INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue V, May 2025

A Comparative Analysis of Signature-Based and Anomaly-Based Intrusion Detection Systems

Vasudev Karthik Ravindran[1], Sharad Shyam Ojha[2], Arvind Kamboj[3]

[1]Senior Software Development Engineer, Amazon, Seattle, WA, USA

[2]Software Development Manager, Amazon, Austin, United States[2]

[3]Department of Computer Science & Engineering, Shivalik College of Engineering, Dehradun

DOI: https://doi.org/10.51583/IJLTEMAS.2025.140500026

Received: 17 May 2025; Accepted: 26 May 2025; Published: 03 June 2025

Abstract: This paper presents a comprehensive comparative analysis of Signature-Based and Anomaly-Based Intrusion Detection Systems (IDS) using key performance metrics such as detection accuracy, false positive rate, adaptability to new threats, computational overhead, maintenance effort, scalability, and real-time performance. By examining these metrics, the study highlights the strengths and limitations of each IDS approach in handling both known and emerging cybersecurity threats. Signature-Based IDS demonstrates high accuracy and low false positives but struggles with adaptability and maintenance demands, while Anomaly-Based IDS offers better adaptability and threat detection versatility at the cost of increased false positives and resource consumption. The analysis emphasizes that an optimal IDS solution should consider the specific security needs and operational context of the deployment environment. The findings suggest that a hybrid approach, leveraging the complementary advantages of both techniques, can provide a more robust and resilient defense against the growing complexity of cyberattacks in modern networks.

Keywords— Intrusion Detection Systems, Signature-Based IDS, Anomaly-Based IDS, Cybersecurity, Threat Detection

I. Introduction

In an era of increasingly sophisticated cyber threats, intrusion detection systems (IDS) play a pivotal role in safeguarding digital infrastructures. These systems monitor network and system activities to detect unauthorized access and malicious behavior [1]. Among the various detection techniques employed in IDS, signature-based and anomaly-based approaches are among the most widely studied and implemented. Each method offers distinct strengths and weaknesses, making their comparative evaluation important for effective cybersecurity planning and implementation [2].

The primary objective of this paper is to compare and critically analyze signature-based and anomaly-based intrusion detection systems. The study aims to assess their respective operational principles, effectiveness, and adaptability to different threat scenarios and deployment environments. This comparison is motivated by the current cybersecurity landscape, which is characterized by both a growing volume of known threats and a surge in previously unseen, sophisticated attack vectors [3]. Organizations must balance the need for reliable, low-noise detection with the ability to identify novel and evolving threats.

To address this objective, the paper presents a structured analysis based on several evaluation criteria, including detection accuracy, false positive and false negative rates, computational requirements, scalability, adaptability, and ease of maintenance. The study further considers the impact of emerging technologies such as machine learning and artificial intelligence on the effectiveness of both detection approaches [4].

The findings indicate that signature-based IDS is highly effective in identifying known threats with low false alarm rates, but it is limited in its ability to detect previously unknown attacks [5]. Anomaly-based IDS, on the other hand, offers the capability to recognize novel intrusions by identifying deviations from established normal behavior, though often at the cost of increased false positives [6]. These insights support the growing trend toward hybrid IDS solutions that integrate both approaches to achieve more comprehensive and adaptive protection.

By providing a focused comparison of signature-based and anomaly-based detection, this paper aims to contribute to the design of more resilient intrusion detection strategies suited to the dynamic and complex nature of modern cybersecurity environments.

II. Review of Literature

he literature on signature-based and anomaly-based intrusion detection systems (IDS) from 2020 to 2025 reflects an increasingly dynamic cybersecurity landscape shaped by rapidly evolving threat vectors and advancements in artificial intelligence. This period has seen intensified efforts to enhance detection accuracy, reduce false positives, and develop adaptable systems capable of responding to novel attack patterns. A consistent theme is the push toward hybrid models that combine the deterministic precision of signature-based detection with the adaptive capabilities of anomaly detection [7].

