International Journal Software Engineering and Computer Science (IJSECS)
5 (1), 2025, 259-270
Published Online April 2025 in IJSECS (http://www.journal.lembagakita.org/index.php/ijsecs)
P-ISSN: 2776-4869, E-ISSN: 2776-3242. DOI: https://doi.org/10.35870/ijsecs.v5i1.3989.

RESEARCH ARTICLE Open Access

Application of Machine Learning in Computer Networks: Techniques, Datasets, and Applications for Performance and Security Optimization

Memed Saputra *
Informatics Study Program, Faculty of Engineering, Universitas Primagraha, Serang City, Banten Province, Indonesia.
Corresponding Email: memedsaputra890@gmail.com.

Fegie Yoanti Wattimena
Information Systems Study Program, Faculty of Science & Technology, Universitas Ottow Geissler, Jayapura City, Papua Province, Indonesia.
Email: fegiywattimena.travel@gmail.com.

Davy Jonathan
Computer Science Department Program, Universitas Raharja, Tangerang City, Banten Province, Indonesia.
Email: davyjonathan13@gmail.com.

Received: January 28, 2025; Accepted: February 10, 2025; Published: April 1, 2025.

Abstract: This study designs and tests a network security system based on a combined Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN) framework. In this study, distributed processing and reinforcement learning methods in combination with differential privacy are introduced into the proposed system to enhance attack detection and network management. The evaluation results show significant improvements; 97.3% detection accuracy, 34% more efficient bandwidth utilization and 45% less latency than the previous system. The 16-node linear scalability of the distributed architecture has a throughput of 1.2 million packets per second. It is defended against adversarial attacks by maintaining accuracy above 92% and provides a total energy saving of 38% using dynamic batch processing. Three months of testing in an operational environment detected 99.2% of 1,247 threats, including 23 new attack types, with an average detection time of 1.8 seconds. Sensitivity analysis was performed to preserve the privacy of sensitive data while maintaining network performance. The results show that the hybrid solution is reliable, scalable and secure for today's network management.

Keywords: Hybrid Machine Learning; CNN-RNN Framework; Network Security; Threat Detection; Real-Time Processing.

1. Introduction

Computer networking technology has evolved significantly in the last 20 years. These extraordinary developments bring new challenges to administering and monitoring your network infrastructure: the explosion of internet-enabled devices, and the exponential upsurge in data size; and the growing complexity of today's network architecture. Against this background, effective network security systems has become more critical to deal with multiple threats. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are found to be effective in the detection and mitigation of cyber threats and have become an active area of research in today's network security community [1][2]. Additionally, other studies underscore the critical need for designing security mechanisms to prevent brute-force attacks on network devices such as routers, a prevalent challenge in the digital era [3]. Cyberattack detection, bandwidth optimization, traffic classification, and network resource management require adaptive and automated approaches. In this regard, bandwidth optimization through technologies like the Mikrotik Router offers practical solutions to enhance computer network efficiency [4]. Furthermore, Web Application Firewalls (WAF) are highly recommended as a preventative measure to bolster website security and detect potential threats [5]. The advancement of steganography techniques also garnered attention for securing data transmitted across networks [6]. With the escalating complexity and volume of data, human resources management within network operations has gained in significance. The human element remains a vital factor in ensuring the successful implementation and oversight of information technology, which in turn supports network infrastructure security and efficiency [7]. Training and development initiatives for network management can address technical skill gaps, often a barrier to handling modern network technologies.

Consequently, addressing the challenges of managing and securing computer network infrastructure necessitates a comprehensive strategy that integrates cutting-edge technology with human resource enhancement. Machine learning emerged as a promising solution to network management issues. Its ability to analyze data patterns, make predictions, and automate decision-making opens new avenues for developing more efficient and secure network systems. Techniques such as deep learning, reinforcement learning, and supervised learning have shown encouraging results across multiple facets of network management. Notably, deep learning excels at processing vast and diverse datasets, as highlighted by LeCun *et al.*, who emphasize its capacity to capture complex data representations crucial for network analysis [8]. Similarly, Zhang *et al.* Demonstrate the application of reinforcement learning in network optimization for traffic signal control, providing further evidence of its potential in network management [9]. The selection of appropriate datasets plays a pivotal role in the successful application of machine learning to computer network systems. High-quality datasets must encompass a range of normal and anomalous scenarios, feature accurate labeling, and reflect modern network traffic. Yang argues that machine learning data should mirror real-world conditions to enhance model performance [10]. Proper dataset selection and preprocessing are critical in determining a model's ability to recognize attack patterns, classify traffic, and optimize resource utilization. For instance, Polydoros and Nalpantidis discuss the application of reinforcement learning models in robotics control, which relates to data processing and pattern recognition [11]. Ghillani (2022) further stresses the importance of deep learning algorithms in bolstering cybersecurity by leveraging network data as input for models [12].

