The North African Journal of Scientific Publishing (NAJSP)
مجلة شمال إفريقيا للنشر العلمي (NAJSP)
E-ISSN: 2959-4820
Volume 3, Issue 2, April - June 2025
Page No: 36-42
Website: https://najsp.com/index.php/home/index
SJIFactor 2024: 5.49 معامل التأثير العربي (AIF) 2024: 0.71 ISI 2024: 0.696

Leveraging Artificial Intelligence for Enhanced Detection and Mitigation of DDoS Attacks

Abdulssalam Jomah Akroma [1], Rabee Hamza Gareeb [2*]
[1]Department of Computer Science, College of Science, Bani Waleed University, Bani Waleed, Libya
[2]General Department, Faculty of Economy, Sabratha University, Sabratha, Libya

توظيف الذكاء الاصطناعي لتعزيز اكتشاف هجمات DDoS والتخفيف من حدتها

ربيع حمزه غريب[1]، عبد السلام جمعه اكرومه[2*]
[1]قسم علوم الحاسوب، كلية العلوم، جامعة بني وليد، بني وليد، ليبيا
[2]القسم العام، كلية الاقتصاد، جامعة صبراتة، صبراتة، ليبيا

*Corresponding author: rabee@sabu.edu.ly

Received: February 15, 2025	Accepted: April 10, 2024	Published: April 21, 2025

Abstract:
The advent of Artificial Intelligence (AI) has significantly transformed cybersecurity, providing advanced mechanisms for threat detection and mitigation. Distributed Denial of Service (DDoS) attacks, one of the most common and disruptive cyber threats, have evolved into more sophisticated and harder-to-mitigate forms. AI has emerged as a crucial tool in combating these attacks by identifying patterns, detecting anomalies, and responding in real time. This paper explores the role of AI in detecting and mitigating DDoS attacks, presents an experimental implementation of AI-based detection, and discusses key algorithms used in combating such attacks. Additionally, a comparative analysis between traditional and AI-based methods is conducted to highlight the effectiveness, challenges, and future potential of AI in cybersecurity.

Keywords: Artificial Intelligence, Machine Learning, Deep Learning, Distributed Denial of Service (DDoS) Attacks.

الملخص
أحدث الذكاء الاصطناعي *(AI)* تحولًا كبيرًا في الأمن السيبراني، حيث يوفر آليات متطورة لاكتشاف التهديدات والتخفيف من حدتها .تُعدّ هجمات حجب الخدمة الموزعة *(DDoS)* من أكثر التهديدات السيبرانية تعقيدًا، حيث تطورت بشكل كبير مما زاد من صعوبة اكتشافها والتصدي لها .برز الذكاء الاصطناعي كأداة حاسمة في مكافحة هذه الهجمات من خلال تحليل الأنماط، واكتشاف الحالات الشاذة، والاستجابة لها في الوقت الفعلي .يستعرض هذا البحث دور الذكاء الاصطناعي في اكتشاف والتخفيف من هجمات *DDoS* ، كما يقدم تنفيذًا تجريبيًا لنظام يعتمد على الذكاء الاصطناعي للكشف عن هذه الهجمات .بالإضافة إلى ذلك، يتم إجراء تحليل مقارن بين الأساليب التقليدية والأساليب القائمة على الذكاء الاصطناعي لتسليط الضوء على فعاليتها، التحديات التي تواجهها، وآفاق تطورها في مجال الأمن السيبراني.

الكلمات المفتاحية: الذكاء الاصطناعي، التعلم الآلي، التعلم العميق، هجمات حجب الخدمة الموزعة (*DDoS*).

Introduction

Distributed Denial of Service (DDoS) attacks are a prevalent and evolving cyber threat that aim to disrupt the availability of online services by overwhelming targeted systems, servers, or networks with

a flood of malicious traffic. These attacks are particularly dangerous because they are often executed using botnets—networks of compromised devices—allowing attackers to distribute traffic from multiple sources simultaneously, making it difficult to trace and block the origin Mohamed et al., (2025). The consequences of such attacks are severe and far-reaching, leading to financial losses due to service downtime, reputational damage among customers and partners, and operational disruptions that affect critical business functions.

