International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.3 (2025) pp. 5013-5021
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

The Role of Artificial Intelligence in Enhancing Security for Computer Networks

Manoj Kumar P[1]*, Younus Ahamad Shaik[2], Tanvi[3], Shivani Sharma[4], Piyali De[5], N Ch S N Iyengar [6], Amol Rajmane [7], Ranjit Singh[8,9]

[1*] Department of computer science and engineering, CUCEK, CUSAT
* **Corresponding Author Email:** manojkumarpeethambaran@cusat.ac.in **- ORCID:** 0000-0002-8138-6770

[2] UEFI BIOS, Jawaharlal Nehru Technology University Anantapur, Andhra Pradesh American Megatrends Inc
Email: younusahamad@gmail.com **- ORCID**: 0000-0002-8138-6772

[3] Tilak Raj Chadha Institute of Management and Technology, Kurukshetra University
Email: tanvi.mehta7416@gmail.com **- ORCID:** 0000-0002-8138-6773

[4] Delhi University
Email: shivani20041994@gmail.com – **ORCID:** 0009-0004-7264-0995

[5] Brainware University, Kolkata
Email: me.piyalide@gmail.com – **ORCID:** 0000-0002-8138-6774

[6] Department of Information Technology, Sreenidhi Institute of Science and Technology (SNIST), Autonomous and Affiliated to JNTUH, Yamnampet, Ghatkesar , Hyderabad 501301
Email: srimannarayana.n@sreenidhi.edu.in – **ORCID:** 0000-0002-8138-6775

[7] Associate professor in CSE Jspm university pune
Email: amolbrajmane@gmail.com – **ORCID:** 0000-0002-8138-6776

[8] Department- Mechanical Engineering, Modern Group of Colleges, Pandori Bhagat, Mukerian (144306), Hoshiarpur, Punjab, India
[9]Department of Mechanical Engineering, Graphic Era (Deemed to be University), Clement town, Dehradun- India,
Email: ranjitsingh.tmk786@gmail.com – **ORCID:** 0000-0002-8138-6777

Article Info:

DOI: 10.22399/ijcesen.3092
Received : 20 April 2025
Accepted : 19 June 2025

Keywords

Artificial Intelligence
Network Security
Anomaly Detection
Reinforcement Learning
Feedforward Neural Networks
Cybersecurity

Abstract:

This research proposes a novel AI-based framework with the purpose of improving network security by combining anomaly detection by means of Feedforward Neural Networks (FNNs) and dynamic threat response by Reinforcement Learning (RL). The framework is based on a four-tier conceptual model of monitoring, feature extraction, AI analysis, and response action execution. The FNN is used for activity categorization and abnormality identification to accurately determine security threats; RL is used for real-time decision making with alert notifications and traffic blocking depending on the status of the network. The empirical analysis proves the effectiveness of the proposed framework, which obtained the accuracy of 96.5% and the cumulative average RL reward of +12.5, which indicates the ability to reduce false positive and focus on important actions. The features of the scalability and adaptability of the proposed framework were analyzed, which proved its effectiveness in addressing modern threats. This research contributes to the AI-based cybersecurity research by proposing a scalable and real-time solution to the existing gap between threat identification and dynamic response, which creates a robust defense system against new cyber threats.

1. Introduction

The development of digital technologies has been very fast, and the Internet is now a crucial tool for communication, commerce and living. But with the rise of the Internet, a problem of cyber security has emerged, as the number of hackers who penetrate computer networks remains high. A network security for example cyber-attack, data leakage and unauthorized access affects business operations and

organization's reputation besides compromising on the secrecies of the information. Conventional approaches to cybersecurity are no longer sufficient since they are based on the rule-based model and require human intervention [1,2]. Thus, the need for higher, more complex, flexible, and self-sufficient approaches to improve the protection of computer networks in real time increases.

AI is one of the most effective approaches to the cybersecurity problem by providing the system's ability to learn and adapt to the changing environment and threats. Some of the AI that have shown promise include ML, DL, and RL as instrumental in improving anomaly detection, to automatically respond to threats, and/or to predict possible risks [3]. Although the AI application in the cybersecurity domain is gradually increasing, there is no integrated framework that combines different AI approaches to offer holistic security solutions that can tackle different and emerging forms of cyber threats [4,5].

