Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 5, 2025

# AN OPTIMAL AI & DEEP LEARNING MECHANISM FOR MITIGATING HACKING THREAT IDENTIFICATION USING SECURE NETWORK INFRASTRUCTURE BASED ON LINUX AND SOFTWARE-DEFINED NETWORK (SDN)

**Nasir Ayub[*1], Zaman Habib[2], Salheen Bakhet[3], Saqlain Riaz[4], Syed Muhammad Rizwan[5], Mahad Abid[6], Ali Hassan[7], Hamayun Khan[8]**

[*1]*Deputy Head of Engineering, Calrom Limited, M1 6EG, United Kingdom*
[2,4]*Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan*
[3]*Department of Computer Science, University of Engineering and Technology, Lahore*
[5]*Department of Computer Engineering, University of Engineering and Technology Lahore, Pakistan*
[6,7,8] *Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, Pakistan*

[*1]nasir.ayyub@hotmail.com, [2]zamanhabib08@gmail.com, [3]salheen@ieee.org, [4]saqlain.123436@gmail.com, [5]rizwan.naqvi@ieee.org, [6]chmahad508@gamil.com, [7]alihassan2590@gmail.com, [8]hamayun.khan@superior.edu.pk

DOI: https://doi.org/10.5281/zenodo.15487738

**Keywords**
*Machine Learning, Deep Neural Network, CNN, Prediction Models, Hybrid Machine Learning, Hacking Attacks Detection, AI, Ethical Hacking, GenAI, ChatGPT, DeepSeek, Cybersecurity*

**Article History**
*Received on 14 April 2025*
*Accepted on 14 May 2025*
*Published on 22 May 2025*


**Corresponding Author: ***
**Nasir Ayub**

**Abstract**
*The invention of deep learning in secure routing triggered an exceptional expansion of the Software-defined Network (SDN). The article explores how generative AI (GenAI) tools, especially ChatGPT, can support and improve ethical hacking practices and how the network can be secured from network threats. Experiments in a controlled virtual environment, targeting Linux-based machines set up in a simulated local network, is conducted. The study looks at all major stages of penetration testing–including reconnaissance, scanning and enumeration, gaining access, maintaining access, and covering tracks to assess how effectively GenAI tools can contribute. The results show clearly that GenAI significantly boosts the efficiency and effectiveness of ethical hacking tasks. Additionally, discussed the potential risks involved with integrating AI, such as misuse, data bias, and becoming overly dependent on AI solutions. This article also integrates both SDN-driven DL techniques for an intelligent network to improve security and solve problems in SDN networks. SDN is regarded as the right option since it helps restructure networks and operate IoT platforms with the help of different data and control planes. The proposed system with ML control provides improved security by enabling the use of detailed security policies that can be quickly modified when necessary. The proposed security module allows the detection of different hacking attacks in the IoT network. The process of training a Deep Learning model in industry relies on data kept in IOT devices. Based on the gathered info, the system decides if the data must be passed on to the fog layer. The prescribed scheme relies on deep learning and CNN to properly choose the best fog node and its features. With a total of 30 nodes, the simulated framework reached an accuracy of 99.59%, up to 80% detection, along with 0.99%*

*throughput and 0.89% delivery rate for packets. It also used 0.11 m joules of energy, set at a high speed of 0.84 bps and a negligible delay of 0.3415 ms and it managed to improve the F1-score by 4% with 10 ms less latency and also used 25 W less energy.*