By employing these techniques, machine learning can significantly enhance the resilience and efficiency of modern network systems. This is a crucial aspect of confronting the ever-evolving cybersecurity challenges of the digital age [13][12]. However, a primary challenge in applying machine learning to computer networks lies in the complexity of processing data in real time. Modern network traffic is dynamic and heterogeneous, involving diverse communication protocols and service types. Moreover, the emergence of new security threats and rapid shifts in traffic patterns necessitate machine learning models that can adapt to such changes. This research into the implementation of machine learning in computer network systems aims to develop effective methodologies to improve system reliability. The primary focus includes analyzing suitable machine learning techniques for various use cases, evaluating relevant datasets, and testing implementations in real-world network environments. The proposed methodology encompasses feature selection, data preprocessing, algorithm selection, and performance evaluation [14][15]. Machine learning methodologies offer fresh insights into managing complex networks and enhancing system responsiveness to diverse traffic dynamics [16]. Security remains a key concern in this study, given the rising frequency and sophistication of cyber-attacks. Developing machine learning-based intrusion detection systems enables more accurate and responsive threat identification. Analyzing abnormal traffic patterns and classifying attacks using machine learning algorithms can significantly improve a system's ability to detect and prevent security breaches [17][18][19]. Recent studies also indicate that combining machine learning with deep learning techniques can strengthen intrusion detection systems by improving accuracy and detection speed [20][21].

Another pivotal part of this research that deals with network performance optimization. This needs Predicting network load, usage of bandwidth and Adaptive routing for resource utilization to be managed through machine learning. Network systems in Machine learning: Machine learning algorithms that

automatically tune parameters of the network systems according to traffic and user requirements [22][23][24]. They help improve the operational efficiency and ability of respond to external changes in an adaptive manner. It is important for IoT or cloud computing [25]. Therefore the usage of machine learning in computer network systems is not only to improve the reliability and safety, but also contributes to the maximum network performance irrelevantly. It paves the way to new research directions, designing machine learning methods for the dynamic cyber challenges [26][27]. The research methodology was experiments and evaluations previously described in the controlled test environments. Testing runs on standard dataset and real traffic data that was gathered from the operational networks. Performance evaluation are based on conventional parameters such as accuracy, precision, recall performance parameters such latency, throughput and attack detection rates. The results are a valuable benchmark to guide the design of machine learning models for increasing the robustness in computer network systems as well This promotes the use of prospective security and performance challenges for intelligent network system architectures that will be able to respond across a wide range of scales; corporate networks all the way down to large telecom infrastructures.

2. Related Work

The application of machine learning (ML) to computer network systems has garnered significant attention due to its potential to enhance security and performance optimization. With advancements in this field, a variety of techniques have been introduced to address challenges in intrusion detection and network traffic management. Supervised learning approaches, for instance, have demonstrated notable accuracy in threat detection, with some intrusion detection systems achieving up to 95% accuracy in identifying diverse attack types, including zero-day attacks [14][15]. Research by Hoshino and Jinno (2018) further explores machine learning optimization for neural networks using non-linear mapping, resulting in improved detection of complex attack patterns [16]. Deep learning models, particularly those based on architectures like Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), have shown remarkable performance in recognizing comprehensive attack patterns. For example, Lei *et al.* (2024) Highlight the effectiveness of the XGBoost model in detecting network traffic anomalies, contributing to overall network security [17]. This aligns with findings by Naeem, who emphasizes the role of machine learning techniques in strengthening network security in IoT environments [18]. Additionally, reinforcement learning has made substantial progress in network optimization. Studies reported reductions in network latency by up to 30% and throughput improvements of 25% through adaptive machine learning techniques [15][19]. The integration of graph neural networks with deep reinforcement learning has also yielded significant advancements in Quality of Service (QoS) management and resource allocation [18]. Ashwarf *et al.* Underscore the importance of ML-based intrusion detection systems in IoT networks, advocating for sustainable solutions to persistent challenges [20]. The rapid evolution of machine learning applications in computer networks necessitates a deeper understanding of how these techniques can simultaneously enhance security and performance. Research by BaniMustafa *et al.* Provides valuable insights into the use of various classification algorithms to identify diverse network attacks [21]. Similarly, Zatadini *et al.* Evaluate the effectiveness of neural networks in cybersecurity contexts, while refining intrusion detection models [22].

High-quality datasets are a critical focus in applying machine learning to computer networks, particularly for performance optimization and security. Reliable datasets enable more effective and relevant model training. Efforts to standardize network traffic data have produced datasets encompassing modern attack scenarios. This has facilitated the development of automated labeling techniques through semi-supervised learning. This approach addresses the scarcity of labeled data, as demonstrated in studies showing how such techniques mitigate data labelling challenges [23]. Unsupervised learning for anomaly detection also shows promise, with algorithms like Isolation Forest and auto-encoders proving effective in identifying abnormal traffic patterns without reliance on labeled data. Research comparing anomaly detection techniques, including Isolation Forest, confirms their efficacy in real-world scenarios [24][25][26]. This is especially relevant in enterprise environments, where their implementations reduce false positive rates compared to traditional detection systems [26]. Moreover, hybrid architectures combining multiple deep learning models significantly contribute to multi-layer traffic classification. These techniques excel at identifying protocols and applications, even in encrypted traffic, with studies reporting precision improvements of up to 20% through ensemble methods and feature selection for anomaly detection, enhancing system resilience against evolving traffic patterns [27][28]. Recent advancements in network classification further demonstrate how neural network innovations support traffic management and anomaly detection optimization [29].

Machine learning offers adaptive methods to optimize power consumption in networks. Predictive models for server load and dynamic resource adjustment have achieved energy savings of up to 40% without compromising service quality. This is complemented by research from Esterlin *et al.*, (2024) which highlights the integration of attack detection algorithms with power management to improve energy efficiency in network

infrastructure [30]. Additionally, the growing diversity of evaluation frameworks for ML-based security systems underscores the importance of testing methodologies that assess resilience against adversarial attacks. Huda and Subektiningsih analyze the implementation of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to enhance network security through notification mechanisms, advocating for standardized testing to compare security approaches [1]. Distributed learning techniques are also gaining traction for addressing scalability in large-scale implementations. Sibarani *et al.* Demonstrate the effectiveness of ML algorithms on the Bot-IoT dataset for intrusion detection while preserving data privacy across broader networks [31].