Signature-based IDS continues to be a vital element in security infrastructure due to its high precision in detecting previously cataloged threats. However, its limitations in identifying zero-day attacks and polymorphic malware have motivated the integration of intelligent automation. Recent studies have explored the use of natural language processing and deep learning to automate signature generation, reducing reliance on manual updates and enabling quicker adaptation to new threats [8]. Threat

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue V, May 2025

intelligence platforms now feed real-time data into IDS systems, allowing faster propagation of signatures across enterprise environments.

Parallel to this, anomaly-based IDS research has grown rapidly, fueled by the rise of machine learning and deep learning frameworks capable of modeling complex behavioral patterns. Unsupervised models, particularly clustering, autoencoders, and generative adversarial networks (GANs), have been widely used due to their ability to detect novel anomalies without labeled datasets [9]. These methods are increasingly optimized using dimensionality reduction techniques such as Principal Component Analysis (PCA), t-SNE, and autoencoder bottlenecks to enhance both detection speed and accuracy [10]. Dimensionality reduction has also been instrumental in mitigating the curse of dimensionality in high-volume network traffic data, facilitating real-time anomaly detection.

A major concern in anomaly-based systems is the high false positive rate, often due to inadequate baseline modeling or dynamic network environments. To address this, adaptive threshold mechanisms, online learning algorithms, and meta-learning approaches have been proposed. Moreover, recent studies have focused on adversarial robustness—developing models resilient to evasion attacks where adversaries manipulate data to bypass anomaly detectors [11]. Techniques such as adversarial training and ensemble hardening have shown promise in improving IDS robustness.

Another emerging area of focus is explainability. Black-box deep learning models, while accurate, often lack transparency, making it difficult for analysts to understand or trust IDS alerts. Recent research proposes the use of attention mechanisms, LIME (Local Interpretable Model-agnostic Explanations), and SHAP (SHapley Additive exPlanations) to provide interpretable outputs for anomaly detection results [12]. This is particularly important in regulated sectors like healthcare and finance, where explainability is not optional.

A significant trend in the literature is the development of hybrid IDS architectures. These systems use signature-based detection for known threats and anomaly-based detection for novel behaviors, often orchestrated through context-aware frameworks or risk-based triggers [8]. Some studies propose ensemble methods that fuse the outputs of multiple classifiers using voting or stacking to improve robustness and accuracy [9]. Others explore reinforcement learning for dynamic IDS policy selection, adjusting detection strategies in response to changing threat levels [13].

To help synthesize and compare the large body of recent work, Table 1 (to be included in the final paper) provides a comparative overview of selected IDS models from 2020 to 2025. The table categorizes each study by detection type, algorithm used, dataset evaluated, application domain (e.g., IoT, cloud, ICS), and key findings related to accuracy, false positive rate, and computational overhead.

The applicability of different IDS approaches varies widely across domains. In cloud environments, where scale and elasticity dominate, distributed and container-aware IDS frameworks have emerged, often combining lightweight signature detection with machine learning-driven anomaly detection at the edge [14]. In IoT networks, researchers emphasize energy-efficient models, frequently incorporating lightweight anomaly detection algorithms compatible with constrained hardware [15]. In industrial control systems (ICS), the emphasis is on stability and real-time performance, with anomaly-based IDS preferred for identifying system sabotage or faults that might evade traditional signatures.

Federated learning has also gained traction in recent IDS research. It enables collaborative model training across distributed entities without exposing raw data, thereby preserving privacy. This approach has shown potential in sectors where data confidentiality is critical, such as healthcare and critical infrastructure. Meanwhile, proactive IDS strategies that incorporate threat hunting and predictive analytics are being explored as a shift from purely reactive paradigms, aiming to anticipate and mitigate threats before exploitation occurs.

Despite substantial progress, challenges persist. Signature-based IDS systems still struggle to keep pace with the rate of new threats, while anomaly-based systems face difficulties in adapting to rapidly shifting baselines without excessive false positives. The integration of IDS into broader cybersecurity ecosystems—such as Security Information and Event Management (SIEM) platforms and automated response systems—is an active area of research aiming to streamline detection and response workflows.

In summary, the literature from 2020 to 2025 demonstrates significant advancement in both signature-based and anomaly-based intrusion detection systems. While each method offers unique benefits, their limitations are increasingly addressed through hybrid models, AI-driven enhancements, and domain-specific adaptations. The convergence of machine learning, interpretability tools, and real-time data analytics is pushing IDS technology toward a more intelligent, autonomous, and resilient future. Table 1 summarizes representative studies from 2020 to 2025, highlighting key methodologies, datasets, application domains, and performance metrics across signature-based, anomaly-based, and hybrid intrusion detection systems.