## INTRODUCTION

XSS Hacking cyberattacks evolve continuously, becoming more complex and out of reach of traditional cybersecurity protocols. No longer can traditional security measures alone be used to counter sophisticated XSS Hacking cyberattacks, which is why there is a need for ethical hacking, a proactive approach aimed at the detection and repair of vulnerabilities before the possibility of exploitation by malicious forces [1, 2]. Ethical hacking consists of penetration testing, vulnerability scanning, and adversarial simulation, all integral components of competent cybersecurity protocols. In the recent past, Artificial Intelligence (AI), particularly generative AI (GenAI), has emerged as a game-changing power in cybersecurity, significantly enhancing the identification, analysis, and reduction of vulnerabilities [3, 4]. Machine learning and deep learning technologies through AI enable real-time threat detection, automated vulnerability scans, and predictive modeling to predict cyberattacks [5]. By examining past XSS Hacking cyberattack patterns and charting attack strategies, predictive modeling assists cybersecurity professionals in preparing for security vulnerabilities, thus minimizing risks and enhancing defense systems [6]. In essence, SDN services are responsible for facilitating data sharing between people subscribed to SDN. An SDN must incorporate all private network traits due to the way it is developed and implemented. The point is still relevant since we should figure out how to make a network system private. Private network services are used to establish a protected environment that allows wanted users to access the network alone [7, 8]. All internal teletraffic uses nodes that are part of the private network. Private networks can separate traffic from other networks. The private traffic network is independent of every traffic type that does not use it. SDN is particularly important since it is developed for use in virtual networks [9, 10]. Modern uses of VPNs build on the current structure and equipment for data and communication. Another name for SDN is Virtual Private Network, since it adds a private network that links through public or shared networks such as the Internet [11]. With an SDN, information can be sent between computers and different internetworks, and it appears as if every network is connected through a single node. The term virtual private networking is used for developing and setting up virtual private networks [12, 13].

**Table 1: Numerous Approaches for Secure Systems**

| Ref. | AI Approach | Security Objective | Dataset | Accuracy |
|---|---|---|---|---|
| [14, 15] | Supervised Learning | Malware Detection | IoTPoT | 97.35% |
| [16] | CNN | Medical Image attack Security | MRI Dataset | 98.91% |
| [17, 18] | DT | Malware attack detection | IoT_Malware dataset | 97.93% |
| [19, 20] | Reinforcement Learning | Malicious data identification | Kitsune network attack database | 95.93% |
| [21, 22] | Unsupervised Learning | Intrusion detection | NSL-KDD | 97.35% |
| [23, 24] | RNN | Intrusion detection | DARPA/KDD Cup '99 | 98.91% |
| [25] | DNN | Anomaly detection | IoT-Botnet 2020 | 99% |
| [26, 27] | MLP | Botnet attack detection | Captured from 9 IoT devices | 97.93% |