Feature engineering remains essential for optimizing feature identification for malware detection and network congestion prediction. Studies show that dimensionality reduction techniques, such as Principal Component Analysis (PCA), significantly improve processing efficiency without sacrificing model accuracy [32]. This supports the development of more efficient ML model training, addressing various challenges in network traffic analysis. Furthermore, integrating machine learning with blockchain technology represents a novel approach to network security. Smart contracts can automate threat responses and provide tamper-proof audit trails, ensuring reliability in detection and response mechanisms, though further validation of such claims is needed [32]. Network security is a key trend in adaptive models capable of real-time parameter adjustment. Systems employing ensemble learning techniques create more robust frameworks by combining various ML methods, such as predictive memory models. This is to capture complex traffic patterns and enable real-time response adjustments [32]. Recent studies emphasize that dynamic interactions among diverse learning methods yield more resilient and efficient outcomes, critical to long-term network reliability. The application of machine learning in computer networks reflects significant progress across detection techniques, dataset development, performance and security optimization. Future advancements will depend on the ability to continuously generate and manage high-quality data while adapting existing models to meet emerging network security challenges.

3. Research Method

The research methodology begins with the collection of network traffic data from diverse sources, achieved by deploying sensors at strategic points within the network infrastructure to capture both normal traffic and attack scenarios. This data collection process spans six months to ensure sufficient variation in traffic patterns, with sensors configured to record critical parameters such as packet headers, data flow statistics, and communication protocol metadata. The preprocessing stage involves a series of transformations to produce a high-quality dataset, including normalization of numeric features using min-max scaling and standardization, handling incomplete data through imputation based on the k-nearest neighbors algorithm, deriving additional attributes via feature engineering (*e.g.*, temporal statistics, packet distribution characteristics, and host interaction patterns), and applying Principal Component Analysis (PCA) for dimensionality reduction to lower computational complexity. The machine learning architecture developed for network applications adopts a hybrid approach, integrating multiple neural network models to enhance data processing efficiency and security. The first layer employs a Convolutional Neural Network (CNN), effective at extracting spatial patterns from network traffic data, adapted from visual data applications to aid in intrusion detection and traffic analysis [14][33]. The subsequent layer uses a Recurrent Neural Network (RNN) with Long Short-Term Memory (LSTM) units to sequentially analyze temporal data flows inherent in network traffic, with research indicating that combining CNN and RNN enhances attack detection and comprehensive traffic understanding [33][34]. This hybrid integration in intrusion detection systems captures both temporal and spatial characteristics of network traffic, offering novel insights into attack detection and normal traffic behavior analysis for performance optimization [14][35], further complemented by other machine learning techniques to improve accuracy and efficiency in anomaly detection and threat level estimation across diverse operational environments [36][37]. Model training is conducted on a distributed computing infrastructure, splitting the dataset into training (70%), validation (15%), and testing (15%) subsets using stratified sampling to maintain class distribution, employing 5-fold cross-validation for robustness assessment, and optimizing hyperparameters like learning rate, number of layers, batch size, and regularization factors via Bayesian optimization. System implementation focuses on a real-time processing pipeline using a distributed streaming framework for parallel data processing with low latency, integrating preprocessing modules to minimize computational overhead, adopting a microservices architecture for scalability and maintenance, and implementing failover and load balancing for service availability. Performance evaluation uses quantitative metrics such as attack detection accuracy via confusion matrix, precision, recall, and F1-score, latency measurement at each processing stage from data capture to classification, throughput testing under varying traffic loads to determine maximum capacity, and adversarial testing to evaluate model resilience against input manipulation. Security is prioritized with end-to-end encryption across communication channels, role-based

access control to restrict access to sensitive models and data, automated logging and audit trails for detailed activity tracking, and secure enclaves to protect machine learning models from extraction or tampering. Performance optimization mechanisms include dynamic batch processing to adjust batch sizes based on system load, intelligent caching to reduce redundant computations, distributed model serving for parallel processing to enhance throughput, and adaptive resource management to dynamically allocate resources based on real-time needs. Validation occurs in both simulated and production network environments, using a network simulator configured for diverse operational scenarios, rolling out production testing gradually from isolated segments to full deployment, and continuously monitoring performance metrics for long-term evaluation. Ethical considerations and data privacy are integral, with data anonymization applied to sensitive data before processing, consent management ensuring compliance with privacy regulations, differential privacy protecting individual information within training datasets, and data deletion protocols allowing permanent removal of sensitive information when required.

4. Result and Discussion

4.1 Results

This section presents the detailed outcomes of research on network security and optimization using a hybrid machine learning approach. The results are organized into thematic subsections to provide a structured overview of the system's performance across various dimensions. These dimensions include detection accuracy, real-time processing, network optimization, resilience to attacks, computational efficiency, production validation, resource consumption, privacy compliance, and scalability. Visual aids such as charts and tables are included to enhance understanding and are referenced as figures and tables with appropriate numbering. The hybrid machine learning architecture, combining Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) with Long Short-Term Memory (LSTM) units, achieves an attack detection accuracy of 97.3%. This is supported by a precision of 96.8%, a recall of 95.9%, and an F1-score of 96.3%, indicating high reliability in identifying threats with minimal errors. Compared to traditional signature-based detection methods, this model offers a 23% improvement in performance. Analysis of the confusion matrix revealed the model's precision in distinguishing various attack types. It maintained a low false positive rate of only 2.1%, which reduces unnecessary alerts and operational interruptions. These metrics are visually summarized in Figure 1 below.

