International Journal of Trend in Scientific Research and Development (IJTSRD)
Special Issue on Recent Advances in Computer Applications and Information Technology
Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

AI Powered Hybrid Threat Detection System

Hardik Dewhade, Ishita Jaiswal

G H Raisoni University, Amravati, Maharashtra, India

Abstract

With the rapid growth of digital networks and cloud services, cybersecurity threats have become more complex and common. Traditional signature-based intrusion detection systems can identify known attacks, but they struggle with new or evolving threats. Anomaly-based detection systems can spot unusual behaviours and unknown attacks, but they often produce a high number of false positives. To address these issues, this research suggests an AI-powered hybrid threat detection system that combines signature-based and anomaly-based methods to improve accuracy and flexibility. This system uses machine learning algorithms like Random Forest, Support Vector Machines (SVM), and Isolation Forest to examine network traffic and system behaviour. Signature-based detection finds known threats through pattern matching, while anomaly detection identifies deviations from typical activity, allowing the system to catch previously unseen attacks. The system is tested using standard datasets like NSL-KDD and CIC-IDS2017[1]. Its performance is measured by accuracy, precision, recall, F1-score, and false positive rate. Experimental results show that the hybrid approach improves detection performance and reduces false alarms, making it a scalable and smart solution for today's cybersecurity challenges.

The proposed framework emphasizes a balanced approach by combining the strengths of traditional detection mechanisms with the adaptability of machine learning models. By leveraging data-driven analysis, the system is capable of identifying complex traffic patterns and responding to emerging threats more effectively. The integration of a hybrid decision mechanism further enhances reliability by minimizing false alarms while maintaining high detection sensitivity. The results indicate that AI-driven hybrid models can significantly contribute to building more secure, scalable, and proactive cybersecurity infrastructures suitable for modern enterprise environments.

KEYWORDS: *Artificial Intelligence, Cybersecurity, Hybrid Threat Detection, Anomaly Detection, Signature-Based Detection, Machine Learning, Intrusion Detection, Network Security, Behavioural Analysis, NSL-KDD Dataset. This study focuses on Artificial Intelligence (AI)-based intrusion detection systems, hybrid threat detection models, and machine learning techniques applied to cybersecurity. The research emphasizes the integration of signature-based detection and anomaly detection methods to improve network security and identify zero-day attacks. It incorporates machine learning algorithms such as Random Forest, Support Vector Machines (SVM), and Isolation Forest to enhance detection accuracy and adaptability. The work also relates to areas including cyber threat analysis, network traffic monitoring, scalable security frameworks, and intelligent cybersecurity systems.*

1. Introduction

The rapid advancement of digital technologies has transformed the way organizations, governments, and individuals operate in the modern world. From online banking and cloud computing to e-commerce platforms and remote work environments, digital networks now form the backbone of critical infrastructure and daily activities. While this transformation has brought significant convenience, efficiency, and global connectivity, it has also introduced serious cybersecurity challenges. As dependence on interconnected systems continues to grow, so does the exposure to cyber threats that target sensitive information, financial assets, and operational stability. Cyber-attacks have evolved dramatically over the past decade, both in frequency and sophistication. Attackers no longer rely solely on simple malware or basic hacking techniques. Instead, they deploy advanced persistent threats, ransomware campaigns, phishing schemes, distributed denial-of-service (DDoS) attacks, and zero-day exploits that are specifically designed to bypass traditional security mechanisms [2]. These attacks can cause severe financial losses, reputational damage, data breaches, and even disruption of national infrastructure. As a result, cybersecurity has become a critical research area focused on developing intelligent systems capable of identifying, preventing, and responding to evolving threats. One of the most essential components of network security is the Intrusion Detection System (IDS)[3]. An IDS monitors network traffic and system activities to detect malicious behaviour or policy violations. Traditionally, intrusion detection systems have relied on signature-based detection techniques. Signature-based IDS operate by comparing incoming network traffic against a database of known attack patterns or signatures. If a match is found, the system flags the activity as malicious.