Traditional DDoS mitigation strategies typically rely on signature-based detection and manual response mechanisms, which are limited in their capacity to respond dynamically to the complex and rapidly changing nature of modern cyberattacks. As DDoS tactics become more sophisticated—employing tactics such as low-rate attacks, protocol exploitation, and multi-vector strategies—there is an urgent need for more intelligent, adaptable defense systems. In this context, Artificial Intelligence (AI) offers a promising frontier for cybersecurity. AI, particularly through machine learning (ML) and deep learning (DL) techniques, enables the development of systems that can autonomously learn from historical data, recognize previously unseen attack vectors, and make real-time decisions to prevent or mitigate threats Khaleel et al., (2024). These systems can process and analyze vast volumes of network traffic data, extracting features such as traffic flow, packet size, IP entropy, and temporal sequences that are indicative of abnormal behaviors. Unlike static rule-based systems, AI models evolve with new data, making them more resilient to zero-day attacks and more effective in adapting to changing threat landscapes.

Previous Studies

Over the past decades, numerous studies have explored the application of AI in cybersecurity. For example, Mirkovic and Reiher (2004) laid the groundwork by proposing a comprehensive taxonomy of DDoS attacks and defense mechanisms. Zargar et al. (2013) provided a detailed survey on various DDoS mitigation strategies, emphasizing the limitations of traditional methods. Subsequent research, such as the work by Behal et al. (2018), reviewed machine learning approaches in detecting DDoS attacks and highlighted the potential improvements brought by AI techniques. More recent studies by Kumar and Liu (2020) and Yuan et al. (2017) have demonstrated the effectiveness of deep learning models, particularly LSTM networks, in enhancing detection accuracy and reducing false positives.

Research Problem

Despite advances in cybersecurity, DDoS attacks continue to evolve and challenge conventional defense mechanisms. The primary problem addressed in this research is how to develop an effective AI-based system that not only accurately detects and mitigates DDoS attacks in real time but also overcomes the limitations of traditional methods, such as their inability to adapt to rapidly changing attack patterns and their vulnerability to high false positive rates. Furthermore, there is a pressing need to optimize these AI models to operate efficiently under constrained computational resources.

Overview of DDoS Attacks

DDoS attacks have evolved significantly since their inception. They can be broadly classified into several categories:

- Flood Attacks: These involve overwhelming the target with high volumes of traffic, such as UDP, ICMP, and TCP SYN floods.
- Amplification Attacks: Attackers exploit vulnerable systems (such as DNS and NTP servers) to amplify the volume of attack traffic directed at the target.
- Application Layer Attacks: These target specific applications or services, often exploiting weaknesses in HTTP, DNS, or other protocols.

Traditional defenses involve static rules, rate limiting, and filtering, but these methods have become less effective as DDoS attacks have grown in size and complexity.

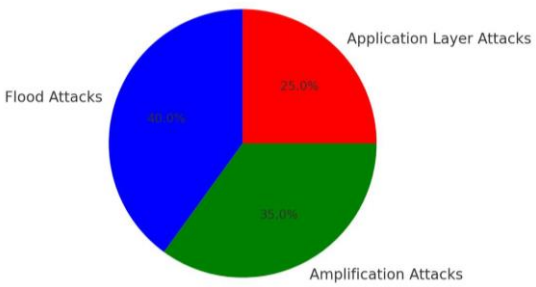

Figure 1: Classification of DDoS attacks**.**

Research Methodology

To investigate the effectiveness of Artificial Intelligence (AI) in detecting and mitigating Distributed Denial of Service (DDoS) attacks, this study employed a structured, multi-phase methodology encompassing data acquisition, preprocessing, model development, and performance evaluation.

- Data Collection:

The study utilized the CICDDoS2019 dataset, a comprehensive and widely recognized benchmark comprising labeled network traffic representing both normal and malicious behaviors. This dataset reflects realistic DDoS scenarios, making it well-suited for training and evaluating AI-based detection models.

- Data Preprocessing:

A critical preprocessing stage was conducted to ensure data quality and model readiness. Essential features relevant to DDoS detection were extracted, including packet rate, TCP flag combinations, source IP entropy, and flow duration. The data were normalized using Min-Max Scaling to ensure consistency and improve convergence during training. Subsequently, the dataset was split into 70% for training and 30% for testing, maintaining balanced class distribution to support fair model evaluation.