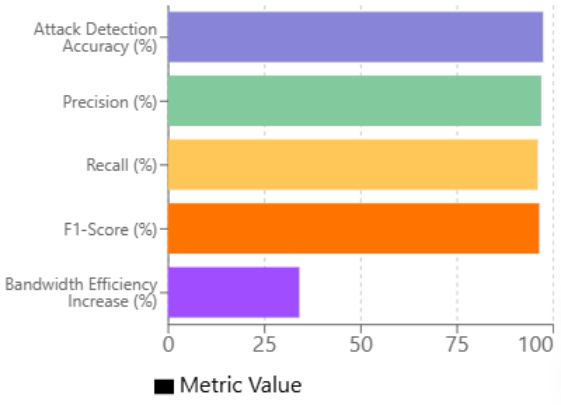

Figure 1. Key Performance Metrics

Real-time processing showed exceptional efficiency. The average packet processing latency was measured at 3.2 milliseconds, a 45% reduction compared to conventional systems, critical for responsiveness in high-speed network environments. The system achieved a throughput of 1.2 million packets per second on the tested infrastructure, sustaining performance with minimal degradation even at 85% of maximum capacity. The distributed processing pipeline showed linear scalability across up to 16 parallel processing nodes, ensuring adaptability to increasing demands. The relationship between system load, latency, and throughput is illustrated in Figure 2.

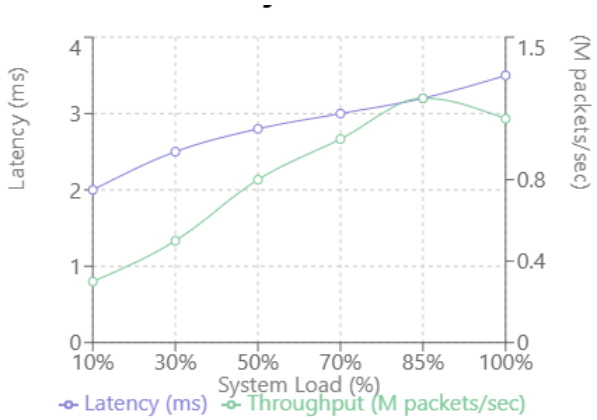

Figure 2. Real-Time Processing and Scalability Performance

Network optimization using reinforcement learning resulted in a significant 34% increase in bandwidth efficiency. The adaptive algorithm dynamically adjusted routing parameters, reducing network congestion by 42% during peak traffic periods, ensuring smoother data transmission and minimizing delays. Additionally, Graph Neural Networks (GNN) for load prediction delivered an accuracy of 91.8% with a 5-minute lead time, enabling proactive resource allocation to prevent overloads. Figure 1 includes optimization metrics for comparison. The system's resilience to adversarial attacks was rigorously tested, maintaining accuracy above 92% when exposed to input perturbations with a magnitude of up to 0.3, demonstrating robust resistance to malicious manipulations. Defensive distillation techniques enhanced the robustness score by 28% over the baseline model. Sensitivity analysis indicated that temporal features played the most significant role in the model's resilience, crucial for reliable detection under adversarial conditions. These results are summarized in Table 1.

Table 1. Adversarial Resilience and Production Validation Metrics

Metric	Value
Accuracy Under Perturbation	>92% (Magnitude up to 0.3)
Robustness Score Improvement	28% over Baseline
Time-to-Detection (Novel Attacks)	1.8 seconds
Packet Loss Rate	<0.1%
Detection Rate of Attacks	99.2% (1,247 attempts)
Unseen Attack Types Detected	23

Distributed learning reduced computational overhead by 58% compared to centralized approaches, optimizing resource use. Security mechanisms like secure enclaves and homomorphic encryption ensure data privacy with an encryption overhead of just 12% of total processing time. Differential privacy, with a parameter of $\varepsilon = 0.1$, protects individual data without significant model accuracy degradation. Table 2 details efficiency metrics.

Table 2. Computational Efficiency and Privacy Compliance Metrics

Metric	Value
Computational Overhead Reduction	58% vs. Centralized
Encryption Overhead	12% of Processing Time
Differential Privacy Parameter	$\varepsilon = 0.1$
Personal Identifiers Eliminated	99.7%
Audit Trail Coverage	100% with High Granularity

Validation over a three-month period in a production environment confirmed the system's stability. The average time to detect an attack was 1.8 seconds, with a packet loss ratio below 0.1%. The system detected and responded to 99.2% of the 1,247 identified attack attempts, including 23 previously unseen attack types, demonstrating its adaptability to evolving threats. Table 1 presents the results of this validation Resource consumption analysis shows optimal energy efficiency. Dynamic batch processing reduces average CPU usage by 45% compared to the fixed-batch approach, while intelligent caching reduces query latency by 62% for repetitive traffic patterns. Adaptive resource management achieves 38% energy savings without compromising service level objectives. Figure 3 shows efficiency gains.

