International Journal of Innovative Computer Science and IT Research

Volume 01, Issue 05 – Sep-Oct 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

# Intrusion Prevention Using Adaptive Network Security Mechanisms

**Hiroki Takakura**

Professor, National Institute of Informatics (NII), Japan, Japan

**Abstract**

The increasing complexity of modern network infrastructures has created significant challenges for conventional intrusion prevention systems. Enterprise networks, cloud environments, Internet of Things devices, distributed applications, and edge computing platforms continuously generate heterogeneous traffic and dynamic security conditions. Static intrusion prevention mechanisms that depend primarily on predefined signatures and fixed security policies may be unable to respond effectively to previously unknown attacks, rapidly changing threats, and evolving network behavior. This paper examines adaptive network security mechanisms for strengthening intrusion prevention in dynamic computing environments. A conceptual framework is proposed that integrates network monitoring, traffic analysis, anomaly detection, threat intelligence, machine learning, adaptive policy enforcement, risk assessment, and automated response. The framework continuously evaluates network conditions and adjusts security controls according to observed threats and contextual risk. Machine learning-based anomaly detection supports identification of deviations from normal traffic behavior, while signature-based mechanisms continue to provide efficient recognition of known attack patterns. Threat intelligence contributes contextual information regarding emerging indicators, malicious infrastructure, and attack characteristics.

The proposed architecture combines these capabilities through an adaptive decision layer that determines appropriate prevention actions, including traffic filtering, session termination, access restriction, rate limiting, isolation, and policy modification. The analysis identifies important application areas across enterprise networks, cloud infrastructures, IoT environments, software-defined networks, and edge computing systems. It also examines factors affecting prevention effectiveness, including detection accuracy, response latency, adaptability, computational overhead, false positives, and explainability. Major challenges include adversarial manipulation, concept drift, heterogeneous traffic, resource limitations, automated response risks, and maintaining reliable security policies. The study concludes that adaptive intrusion prevention can provide stronger protection than purely static security mechanisms by continuously adjusting defensive controls according to changing network conditions. Future development should emphasize explainable machine learning, automated threat intelligence integration, distributed security architectures, adversarially robust models, and policy-aware autonomous defense.

***Keywords:*** Intrusion Prevention, Adaptive Network Security, Network Security, Intrusion Detection, Machine Learning, Anomaly Detection, Threat Intelligence, Cybersecurity, Automated Response, Network Defense.

International Journal of Innovative Computer Science and IT Research

Volume 01, Issue 05 – Sep-Oct 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

## 1. Introduction

Modern computer networks have evolved into highly interconnected environments supporting cloud applications, enterprise services, Internet of Things devices, remote users, distributed computing platforms, and edge infrastructures. This transformation has increased both the volume and complexity of network traffic. At the same time, cyberattacks have become more adaptive, automated, and difficult to identify using conventional security controls. Attackers increasingly modify their techniques, exploit previously unknown vulnerabilities, and use legitimate network behavior to conceal malicious activities. These developments require intrusion prevention systems capable of responding dynamically to changing security conditions.

Traditional intrusion prevention mechanisms commonly rely on signatures, predefined rules, static access policies, and known attack indicators. Signature-based approaches can provide efficient detection of previously recognized threats, but they are generally dependent on prior knowledge of attack characteristics. When a new or modified attack does not match an existing signature, its detection may be delayed. Fixed policies can similarly become ineffective when network architectures or traffic patterns change. Consequently, static security mechanisms may create gaps between emerging threats and available defensive controls.

Adaptive network security provides an alternative approach by enabling security mechanisms to modify their behavior according to observed network conditions. Adaptive systems can incorporate anomaly detection, machine learning, behavioral analysis, threat intelligence, and contextual risk assessment to identify changing attack patterns. Instead of treating security policies as permanently fixed, adaptive mechanisms can dynamically modify filtering rules, access privileges, traffic controls, or isolation strategies in response to detected threats. This capability is particularly relevant to distributed and software-defined network environments where security policies can be programmatically adjusted.