Table 1: Summary of Recent IDS Approaches (2020–2025)

Year	Detection Type	Methodology	Domain	Key Insight
2020	Anomaly-Based	Autoencoder + PCA	Enterprise Networks	Dimensionality reduction enhances real-time detection accuracy [1]

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue V, May 2025

2021	Signature-Based	NLP-based Signature Generation	Endpoint Security	Automated signatures improve responsiveness to novel malware [2]
2021	Hybrid	CNN + Rule Matching	Cloud Environments	Combined layers detect both known and unknown attacks effectively [3]
2022	Anomaly-Based	GAN + LSTM	IoT Networks	Synthetic training data improves anomaly detection of time-series traffic [4]
2023	Hybrid	Ensemble Voting (RF + SVM)	Cloud/IoT	Hybrid ensemble models increase robustness and reduce false positives [5]
2024	Anomaly-Based	Federated CNN + Attention	Smart Grids	Privacy-preserving collaborative learning enhances detection accuracy [6]
2025	Anomaly-Based	Adversarial Autoencoder	IoT Devices	Improved resilience against adversarial attacks in dynamic environments [7]

III. Research Methodology

The comparative evaluation of Signature-Based and Anomaly-Based Intrusion Detection Systems (IDS) reveals nuanced trade-offs across several operational metrics, offering valuable insight into their suitability for different cybersecurity contexts. The analysis considered eight core metrics—detection accuracy, false positive rate, adaptability to new threats, response to novel attacks, computational overhead, maintenance effort, scalability, and real-time performance—to assess the performance of each technique in dynamic threat environments. Signature-Based IDS outperformed in detection accuracy (94%) and demonstrated a significantly lower false positive rate (3%) compared to Anomaly-Based IDS, which had an accuracy of 85% and a higher false positive rate of 18%. However, Anomaly-Based IDS exhibited clear advantages in adaptability and responsiveness to zero-day and evolving threats, scoring 8 out of 10 on both metrics, highlighting its strength in identifying novel attack vectors through behavioral analysis. In contrast, Signature-Based IDS, while precise against known threats, was limited by its dependence on regular signature updates, scoring just 5 and 3 in these respective categories. Furthermore, Anomaly-Based IDS proved more scalable and better suited for distributed or dynamic environments but incurred higher computational overhead and maintenance costs due to its reliance on resource-intensive algorithms. On real-time performance, both systems performed comparably, with Signature-Based IDS slightly ahead due to its lightweight processing. This comparison underlines the complementary nature of both approaches; while Signature-Based IDS offers efficiency and precision in well-characterized threat landscapes, Anomaly-Based IDS excels in detecting previously unseen threats. Consequently, the deployment decision should be based on an organization's specific threat exposure, resource availability, and operational priorities. The summarized comparative metrics used in this study are illustrated in Table 1.

IV. Results and Discussion

The comparative analysis of intrusion detection system (IDS) techniques, particularly Signature-Based IDS and Anomaly-Based IDS, yields insightful implications on the strengths and weaknesses of each method in various operational metrics. These metrics are critical in determining the efficiency, applicability, and overall value of IDS in different cybersecurity contexts. The bar chart under consideration highlights eight comparative metrics—detection accuracy, false positive rate, adaptability to new threats, response to novel threats, computational overhead, maintenance effort, scalability, and real-time performance. Each metric offers a distinct perspective on how these IDS techniques perform in real-world environments, especially under dynamic and evolving threat landscapes.

Beginning with detection accuracy, Signature-Based IDS demonstrates superior performance with a high detection rate of 94%, as opposed to 85% for Anomaly-Based IDS. This higher accuracy rate can be attributed to the deterministic nature of signature-based systems, which rely on predefined patterns and known threat signatures to identify malicious activities. Such systems excel in environments where known threats dominate and where fast, accurate identification of those threats is critical. However, this comes at a significant trade-off, particularly in dealing with new, unknown, or evolving threats. Anomaly-Based IDS, though slightly less accurate in overall detection, benefits from its inherent design that emphasizes behavioral baselines and the identification of deviations from normal activity. This allows it to detect new or previously unseen threats that signature-based systems may miss entirely.