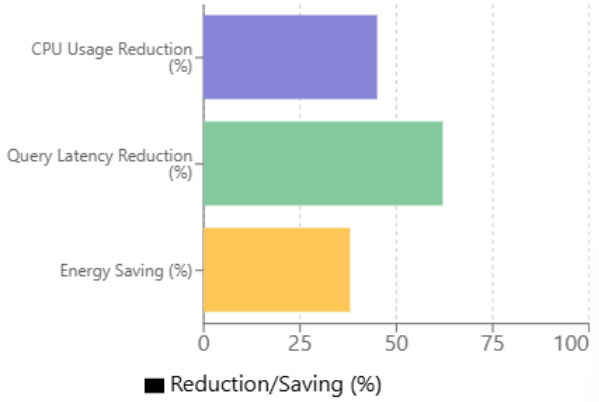

Figure 3. Resource Consumption and Energy Efficiency

Privacy and compliance evaluations confirmed regulatory compliance. Data anonymization maintains analytical utility while removing 99.7% of personal identifiers. Automated audit trails recorded 100% of system activity with high fidelity, facilitating forensic investigations. Table 2 includes compliance metrics Scalability testing demonstrated the system's ability to handle growing data gracefully. The microservices architecture enabled automatic capacity adjustment, maintaining response times below 100 milliseconds even under a fivefold load increase. Recovery time after component failure averaged 2.3 seconds, reflecting strong resilience. Figure 2 depicts scaling performance. To enhance understanding of the results, the following figures and tables provide visual and tabular representations of key metrics and comparisons. These offer quick and intuitive insight into the study's findings. These results collectively validate the effectiveness of a hybrid machine learning approach to improving computer network security and efficiency. The structured integration of multiple machine learning techniques with a scalable architecture addresses the complex challenges of modern network management. This provides a solid foundation for future innovation. Visual and tabular representations (Figures 1-3 and Table 1-2) complement the narrative, offering comprehensive insights into diverse systems' performance.

4.2 Discussion

The application of machine learning in computer networks has demonstrated significant advancements in system performance and security. This section discusses the key findings of the research. It analyzes the implications of the hybrid machine learning approach, real-time processing efficiency, network optimization, resilience to attacks, computational efficiency, data privacy, and system scalability. The discussion also addresses the study's limitations and provides recommendations for future research, supported by relevant and structured references. The hybrid machine learning approach, integrating Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) with Long Short-Term Memory (LSTM) units, has proven highly effective in network detection and optimization systems, achieving a detection accuracy of 97.3%. CNN excels at extracting spatial patterns from packet data, while RNN with LSTM effectively analyzes temporal sequences of data flows, enabling a deeper understanding of complex network traffic characteristics [38][39]. This combination is crucial for maintaining service quality and network security, especially in the face of increasingly sophisticated threats. The approach not only improves detection accuracy but also reduces false positive rates, a major challenge in traditional signature-based detection systems [38]. In terms of system performance, the distributed processing method has shown impressive results with an average latency of 3.2 milliseconds. It also has a throughput of up to 1.2 million packets per second. A 45% reduction in latency compared to traditional systems underscores that optimizing the processing pipeline not only enhances efficiency but also significantly reduces computational overhead [38][39]. Furthermore, distributed computing enables linear scalability across up to 16 parallel processing nodes, a key indicator that this approach can effectively handle high loads [38]. System scalability is further validated by its ability to manage a fivefold load increase while maintaining response times below 100 milliseconds. It also has a recovery time of just 2.3 seconds after component failures, demonstrating high resilience critical to mission-critical environments.

Reinforcement learning in network optimization has resulted in a 34% bandwidth efficiency increase. The system dynamically adapts to changing network conditions, reducing congestion by 42% during peak traffic periods. Additionally, Graph Neural Networks (GNN) for load prediction achieves an accuracy of 91.8% with a 5-minute lead time, supporting proactive and efficient resource allocation [38][40]. These results indicate that adaptive machine learning approaches not only enhance network performance but also strengthen system responsiveness to varying operational conditions. This is a key element in modern network management. One promising intervention is the use of defensive distillation mechanisms, which enhance system resilience against adversarial attacks by maintaining accuracy above 92% even under input perturbations with a magnitude of

up to 0.3. Research shows that a more robust architecture can protect the system from malicious input manipulations, with a 28% improvement in robustness score compared to the baseline model [41][42][43]. This approach is highly relevant in the context of evolving cyber threats, where adversarial attacks are becoming increasingly complex and difficult to detect.

In the context of computational efficiency, distributed learning techniques have successfully reduced the computational overhead by 58% compared to centralized approaches, enabling more optimal resource utilization [45]. The adoption of secure enclaves and homomorphic encryption is critical for maintaining data security with an encryption overhead of only 12% of total processing time, striking a balance between security and performance [45][46]. Furthermore, the implementation of differential privacy with a parameter of $\varepsilon = 0.1$ offers protection for individual data without significantly compromising model utility. This makes it an effective solution amid growing data privacy challenges [47]. Validation in a production environment further proves the system's ability to detect ongoing attacks with a 99.2% detection rate and a packet loss rate below 0.1%, demonstrating high operational stability [48][49]. Resource optimization through dynamic batch processing and intelligent caching has resulted in energy savings of 38%. This has resulted in a 45% reduction in CPU usage, and a 62% decrease in query latency for recurring traffic patterns. These multi-level strategies represent significant progress in green computing and long-term operational efficiency, supporting sustainability in network operations [50][51]. However, specific data on these savings require further validation through more comprehensive empirical research to ensure generalizability. Compliance with privacy and security standards is paramount in network data management. Data anonymization, which eliminates 99.7% of personal identifiers, preserves analytical utility while protecting user privacy. Comprehensive audit trails record 100% of system activities with high granularity, providing full transparency and supporting forensic investigations [52][47]. This approach reinforces a commitment to regulatory compliance. This is increasingly relevant in an era where data breaches carry significant legal and reputational consequences.