Machine learning has become an important component of adaptive security because it can identify complex relationships within large volumes of network data. Supervised learning can classify known attack categories, whereas unsupervised and semi-supervised methods can identify deviations from established network behavior. Deep learning can further process complex traffic representations, although its computational requirements and interpretability limitations must be considered. Machine learning should therefore complement rather than completely replace conventional security mechanisms.

This paper develops a conceptual framework for intrusion prevention using adaptive network security mechanisms. The proposed approach integrates network monitoring, traffic preprocessing, signature-based analysis, anomaly detection, threat intelligence, adaptive decision-making, policy enforcement, and continuous feedback. The study analyzes the major architectural components, application areas, operational factors, challenges, and future research directions. The objective is to establish a structured foundation for developing intelligent intrusion prevention systems capable of adapting to dynamic network threats while maintaining security, availability, and operational efficiency.

## 2. Objectives

### 2.1 Primary Objective

The primary objective of this study is to examine an adaptive intrusion prevention framework capable of dynamically responding to evolving network threats. The framework combines conventional security

controls with machine learning, anomaly detection, behavioral analysis, threat intelligence, and adaptive policy enforcement to improve the responsiveness and resilience of network defense systems.

### 2.2 Development of an Adaptive Security Architecture

The first objective is to develop a conceptual architecture integrating network monitoring, traffic analysis, threat detection, risk assessment, and automated prevention. The architecture emphasizes continuous feedback so that security policies can be modified according to changing traffic patterns and threat conditions.

### 2.3 Integration of Intelligent Detection Mechanisms

The second objective is to examine how supervised, unsupervised, and behavioral machine learning approaches can support adaptive intrusion prevention. The study considers the complementary roles of signature-based detection, anomaly detection, behavioral profiling, and threat intelligence in identifying known and emerging security threats.

### 2.4 Evaluation of Adaptive Prevention Challenges

The third objective is to identify technical and operational challenges associated with adaptive intrusion prevention. These include false positives, concept drift, adversarial manipulation, response latency, computational overhead, heterogeneous network environments, policy conflicts, and the risks associated with automated security actions.

## 3. Review of Literature

### 3.1 Intrusion Detection and Prevention Systems

Intrusion detection and prevention systems have traditionally been developed around signature-based and anomaly-based detection approaches. Signature-based systems compare observed traffic against known attack patterns and are effective for recognizing previously identified threats. Anomaly-based systems establish representations of normal activity and identify deviations that may indicate malicious behavior. Each approach provides distinct advantages, but neither is sufficient for all threat conditions. Combining both approaches can provide broader detection coverage.

Intrusion prevention extends detection by automatically applying controls intended to stop or contain malicious activity. These controls may include packet filtering, connection termination, access restriction, rate limiting, or network isolation. Automated prevention can reduce response time but also introduces the risk of disrupting legitimate traffic. Therefore, prevention mechanisms require accurate classification and appropriate confidence thresholds before taking high-impact actions.

### 3.2 Machine Learning for Adaptive Network Security

Machine learning enables intrusion prevention systems to identify complex patterns within network traffic. Supervised models can learn from labeled attack datasets, while unsupervised approaches can identify previously unknown patterns without requiring extensive labeled examples. Ensemble learning can combine multiple classifiers to improve robustness, while deep learning can learn hierarchical representations from complex network data. However, machine learning models may be affected by changing traffic distributions. Network environments evolve because of new applications, devices, users,

protocols, and operational patterns. A model trained on historical traffic may therefore become less accurate when the underlying distribution changes. Continuous model monitoring, retraining, concept-drift detection, and adaptive feature management are consequently important for maintaining long-term effectiveness.

### 3.3 Adaptive and Software-Defined Network Defense

Software-defined networking provides programmable control over network infrastructure, creating opportunities for dynamic security policy enforcement. Centralized controllers can receive threat information and modify forwarding, filtering, or segmentation policies. This programmability can support rapid response to detected attacks and facilitate integration between detection and prevention mechanisms.

