditions:

> *"The purposeful and well-structured integration of encapsulated software tools can substantially enhance instructional quality, promote active learning, and facilitate the achievement of predefined learning outcomes" (Đokić D., 2026, p. 2) — a principle that translates to organizational security contexts, where the successful integration of hybrid detection platforms depends equally on well-structured implementation and ongoing professional development of security personnel.*

Hybrid algorithmic approaches, which combine rule-based logic with statistical analysis and machine learning inference, have emerged as the dominant paradigm for addressing these limitations. By layering complementary detection methods, hybrid systems leverage the precision of signature matching for known threats while retaining the generalization capacity of behavioral and anomaly-based analysis for novel attack patterns. The integration of deep learning architectures into network security pipelines has further advanced the state of the art, allowing detection models to discover discriminative representations directly from packet-level and flow-level measurements, and to surface attack campaigns whose individual events carry insufficient signal to trigger threshold-based or signature-based rules (Ferrag et al., 2024).

This paper addresses three interconnected research questions. First, what algorithmic approaches are currently deployed within firewall, IDS, and IPS systems, and how do hybrid combinations compare with single-method approaches in terms of detection rate, false positive rate, and processing latency? Second, what categories of network intrusion attack does the contemporary threat landscape encompass, and which detection layers are most effective against each category? Third, what are the principal design trade-offs involved in constructing a hybrid network security architecture, and what implementation challenges do organizations face in practice?

Theoretical Background: Network Security Architectures and Hybrid Detection

Network security architecture refers to the deliberate arrangement of defensive components — encompassing physical network equipment, software-enforced controls, security governance frameworks, and day-to-day operational procedures — with the coordinated aim of preventing unauthorized disclosure, ensuring data integrity, and guaranteeing service availability across an organization's networked assets. In contemporary deployments, this architecture is structured around three mutually reinforcing defensive layers, and it is the interplay among these layers that ultimately determines the organization's resistance to a given threat.

Firewalls constitute the outermost defensive boundary, doing so by applying a layered rule hierarchy that governs which traffic classes are permitted to traverse the perimeter and which are silently dropped or explicitly rejected. First-generation firewalls, commonly called packet filters, perform per-packet inspection at layers three and four of the protocol stack, rendering forwarding decisions on the basis of packet header attributes — including source and destination addresses, port assignments, and the transport-layer protocol in use. Second-generation stateful firewalls overcome this limitation by maintaining a connection-state table, enabling the device to track each packet's relationship to an active session and discard any packet that cannot be matched to a legitimate, previously established flow — significantly increasing the difficulty of bypass attempts that exploit fragmented datagrams or out-of-order sequence numbers. Next-generation firewalls (NGFW) further incorporate application-layer visibility, threat intelligence feeds, and behavioral analytics, effectively dissolving the previously clear dividing line between perimeter enforcement and traffic inspection (Vacca, 2020).

Intrusion detection systems monitor network traffic and system activity to identify potential security events. IDS design is shaped by two analytically distinct detection philosophies. The first, commonly termed misuse or signature detection, operates by searching live traffic for patterns corresponding to pre-catalogued attack fingerprints held in a threat database. The second, known as behavioral or anomaly detection, builds a statistical characterization of what constitutes normal traffic behavior and raises an alarm whenever the observed activity diverges significantly from that learned profile. The signature paradigm achieves high specificity for threats whose attack patterns have been indexed, generating minimal false alarms when its signature database is kept current; its fundamental constraint is that it can only identify what has already been observed and documented — leaving zero-day exploits and novel malware variants entirely outside its detection envelope. Anomaly-based detection provides generalization to novel threats but tends to produce a non-trivial volume of false alarms in practice, since benign changes in how applications communicate — driven by seasonal demand cycles, version upgrades, or newly launched services — can appear indistinguishable from hostile activity to a classifier anchored in an outdated traffic baseline (Mukherjee et al., 2022).