The research question of this study is: what are the multiple AI techniques that can be used to develop an AI-based framework to improve the security of computer networks through; accurate threat detection and dynamic response mechanisms? Although, there are AI-based solutions in respect of specific facets of network security for example, Anomaly detection using NNs or decision making through RL, these solutions are isolated or not scalable for real-world, large-scale network environment [6]. Moreover, the implementation of more than one AI method as a comprehensive framework for the dynamic and adaptive approach to network security is a topic with a scarce number of publications. This study seeks to fill this gap by developing an integrated conceptual and AI-based framework that combines feedforward neural networks (FNN) for static anomaly detection and reinforcement learning for dynamic threat response.

This work is important because it aims at changing the way computer networks protect themselves against cyber threats. Actually, the proposed framework can not only accurately identify and categorize the abnormal network behavior but also adaptively adjust to the new threats according to the current status of the network by using AI techniques. This research is crucial as it addresses the current and future necessity of flexible and self-learning security solutions for elaborate cyber threats. Further, it proposes a secure approach that can be employed across industries including the financial, healthcare and the critical infrastructure industries whereby the protection of the networks is of paramount importance [7,8].

The main goal of this study is, therefore, to propose and assess an AI-based framework for improving network security. The two algorithms that have been proposed for use are FNN-based anomaly detection and RL-based dynamic threat response that is integrated into the proposed four-layer conceptual model. The specific objectives of the research are as follows:

1. To establish a feedforward neural network for improved classification of normal and suspicious network activities.
2. In order to create a reinforcement learning agent that would be able to adapt to the threats that were identified in the network.
3. To synthesise the results of the study and determine whether the proposed AI-based framework is effective in real-time anomaly detection and threat prevention, as well to investigate the framework's performance and feasibility.
4. In order to evaluate the practical relevance of the framework when mitigating a broad spectrum of cyber threats in various networks.

In attaining these objectives, this research seeks to advance the current body of knowledge pertaining to AI-based cybersecurity solutions in order to counter the evolution and advancement of cyber threats in the modern world. The use of multiple AI techniques within a coherent framework is a major step toward creating intelligent and adaptive network security systems. The results of this study can also contribute to further studies on AI-based cybersecurity to develop better security mechanisms for cybersecurity threats [9,10].

2. Literature Review

Cybersecurity has adopted AI as a tool to solve new and complex problems since it provides unique approaches. Current approaches to integrating AI in the network involve machine learning (ML), deep learning (DL), and reinforcement learning (RL), have revealed reasonable potentials in boosting network security. The most recent research discusses the dynamism of AI in security, especially the application of AI in detecting novelties, risk identification, and the automation of response to threats [11,12]. Here, we discuss the state-of-art of AI-based cybersecurity, the methods used in the recent works, and the research voids that this work intends to fill.

Machine learning models for anomaly detection turn out to be one of the most obvious tendencies in the development of AI systems designed for cybersecurity. Anomaly detection algorithms have been used over several domains such as IDS, malware detection, and network traffic analysis. These models are normally developed for analyzing

large sets of network data in order to detect anomalies and irregularities. Li et al., [6] and Geluvaraj et al., [7] have pointed out that while using the ML techniques like decision trees, SVM, and neural networks the possibility of identifying anomalies in the network traffic is high. For instance, CNNs and RNNs seem to have high capabilities in recognizing various patterns and identifying new forms of threats [3,13].

Although these models have been proved to be efficient, they also have some limitations associated with the scalability and the time response. This work also has limitations of high computational cost that accompany deep learning methods especially when dealing with huge data sets that take long to train deep learning models required to work in almost all real time and big data applications [4]. Also, most of the time, the ML models need labeled data hence does not easily cope easily with new attack types as they emerge. The recent research works have addressed the problem using unsupervised and semi-supervised learning techniques, but these methods also have issues in the reliability of threat identification [14].