Adaptive defense can also benefit from threat intelligence, which provides information about malicious IP addresses, domains, attack techniques, vulnerabilities, and indicators of compromise. Integrating threat intelligence with local network observations can improve contextual risk assessment. However, threat intelligence quality varies, and excessive dependence on external indicators can result in inaccurate or outdated decisions. Effective adaptive systems therefore require mechanisms for validating and contextualizing threat information.

## 4. Methodology

### 4.1 Research Design

This study adopts a conceptual and analytical research design for examining adaptive intrusion prevention in dynamic network environments. The methodology organizes prevention into multiple stages, including network monitoring, data preparation, threat detection, contextual risk assessment, adaptive decision-making, policy enforcement, and feedback. The framework is designed to integrate established security mechanisms with intelligent analytical techniques rather than replacing conventional controls completely.

The proposed methodology evaluates adaptive intrusion prevention according to detection accuracy, response time, adaptability, false-positive control, computational efficiency, scalability, and security impact. These dimensions provide a structured basis for assessing whether a prevention mechanism can operate effectively under changing network conditions. The approach does not claim experimental performance from an original dataset; instead, it establishes a conceptual architecture suitable for future implementation and empirical validation.

### 4.2 Adaptive Intrusion Prevention Model

The proposed model begins with continuous monitoring of network packets, flows, sessions, and security events. Preprocessing converts raw traffic into structured representations suitable for analysis. Signature-based detection identifies known threats, while anomaly detection evaluates deviations from normal traffic behavior. Behavioral analysis provides additional context regarding users, devices, sessions, and communication patterns. Threat intelligence can further enrich observations with external information about known malicious indicators.

The outputs of these mechanisms are combined within an adaptive risk-assessment layer. Each event can receive a risk score based on attack indicators, behavioral deviation, contextual information,

and model confidence. Prevention policies are subsequently selected according to the assessed risk. Low-risk events may be monitored, while high-risk events can trigger blocking, session termination, rate limiting, or isolation. Feedback from subsequent network behavior can be used to update detection and policy decisions.

### 4.3 Key Methodological Components

**The proposed methodology incorporates the following components:**

- **Network Monitoring:** Continuous observation of packets, flows, sessions, and security events.
- **Traffic Preprocessing:** Normalization and extraction of relevant traffic characteristics.
- **Signature Analysis:** Identification of known attack patterns and indicators.
- **Anomaly Detection:** Identification of deviations from expected network behavior.
- **Behavioral Analysis:** Evaluation of user, device, and session activity.
- **Threat Intelligence:** Integration of contextual threat indicators.
- **Risk Assessment:** Assignment of contextual security risk scores.
- **Adaptive Policy Engine:** Dynamic selection or modification of security controls.
- **Automated Prevention:** Blocking, isolation, rate limiting, or session termination.
- **Feedback Mechanism:** Continuous evaluation of prevention outcomes and network changes.

The methodology emphasizes a feedback-driven security cycle. Detection results influence prevention decisions, while the consequences of those decisions provide information for subsequent security assessment. This architecture supports adaptive behavior while preserving conventional rule-based protection for known threats. Such hybridization can improve resilience because machine learning and anomaly detection can identify changing patterns while signatures provide efficient recognition of established attacks.

## 5. Analysis

### 5.1 Architecture of Adaptive Intrusion Prevention

An adaptive intrusion prevention system requires coordinated interaction among monitoring, detection, intelligence, decision-making, and enforcement components. The architecture begins with continuous network observation and progresses toward analytical processing and contextual risk evaluation. The adaptive policy engine then determines appropriate defensive actions.