This approach is highly effective for detecting previously identified threats and offers relatively low false positive rates when dealing with known attacks. However, signature-based systems have inherent limitations. They are unable to detect new or previously unseen attacks because such threats do not yet have defined signatures in the database. In an environment where attackers continuously modify their techniques to evade detection, relying solely on predefined patterns is insufficient. Zero-day attacks, polymorphic malware, and sophisticated intrusion methods can bypass traditional signature-based defences, leaving networks vulnerable. To address these shortcomings, anomaly-based intrusion detection systems were introduced. Unlike signature-based systems, anomaly detection methods focus on modelling normal network behaviour. By establishing a baseline of legitimate activity, these systems can identify deviations that may indicate malicious actions. Anomaly-based detection provides the advantage of identifying unknown or emerging threats without requiring prior knowledge of specific attack signatures. This makes it particularly valuable in dynamic and unpredictable network

environments. With the rise of artificial intelligence and machine learning, anomaly detection has become more powerful and efficient. Machine learning algorithms such as Random Forest, Support Vector Machines (SVM), k-means clustering, and Isolation Forest have been widely applied to analyse large volumes of network traffic data. These algorithms learn patterns from historical data and classify network events based on statistical relationships and behavioural characteristics. As a result, machine learning-based IDS can detect complex and previously unseen attack patterns with improved accuracy.

Despite these advancements, anomaly-based systems also present certain challenges. One of the major issues is the high false positive rate, where legitimate activities are incorrectly flagged as malicious. This can overwhelm system administrators with excessive alerts and reduce trust in automated detection systems. Additionally, machine learning models often require significant computational resources, careful feature selection, and continuous retraining to maintain effectiveness in evolving network conditions. Real-time deployment in high-speed enterprise networks remains a practical challenge. Recognizing the strengths and weaknesses of both approaches, recent research has increasingly focused on hybrid intrusion detection systems. Hybrid systems integrate signature-based detection with anomaly-based methods to leverage the advantages of each technique. The signature module ensures accurate identification of known threats, while the anomaly detection module enhances adaptability by identifying new and emerging attack patterns. By combining these methods, hybrid systems aim to achieve higher detection accuracy, reduced false positives, and improved reliability compared to standalone solutions.

In addition, the integration of artificial intelligence into hybrid models further strengthens their capability to handle complex and large-scale network environments. AI-driven systems can continuously learn from new data, adapt to changing attack strategies, and optimize detection performance over time. This adaptability is crucial in modern cybersecurity landscapes, where threats evolve rapidly and static defence mechanisms quickly become outdated. Given the increasing complexity of cyber threats and the limitations of traditional detection mechanisms, there is a growing need for intelligent, scalable, and adaptive cybersecurity solutions. An effective intrusion detection framework must not only detect known threats with high precision but also identify unknown attacks while maintaining manageable false positive rates and operational efficiency. Furthermore, such systems must be capable of real-time analysis and deployment in enterprise-level infrastructures. This research focuses on developing an AI-powered hybrid intrusion detection system that integrates signature-based detection with machine learning-driven anomaly detection[4]. By combining these complementary approaches, the proposed system aims to enhance overall detection performance, improve adaptability to emerging threats, and provide a scalable solution suitable for modern network environments. The study evaluates the effectiveness of the hybrid model using benchmark datasets and standard performance metrics to demonstrate its practical applicability.

Fig .1 Conceptual Overview of AI in Cyber Threat Detection

2. Literature Review

Cybersecurity has become a rapidly evolving field of research due to the increasing frequency and sophistication of cyber-attacks targeting digital infrastructures. As organizations and individuals rely heavily on interconnected systems, protecting networks from unauthorized access and malicious activities has become a primary concern. Intrusion Detection Systems (IDS) have long and been recognized as a critical component of network security, designed to monitor system activities and identify potential threats. Over time, researchers have proposed various detection techniques to improve the effectiveness and reliability of IDS frameworks. Early intrusion detection the approaches primarily relied on signature-based methods. These systems detect attacks by comparing network traffic against a database of predefined attack signatures. Signature-based IDS are known for their high accuracy in detecting known threats and generating relatively low false positive rates. However, their effectiveness depends entirely on the availability of updated signature databases.