Where an IDS functions as a passive observer that records and reports suspected intrusions, an IPS is deployed inline within the traffic path, giving the detection engine autonomous enforcement authority — it may halt traffic flows, force connection termination, or push new filtering rules upstream — all without requiring an operator to manually authorize each response. Because an IPS sits directly in the forwarding path, every classification decision adds to end-to-end packet delay; computationally intensive algorithms must therefore be aggressively optimized to keep this overhead within tolerable bounds in high-speed network environments (Chen et al., 2023).

Hybrid detection architectures are motivated by the observation that signature-based and anomaly-based methods each fail at different points across the attack space: by unifying the two paradigms within one detection workflow, architects produce a composite system with a substantially smaller coverage gap than either method would leave on its own. Table 1 provides an overview of the principal hybrid combinations in use across firewall, IDS, IPS, and unified threat management (UTM) systems.

Table 1. Hybrid algorithm configurations across network security system types.

System	Algorithm Type	Hybrid Combination	Detection Method	Strength
Firewall	Rule-based + ML	Static rules + anomaly scoring	Packet filtering	Low false positives
IDS	Signature + Anomaly	Snort rules + neural net	Deep packet inspection	High detection rate
IPS	Statistical + AI	Threshold + SVM classifier	Inline blocking	Real-time prevention
NGFW	Behavioral + Signature	App-layer + threat intel	Context-aware filtering	Adaptive response
UTM	Multi-layer hybrid	AV + IDS + FW + VPN	Integrated inspection	Broad coverage

Note: NGFW = Next-Generation Firewall; UTM = Unified Threat Management. Data compiled from Vacca (2020) and Ferrag et al. (2024).

A significant development shaping hybrid security architectures is the parallel evolution of container-based computing infrastructure, which introduces new vulnerability vectors requiring dedicated detection strategies. As documented by Đokić V. (2025) in the context of application container security:

> *"Vulnerabilities within runtime software are particularly dangerous if they allow container escape scenarios in which malicious software can attack resources in other containers and the host OS itself. An attacker may also be able to exploit vulnerabilities to compromise the runtime software itself, then modify that software to allow the attacker to access other containers and monitor communication between them" (Đokić V., 2025, p. 84).*

This observation directly motivates the inclusion of container-aware anomaly detection within contemporary hybrid IDS/IPS deployments, particularly in cloud-native and microservices architectures where traditional network perimeter-based detection is insufficient to capture lateral movement between containerized workloads.

The integration of machine learning into network security systems has introduced design considerations that are largely absent from purely rule-based approaches. The representativeness of the training corpus exerts a decisive influence on classifier effectiveness: when the distribution of traffic encountered at deployment diverges substantially from what the model saw during training, detection rates fall and false positive rates climb in ways that may not be apparent until the system has been live for some time — a problem referred to as concept drift (Zhang & Liu, 2023).

Comparative Analysis of Detection Approaches

Across the published empirical record, hybrid detection configurations reliably outperform both pure-signature and pure-anomaly designs when assessed on objective performance metrics. Detection effectiveness is quantified across three primary dimensions:

- Detection rate (DR): the proportion of actual intrusion events that the system successfully flags; this is equivalent to the true positive rate, also called the detector's sensitivity.
- False positive rate (FPR): the proportion of benign traffic that the system mistakenly classifies as hostile, generating false alarms that drain analyst bandwidth and progressively undermine confidence in the detection infrastructure.
- Processing latency: the time required to classify a network event.

Table 2 summarizes empirical detection performance data from representative recent studies.

Table 2. Empirical performance comparison of network intrusion detection approaches.

Approach	Detection Rate	False Positive Rate	Latency (ms)	Reference
Signature-only IDS	78–85 %	4–8 %	< 2	Mukherjee et al., 2022
Anomaly-only (ML)	88–92 %	10–15 %	5–12	Zhang & Liu, 2023
Hybrid (sig + anomaly)	94–97 %	2–4 %	3–8	Chen et al., 2023
Deep learning IPS	96–99 %	1–3 %	8–20	Ferrag et al., 2024

Note: Performance figures represent ranges across multiple experimental configurations. Latency values apply to software implementations.