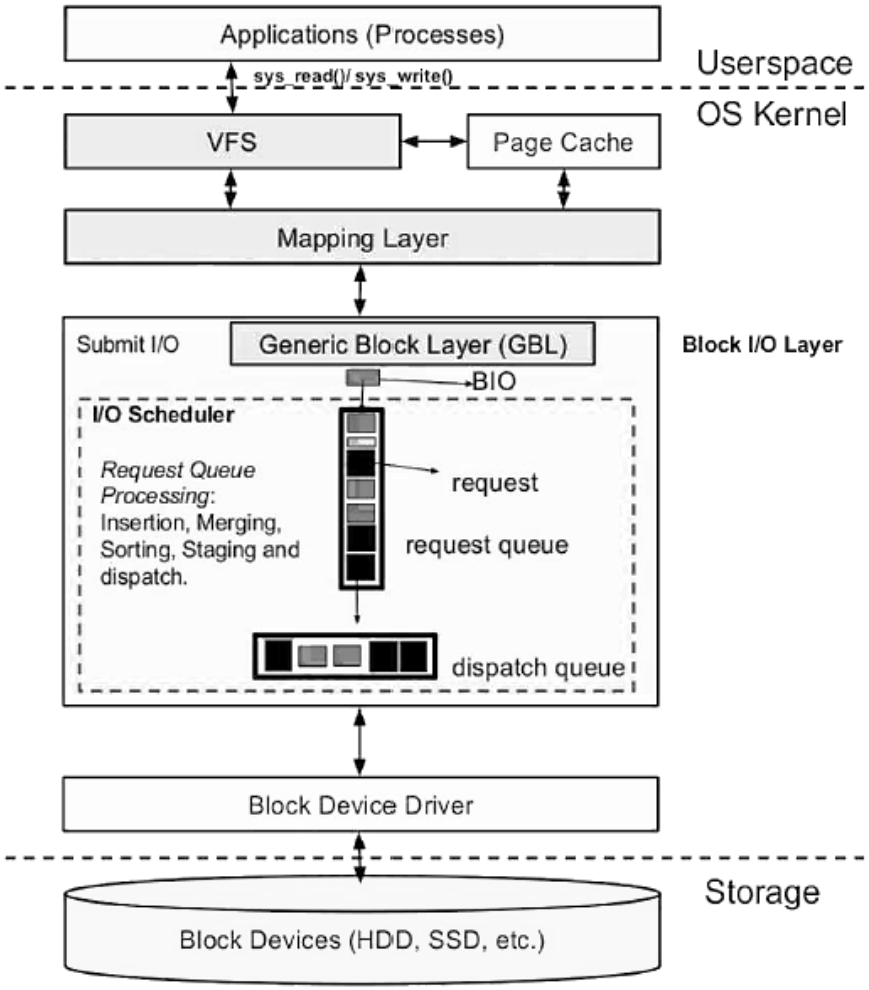


**Figure 1: Generalized Architecture of ML-based Linux Kernel Stack used to Secure System from Hacking [28]**

### 1.1 Machine Learning Algorithms

Networks can gather massive amounts of information and, using the knowledge gained, decide how to use that data. Networks apply several types of ML algorithms. The process includes teaching algorithms on marked data to predict or categorize new information. Usually, Machine Learning is utilized for tasks such as finding objects and understanding speech and it makes use of techniques including neural networks or decision trees. One example is that CNNs can recognize objects with more than 90% accuracy on standard benchmarks [29, 30]. You can think of this method as a Network trying to spot patterns in unmarked data. As an illustration, clustering is effective in finding anomalies, while reducing dimensionality helps identify important features by looking for patterns in unlabeled data. K-means clustering has achieved good results in dividing the Network vision data into various groups. Networks are taught using this method by praising them when they respond correctly. However, it is noteworthy that artificial neural networks easily find complex actions and ways to control them [31, 34].