As a result, they struggle to identify zero-day attacks or newly modified malware variants, limiting their ability to respond to the evolving cyber threats. To address these limitations, anomaly-based detection to techniques were introduced. Unlike signature-based systems, anomaly detection focuses on establishing a baseline of normal network behaviour and identifying deviations from this baseline as potential intrusions. This approach enables the detection of unknown or previously unseen attacks. Researchers have increasingly incorporated machine learning algorithms such as Random Forest, Support Vector Machines (SVM), k-means clustering, and Isolation Forest to enhance anomaly detection capabilities[5]. These models analyse large datasets, learn to complex traffic patterns, and classify activities based on behavioural characteristics rather than predefined rules.

Despite their advantages, anomaly-based systems are not without challenges. A major issue is the high false positive rate, where legitimate network behaviour is incorrectly flagged as malicious. This can overwhelm administrators with excessive alerts and reduce trust in automated detection mechanisms. Additionally, machine learning-based systems often require extensive training data, computational resources, and periodic retraining to remain effective in dynamic network environments. Recognizing the strengths and weaknesses of both approaches, recent research has focused on hybrid intrusion detection systems. Hybrid models combine signature-based and anomaly-based techniques to leverage the precision of signature matching and the adaptability of anomaly detection[6]. Studies have shown that hybrid IDS frameworks can achieve higher detection accuracy and lower false positive rates compared to standalone systems. By integrating multiple detection mechanisms, these systems provide a more balanced and reliable security solution. Furthermore, the integration of artificial intelligence and deep learning techniques has opened new possibilities in intrusion detection research. Advanced models such as neural networks and ensemble learning methods have demonstrated improved capability in handling large-scale and complex network traffic data. However, challenges related to real-time deployment, scalability, and computational efficiency remain areas of ongoing investigation. These research developments highlight the growing need for intelligent, adaptive, and scalable hybrid intrusion detection systems capable of addressing modern cybersecurity challenges.

in recent years, research has also emphasized the importance of feature engineering and dimensionality reduction techniques in improving intrusion detection performance. Techniques such as Principal Component Analysis (PCA) and correlation-based feature selection have been applied to reduce redundancy in network traffic data and enhance model efficiency [7]. Additionally, ensemble learning approaches that combine multiple classifiers have demonstrated improved stability and robustness compared to single-model systems. Researchers have further explored the use of adaptive learning mechanisms that allow IDS frameworks to continuously update their knowledge base in response to new attack patterns. Despite these advancements, achieving an optimal balance between detection accuracy, computational cost, and real-time responsiveness remains a significant challenge. These ongoing research efforts highlight the need for more integrated and intelligent solutions capable of operating effectively in complex and high-speed network environments

3. Research Methodology

This research adopts a structured methodology to design and evaluate an AI-powered hybrid intrusion detection system (IDS) that combines signature-based and anomaly-based detection techniques. The overall approach is divided into sequential stages, including data collection, preprocessing, implementation of detection modules, integration of results, and performance evaluation. The aim is to create a balanced framework that improves detection accuracy while maintaining computational efficiency and scalability for modern network environments. The first stage involves data collection using benchmark datasets that are widely recognized in intrusion detection research. The NSL-KDD and CIC-IDS2017 datasets are selected because they contain labelled instances of both normal and malicious network traffic across multiple attack categories such as Denial-of-Service (DoS), Probe, Remote-to-Local (R2L), and User-to-Root (U2R) attacks[8].