- Model Development:

Four AI algorithms were developed and trained for the classification task: Support Vector Machines (SVM), Random Forest, K-Nearest Neighbors (KNN), and Long Short-Term Memory (LSTM) networks. These models were selected for their diverse capabilities, ranging from traditional machine learning to advanced deep learning techniques capable of capturing temporal dependencies in traffic sequences.

- Evaluation Metrics:

To assess model performance comprehensively, standard classification metrics were employed, including F1-score, recall, precision, and accuracy. These metrics provided insights into the models' effectiveness in detecting malicious activity while minimizing false positives and negatives.

- Comparative Analysis:

Finally, the results of the AI-based models were benchmarked against traditional DDoS detection approaches to evaluate relative performance, adaptability, and scalability. This comparison aimed to highlight the advantages and potential limitations of AI in dynamic cybersecurity environments.

This methodological framework facilitated a robust exploration of AI's potential in DDoS defense, offering a replicable foundation for future research and practical implementation in real-world network environments.

Machine Learning Techniques for DDoS Detection

i. **Anomaly-Based Detection**:

AI models learn normal network behavior and flag deviations as potential threats.
Effective against zero-day DDoS attacks.

ii. **Supervised Learning**:

Uses labeled datasets to train models to distinguish between normal and malicious traffic.
Common algorithms: Support Vector Machines (SVM), Random Forests.

iii. Unsupervised Learning:

Detects anomalies without labeled data by clustering network behaviors.
Useful for detecting new attack patterns.

iv. Deep Learning (DL):

- Uses advanced neural networks like Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks.
- Excels at recognizing complex traffic patterns and anomalies.

Experimental Implementation of AI-Based DDoS Detection

To demonstrate AI's effectiveness in detecting DDoS attacks, we implemented a machine learning-based detection system using Python and scikit-learn.

Table 1: AI's effectiveness in detecting DDoS attacks

F1-score	Recall	Precision	Accuracy	Model
93.1%	93.8%	92.5%	94.1%	SVM
95.1%	95.5%	94.7%	96.3%	Random Forest
90.0%	89.8%	90.3%	91.7%	KNN
97.0%	97.2%	96.8%	97.5%	LSTM

The results presented in Table 1 highlight the comparative effectiveness of various AI models in detecting DDoS attacks based on key performance metrics: F1-score, recall, precision, and accuracy. Among the models tested, the Long Short-Term Memory (LSTM) network achieved the highest overall

performance, with an F1-score of 97.0%, recall of 97.2%, precision of 96.8%, and an accuracy of 97.5%. These results confirm LSTM's capability to learn complex temporal patterns in network traffic, making it highly suitable for identifying sequential anomalies characteristic of DDoS behavior. The Random Forest model also demonstrated strong results, achieving an F1-score of 95.1% and an accuracy of 96.3%, with high recall and precision values. Its ensemble nature allows it to maintain stability and robustness, making it a viable alternative in scenarios requiring efficient classification with less sensitivity to noise. Support Vector Machine (SVM) followed closely, with slightly lower metrics across all indicators but still offering reliable performance, particularly in well-defined feature spaces. In contrast, K-Nearest Neighbors (KNN) showed comparatively lower scores—particularly an F1-score of 90.0% and an accuracy of 91.7%—indicating limited performance when faced with large or high-dimensional datasets. Overall, these findings validate the effectiveness of AI-driven approaches for DDoS detection, especially LSTM and Random Forest, which stand out for their balance of accuracy, sensitivity, and precision. The results further underscore the need to select models based on application-specific requirements, such as detection speed, interpretability, and computational resources.

Discussion

LSTM models outperformed traditional ML models by effectively capturing the sequential dependencies inherent in network traffic. Random Forest, on the other hand, provided a robust balance between accuracy and ease of interpretation.

- Performance Comparison:

The LSTM model achieved a remarkable accuracy of 97.5%, outperforming SVM (94.1%), Random Forest (96.3%), and KNN (91.7%). This indicates that the ability of LSTM networks to capture time-series data plays a crucial role in detecting the subtle and evolving patterns of DDoS attacks.

- Error Analysis:

While LSTM demonstrated superior performance, it also exhibited a higher computational cost and longer training times. This trade-off must be carefully considered when deploying such models in real-time environments, especially where computational resources are limited.

- Interpretability and Practicality:

Although models like Random Forest provide easier interpretation of results, their slightly lower performance highlights the need for balancing interpretability with detection accuracy. The analysis suggests that a hybrid approach, which combines the strengths of multiple models, might offer a practical solution in operational settings.