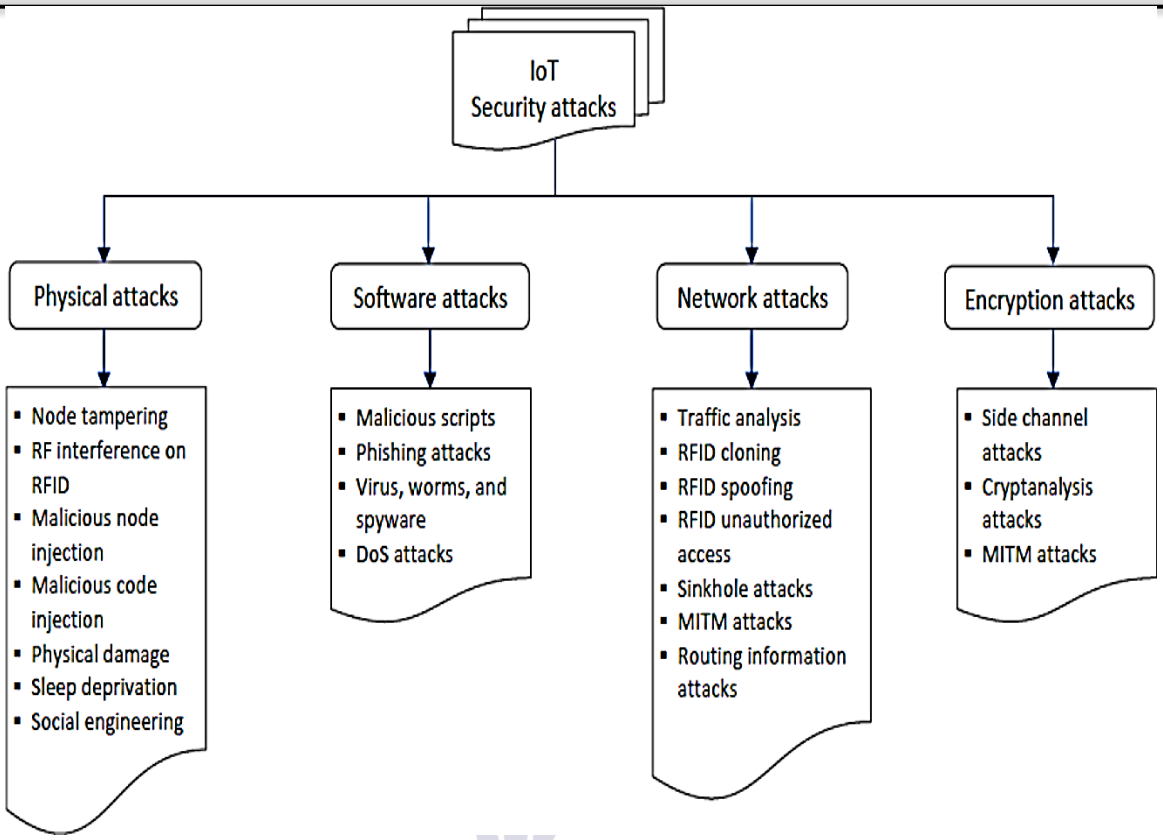


**Figure 2: Attacks on Routing Infrastructure based on IoTs [35]**

### 1.2 Generative Ai

ChatGPT has shown that GenAI is a groundbreaking advance in artificial intelligence and is taking the lead. Unlike before, GenAI goes beyond classification, predictions and rules by producing high-quality information in human-like speech, images, examples of code and other text [36, 37]. It opens up new opportunities in both producing content and areas like cybersecurity and ethical hacking. GPT, which is created by OpenAI, is at the heart of GenAI. ChatGPT and GPT-4o, as well as other models, rely on deep learning and transformer technology [38, 39]. The transformer model relies on attention, allowing certain words in a sequence to be given higher importance depending on their usefulness to the work the model is designed for. Thanks to this innovation, the model understands both the grammatical and meaningful aspects of text, ensuring that the resulting content is both meaningful and accurate [40]. Generative AI is capable of producing content on its own at any requested time. Each genAI model uses a specific approach and has its usefulness. There are several common models.

#### 1.2.1 Variational Auto encoders (VAEs) and GANs

It is made up of two deep learning neural networks connected. One gathers all unstructured data and the other takes the data parameters to restore the content. You can apply machine learning to image recognition, work with natural language processing and identify irregularities [42, 43]. GANs consist of two artificial neural networks. The generator is responsible for creating data, while the discriminator proves how accurate and good the created data is. Most of the time, GAN is applied to produce images and videos [44, 45].

**Table 2: Network Security Challenges**

| Ref. | Area/Field | Description | Solutions |
|---|---|---|---|
| [46, 47] | Device-level security challenges. | Measure to secure individual IoT devices | Secure enclosures, tamper-evident seals, and physical locks<br>Regular security |
| [48, 49] | Data Security Challenges | Ensuring the confidentiality, integrity, and privacy of IoT data | Assessments, code review, patch management |
| [50, 51-52] | Privacy Challenges | Challenges associated with data collection | Strong authentication protocols (2FA, biometrics), access control mechanisms (RBAC, ABAC) |
| [53, 54] | Network Security Challenges | Securing the communication infrastructure connecting IoT devices | TLS, DTLS, Regular assessments, firmware updates, and best practices. |
| [55, 56] | Data Security Challenges | Processing and user consent in IoT systems | Monitoring, anomaly detection, rate limitation, and traffic filtering |
| [57, 58 ] | Data Security Challenges | Ensuring confidentiality, integrity | AES, ECC, Digital signature, Hash functions Encrypted databases |
| [61, 62] | Privacy Challenges | Challenges associated with data collection | Differential privacy |
| [63, 64] | Data Security Challenges | Protection of user privacy in IoT data collection | Secure multiparty computation and federated learning. |
| [65, 66 ] | Data Security Challenges | Privacy of IoT data | Secure communication channels (e.g, HTTP, MQTT with TLS) |
| [67, 68] | Network Security Challenges | Ensuring confidentiality, integrity | Rate limitation, traffic filtering |