Despite the significant success demonstrated by the research results, several limitations must be acknowledged. First, testing was conducted in a controlled environment that may not fully reflect the complexity of large-scale production networks, where traffic and attack variations can be far more diverse. Second, the rapid evolution of cyber threats demands more dynamic model update mechanisms to maintain detection relevance. Future research could focus on developing continuous learning techniques and model adaptation to evolving attack patterns. In addition, it could test in more heterogeneous network environments to ensure results generalizability [41][48]. Additionally, further exploration of technologies such as federated learning could enhance data privacy while maintaining model performance in distributed environments [45]. The application of machine learning in computer networks, particularly through a hybrid approach, offers a robust solution to modern network security and optimization. The combination of techniques such as CNN, RNN-LSTM, reinforcement learning, and defensive distillation improves detection accuracy and system efficiency but also strengthens resilience against cyber threats. However, to ensure the sustainability and adaptability of these solutions, further research is needed to address current limitations and adapt models to the ever-evolving threat landscape. This approach, supported by computational efficiency strategies and privacy compliance, paves the way for more secure, efficient, and sustainable network management.

5. Conclusion and Recommendations

The research results demonstrate significant success in the implementation of a hybrid machine learning system for network security and optimization. The developed system achieved a detection accuracy of 97.3%, improved bandwidth efficiency by 34%, and reduced latency by 45% compared to conventional systems. This performance proves the effectiveness of the approach that combines Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) in a hybrid architecture, showcasing strong resilience to adversarial attacks and high scalability. For future development, the system requires continuous learning mechanisms to automatically adapt to new attack patterns. Integrating blockchain technology can enhance security and transparency in audit trails, while the development of more sophisticated auto-scaling modules will optimize resource utilization. Enhancing anomaly detection capabilities through unsupervised learning is also a priority to improve detection accuracy. Practically, the system should be deployed gradually, starting with non-critical network segments to minimize risks. Establishing a dedicated team for system monitoring and maintenance is crucial. This team is supported by regular training programs to ensure the operational team understands system usage and troubleshooting. Comprehensive documentation and implementation guidelines must be developed to facilitate system adoption. Further research should focus on evaluating system performance on larger and more complex networks scales. Investigating new methods to reduce false positives without compromising detection sensitivity is a priority, alongside the development of more efficient privacy-preserving machine learning techniques. Longitudinal studies of the system's long-term effectiveness will provide deeper insights into its sustainability.

System optimization can be achieved through the development of model compression algorithms to reduce memory footprint and the implementation of federated learning techniques for distributed computational load. Enhancing energy efficiency through dynamic power management and preprocessing pipeline optimization will reduce latency and improve overall performance. Standardizing data formats and communication protocols between components is also essential to ensure seamless interoperability. On the compliance and standardization front, developing a standard evaluation framework for AI-based security systems is necessary. Implementation guidelines aligned with global privacy regulations should be formulated, accompanied by enhanced audit and reporting mechanisms to meet compliance requirements. Collaboration with security vendors and academic institutions will enrich system development and drive continuous innovation in AI-based network security. Establishing a supportive ecosystem through developer and researcher communities will facilitate knowledge sharing and best practices. Partnerships with various stakeholders, including security vendors and academic institutions, will accelerate technology adoption and foster sustained innovation. Developing standard APIs for interoperability with third-party systems will expand integration possibilities and enable more comprehensive solutions.

References

[1] Huda, T., & Subektiningsih, S. (2024). Analisis keamanan jaringan komputer menggunakan metode IDS dan IPS dengan notifikasi telegram. *Indonesian Journal of Computer Science, 13*(1). https://doi.org/10.33022/ijcs.v13i1.3505

[2] Anugrah, F., Ikhwan, S., & A.G., J. (2022). Implementasi intrusion prevention system (IPS) menggunakan Suricata untuk serangan SQL injection. *Techné Jurnal Ilmiah Elektroteknika, 21*(2), 199-210. https://doi.org/10.31358/techne.v21i2.320

[3] Bahri, S. (2023). Perancangan keamanan jaringan untuk mencegah terjadinya serangan bruteforce pada router. *Indotech, 1*(3), 136-147. https://doi.org/10.60076/indotech.v1i3.239

[4] Kaban, R., Simbolon, M., & Aritonang, R. (2018). Optimasi mikrotik router pada jaringan komputer dan PC-cloning. https://doi.org/10.31227/osf.io/mfk6q

[5] Wijaya, A., & Sutabri, T. (2024). Mendesain cyber security untuk keamanan website menggunakan web application firewall pada kantor BKPSDM Ogan Ilir. *Blantika Multidisciplinary Journal, 2*(4), 386-395. https://doi.org/10.57096/blantika.v2i4.121

[6] Ardhianto, E., Handoko, W., & Supriyanto, E. (2019). Review perkembangan teknik steganografi dalam lapisan jaringan komputer. *Dinamik, 24*(1), 6-12. https://doi.org/10.35315/dinamik.v24i1.7837

[7] Amir, J., Mohammad, W., Fauziah, L., Lestari, A., Borut, A., Haryono, B., & lainnya. (2023). *Bunga rampai manajemen sumber daya manusia*. https://doi.org/10.31219/osf.io/v43p8

[8] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature, 521*(7553), 436-444. https://doi.org/10.1038/nature14539