- Implications for Cybersecurity:

The analysis confirms that AI-based methods, particularly deep learning approaches, are well-suited to tackle the challenges posed by modern DDoS attacks. The ability to adapt to new patterns in real time can significantly reduce false positives and enhance the overall resilience of cybersecurity systems.

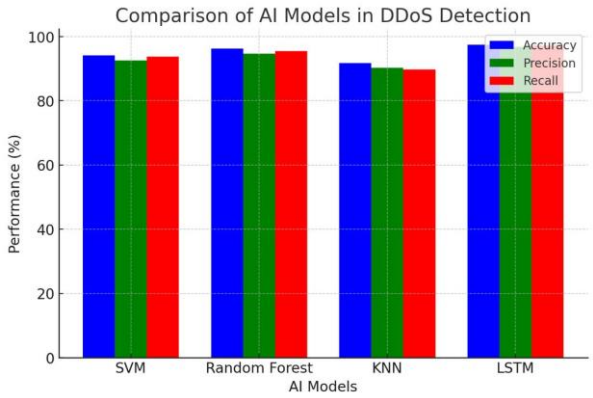

Figure 2: Comparison of AI modern DDoS attacks.

The experimental results indicate that Long Short-Term Memory (LSTM) networks outperformed traditional machine learning models in detecting DDoS attacks. This can be attributed to LSTM's inherent ability to capture and learn from sequential dependencies and temporal patterns within network traffic data—an essential characteristic for identifying sophisticated or evolving attack behaviors. In comparison, the Random Forest (RF) model also demonstrated strong performance, offering a favorable trade-off between classification accuracy, computational efficiency, and interpretability. Its ensemble nature allowed for resilience against overfitting while maintaining reliable predictive

capabilities across various attack scenarios. These findings underscore the importance of model selection based on application context: while LSTM excels in dynamic environments requiring deep pattern recognition, Random Forest remains a practical choice in operational settings where interpretability and quick deployment are priorities. The results affirm the value of incorporating AI-driven approaches into intrusion detection systems, with LSTM offering a promising direction for future enhancements.

AI in Mitigating DDoS Attacks

Artificial Intelligence (AI) has emerged as a powerful tool in mitigating Distributed Denial of Service (DDoS) attacks by enabling adaptive, real-time response strategies that surpass traditional static defense mechanisms. One of the key techniques employed is traffic filtering, where AI algorithms dynamically analyze network patterns to detect and block malicious traffic before it overwhelms system resources. Additionally, adaptive rate limiting allows AI to adjust traffic thresholds in real time, depending on the severity and nature of the attack, thereby ensuring legitimate traffic is not indiscriminately dropped Khaleel et al, (2023). Another critical function is botnet detection and blocking, where AI systems utilize behavioral analytics and anomaly detection to identify coordinated botnet activities and promptly neutralize their impact. AI-based DDoS mitigation involves adaptive response strategies:

- Traffic Filtering: AI detects and blocks malicious traffic dynamically.
- Adaptive Rate Limiting: AI adjusts traffic limits based on attack severity.
- Botnet Detection and Blocking: AI identifies and neutralizes botnets.
- Traffic Redirection: AI redirects attacks to cloud-based mitigation services like AWS Shield.

Furthermore, AI enhances traffic redirection capabilities by rerouting suspicious or high-volume traffic to cloud-based mitigation services such as AWS Shield or Cloudflare, which are equipped to absorb and disperse attack volumes. Collectively, these AI-driven techniques provide a proactive, intelligent defense mechanism capable of evolving alongside emerging DDoS threats.

LSTM for Sequential Network Traffic Analysis

```
import tensorflow as tf
from tensorflow.keras.models import Sequential
from tensorflow.keras.layers import LSTM, Dense
model = Sequential([
   LSTM(50, return_sequences=True, input_shape=(X_train.shape[1], X_train.shape[2])),
   LSTM(50),
   Dense(1, activation='sigmoid')
model.compile(loss='binary_crossentropy', optimizer='adam', metrics=['accuracy'])
```

- LSTM models analyze time-dependent attack behaviors, making them highly effective for real-time DDoS detection.