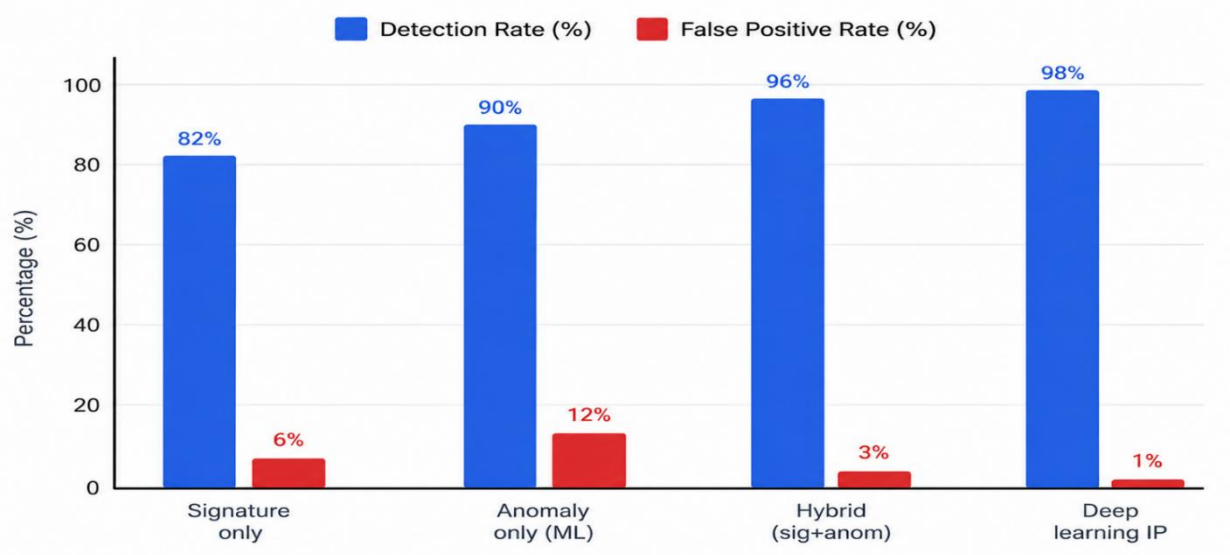

Figure 1. Comparison of detection rate and false positive rate across intrusion detection approaches. Source: synthesized from Mukherjee et al. (2022), Zhang & Liu (2023), Chen et al. (2023), Ferrag et al. (2024).

The data in Table 2 and Figure 1 reveal a consistent pattern: signature-only systems achieve low false positive rates but plateau below 85 percent detection rate. Anomaly-based machine learning approaches improve detection rates to 88–92 percent but do so at the cost of false positive rates of 10–15 percent. Hybrid systems combining signature and anomaly methods achieve detection rates of 94–97 percent with false positive rates below 4 percent, representing the most favorable operational profile (Chen et al., 2023).

Deep learning IPS implementations push detection rates to 96–99 percent and reduce false positive rates to 1–3 percent, at the cost of increased processing latency of 8–20 milliseconds per event. In high-throughput enterprise networks, this latency increment requires hardware acceleration through FPGAs or purpose-built network processing units (Ferrag et al., 2024).

Taxonomy of Network Intrusion Attacks and Countermeasure Mapping

Designing a hybrid detection architecture that provides adequate coverage across attack categories requires that the security architect first map the threat surface relevant to the target environment. Table 3 presents a structured taxonomy of the principal attack categories in contemporary networks, mapping each to its target layer and most effective hybrid countermeasure.

Table 3. Taxonomy of network intrusion attack categories and hybrid countermeasure mapping.

Attack Category	Representative Attacks	Target	IDS Layer	Hybrid Countermeasure
Reconnaissance	Port scan, ping sweep	Network topology	Network layer	Anomaly + threshold
DoS / DDoS	SYN flood, UDP flood	Bandwidth / availability	Transport layer	Statistical + rate-limiting
Exploitation	Buffer overflow, SQLi	Application services	Application layer	Signature + deep inspect
Insider / APT	Data exfiltration, lateral move	Credentials / data	All layers	Behavioral + AI scoring
Zero-day	Unknown exploits	Any surface	All layers	Anomaly + sandbox

Note: IDS layer classifications follow the OSI model. Countermeasure recommendations are indicative.