$$E_c = \frac{1}{K} \times \sum_{g=1}^{k} J_v^{b,t} - k_v \qquad \text{Eq(1)}$$

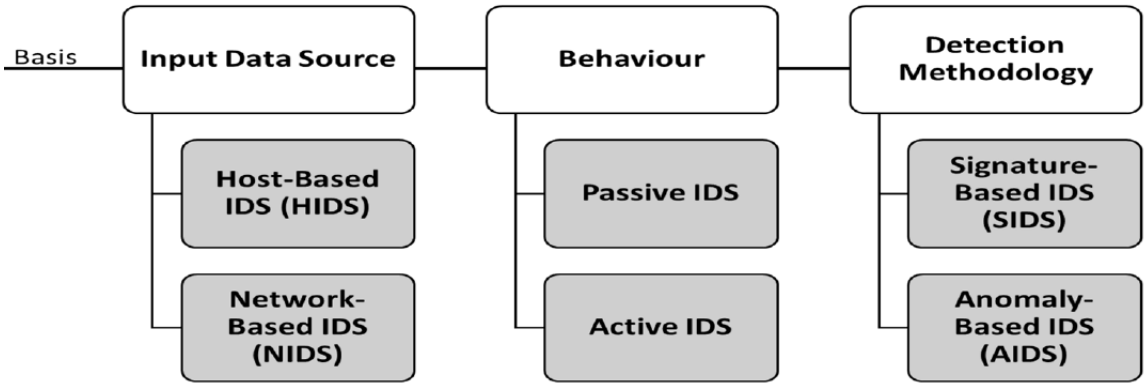


**Figure 3: Machine Learning based IDS [69]**

**2. CNN Classification**

CNNs demonstrate exceptional performance in data arrangements with grid-like structures, such as images that equal two-dimensional pixel grids. The study reviewed the foundation of neural networks and their advanced structures alongside their primary medical diagnostic applications [70].