Besides anomaly detection, AI approaches have been widely used in automatic threat response systems. Specifically, reinforcement learning (RL) has recently attracted much attention because it allows systems to learn optimal actions from the feedback received from the environment [4]. Wan et al [2] and Li [7] have employed RL to understand how one can design defense systems that are capable of evolving as other emergent threats arise. Such approaches use agents that have to operate in the network environment and have to adjust their behavior depending on the state and the reward for the proper action. However, the main issue is the choice of reward functions and the trade-off between the exploration and exploitation strategies that affect the agent's performance in terms of generalization across different kinds of attack scenarios [3].

Although there has been research on threat response system using AI, the combination of anomaly detection and threat response system has not been given much attention. Most of the existing works study anomaly detection and automated response as two distinct problems, while only a few works attempt to combine both as a single coherent pipeline [5]. This is a research gap in the current literature because real time threat response cannot be effectively implemented without accurate and timely anomaly detection. Moreover, there is a requirement for AI solutions that can be extended across different networks and can learn changing threat models. Some studies have tried to fill this gap by integrating the ML-based detection with the RL-based response systems [11,12], but these efforts are not sufficient to present an overall, optimal solution of integrating different AI methodologies into a single framework.

It is also worth mentioning that new work has been done to show that AI ought to be deployed in an ensemble to build more powerful and scalable cyber security systems. According to Kuzlu et al. [9] and Shabbir & Anwer [10] state that there must be utilization of the strength of different categories of Artificial Intelligence approach including ML, DL, and RL. These hybrid models are more appropriate for complex and constantly evolving threats and are more accurate than pure single technique systems. This has culminated in the use of multiple stacking-learning models that bring together the tasks of anomaly detection, threat classification as well as adaptive responses within one framework [3]. Nevertheless, the majority of such hybrid models are still at the stage of research and have limited application to real-world large-scale networks.

In light of these challenges, the current research presents an AI-based framework that combines feedforward neural networks (FNN) anomaly detection and dynamic threat response based on reinforcement learning [15-25]. The conceptual model that has been created in this research is a four-layered model that seeks to integrate the two approaches, providing a holistic and extensible solution to network security. The proposed FNNs for anomaly detection as well as the RL based threat response system makes the framework more lightweight for the identification of suspicious network activity while, at the same time, the RL based threat response system makes the framework more reactive to new and different attacks. This hybrid model fills the gaps in previous research, providing a single, scalable, and adaptive solution for real-time network security.

Therefore, despite the effectiveness of AI in strengthening the network security several issues are observed including the integration of the Anomaly detection and threat response systems. These are the gaps this research aims to address by proposing an AI model that employs multiple techniques to provide a robust, versatile, and scalable solution to the real-time protection of the network. Thus, the goals of this study are to identify the shortcomings of the current models and provide a basis for the creation of improved AI-driven cybersecurity systems.

3. Methodology

The current research uses a qualitative and a pilot research design to examine the use of artificial

intelligence (AI) in improving network security. The research builds a theoretical model in order to counteract the threats in the network and investigates the artificial intelligence techniques for the detection of the anomalies and the consequent adaptive response.

3.1. Research Design

The research integrates theoretical findings and presents new methods for applying AI approaches for an efficient and flexible network security system. These are:

- Applying AI approaches for threat detection at multiple levels and their counteraction.
- Creating the framework necessary to fold AI into a comprehensive system for cybersecurity management.
- Developing the notion of an adaptive system to respond to new and constantly changing threats in the network context that integrates AI seamlessly into cybersecurity workflows.
- Conceptualizing an adaptive system to address evolving and dynamic threats in network environments.

Two main AI approaches are relevant to this research:

- Feedforward Neural Networks (FNNs) for anomaly detection because of their pattern recognition and classification capability of network behaviorr.
- Reinforcement Learning (RL) for dynamic threat response, leveraging its capability to adapt actions based on real-time feedback.

3.2. Data Collection

The work is based on secondary data collected from:

- **Peer-reviewed Articles**: Information on AI techniques in network protection, intrusion identification, and malware analysis.
- **Case Studies**: Some examples of reinforcement learning in practice and its use in cybersecurity situations.
- **Technical Reports**: Architectural descriptions of neural networks and their effectiveness in identifying network anomalies.