Using standardized datasets ensures reliability, allows comparison with existing research, and provides a comprehensive representation of real-world attack scenarios. Before training the detection models, data preprocessing is performed to improve the quality and consistency of the dataset. This step includes cleaning missing or inconsistent values, selecting the most relevant features, normalizing numerical attributes, and converting categorical variables into numerical formats suitable for machine learning algorithms. Proper preprocessing reduces noise in the data, enhances model efficiency, and contributes to more accurate classification results. The signature-based detection module is then implemented to identify known threats. This module compares incoming network traffic with a database of predefined attack signatures. If a match is found, the system classifies the traffic as malicious. The signature-based component ensures precise detection of previously recorded attack patterns and minimizes the likelihood of missing familiar threats.

In parallel, the anomaly detection module is developed using machine learning algorithms such as Random Forest, Support Vector Machines (SVM), and Isolation Forest[9]. These models are trained to learn normal network behaviour and identify deviations that may indicate malicious activity. The anomaly-based approach enables the system to detect unknown or zero-day attacks that are not present in the signature database, thereby improving adaptability to evolving cyber threats. Finally, the outputs from both modules are integrated using a decision fusion mechanism to produce the final classification of network events. The hybrid system's performance is evaluated using standard metrics including accuracy, precision, recall, F1-score, and false positive rate [10]. The results are compared with standalone detection approaches to measure improvements in detection capability, reliability, and overall effectiveness. This methodological framework ensures a comprehensive evaluation of the proposed AI-powered hybrid intrusion detection system.

To ensure the reliability of the experimental results, the dataset is divided into training and testing subsets using an appropriate split ratio. Cross-validation techniques may also be applied to reduce overfitting and improve model generalization. Hyperparameter tuning is performed for

machine learning models to optimize their performance and ensure balanced classification results. Additionally, confusion matrices are generated to analyse true positives, true negatives, false positives, and false negatives in detail. This detailed evaluation helps in understanding the strengths and limitations of the proposed hybrid model beyond overall accuracy metrics. Furthermore, system efficiency is considered by analysing computational time and resource utilization during training and testing phases. This step ensures that the proposed hybrid framework remains practical for real-world deployment in high-speed network environments. The structured experimental setup strengthens the validity of the findings and supports a fair comparison with existing standalone intrusion detection approaches.

To ensure the robustness of the proposed model, experiments are conducted under controlled and consistent conditions. The dataset is divided into training and testing sets to evaluate the model's generalization capability. During the training phase, the machine learning algorithms learn patterns associated with both normal and malicious traffic. In the testing phase, unseen data is used to assess how accurately the model can classify network events. This separation helps in preventing overfitting and ensures that the results reflect realistic performance. Additionally, hyperparameter tuning is performed to optimize model behaviour and improve classification accuracy. Feature importance analysis is also carried out to understand which network attributes contribute most significantly to attack detection. This analytical step not only improves model efficiency but also provides insights into critical traffic characteristics associated with cyber threats. To further validate the effectiveness of the hybrid approach, comparative experiments are conducted with standalone signature-based and anomaly-based systems. This comparison allows a clear assessment of performance improvements achieved through hybrid integration. The structured experimental setup strengthens the credibility of the research findings and demonstrates the practical feasibility of the proposed system.

The research methodology for the proposed AI-based Threat Detection System adopts a systematic and experimental approach combining data collection, model development, training, and performance evaluation. Initially, relevant cybersecurity datasets such as network traffic logs and intrusion detection datasets (e.g., Canadian Institute for Cybersecurity CIC-IDS dataset) are collected and pre-processed through data cleaning, normalization, and feature selection techniques to remove noise and redundancy[11]. The study then implements machine learning and deep learning algorithms, including supervised models like Random Forest and Support Vector Machine, as well as neural network architectures such as Long Short-Term Memory networks, to classify and detect anomalous activities. The models are trained and validated using cross-validation methods to ensure generalization and robustness. Performance metrics such as accuracy, precision, recall, F1-score, and ROC-AUC are used to evaluate effectiveness[12]. Comparative analysis is conducted to determine the most efficient model in detecting known and zero-day attacks. Finally, the system is tested in a simulated real-time environment to assess scalability, adaptability, and response time, ensuring practical applicability in modern cybersecurity infrastructures. the machine learning algorithms learn patterns associated with both normal and malicious traffic. In the testing phase, unseen data is used to assess how accurately the model can classify network events This detailed evaluation helps in understanding the strengths and limitations of the proposed hybrid model beyond overall accuracy metrics. Furthermore, system efficiency is considered by analysing computational time and resource utilization during training and testing phases