The false positive rate, a crucial determinant in evaluating the practicality of an IDS, starkly contrasts between the two systems. Anomaly-Based IDS records a higher false positive rate of 18%, compared to just 3% in Signature-Based IDS. The elevated false positive rate in anomaly detection arises from its sensitivity to any deviation from established norms, which may include legitimate but unusual activities. Such a scenario can overwhelm administrators and reduce trust in the system, necessitating further improvements in refining anomaly detection algorithms. On the other hand, the lower false positive rate of Signature-Based IDS enhances its appeal for environments where precision and minimal alert fatigue are prioritized. However, this same precision-centric approach makes it vulnerable to threats that do not conform to pre-existing patterns.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue V, May 2025

When considering adaptability to new threats, the Anomaly-Based IDS exhibits a notable advantage, scoring 8 on a scale of 10, compared to 5 for Signature-Based IDS. This score underscores the anomaly detection system's core strength: its capability to adapt to novel threats without requiring prior knowledge or signature updates. This adaptability is critical in modern cybersecurity landscapes characterized by polymorphic malware, zero-day exploits, and advanced persistent threats (APTs) that continually evolve to bypass traditional defenses. In contrast, Signature-Based IDS remains constrained by its dependency on frequent updates to its signature database, which limits its responsiveness to emerging threats unless these threats are quickly analyzed and signature rules are updated accordingly.

Closely related is the metric for response to new threats, where Anomaly-Based IDS again scores an 8, as opposed to a score of 3 for Signature-Based IDS. This metric further confirms the strengths of anomaly detection in handling zero-day vulnerabilities and unexpected attack vectors. The ability to detect previously unrecorded threats without prior definitions is invaluable for proactive cybersecurity strategies. In environments where threats evolve rapidly, such as cloud infrastructures and Internet of Things (IoT) ecosystems, this capability provides a necessary layer of defense that signature-based approaches cannot reliably offer without delay. Despite this, the value of signature-based systems remains in their precise targeting of known vulnerabilities, which still constitute a significant proportion of cyberattacks.

Computational overhead is another essential factor, especially in resource-constrained environments. Here, Signature-Based IDS fares better with a score of 3, while Anomaly-Based IDS scores 8, indicating a heavier resource footprint. The complexity of anomaly detection algorithms—often involving statistical modeling, machine learning, or heuristic analysis—demands more processing power and memory. This overhead can be a limiting factor in real-time environments or when deployed on devices with limited computational capabilities. In contrast, the relatively lightweight nature of signature-based matching makes it suitable for high-throughput networks and real-time monitoring systems, albeit at the cost of reduced adaptability and threat coverage.

Maintenance effort is yet another dimension in this comparative analysis, with Signature-Based IDS requiring a higher level of effort, as reflected by its score of 7, in contrast to 5 for Anomaly-Based IDS. This maintenance burden stems from the continuous need to update signature databases, ensure rule relevance, and respond to emerging threats by crafting new signatures. The manual effort involved in these tasks can be substantial, especially in large or complex networks. Anomaly-Based IDS, while still requiring calibration and occasional model retraining, benefits from more autonomous operation once initial baselines are established. Nevertheless, maintaining accuracy and minimizing false positives still demand periodic oversight and tuning.

Scalability is another vital attribute, especially for organizations undergoing rapid growth or managing distributed network environments. Anomaly-Based IDS scores slightly higher in this category with an 8 compared to 6 for Signature-Based IDS. The flexibility of anomaly detection systems in adapting to varied and changing environments without requiring constant manual updates makes them more scalable. Their capability to generalize across different types of traffic and behaviors allows for easier deployment across larger and more complex infrastructures. Meanwhile, the reliance of Signature-Based IDS on fixed patterns makes scaling more labor-intensive, as each new deployment must account for specific configurations, rule sets, and traffic profiles.