**Table 1: Core Components of an Adaptive Intrusion Prevention Architecture**

| Component | Primary Function | Security Contribution |
|---|---|---|
| Network Monitoring | Collect network events | Provides continuous visibility |
| Traffic Preprocessing | Prepare traffic data | Improves analytical consistency |
| Signature Detection | Identify known attacks | Efficient known-threat detection |
| Anomaly Detection | Detect unusual behavior | Supports unknown-threat identification |
| Behavioral Analytics | Analyze contextual activity | Identifies behavioral deviations |

| Component | Primary Function | Security Contribution |
|---|---|---|
| Threat Intelligence | Add external context | Enriches threat assessment |
| Risk Assessment | Estimate attack severity | Supports risk-based decisions |
| Adaptive Policy Engine | Select security actions | Dynamically modifies controls |
| Prevention Layer | Block or contain threats | Stops or limits malicious activity |
| Feedback Mechanism | Evaluate outcomes | Enables continuous adaptation |

**Interpretation:** Demonstrates that adaptive intrusion prevention depends on multiple coordinated layers. Signature detection remains valuable for established threats, while anomaly and behavioral analysis provide broader capabilities for detecting unusual activity. Threat intelligence strengthens contextual assessment, and the adaptive policy engine converts analytical results into security actions. The feedback mechanism is particularly important because it allows the system to respond to changes in network behavior rather than operating according to permanently fixed assumptions.

### 5.2 Application Areas of Adaptive Intrusion Prevention

Adaptive security mechanisms can be deployed across different network environments with varying requirements. Enterprise networks require protection against unauthorized access, malware, lateral movement, and abnormal internal activity. Cloud environments introduce dynamic workloads and distributed resources. IoT networks contain large numbers of heterogeneous and resource-constrained devices, while software-defined networks provide programmable infrastructure that can facilitate dynamic security control.

**Table 2: Application Areas of Adaptive Network Security Mechanisms**

| Environment | Major Threat Context | Adaptive Prevention Capability |
|---|---|---|
| Enterprise Networks | Unauthorized access and lateral movement | Dynamic segmentation and filtering |
| Cloud Networks | Distributed and changing workloads | Adaptive access and traffic controls |
| IoT Networks | Device compromise and abnormal traffic | Behavioral device isolation |
| Software-Defined Networks | Rapidly changing traffic policies | Programmable security enforcement |

| Environment | Major Threat Context | Adaptive Prevention Capability |
|---|---|---|
| Edge Computing | Distributed attack surfaces | Localized threat containment |
| Data Centers | High-volume network activity | Automated traffic filtering |
| Wireless Networks | Dynamic access and device behavior | Adaptive authentication and control |
| Critical Infrastructure | High-impact network attacks | Risk-based containment and monitoring |

**Interpretation:** Illustrates the broad applicability of adaptive intrusion prevention. Different environments require different prevention strategies because network architectures, traffic patterns, device capabilities, and threat consequences vary. IoT systems may benefit from behavioral device profiling, whereas software-defined networks can exploit programmable policy enforcement. Critical infrastructures may require conservative automated responses because aggressive blocking can affect essential services. Consequently, adaptive prevention policies should be context-aware rather than universally applied.

### 5.3 Factors Affecting Prevention Effectiveness

The effectiveness of adaptive intrusion prevention depends on the quality and timeliness of network information. Incomplete traffic visibility can prevent accurate identification of malicious activity, while noisy or inconsistent data can increase false positives. Model performance is also affected by the representativeness of training data. If historical datasets fail to reflect current network conditions, machine learning models may produce unreliable decisions.

Response latency is another critical factor. Security mechanisms must identify threats and enforce appropriate controls quickly enough to limit attack progression. However, faster response does not always imply better security because aggressive automated actions may interrupt legitimate services. Risk-aware response policies can therefore assign different actions according to confidence and potential impact. High-confidence threats may trigger immediate blocking, whereas uncertain events can be subjected to enhanced monitoring.

Adaptability must also be balanced against security stability. Excessive policy changes can produce inconsistent network behavior and create opportunities for attackers to manipulate defensive mechanisms. Continuous feedback should therefore be governed by validation mechanisms, confidence thresholds, and policy constraints. Explainability can further assist security analysts in understanding why a particular adaptive decision was made.