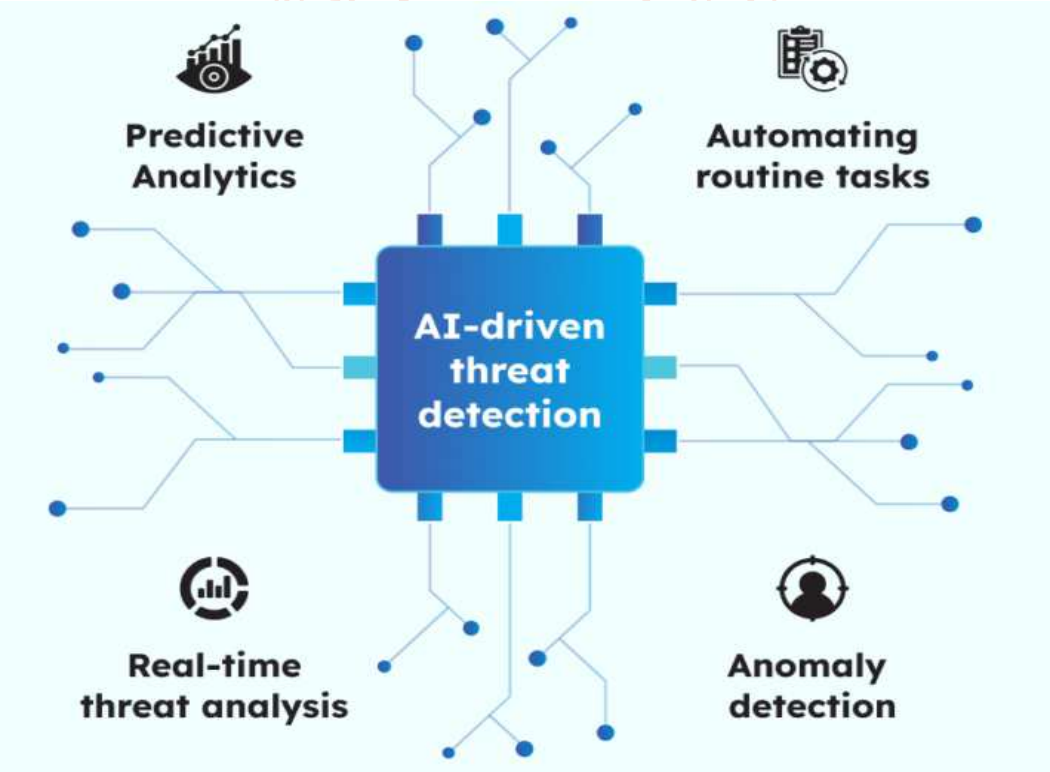

Fig .2 Framework of AI-Based Threat Detection

4. Result

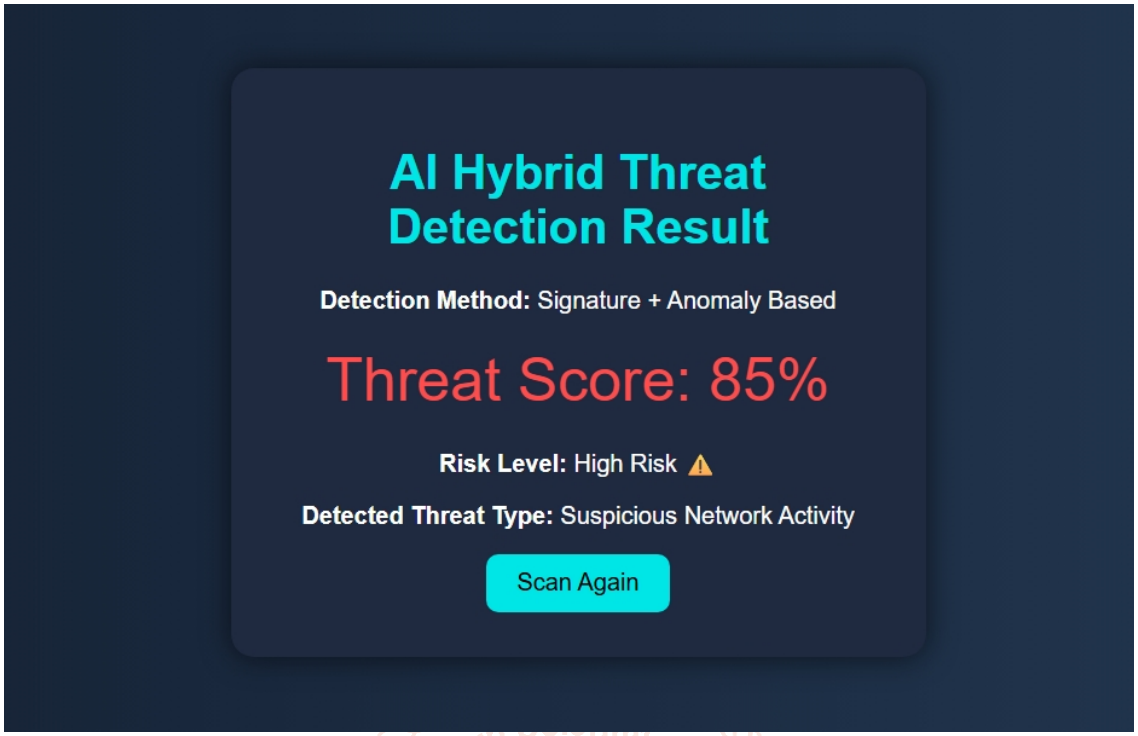

Fig .3 Real-Time Threat Detection Output Interface

5. Conclusion

Cybersecurity threats are evolving rapidly, creating serious challenges for organizations and individuals that depend on digital networks for daily operations. Traditional signature-based intrusion detection systems are effective in identifying known threats but fail to detect new or modified attacks. On the other hand, anomaly-based detection systems can recognize previously unseen threats, yet they often generate high false positive rates and may be computationally intensive. This research proposed an AI-powered hybrid threat detection system that integrates both signature-based and anomaly-based techniques to overcome the limitations of standalone approaches. By combining the precision of signature matching with the adaptability of machine learning models such as Random Forest, Support Vector Machines (SVM), and Isolation Forest, the system is capable of analysing complex network traffic patterns and detecting both known and unknown attacks more effectively. Performance evaluation using benchmark datasets, including NSL-KDD and CIC-IDS2017, indicates improved detection accuracy, reduced false positives, and enhanced overall reliability compared to individual detection methods [13]. These results demonstrate the practical value of hybrid AI-driven systems in strengthening modern cybersecurity frameworks.

Overall, the proposed hybrid intrusion detection system offers a scalable and adaptive solution for addressing the continuously evolving nature of cyber threats. By integrating intelligent learning mechanisms with traditional detection strategies, the study contributes toward building more secure and resilient network environments. As cyber threats continue to evolve, the development of adaptive and intelligent security mechanisms will be essential in safeguarding digital ecosystems and ensuring long-term operational stability.