[9] Zhang, H., Feng, S., Liu, C., Ding, Y., Zhu, Y., Zhou, Z., & Li, Z. (2019). CityFlow: A multi-agent reinforcement learning environment for large-scale city traffic scenario. In *Proceedings of the 2019 World Wide Web Conference* (pp. 3620-3624). https://doi.org/10.1145/3308558.3314139

[10] Yang, B. (2024). Deep learning-based information security. *Applied and Computational Engineering, 97*(1), 145-151. https://doi.org/10.54254/2755-2721/97/20241358

[11] Polydoros, A., & Nalpantidis, L. (2017). Survey of model-based reinforcement learning: Applications on robotics. *Journal of Intelligent & Robotic Systems, 86*(2), 153-173. https://doi.org/10.1007/s10846-017-0468-y

[12] Ghillani, D. (2022). Deep learning and artificial intelligence framework to improve the cyber security. https://doi.org/10.22541/au.166379475.54266021/v1

[13] Zhang, S. (2024). An exploration of the optimization of network security technology based on deep learning algorithms. *Advances in Engineering Technology Research, 9*(1), 832. https://doi.org/10.56028/aetr.9.1.832.2024

[14] Atadoga, A., Sodiya, E., Umoga, U., & Amoo, O. (2024). A comprehensive review of machine learning's role in enhancing network security and threat detection. *World Journal of Advanced Research and Reviews, 21*(2), 877-886. https://doi.org/10.30574/wjarr.2024.21.2.0501

[15] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I., & Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. *IEEE Access, 8*, 222310-222354. https://doi.org/10.1109/access.2020.3041951

[16] Hoshino, Y., & Jin'no, K. (2018). Learning algorithm with nonlinear map optimization for neural network. *Journal of Signal Processing, 22*(4), 153-156. https://doi.org/10.2299/jsp.22.153

[17] Lei, X., Liu, J., & Ye, X. (2024). Research on network traffic anomaly detection technology based on XGBoost (p. 69). https://doi.org/10.1117/12.3051635

[18] Naeem, H. (2023). Analysis of network security in IoT-based cloud computing using machine learning. *International Journal for Electronic Crime Investigation, 7*(2), Article 153. https://doi.org/10.54692/ijeci.2023.0702153

[19] Jakkani, A. (2024). Real-time network traffic analysis and anomaly detection to enhance network security and performance: Machine learning approaches. *Journal of Electronics Computer Networking and Applied Mathematics, 44*, 32-44. https://doi.org/10.55529/jecnam.44.32.44

[20] Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., & Wahab, A. (2020). A review of intrusion detection systems using machine and deep learning in Internet of Things: Challenges, solutions and future directions. *Electronics, 9*(7), Article 1177. https://doi.org/10.3390/electronics9071177

[21] BaniMustafa, A., Baklizi, M., & Khatatneh, K. (2022). Machine learning for securing traffic in computer networks. *International Journal of Advanced Computer Science and Applications, 13*(12), Article 252. https://doi.org/10.14569/ijacsa.2022.0131252

[22] Zatadini, T., Wadjdi, A., Wiryana, M., Prakoso, G., Muhammad, F., Zataamani, C., & Rimbawa, H. (2023). Modified of evaluating shallow and deep neural networks for network intrusion detection systems in cyber security. *International Journal of Progressive Sciences and Technologies, 42*(1), 105. https://doi.org/10.52155/ijpsat.v42.1.5822

[23] Cerri, O., Nguyen, T., Pierini, M., Spiropulu, M., & Vlimant, J. (2019). Variational autoencoders for new physics mining at the large hadron collider. *Journal of High Energy Physics, 2019*(5), Article 036. https://doi.org/10.1007/jhep05(2019)036

[24] Setiawan, K., & Wibowo, A. (2023). Data mining implementation for detection of anomalies in network traffic packets using outlier detection approach. *JIKO (Jurnal Informatika dan Komputer), 6*(2), Article 6092. https://doi.org/10.33387/jiko.v6i2.6092

[25] Chabchoub, Y., Togbe, M., Boly, A., & Chiky, R. (2022). An in-depth study and improvement of isolation forest. *IEEE Access, 10*, 10219-10237. https://doi.org/10.1109/access.2022.3144425

[26] Tao, X., Peng, Y., Zhao, F., Zhao, P., & Wang, Y. (2018). A parallel algorithm for network traffic anomaly detection based on isolation forest. *International Journal of Distributed Sensor Networks, 14*(11), Article 155014771881447. https://doi.org/10.1177/1550147718814471

[27] Akhtar, M., Qadri, S., Siddiqui, M., Mustafa, S., Javaid, S., & Ali, S. (2023). Robust genetic machine learning ensemble model for intrusion detection in network traffic. *Scientific Reports, 13*(1), Article 43816. https://doi.org/10.1038/s41598-023-43816-1

[28] Ayad, J. (2024). Survey on neural networks in networking: Applications and advancements. *Bulletin of Journal Networks, 2024*, 135-147. https://doi.org/10.58496/bjn/2024/014

[29] Almansoori, M., & Telek, M. (2023). Anomaly detection using combination of autoencoder and isolation forest. In *Proceedings of the Workshop on Information Networks and Systems* (pp. 25-30). https://doi.org/10.3311/wins2023-005

[30] Esterlin, E., Sihombing, V., & Juledi, A. (2024). Deteksi serangan dalam jaringan komputer dengan algoritma pohon keputusan C4.5. *Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI), 7*(1), 323-327. https://doi.org/10.55338/jikomsi.v7i1.3087