## 6. Discussion

### 6.1 From Static to Adaptive Intrusion Prevention

Traditional intrusion prevention systems generally depend on predefined rules and known indicators. Although these mechanisms remain useful, their effectiveness can decrease when attack characteristics

change rapidly. Adaptive security introduces continuous analysis and policy adjustment, allowing defensive mechanisms to respond to changing network conditions.

The transition toward adaptive prevention does not require eliminating conventional security controls. Instead, static signatures can operate as one layer within a broader architecture. Machine learning, behavioral analytics, and threat intelligence can provide additional evidence for detecting threats that do not match existing signatures. This hybrid model can improve coverage while preserving efficient detection of known attacks.

### 6.2 Intelligent Risk-Based Response

An important advantage of adaptive intrusion prevention is the ability to use risk-based response rather than applying identical actions to every detected anomaly. Security events can be evaluated according to severity, confidence, affected assets, behavioral context, and potential consequences. This approach can reduce unnecessary disruption while ensuring that high-risk events receive immediate attention.

Risk-based prevention can also support graduated responses. Low-confidence anomalies may generate alerts and increased monitoring, while medium-risk events may trigger rate limiting or additional authentication. High-confidence threats can result in blocking, session termination, or device isolation. Such graduated mechanisms can improve operational reliability compared with systems that rely exclusively on binary allow-or-deny decisions.

### 6.3 Adaptive Security and Autonomous Defense

The combination of machine learning, threat intelligence, programmable networking, and automated policy enforcement creates opportunities for increasingly autonomous network defense. Autonomous systems can process large numbers of security events more rapidly than manual security operations.

They can also continuously monitor network behavior and modify controls in response to emerging threats. Nevertheless, autonomous defense requires careful governance Incorrect automated decisions can cause service disruption or unintentionally block legitimate users. Attackers may also attempt to manipulate learning processes or feedback mechanisms.

Therefore, autonomous prevention should incorporate confidence thresholds, policy constraints, explainability, human oversight for high-impact decisions, and secure model-update procedures.

## 7. Challenges

Adaptive intrusion prevention faces significant challenges associated with rapidly changing network behavior. Legitimate traffic can change because of new applications, cloud workloads, remote users, device deployments, or organizational activities. These changes can resemble malicious anomalies and produce false positives. Machine learning models may also experience concept drift when the statistical characteristics of network traffic evolve over time. Continuous monitoring and controlled model adaptation are therefore necessary.

Adversarial manipulation presents another major challenge. Attackers can deliberately modify traffic characteristics to evade detection models or manipulate the behavior of adaptive security mechanisms. Machine learning systems may be particularly vulnerable when attackers understand the features used by detection models. Robust training, adversarial evaluation, multiple evidence sources, and secure model-management processes are therefore essential for maintaining defensive reliability.

Volume 01, Issue 05 – Sep-Oct 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

Scalability and automated response also create practical difficulties. Large networks generate massive volumes of traffic and security events, requiring efficient processing and low-latency decision-making. At the same time, aggressive automated responses can disrupt legitimate services. Adaptive systems must therefore balance speed, accuracy, and operational safety. Policy conflicts can additionally occur when multiple security mechanisms attempt to modify network controls simultaneously.

## 8. Future Research

Future research should investigate adaptive intrusion prevention models that combine multiple machine learning paradigms. Hybrid architectures integrating supervised classification, unsupervised anomaly detection, sequential modeling, and behavioral profiling could provide broader detection coverage. Research should also examine continual learning mechanisms capable of adapting to new traffic patterns without completely forgetting previously learned attack characteristics. Such models could improve long-term resilience against evolving threats.

Another important research direction is the development of distributed adaptive security architectures for cloud, edge, IoT, and software-defined networks. Distributed detection can reduce response latency by processing threats closer to their source. Collaborative learning could enable multiple network domains to improve detection without requiring centralized sharing of sensitive traffic data. Secure coordination mechanisms will be necessary to prevent compromised nodes from influencing collective defensive decisions.