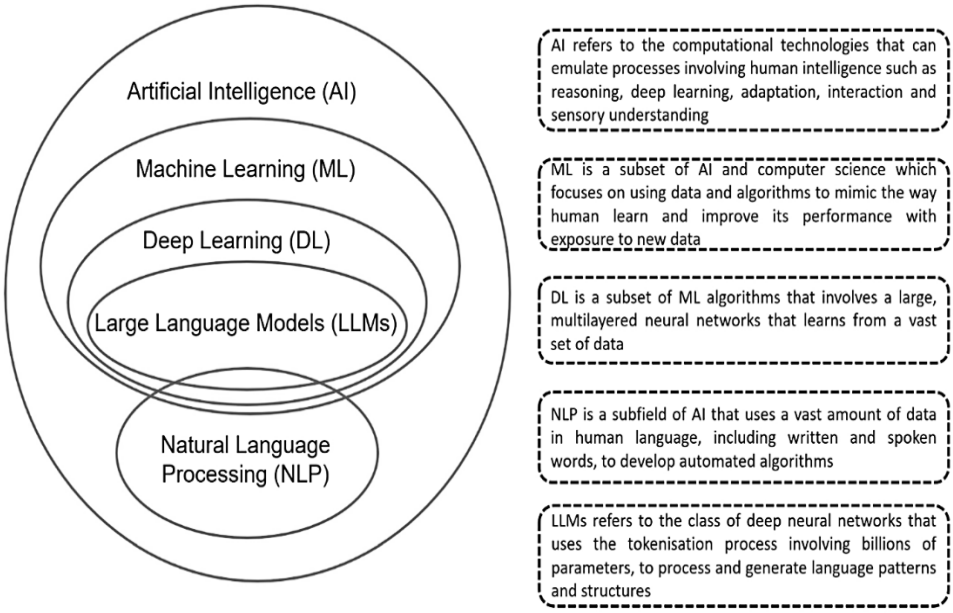


**Figure 4: Classification of AI Techniques [71]**

**3. Machine Learning Based Hacking Threat Identification Based on Secure Routing**

Due to global connectivity, both network security and privacy are more important than they used to be. The more we do our daily activities online, the higher the risk of online security threats becomes. The conveniences brought by new technology have resulted in new threats when it comes to communication and the sharing of data. It allows people to communicate privately, especially when using potentially public networks like the internet. Even so, threats from cyber attacks can develop rapidly. Various hacking strategies, data capture and identity theft significantly hinders the security of networks. Furthermore, surveillance by the government, data tracking by companies and censorship complicate being able to maintain personal privacy online. The issue being explored in this research is how to respond to the growing risks to network security and privacy. Technical measures that maintain security keep threats away and protect online data. This work examines the concept of Routing protocols from a qualitative perspective, mainly by applying machine learning. It aims to reveal how several Networking protocols function, ensure security and work properly. Leveraging items such as academic papers, industry reports and technical documentation is used in this way to build a strong set of protocol features in modern networks. The proposed classifier contains i to represent random units of the b-layer units and y to represent the total b-layer units.

$$B_{m,n}(q+1)(1-\frac{1-X(0,1)-X(-1,1)}{1-c_{m,n}\times f_{mn}(q)}) = X(0,1)\times R_{s,n}$$

Eq (2)

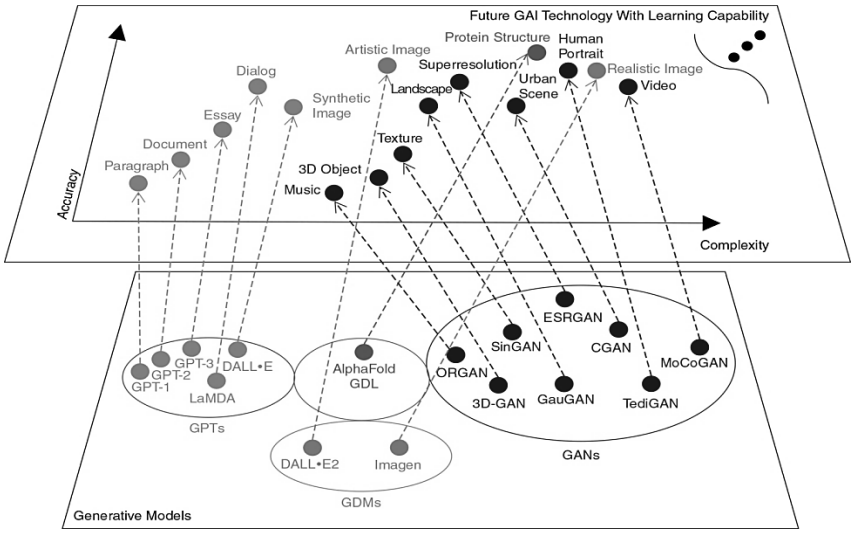


**Figure 5: Generative AI models for Network Security**

$$S_i^{(b,t)} = \sum_{z=1}^{E} p_{iz}^{(b)} J_z^{(b-1,t)} + \sum_{i'}^{y} x_{ii'}^{(b)} J_{i'}^{(b,t-1)}$$

Eq (3)

$$J_i^{(b,t)} = \beta^{(b)}(S_i^{(b,t)})$$

Eq (4)

$$P(w) = \sqrt{\frac{t}{f(w)}} + \frac{t}{f(w)},$$

Eq (5)

4. Results and Classification of Performance

Algorithms are simulated before they are deployed in the real world. Simulations provide a way to evaluate network behaviors and interactions in controlled environments and can highlight issues that might appear.

$$O_t = \sigma(W_O.[h_{(t-1)}, x_t] + b_o),$$

Eq (6)