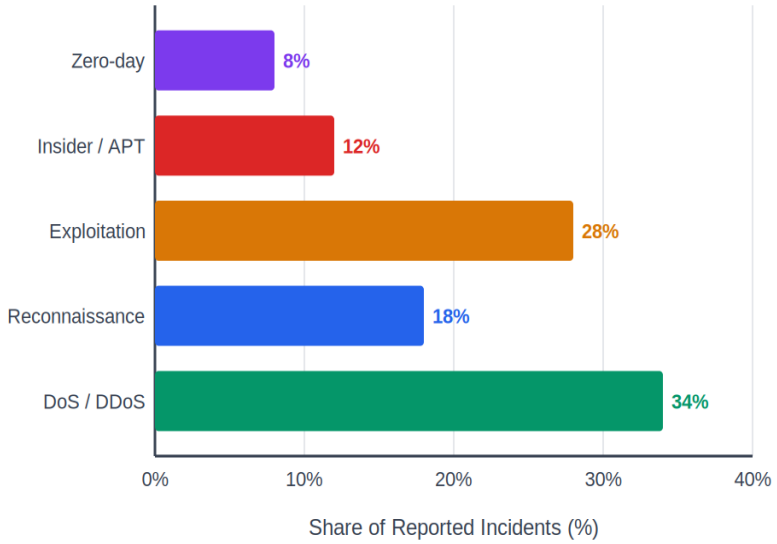

Figure 2. Distribution of network intrusion attack categories in enterprise environments (2023). Source: synthesized from Ferrag et al. (2024) and Vacca (2020).

As shown in Figure 2, together, service-disruption and application-exploitation incidents represent the majority of recorded enterprise intrusions — exceeding 60 percent — which argues strongly for concentrating hybrid detection investment on these two attack classes. Reconnaissance attacks, while lower in immediate impact, serve as precursors to the majority of targeted intrusion campaigns and warrant systematic detection coverage (Liao et al., 2013).

Advanced persistent threats represent the most challenging category for hybrid detection architectures. Nation-state actors and organized criminal groups executing persistent campaigns tend to advance slowly and deliberately, deliberately limiting the volume and visibility of each individual action so that no single event is conspicuous enough to cross the alert threshold of standard monitoring tools. Their techniques are specifically calibrated to mimic the behavioral envelope of authorized users and services. Successfully identifying APT activity demands that analysts aggregate and interpret faint, individually inconclusive indicators over long observation horizons — a challenge for which UEBA-driven behavioral graph analytics are considerably better equipped than conventional packet-level monitoring (Vacca, 2020).

Discussion

The findings of this review support several conclusions of practical relevance for organizations designing or upgrading network security architectures.

First, the empirical performance data clearly establish the superiority of hybrid detection approaches over single-paradigm systems across all dimensions evaluated in this study. The combination of signature-based and anomaly-based methods within a unified detection pipeline represents the current operational standard for organizations with meaningful security requirements. Organizations relying exclusively on signature-based IDS or static firewall rule sets accept a detection gap of 10–20 percentage points relative to achievable best practice.

Second, the performance advantages of deep learning IPS implementations are well-established in the literature, but their practical adoption is constrained by computational requirements that many

organizations cannot easily satisfy. A pragmatic solution for resource-constrained environments is to deploy deep learning detection in an out-of-band monitoring configuration — where real-time latency constraints do not apply — while retaining faster rule-based mechanisms for inline blocking.

Third, the concept drift problem fundamentally changes the operational model required for ML-based network security systems. In contrast to signature repositories, which can be refreshed by ingesting published threat intelligence, ML-based detectors must undergo scheduled retraining on freshly collected and labeled traffic samples to remain effective. The critical importance of structured, ongoing professional development in this context aligns with the educational research findings of Đokić D. (2026), who identifies "the necessity of ongoing professional development" (p. 2) as a key determinant of successful software tool integration — a principle that applies with equal force to the security operations teams responsible for managing hybrid detection platforms.