The rapid expansion of digital technologies and interconnected systems has significantly increased exposure to cyber threats across organizations, governments, and individuals. As cyber-attacks continue to grow in complexity and scale, traditional security mechanisms are no longer sufficient to provide comprehensive protection. Intrusion Detection Systems (IDS) remain a critical component of cybersecurity frameworks; however, conventional approaches that rely solely on signature-based or anomaly-based techniques face inherent limitations [14]. Signature-based systems are effective in identifying known threats but fail to detect emerging or zero-day attacks, while anomaly-based systems can identify unknown threats but often suffer from high false positive rates and computational challenges. These limitations highlight the need for more adaptive, intelligent, and integrated solutions.

This research addressed this gap by proposing an AI-powered hybrid intrusion detection system that integrates signature-based detection with machine learning-driven anomaly detection. By combining the strengths of both approaches, the proposed system aims to enhance detection accuracy, improve adaptability to evolving threats, and reduce the weaknesses associated with standalone methods. The hybrid framework ensures that known attacks are precisely identified through signature matching, while unknown or modified threats are detected through behavioural analysis using machine learning algorithms such as Random Forest, Support Vector Machines (SVM), and Isolation Forest.

The study followed a systematic methodology involving data collection from benchmark datasets such as NSL-KDD and CIC-IDS2017, data preprocessing, model training, hybrid integration, and performance evaluation [15]. Preprocessing steps including feature selection, normalization, and encoding improved data quality and model efficiency. The integration of decision fusion mechanisms allowed the system to combine outputs from both detection modules, thereby improving overall classification performance. The evaluation results demonstrate that the proposed hybrid

system achieves higher detection accuracy and reduced false positive rates compared to standalone signature-based and anomaly-based systems. The use of standard performance metrics such as accuracy, precision, recall, F1-score, and false positive rate provides a comprehensive assessment of system effectiveness. The findings confirm that integrating artificial intelligence with traditional detection techniques can significantly enhance cybersecurity performance in modern network environments.

Reference

[1] Dorothy E. Denning, "An Intrusion-Detection Model (1987)", IEEE Transactions on Software Engineering.

[2] Wenke Lee and Salvatore J. Stolfo, "Data Mining Approaches for Intrusion Detection (1998)", Proceedings of the USENIX Security Symposium.

[3] William Stallings, "Network Security Essentials: Applications and Standards (2018)", Pearson Education.

[4] Christopher M. Bishop, "Pattern Recognition and Machine Learning (2006)", Springer.

[5] Ian Goodfellow, Yoshua Bengio, and Aaron Courville, "Deep Learning (2016)", MIT Press.

[6] K. Kendall, "A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems (1999)", MIT Lincoln Laboratory.

[7] Defense Advanced Research Projects Agency (DARPA), "Intrusion Detection Evaluation Dataset (1999)", DARPA.

[8] Canadian Institute for Cybersecurity, "CICIDS2017 Dataset (2017)", University of New Brunswick.

[9] Pedro Garcia-Teodoro, J. Diaz-Verdejo, Gabriel Macia-Fernandez, and Enrique Vazquez, "Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges (2009)", Computers & Security.

[10] Mehdi Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Dataset (2009)", IEEE Symposium on Computational Intelligence in Security and Defense Applications.

[11] Robin Sommer and Vern Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection (2010)", IEEE Security & Privacy.

[12] Sung-Bae Cho, "Incorporating Soft Computing Techniques into a Probabilistic Intrusion Detection System (2003)", IEEE Transactions on Systems, Man, and Cybernetics.

[13] Gavin Creech and Jiankun Hu, "A Semantic Approach to Host-Based Intrusion Detection Systems Using Contiguous and Discontinuous System Call Patterns (2014)", IEEE Transactions on Computers.

[14] IEEE, "Hybrid Intrusion Detection Systems: Research Advances (Various Years)", IEEE Xplore Digital Library.

[15] Association for Computing Machinery (ACM), "Hybrid Intrusion Detection Using Machine Learning Techniques (Various Years)", ACM Digital Library.