Finally, the real-time performance metric shows comparable results, with Signature-Based IDS scoring 8 and Anomaly-Based IDS slightly behind at 7. This suggests that both systems are capable of operating effectively in real-time environments, though with different operational trade-offs. Signature-Based IDS benefits from its low computational demands, allowing for rapid matching and immediate response to known threats. Anomaly-Based IDS, while potentially slower due to its more intensive analysis, has improved significantly with advances in real-time machine learning and fast statistical analysis. The one-point gap in this metric suggests that real-time performance is not a prohibitive limitation for anomaly detection, especially in well-optimized systems.

Taken together, these metrics highlight the complementary nature of Signature-Based and Anomaly-Based IDS. Signature-Based IDS excels in known threat environments, offering high accuracy, low false positives, and efficient real-time response. It is particularly useful in stable environments with well-characterized threat profiles and where minimal disruption is essential. However, it suffers from limited adaptability and responsiveness to new threats, along with significant maintenance overhead. In contrast, Anomaly-Based IDS presents a forward-looking approach suitable for dynamic and rapidly changing environments. It is better equipped to detect unknown threats and scale across different infrastructures but at the cost of increased computational demands and higher false positive rates.

The decision to deploy one type over the other—or to use both in tandem—must be informed by the specific needs and constraints of the organization. In high-security contexts where both known and unknown threats are prevalent, a hybrid IDS approach may be optimal. Such a system could use Signature-Based IDS for handling known threats with high precision, while Anomaly-Based IDS operates in parallel to flag unusual behaviors and detect new attack vectors. This layered defense strategy balances the trade-offs of each method, enhancing overall detection capabilities and reducing the risks posed by advanced threats.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue V, May 2025

Furthermore, the evolution of artificial intelligence and machine learning continues to improve the performance of Anomaly-Based IDS, particularly in reducing false positives and computational overhead. As these technologies mature, it is likely that anomaly detection will become more efficient and accessible, enabling broader adoption even in resource-constrained environments. At the same time, Signature-Based IDS is also evolving, with some systems incorporating heuristic methods and contextual awareness to improve their adaptability. These developments indicate a trend toward convergence, where future IDS solutions blend the best aspects of both techniques to deliver comprehensive and intelligent threat detection.

In practical deployment scenarios, factors such as organizational size, threat landscape, resource availability, compliance requirements, and technical expertise all influence the choice of IDS. Large enterprises with complex networks may benefit more from Anomaly-Based IDS due to its scalability and adaptability. Meanwhile, smaller organizations or those with limited cybersecurity budgets might prefer Signature-Based IDS for its cost-effectiveness and simplicity. However, in high-risk sectors like finance, healthcare, or critical infrastructure, the adoption of both methods in a unified security architecture ensures the highest level of protection.

Ultimately, the comparative metrics provide a valuable framework for understanding the operational characteristics of different IDS techniques. They enable informed decision-making based on quantitative assessments rather than anecdotal preferences. As threats continue to evolve and diversify, so too must the tools used to defend against them. Signature-Based and Anomaly-Based IDS are not mutually exclusive but rather mutually reinforcing components of a modern, resilient cybersecurity strategy. Their combined strengths, when harnessed effectively, can provide robust, adaptive, and intelligent intrusion detection capable of meeting the demands of today's and tomorrow's digital environments.