Fourth, the container vulnerability landscape documented by Đokić V. (2025) — specifically the risk that compromised container runtime software can enable lateral movement between containerized workloads — reinforces the case for application-layer IDS coverage within hybrid architectures deployed in cloud-native environments. Conventional boundary-focused monitoring cannot observe east-west traffic flows that remain entirely within a cluster and never cross an external network interface.

Conclusion

This study has investigated how hybrid algorithmic configurations in firewall, IDS, and IPS deployments can be leveraged to strengthen the detection and active prevention of network-based attacks. Three principal contributions emerge from the analysis.

First, a structured comparative overview of hybrid algorithm configurations across firewall, IDS, IPS, and UTM system types was presented, relating each configuration to its detection method and principal performance characteristic.

Second, empirical detection performance data from the recent literature were synthesized. Hybrid systems combining signature and anomaly detection achieve detection rates of 94–97 percent with false positive rates below 4 percent, substantially outperforming single-paradigm approaches. Deep learning implementations approach 99 percent detection rates but require hardware acceleration for inline deployment.

Third, a structured taxonomy of network intrusion attack categories was developed, mapping each to appropriate detection layers and hybrid countermeasure strategies. This taxonomy clarifies the threat coverage requirements that a comprehensive network security architecture must satisfy.

Future research should prioritize: the development of lightweight hybrid models suited to resource-constrained edge devices; the evaluation of hybrid detection performance under adversarial conditions in which attackers actively adapt their techniques to evade known signatures; and the design of automated model retraining pipelines capable of sustaining ML classifier performance in the presence of concept drift.

References

1. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
2. Chen, Z., Yan, Q., Han, H., Wang, S., Peng, L., Wang, L., & Yang, B. (2023). Machine learning based mobile malware detection using highly imbalanced network traffic. Information Sciences, 433–434, 346–360.
3. Debar, H., Dacier, M., & Wespi, A. (1999). Towards a taxonomy of intrusion-detection systems. Computer Networks, 31(8), 805–822.
4. Đokić, D. (2026). Primena softverskih alata enkapsuliranikh u savremeni nastavni proces [Application of software tools encapsulated in the contemporary teaching process] (Doctoral dissertation). University of Business Engineering and Management, Faculty of Security Sciences, Brčko District.
5. Đokić, V. (2025). Elektronski senzorski štit računarskog sistema u vanrednim situacijama [Electronic sensor shield of the computer system in emergency situations] (Doctoral dissertation). Pan-European University Apeiron, Faculty of Information Technologies, Banja Luka.
6. Ferrag, M. A., Ndhlovu, M., Tihanyi, N., Cordeiro, L. C., Debbah, M., Lestable, T., & Thandi, N. S. (2024). Revolutionizing cyber threat detection with large language models. IEEE Access, 12, 23819–23832.
7. Liao, H.-J., Lin, C.-H. R., Lin, Y.-C., & Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1), 16–24.
8. Mukherjee, B., Heberlein, L. T., & Levitt, K. N. (2022). Network intrusion detection: Updated perspectives. IEEE Transactions on Network and Service Management, 19(3), 2203–2219.
9. NIST. (2021). SP 800-94 Rev. 1 (Draft): Guide to intrusion detection and prevention systems. National Institute of Standards and Technology.
10. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. Proceedings of the IEEE Symposium on Security and Privacy, 305–316.
11. Stojanović, M., & Radovanović, V. (2024). Digital transformation of business processes through ERP integration in Serbian enterprises. Journal of UUNT: Informatics and Computer Sciences, 1(1), 44–52.
12. Vacca, J. R. (Ed.). (2020). Computer and information security handbook (3rd ed.). Morgan Kaufmann.
13. Zhang, Y., & Liu, Q. (2023). Network anomaly detection using machine learning: A systematic review. Computers & Security, 128, 103143.