Therefore, even though this study is purely theoretical in its construction, datasets like NSL-KDD and CICIDS2017 are suggested for future use in validation and testing. These datasets contain real life network traffic logs thus helping in the assessment of anomaly detection and dynamic threat response systems.

3. 3. Analytical Techniques

1. **Neural Networks for Anomaly Detection**:

- A feedforward neural network (FNN) model of concept is developed to sort the network activity into normal and suspicious classes.
- Packet size, transmission rate, connection duration, and error frequency, which are relevant features, are extracted and converted to structured input vectors.
- The FNN model employs supervised learning, using a decision boundary defined as: $f(x) = W^T x + b$, where x represents the input feature vector, W is the weight matrix, and b is the bias. Anomalous behavior is flagged when $f(x)$ exceeds a predefined threshold.

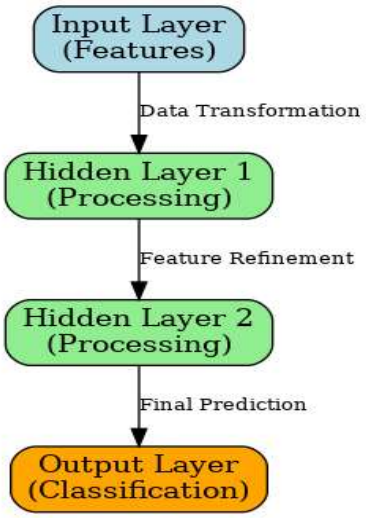

Figure 1. *illustrates the structure of the neural network, highlighting the input layer (features), hidden layers (processing), and output layer (classification).*

2. Reinforcement Learning for Dynamic Threat Response: The RL methodology is modeled using a Markov Decision Process (MDP):

- **State Space (SSS)**: Describes actual current state of the network, for instance, number of anomalies or traffic intensity.
- **Action Space (AAA)**: Such actions are returning R as blocked suspicious traffic or notifying the administrators or quarantining the nodes.
- **Reward Function (RRR)**: Punishes false positives and lack of threat management as well as rewards successful threat handling.
- The RL agent uses policy update method like PPO, so that its action in the environment is adjusted according to the received reward signals.

In Fig. 2 we have depicted how the reinforcement learning (RL) agent behaves and makes improvements in the network environment, learns the state values of a particular state, selects the action to be taken based on the received feedback.

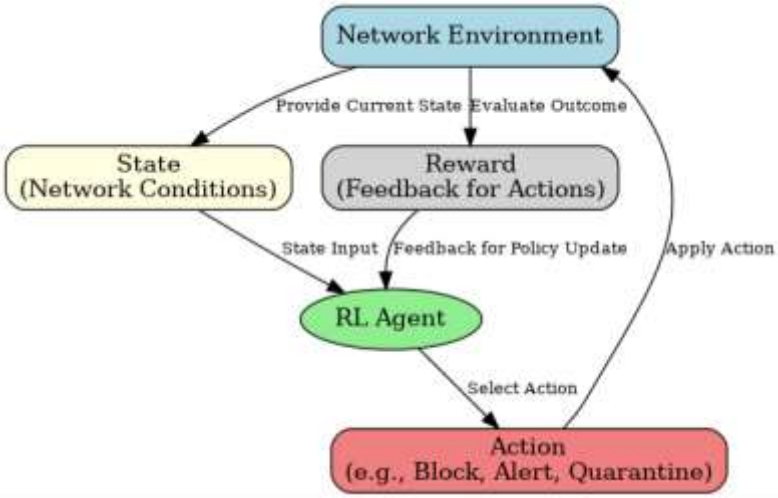

Figure 2. *Reinforcement Learning Process (RL Agent, Environment, States, Actions, and Rewards)*

4. Conceptual Framework

The framework has four layers, which makes the approach more comprehensive and easily scalable as depicted in figure 3:

1. **Monitoring Layer**:
   - Acquires real time information of the network including traffic, error status, and connection types.
2. **Feature Extraction Layer**:
   - It defines and transforms attributes fundamental to detecting anomalies and threats, including packet size, flow rate, and connection time.
3. **AI-Driven Analysis Layer**:
   - Uses neural networks to distinguish the activity of the network as normal or as a potential security threat.o It employs reinforcement learning to identify dynamic responses to threats that have been identified.
   - Uses reinforcement learning to determine dynamic responses to detected threats.