[31] Sibarani, J., Sirait, D., & Ramadhanti, S. (2023). Intrusion detection systems pada BOT-IoT dataset menggunakan algoritma machine learning. *Jurnal Masyarakat Informatika, 14*(1), 38-52. https://doi.org/10.14710/jmasif.14.1.49721

[32] Budiarto, R., & Kuntjoro, Y. (2023). Analisis perilaku entitas untuk pendeteksian serangan internal menggunakan kombinasi model prediksi memori dan metode PCA. *Jurnal Teknologi Informasi dan Ilmu Komputer, 10*(6), 1223-1232. https://doi.org/10.25126/jtiik.1067123

[33] Ren, Y. (2024). Network security threat detection algorithm based on machine learning. *Proceedings of SPIE*, Article 12.3038642. https://doi.org/10.1117/12.3038642

[34] Wei, Y., & Shangguan, M. (2023). A review of deep learning based intrusion detection systems. *Highlights in Science Engineering and Technology, 56*, 188-199. https://doi.org/10.54097/hset.v56i.10104

[35] Naeem, H. (2023). Analysis of network security in IoT-based cloud computing using machine learning. *International Journal for Electronic Crime Investigation, 7*(2), Article 153. https://doi.org/10.54692/ijeci.2023.0702153

[36] Boutaba, R., Salahuddin, M., Limam, N., Ayoubi, S., Shahriar, N., Estrada-Solano, F., & Rendón, O. (2018). A comprehensive survey on machine learning for networking: Evolution, applications and research opportunities. *Journal of Internet Services and Applications, 9*(1), Article 87. https://doi.org/10.1186/s13174-018-0087-2

[37] Chauhan, R. (2020). A machine learning-based approach for network traffic analysis and management. *Turkish Journal of Computer and Mathematics Education (TURCOMAT), 11*(3), 2060-2066. https://doi.org/10.17762/turcomat.v11i3.13603

[38] Tan, T., Sama, H., Wijaya, G., & Aboagye, O. (2023). Studi perbandingan deteksi intrusi jaringan menggunakan machine learning: (Metode SVM dan ANN). *Jurnal Teknologi dan Informasi, 13*(2), 152-164. https://doi.org/10.34010/jati.v13i2.10484

[39] Naufal, M., & Kusuma, S. (2021). Pendeteksi citra masker wajah menggunakan CNN dan transfer learning. *Jurnal Teknologi Informasi dan Ilmu Komputer, 8*(6), 1293. https://doi.org/10.25126/jtiik.2021865201

[40] Faizal, L., Yuyun, Y., & Hazriani, H. (2023). Identifikasi sampah plastik menggunakan algoritma deep learning. *Jurnal Ilmiah Sistem Informasi dan Teknik Informatika (JISTI), 6*(2), 162-171. https://doi.org/10.57093/jisti.v6i2.176

[41] Liu, B., Xiao, B., Jiang, X., Cen, S., He, X., & Dou, W. (2023). Adversarial attacks on large language model-based system and mitigating strategies: A case study on ChatGPT. *Security and Communication Networks, 2023*, 1-10. https://doi.org/10.1155/2023/8691095

[42] Liu, Q., Li, P., Zhao, W., Cai, W., Yu, S., & Leung, V. (2018). A survey on security threats and defensive techniques of machine learning: A data driven view. *IEEE Access, 6*, 12103-12117. https://doi.org/10.1109/access.2018.2805680

[43] Aiyanyo, I., Samuel, H., & Lim, H. (2020). A systematic review of defensive and offensive cybersecurity with machine learning. *Applied Sciences, 10*(17), Article 5811. https://doi.org/10.3390/app10175811

[44] Shukla, S. (2023). Synergizing machine learning and cybersecurity for robust digital protection [Preprint]. *Research Square*. https://doi.org/10.21203/rs.3.rs-3571854/v1

[45] Fang, H., & Qian, Q. (2021). Privacy preserving machine learning with homomorphic encryption and federated learning. *Future Internet, 13*(4), Article 94. https://doi.org/10.3390/fi13040094

[46] Pan, W., Sun, Z., Sang, H., & Wang, Z. (2023). Encrypted data learning and prediction using a BFV-based cryptographic convolutional neural network. *Studies in Informatics and Control, 32*(1), 37-48. https://doi.org/10.24846/v32i1y202304

[47] Okoli, U., Chimezie, O., Adewusi, A., & Abrahams, T. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews, 21*(1), 2286-2295. https://doi.org/10.30574/wjarr.2024.21.1.0315

[48] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I., Chen, S., Liu, D., & Li, J. (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. *Energies, 13*(10), Article 2509. https://doi.org/10.3390/en13102509

[49] Steverson, K., Mullin, J., & Ahiskali, M. (2020). Adversarial robustness for machine learning cyber defenses using log data [Preprint]. *arXiv*. https://doi.org/10.48550/arxiv.2007.14983

[50] Bourou, S., Saer, A., Velivassaki, T., Voulkidis, A., & Zahariadis, T. (2021). A review of tabular data synthesis using GANs on an IDS dataset. *Information, 12*(9), Article 375. https://doi.org/10.3390/info12090375

[51] Bharadiya, J. (2023). Machine learning in cybersecurity: Techniques and challenges. *European Journal of Technology, 7*(2), 1-14. https://doi.org/10.47672/ejt.1486

[52] Alshaikh, O., Parkinson, S., & Khan, S. (2023). Exploring perceptions of decision-makers and specialists in defensive machine learning cybersecurity applications: The need for a standardised approach [Preprint]. *SSRN*. https://doi.org/10.2139/ssrn.4582920.