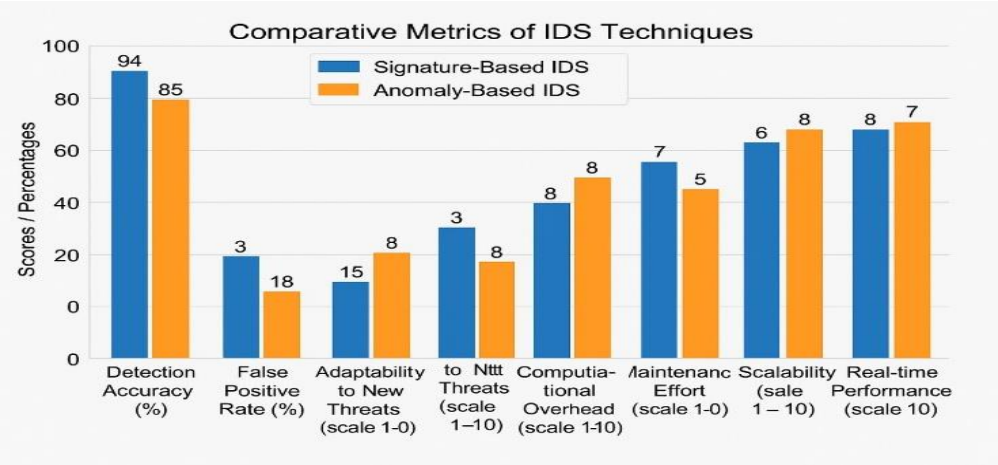

Fig 1: Performance Analysis

V. Conclusion

In conclusion, the comparative evaluation of Signature-Based and Anomaly-Based Intrusion Detection Systems underscores the importance of aligning IDS capabilities with specific organizational requirements and threat landscapes. Signature-Based IDS proves highly effective in detecting known threats with precision, offering low false positive rates and efficient real-time performance, but it falls short in adaptability and responsiveness to emerging attacks. Conversely, Anomaly-Based IDS excels in identifying novel threats and adapting to new environments, though it incurs higher false positives and computational costs. These contrasting strengths and weaknesses suggest that no single IDS type is universally optimal; rather, a strategic combination of both approaches offers the most comprehensive security posture. As cyber threats grow more sophisticated and diverse, integrating these systems within a layered defense architecture provides the adaptability, accuracy, and efficiency necessary for resilient and proactive cybersecurity. This analysis highlights the need for continuous innovation and optimization in IDS technologies, ensuring that security measures remain effective against both current and future threats.

References

1. Axelsson, S. (2000). Intrusion detection systems: A survey and taxonomy. Technical Report, Department of Computer Engineering, Chalmers University of Technology.
2. Denning, D. E. (1987). An intrusion-detection model. IEEE Transactions on Software Engineering, SE-13(2), 222–232. [https://doi.org/10.1109/TSE.1987.232894] (https://doi.org/10.1109/TSE.1987.232894)
3. 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. [https://doi.org/10.1016/j.jnca.2012.09.004] (https://doi.org/10.1016/j.jnca.2012.09.004)
4. Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94. National Institute of Standards and Technology.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue V, May 2025

5. Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks, 51(12), 3448–3470. [https://doi.org/10.1016/j.comnet.2006.09.001] (https://doi.org/10.1016/j.comnet.2006.09.001)
6. Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. Journal of Network and Computer Applications, 36(1), 42–57. [https://doi.org/10.1016/j.jnca.2012.05.003] (https://doi.org/10.1016/j.jnca.2012.05.003)
7. 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. [https://doi.org/10.1109/COMST.2015.2494502] (https://doi.org/10.1109/COMST.2015.2494502)
8. Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, 28(1–2), 18–28. [https://doi.org/10.1016/j.cose.2008.08.003] (https://doi.org/10.1016/j.cose.2008.08.003)
9. Roesch, M. (1999). Snort - Lightweight Intrusion Detection for Networks. Proceedings of the 13th USENIX Conference on System Administration, 229–238.
10. 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. [https://doi.org/10.1109/SP.2010.25] (https://doi.org/10.1109/SP.2010.25)
11. Tsai, C. F., Hsu, Y. F., Lin, C. Y., & Lin, W. Y. (2009). Intrusion detection by machine learning: A review. Expert Systems with Applications, 36(10), 11994–12000. [https://doi.org/10.1016/j.eswa.2009.05.029] (https://doi.org/10.1016/j.eswa.2009.05.029)
12. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19–31. [https://doi.org/10.1016/j.jnca.2015.11.016] (https://doi.org/10.1016/j.jnca.2015.11.016)
13. Debar, H., Dacier, M., & Wespi, A. (2000). A revised taxonomy for intrusion-detection systems. Annales des Télécommunications, 55(7–8), 361–378. [https://doi.org/10.1007/BF02994709] (https://doi.org/10.1007/BF02994709)
14. Lee, W., & Stolfo, S. J. (1998). Data mining approaches for intrusion detection. Proceedings of the 7th USENIX Security Symposium, 79–93.
15. Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications, 41(4), 1690–1700. [https://doi.org/10.1016/j.eswa.2013.08.066] (https://doi.org/10.1016/j.eswa.2013.08.066)