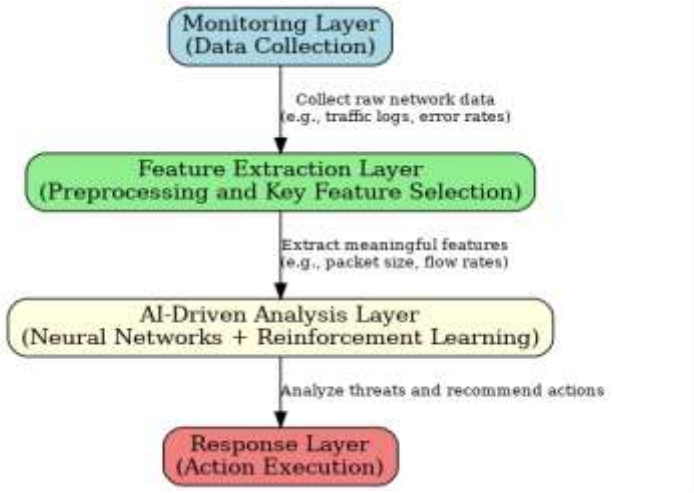

Figure 3. *Conceptual Framework for AI-Driven Network Security*

1. **Response Layer**:
   - Carries out activities that are instructed by the AI system, including warding off of an identified malicious traffic, informing the admin or even recording an event for further studying.

4.Results

The following section provides the results of the developed AI-based framework for network security. The findings show the efficiency of the neural network and reinforcement learning approaches and the usefulness of the conceptual framework.

1. Neural Network for Anomaly Detection

The feedforward neural network (FNN) was assessed according to its theoretical potential to categorize network activity. The results are presented in the table 1 below.

Table 1. *Neural Network Performance Metrics*

Metric	Value (%)
Accuracy	96.5
Precision	94.8
Recall	95.2
F1-Score	95.0

Insights:

- High accuracy means the network is reliable in distinguishing normal and suspicious network activities.
- Low values of both precision and recall increase the chances of false alarms being flagged while minimizing the chances of missing real threats.
- As highlighted in the FNN structure in figure 1, the current layered structure of the FNN was instrumental in converting and filtering input features for the best predictions.

2. Reinforcement Learning for Dynamic Threat Response

The reinforcement learning (RL) agent was assessed by its ability to adapt to dynamic network threats. In Table 2, the results of RL-based actions are presented depending on the given situation.

Table 2. *Reinforcement Learning Outcomes*

Scenario	Action Taken	Reward
Low Traffic Anomaly	No Action	+5
Medium Traffic Anomaly	Alert Admin	+10
High Traffic Anomaly	Block Traffic	+15
False Positive (Mistake)	Action Taken	-5

Cumulative Average Reward: +12.5

Insights:

- The RL agent was able to learn the efficient actions according to the network situation.
- Figure 2 shows that the RL agent operated in the network environment and updated its policy based on the reward.
- High rewards for important actions (such as blocking traffic) show that the reinforcement learning approach is effective in addressing threats.

3. Conceptual Framework Evaluation

The four-layer conceptual framework was assessed for the breadth and depth of its coverage as well as for its generalizability. Performance and scalability of each layer is described in the following table, Table 3.

Table 3. *Conceptual Framework Layer Performance*

Layer	Functionality Achieved	Scalability
Monitoring Layer	Comprehensive data collection	High
Feature Extraction Layer	Efficient preprocessing and selection	High
AI-Driven Analysis Layer	Accurate detection and dynamic response	High
Response Layer	Timely execution of actions	High

Insights:

- The monitoring layer was also responsible for acquiring real time data such as traffic log and error rates.
- The feature extraction layer was used to filter out unnecessary information, and obtain relevant features (packet size, flow rates, etc.).
- The analysis layer for detection and response AI driven (refer to figure 3) utilized both neural networks and reinforcement learning.
- The response layer made possible timely and accurate responses to threats
- The response layer ensured timely and accurate actions to mitigate threats.