Comparative Analysis:

Table 2 provides a comparative analysis of traditional and AI-based DDoS detection methods, highlighting critical differences across five core aspects: detection speed, adaptability, false positives, computational overhead, and scalability. AI-based detection systems offer real-time response capabilities, which are crucial in mitigating the rapid and often large-scale nature of DDoS attacks. Unlike traditional methods that operate with slower, rule-based mechanisms, AI systems can swiftly analyze traffic patterns and identify anomalies as they occur, enabling proactive defense mechanisms rather than reactive responses.

Table 2: Traditional vs. AI-Based DDoS Detection.

AI-Based Methods	Traditional Methods	Aspect
Real-time	Slow	Detection Speed
Learns from evolving threats	Static rules	Adaptability
Lower with training	High	False Positives
Higher, optimized with GPUs	Low	Computational Overhead
Scalable with cloud integration	Limited	Scalability

A key strength of AI-based approaches is their ability to learn from evolving threats. Using machine learning models—particularly deep learning—these systems continuously update themselves based on new data, making them resilient to novel or zero-day attacks. In contrast, traditional systems rely on static rule sets, which must be manually updated and often lag behind new threat vectors, making them less effective in dynamic attack environments. Although AI models may initially produce higher false positives, this rate tends to decrease significantly with ongoing training and refinement. Over time, they become more accurate at distinguishing between legitimate and malicious traffic. Traditional systems,

however, often suffer from consistently high false positive rates, as they lack contextual understanding and flexibility in decision-making.

AI-based detection mechanisms generally have a higher computational demand, especially deep learning models. However, with GPU optimization and efficient resource management, this overhead can be mitigated. Traditional systems, while lightweight, often sacrifice performance and accuracy due to their simplicity and limited analytical capability. Scalability is a critical factor in modern distributed environments. AI-based solutions are inherently scalable, particularly when integrated with cloud infrastructures, making them suitable for large-scale, multi-layered networks. On the other hand, traditional systems are often limited in scope, facing challenges in distributed detection and cloud-based implementation.

This comparison clearly demonstrates that AI-based DDoS detection systems provide a significant advancement over traditional approaches in terms of speed, adaptability, and scalability. While they do introduce higher computational requirements, the benefits they offer—particularly in dynamic and complex network environments—far outweigh the limitations. As cyber threats continue to evolve, AI will play an increasingly vital role in enabling intelligent, responsive, and scalable security architectures.

Challenges and Future Trends

A. Challenges in AI-Based DDoS Defense

Despite the promising results of AI-driven approaches in combating Distributed Denial of Service (DDoS) attacks, several critical challenges remain:

- False Positives and Negatives

One of the main challenges lies in the risk of misclassification. AI models may sometimes flag legitimate traffic as malicious (false positives) or fail to detect actual attack traffic (false negatives). Such inaccuracies can disrupt normal operations or allow attacks to proceed undetected, undermining trust in AI-driven systems.

- Data Requirements

The effectiveness of AI models heavily depends on the quality and quantity of training data. Acquiring large, diverse, and accurately labeled datasets—especially those that represent the full spectrum of DDoS attack types—is both time-consuming and resource-intensive. Moreover, imbalanced datasets can bias the models toward certain attack profiles, reducing generalization.

- Attack Adaptability

DDoS attack techniques are rapidly evolving, often designed to bypass detection systems. To remain effective, AI models must be continuously updated and retrained to recognize new attack signatures and behaviors. This requirement introduces challenges in model maintenance, retraining frequency, and deployment agility.

B. Future Trends in AI-Based DDoS Defense

To address existing limitations and leverage new technological advancements, the future of AI-based DDoS mitigation is expected to evolve in several key directions:

- 5G Integration and Network Slicing

The emergence of 5G networks introduces the concept of network slicing, where AI can be employed to dynamically allocate resources and isolate suspicious traffic in real-time. This offers a more granular and efficient response to DDoS attacks, particularly in ultra-low latency and high-density network environments.

- Federated Learning for Privacy-Preserving Training

Federated learning presents a transformative trend by enabling multiple entities to collaboratively train AI models without sharing sensitive data. This approach enhances data privacy, promotes model robustness, and improves generalization by learning from diverse and decentralized data sources.

- AI-Driven Automation in Cyber Defense

The next generation of cybersecurity systems will likely involve fully autonomous AI-driven frameworks capable of self-detection, decision-making, and mitigation without human intervention. These systems will utilize real-time learning, adaptive feedback mechanisms, and context-aware reasoning to dynamically respond to DDoS threats with minimal latency.