Future systems should additionally emphasize explainable and policy-aware autonomous defense. Adaptive models should provide interpretable evidence for security decisions and distinguish between high-confidence attacks and uncertain anomalies. Automated prevention should operate within predefined safety boundaries, with human intervention available for high-impact decisions. Integration with threat intelligence, zero-trust architectures, security orchestration platforms, and programmable network infrastructure could further support coordinated and resilient network defense.

## 9. Conclusion

Modern network environments are increasingly dynamic, distributed, and heterogeneous, making static intrusion prevention mechanisms insufficient for many evolving threat conditions. This study examined an adaptive network security framework that combines continuous monitoring, signature detection, anomaly analysis, behavioral analytics, threat intelligence, risk assessment, adaptive policy enforcement, and automated response. The proposed architecture treats intrusion prevention as a continuous process in which security controls are adjusted according to observed network conditions rather than remaining permanently fixed.

The analysis demonstrates that adaptive prevention can complement conventional security mechanisms by extending protection beyond known attack signatures. Machine learning and behavioral analytics can identify deviations and complex patterns, while threat intelligence adds contextual information that can improve risk assessment. The adaptive policy engine can then apply graduated responses such as monitoring, rate limiting, blocking, session termination, or isolation. However, effective deployment requires careful management of false positives, concept drift, computational overhead, adversarial manipulation, and the operational risks associated with automated decisions.

Future intrusion prevention systems should therefore move toward intelligent, distributed, explainable, and policy-aware defense architectures. Continual learning, adversarially robust models, privacy-preserving collaborative security, edge-based detection, and programmable network controls can strengthen adaptability while reducing response latency. Autonomous prevention should remain constrained by security policies and confidence thresholds to prevent inappropriate actions.

**References**

1. Ali, A. H., Charfeddine, M., Ammar, B., Hamed, B. B., Albalwy, F., Alqarafi, A., & Hussain, A. (2024). Unveiling machine learning strategies and considerations in intrusion detection systems: A comprehensive survey. *Frontiers in Computer Science, 6*, 1387354. https://doi.org/10.3389/fcomp.2024.1387354
2. Muneer, A., et al. (2024). A critical review of artificial intelligence based approaches in intrusion detection: A comprehensive analysis. *Journal of Engineering, 2024*, 3909173. https://doi.org/10.1155/2024/3909173
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. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity, 2*, 20. https://doi.org/10.1186/s42400-019-0038-7
5. Ahmad, Z., Shahid Khan, A., Shiang, C. W., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies, 32*(1), e4150. https://doi.org/10.1002/ett.4150
6. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. *2015 Military Communications and Information Systems Conference (MilCIS)*, 1–6.
7. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 108–116.
8. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 1–6.
9. Gümüşbaş, D., Yıldırım, T., Genovese, A., & Scotti, F. (2021). A comprehensive survey of databases and deep learning methods for cybersecurity and intrusion detection systems. *IEEE Systems Journal, 15*(2), 1717–1731. https://doi.org/10.1109/JSYST.2020.2992966
10. Drewek-Ossowicka, A., Pietrołaj, M., & Rumiński, J. (2021). A survey of neural networks usage for intrusion detection systems. *Journal of Ambient Intelligence and Humanized Computing, 12*, 497–514. https://doi.org/10.1007/s12652-020-02014-x
11. Ahmad, I., Basheri, M., Iqbal, M. J., & Rahim, A. (2018). Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection. *IEEE Access, 6*, 33789–33795.

12. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence, 2*(1), 41–50.
13. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access, 5*, 21954–21961.
14. Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection. *Proceedings of the Network and Distributed System Security Symposium (NDSS)*.
15. Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders. *IEEE Pervasive Computing, 17*(3), 12–22.
16. 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.
17. 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.
18. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *2010 IEEE Symposium on Security and Privacy*, 305–316.
19. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys, 41*(3), Article 15. https://doi.org/10.1145/1541880.1541882.
20. Garcia-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security, 28*(1–2), 18–28.