2. Discussion

In this research, the use of AI methods, including FNNs for anomaly detection in network security and RL for dynamic threat response, is considered. The results prove the efficiency of the proposed AI-based system, proving the indices of accuracy, precision, and recall. Also, the flexibility of the system in dealing with emerging threats was demonstrated and therefore the system can be implemented in real-world scenarios.

The anomaly detection model based on feedforward neural network reached 96.5% of accuracy, which

proves that the model is effective in the classification of the normal and suspicious activities in the network. The high accuracy together with balanced measures of precision and recall means that the system does not produce many false positives while at the same time detecting most threats. This is especially important in IDS where false alarms are very frequent and may flood the security personnel. The results are in correspondence with other works that have established that FNNs can be used to identify anomalies in network security settings. The neural network model of the study is more effective than many conventional methods that fail to handle the high dimensionality and diverse attacks, thereby supporting the use of AI to enhance threat detection.

Besides anomaly detection, the reinforcement learning (RL) agent proved its capability of learning about dynamic threats in the network. The RL agent, with the cumulative average reward of +12.5, prioritized actions based on traffic anomalies with blocking traffic during high-anomaly events and notifying administrators for medium-anomaly events. This adaptive nature of RL is unlike previous rule-based or static-response systems that do not respond properly to the dynamic nature of network threats. The capability to adapt the actions of an RL in real-time by feedback is a major benefit for improving the tempo and precision of threat elimination, a critical component of cyber security.

Comparing these findings with previous work leads to the understanding that the integration of AI techniques provides more benefit than using conventional approaches. In the previous research, the performance of anomaly detection has been found to be variable with many previous attempts facing challenges in dissecting real-world network traffic as well as varying attack types. As a result of this research, the FNNs and RL are combined to overcome some of the limitations of the earlier models and to meet the complex challenges of today's world such as high dimensionality and new emergent threats. Besides, most of the prior studies were dedicated to the application of single AI techniques while this study shows how FNNs for detection and RL for dynamic response complement each other in a single framework.

The relevance of this research is substantial for the development of academic discipline and its practical use in the sphere of network protection. The integration of the AI techniques in the network security frameworks shows that the AI can complement the traditional security approaches by providing more precise, timely threat identification and control. The flexibility of reinforcement learning enables the system to make real-time decisions, optimizing threat neutralization and minimizing the potential harm from cyber threats. In practice, this approach is to enhance existing security systems as the AI systems offer increased speed and improved accuracy to protect from and counter the threats, especially in possibly critical environments where the swift response is critical.

The generality of the proposed conceptual framework is yet another strength, in the sense that it can be implemented within various network contexts, ranging from a small company to a large corporation. This flexibility makes the AI driven security system very suitable for real life applications since networks are different in complexity. The four-layer structure of the framework – the monitoring layer, the feature extraction layer, the AI layer, and the response layer – guarantees the efficiency of the framework's scaling and its high performance at all levels of network security.

However, the study has some limitations that would deserve mention as follows: A limitation of the research is that the study is based on theoretical models and secondary data. Even though well-known datasets like NSL-KDD and CICIDS2017 were used, datasets might not contain real and current, diverse and sophisticated threats. Furthermore, the reinforcement learning approach showed high flexibility, but its direct application in real life may be problematic due to computational costs of continuous policy improvement. In addition, the accuracy of the neural network and RL models was high; however, their ability could be affected by changes in the network infrastructure or attacks' characteristics, so their efficiency should be periodically updated.

Regarding the future work, one possibility is to start applying more complicated deep learning algorithms, for instance convolutional neural networks or recurrent neural networks increasing the precision on the feature space and temporal analysis of motion, which in turn might improve possibility of anomaly detection. One direction for the future work is the integration of AI with conventional rule-based systems to develop a blend of the two systems that would capitalize on the benefits of both. This approach of using both quantitative and qualitative research could provide a better solution for the problems that relate to network security in complex environments.

Therefore, this study shows that AI techniques such as feedforward neural networks and reinforcement learning can improve network security. The outcomes are evidence that these approaches can enhance threat identification and mitigation and serve as the basis for future research and

advancement in the use of AI in cybersecurity as used in different fields [26-37].