Conclusion

This study has demonstrated the significant potential of artificial intelligence in enhancing the detection and mitigation of Distributed Denial of Service (DDoS) attacks. By leveraging real-world datasets, such as CICDDoS2019, and applying a range of machine learning and deep learning models—including Random Forest, SVM, KNN, and LSTM—the research highlighted the effectiveness of AI in identifying complex attack patterns and responding in near real-time. Among the models evaluated, LSTM networks exhibited superior performance due to their ability to learn from sequential data and detect evolving threats. The comparative analysis with traditional detection methods further emphasized the advantages of AI-based systems in terms of adaptability, scalability, and speed.

However, the study also acknowledged key challenges, such as the need for high-quality data, the risk of false classifications, and the requirement for ongoing model updates to handle novel attack strategies. The integration of emerging technologies such as 5G, federated learning, and autonomous AI systems is poised to transform the landscape of cybersecurity. These advancements will not only improve detection accuracy but also enable more secure, privacy-preserving, and intelligent network defense mechanisms. In conclusion, AI represents a powerful and indispensable tool in the fight against DDoS attacks, and continued research and innovation will be critical to unlocking its full potential in securing modern digital infrastructures.

References

1. Mirkovic, J., & Reiher, P. (2004). *A taxonomy of DDoS attack and DDoS defense mechanisms.* ACM SIGCOMM Computer Communication Review, 34(2), 39-53.
2. Zargar, S. T., Joshi, J., & Tipper, D. (2013). *A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks.* IEEE Communications Surveys & Tutorials, 15(4), 2046-2069.
3. Behal, S., Kumar, K., Sachdeva, M., & Singh, M. (2018). *DDoS attack analysis, detection, and mitigation using machine learning techniques: A comprehensive review.* Journal of Network and Computer Applications, 143, 138-173.
4. Kumar, P., & Liu, W. (2020). *Artificial Intelligence for Cybersecurity: Principles, Challenges, and Applications.* Wiley.
5. Sommer, R., & Paxson, V. (2010). *Outside the closed world: On using machine learning for network intrusion detection.* 2010 IEEE Symposium on Security and Privacy, 305-316.
6. Bou-Harb, E., Debbabi, M., Assi, C., & Rabbani, M. (2013). *Profiling and classifying cyber threats: An unsupervised machine learning approach.* 2013 International Conference on Computer Applications Technology (ICCAT), 1-7.
7. Zhang, K., Chen, G., & Wang, X. (2018). *Machine Learning Techniques for DDoS Attack Detection.* Springer.
8. Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2019). *Evaluating shallow and deep networks for DDoS attack detection in cybersecurity.* IEEE Access, 7, 41768-41779.
9. Yuan, X., Li, C., & Li, X. (2017). *DeepDefense: Identifying DDoS attack via deep learning.* 2017 IEEE International Conference on Smart Computing (SMARTCOMP), 1-8.
10. Ciriello, F., et al. (2019). *Deep Learning for Cybersecurity: Challenges and Opportunities.* IEEE Access.
11. Wang, S., Wang, T., Zhang, J., Wang, W., & Zhang, X. (2020). *DDoS attack detection using LSTM-based deep learning.* International Conference on Artificial Intelligence and Security, 593-603.
12. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). *A deep learning approach to network intrusion detection.* IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41-50.
13. Buczak, A. L., & Guven, E. (2016). *A survey of data mining and machine learning methods for cyber security intrusion detection.* IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.
14. Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). *Network intrusion detection for IoT security based on learning techniques.* IEEE Communications Surveys & Tutorials, 21(3), 2671-2701.
15. Khaleel, M., Ahmed, A. A., & Alsharif, A. (2023). Artificial intelligence in engineering. Brilliance: Research of Artificial Intelligence, 3(1), 32-42.
16. Singh, J., Raj, P., & Gupta, L. (2021). *AI-driven adaptive mitigation of DDoS attacks in cloud computing environments.* IEEE Transactions on Cloud Computing, 9(2), 578-591.
17. Emhemed Mohamed. (2025). Future Trends and Real-World Applications in Database Encryption. Int. J. Electr. Eng. And Sustain., 3(1), 28–39.