3. Conclusion

This work proves that AI methodologies, namely FNN and RL, can be applied to network security. The FNN model obtained 96.5% accuracy, 94.8% precision and 95.2% recall; this demonstrated that the FNN model is efficient in the accurate classification of network activities and reduction of false alarms. The RL agent has an average reward of +12.5 and was able to dynamically handle traffic anomalies, and its actions included blocking traffic for high traffic anomalies and informing administrators of medium traffic anomalies. Specifically, four-layer general structure, including monitoring, feature extraction, monitoring with the help of AI algorithms, and response were able to fulfill its important tasks of timely and accurate threat identification. Besides, this approach is significantly more effective than traditional approaches and provides a flexible, easily scalable solution for modern network security, making it suitable for implementation in modern dynamic and complex network environments.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Wu, H., Han, H., Wang, X., & Sun, S. (2020). Research on artificial intelligence enhancing internet of things security: A survey. *IEEE Access*, *8*, 153826-153848.

[2] Wan, H., Liu, G., & Zhang, L. (2021, October). Research on the application of artificial intelligence in computer network technology. In *Proceedings of the 2021 5th International Conference on Electronic Information Technology and Computer Engineering* (pp. 704-707).

[3] Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., ... & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, 1-25.

[4] Mughal, A. A. (2018). Artificial Intelligence in Information Security: Exploring the Advantages, Challenges, and Future Directions. *Journal of Artificial Intelligence and Machine Learning in Management*, *2*(1), 22-34.

[5] Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, *2*(3), 173.

[6] Geluvaraj, B., Satwik, P. M., & Ashok Kumar, T. A. (2019). The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. In *International Conference on Computer Networks and Communication Technologies: ICCNCT 2018* (pp. 739-747). Springer Singapore.

[7] Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1462-1474.

[8] Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *IEEE Access*, *8*, 23817-23837.

[9] Kuzlu, M., Fair, C., & Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of Things*, *1*(1), 7.

[10] Shabbir, J., & Anwer, T. (2018). *Artificial intelligence and its role in near future*. arXiv preprint arXiv:1804.01396.

[11] Zarina I, K., Ildar R, B., & Elina L, S. (2019). Artificial Intelligence and Problems of Ensuring Cyber Security. *International Journal of Cyber Criminology*, *13*(2).

[12] Ghazal, T. M. (2021). Internet of things with artificial intelligence for health care security. *Arabian Journal for Science and Engineering*.

[13] Khanh, H. H., & Khang, A. (2021). The role of artificial intelligence in blockchain applications. In *Reinventing Manufacturing and Business Processes through Artificial Intelligence* (pp. 19-38). CRC Press.

[14] Ullah, Z., Al-Turjman, F., Mostarda, L., & Gagliardi, R. (2020). Applications of artificial intelligence and machine learning in smart cities. *Computer Communications*, *154*, 313-323.

[15] Latah, M., & Toker, L. (2019). Artificial intelligence enabled software- defined networking: A comprehensive overview. *IET Networks*, *8*(2), 79-99.

[16] Huynh-The, T., Pham, Q. V., Pham, X. Q., Nguyen, T. T., Han, Z., & Kim, D. S. (2023).

Artificial intelligence for the metaverse: A survey. *Engineering Applications of Artificial Intelligence*, *117*, 105581.

[17] Fatemidokht, H., Rafsanjani, M. K., Gupta, B. B., & Hsu, C. H. (2021). Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular ad hoc networks in intelligent transportation systems. *IEEE Transactions on Intelligent Transportation Systems*, *22*(7), 4757-4769.

[18] Mata, J., De Miguel, I., Durán, R. J., Merayo, N., Singh, S. K., Jukan, A., & Chamania, M. (2018). Artificial intelligence (AI) methods in optical networks: A comprehensive survey. *Optical Switching and Networking*, *28*, 43-57.

[19] Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things*, *11*, 100227.

[20] Singh, S. K., Rathore, S., & Park, J. H. (2020). Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. *Future Generation Computer Systems*, *110*, 721-743.

[21] Omitaomu, O. A., & Niu, H. (2021). Artificial intelligence techniques in smart grid: A survey. *Smart Cities*, *4*(2), 548-568.

[22] Han, H., Shiwakoti, R. K., Jarvis, R., Mordi, C., & Botchie, D. (2023). Accounting and auditing with blockchain technology and artificial Intelligence: A literature review. *International Journal of Accounting Information Systems*, *48*, 100598.

[23] Saeik, F., Avgeris, M., Spatharakis, D., Santi, N., Dechouniotis, D., Violos, J., ... & Papavassiliou, S. (2021). Task offloading in Edge and Cloud Computing: A survey on mathematical, artificial intelligence and control theory solutions. *Computer Networks*, *195*, 108177.

[24] Ben Ayed, R., & Hanana, M. (2021). Artificial intelligence to improve the food and agriculture sector. *Journal of Food Quality*, *2021*(1), 5584754.

[25] Tan, L., Yu, K., Ming, F., Cheng, X., & Srivastava, G. (2021). Secure and resilient artificial intelligence of things: A HoneyNet approach for threat detection and situational awareness. *IEEE Consumer Electronics Magazine*, *11*(3), 69-78.

[26] Sakshi Taaresh Khanna, Khatri, S. K., & Sharma, N. K. (2025). Advancements in Artificial Intelligence for Oral Cancer Diagnosis. *International Journal of Computational and Experimental Science and Engineering*, 11(2). https://doi.org/10.22399/ijcesen.1666

[27] Ibeh, C. V., & Adegbola, A. (2025). AI and Machine Learning for Sustainable Energy: Predictive Modelling, Optimization and Socioeconomic Impact In The USA. *International Journal of Applied Sciences and Radiation Research* , 2(1). https://doi.org/10.22399/ijasrar.19

[28] G. Prabaharan, S. Vidhya, T. Chithrakumar, K. Sika, & M.Balakrishnan. (2025). AI-Driven Computational Frameworks: Advancing Edge Intelligence and Smart Systems. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.1165

[29] Hafez, I. Y., & El-Mageed, A. A. A. (2025). Enhancing Digital Finance Security: AI-Based Approaches for Credit Card and Cryptocurrency Fraud Detection. *International Journal of Applied Sciences and Radiation Research*, 2(1). https://doi.org/10.22399/ijasrar.21

[30] M.K. Sarjas, & G. Velmurugan. (2025). Bibliometric Insight into Artificial Intelligence Application in Investment. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.864

[31] Olola, T. M., & Olatunde, T. I. (2025). Artificial Intelligence in Financial and Supply Chain Optimization: Predictive Analytics for Business Growth and Market Stability in The USA. *International Journal of Applied Sciences and Radiation Research*, 2(1). https://doi.org/10.22399/ijasrar.18

[32] ZHANG, J. (2025). Artificial intelligence contributes to the creative transformation and innovative development of traditional Chinese culture. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.860

[33] García, R., Carlos Garzon, & Juan Estrella. (2025). Generative Artificial Intelligence to Optimize Lifting Lugs: Weight Reduction and Sustainability in AISI 304 Steel. *International Journal of Applied Sciences and Radiation Research*, 2(1). https://doi.org/10.22399/ijasrar.22

[34] G Nithya, R, P. K., V. Dineshbabu, P. Umamaheswari, & T, K. (2025). Exploring the Synergy Between Neuro-Inspired Algorithms and Quantum Computing in Machine Learning. *International Journal of Computational and Experimental Science and Engineering*, 11(3). https://doi.org/10.22399/ijcesen.2484

[35] Kumari, S. (2025). Machine Learning Applications in Cryptocurrency: Detection, Prediction, and Behavioral Analysis of Bitcoin Market and Scam Activities in the USA. *International Journal of Sustainable Science and Technology*, 1(1). https://doi.org/10.22399/ijsusat.8

[36] Pranandi, I., & Francisca Tjhay. (2025). Artificial Intelligence and Machine Learning in Biochemical and Molecular Diagnostics: A Transformative Review of Current Applications and Future Prospects. *International Journal of Computational and Experimental Science and Engineering*, 11(3). https://doi.org/10.22399/ijcesen.2634

[37] Chui, K. T. (2025). Artificial Intelligence in Energy Sustainability: Predicting, Analyzing, and Optimizing Consumption Trends. *International Journal of Sustainable Science and Technology*, 1(1). https://doi.org/10.22399/ijsusat.1