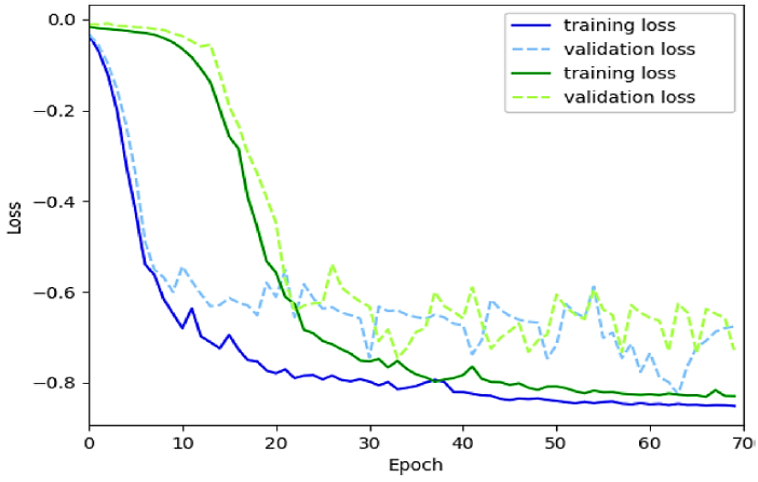


**Figure 6:** Segmentation Loss curve for train and Test

Table 3: Analysis of Critical Infrastructure with Intrusion Detection

| Attack Type | Error Detection | Delay | Datagram Drop | Throughput | Data rate |
|---|---|---|---|---|---|
| DOS-P1 | 0.2119 | 0.1985 | 0.2119 | 0.1985 | 0.84 bps |
| DDOS- P1 | 0.3813 | 0.2119 | 0.3813 | 0.4144 | 0.74 bps |
| DOS Passive P2 | 0.5449 | 0.3813 | 0.5449 | 0.1985 | 0.64 bps |
| DOS Active P2 | 0.2215 | 0.5449 | 0.1985 | 0.2351 | 0.77 bps |
| DDOS Passive P2 | 0.2119 | 0.1985 | 0.666 | 0.1342 | 0.17 bps |
| DOS Tire 1 | 0.2241 | 0.2351 | 0.3581 | 0.2241 | 0.84 bps |
| DDOS Tire 2 | 0.3198 | 0.6581 | 0.4814 | 0.3198 | 0.43 bps |
| DOS Tire 2 | 0.3184 | 0.5119 | 0.6985 | 0.3184 | 0.67 bps |
| DOS Active Tire 2 | 0.4555 | 0.4813 | 0.7144 | 0.4555 | 0.76 bps |
| DDOS Passive T2 | 0.4986 | 0.7449 | 0.8985 | 0.4986 | 0.43 bps |

## 5. Conclusion and Recommendations

Software-defined Networks (SDN) is heavily used in combination with AI & Deep Learning. This article integrates SDN-driven DL techniques for an intelligent network to improve security and solve problems in SDN networks specially the threat mitigation due hackers attack on netwok. SDN is regarded as the right option since it helps restructure networks and operate IoT platforms with the help of different data and control planes. Many in the field wish to explore how mobile applications of IOT networks can best be protected and optimized by routing and intrusion detection in critical IoT infrastructure. They are more likely to experience various attacks due to their nature of how they function. Many forms of attacks can be expected for these kinds of threats. These IOTS encounter a major issue in being adopted by many people. The main issues facing the network are its power usage and the weaknesses in its security. With the help of the routing system, developers keep the network running and safe from both energy exhaustion and security dangers. Implementing machine learning-based calculations allowed for a solution that improved secure routing with SDN. By applying the suggested method of clustering with the greatest possible values, it is possible to perform process identification of trusted nodes using indirect trust, direct trust and recent trust. Node intrusion detection is carried out by a set of limits or boundaries. Many hops are needed for the data to reach the CHs that direct it to the drain. Deciding on the routing protocol to be used for MANET is determined by the procedure chosen for optimization. As a result of this approach, the method speeds up its running process. Everything else is put aside in the deep learning hybrid system, as storage productivity comes first. It achieved an 80% detection, a 0.99% ideal throughput and packet delivery of 0.89%, consumed 0.11mJoules, ran at 0.84 bps and had a negligible delay of 0.3415 ms when tested with 30 nodes. Analysts should consider surfacing various security threats for the future system to encounter in stability and stress tests.



## References

Saiyed, A. (2025). AI-Driven Innovations in Fintech: Applications, Challenges, and Future Trends. International Journal of Electrical and Computer Engineering Research, 5(1), 8-15.

Olutimehin, A. T. (2025). Advancing cloud security in digital finance: AI-driven threat detection, cryptographic solutions, and privacy challenges. Cryptographic Solutions, and Privacy Challenges (February 13, 2025).

Gao, J., Wang, H., & Shen, H. (2020). Task failure prediction in cloud data centers using deep learning. IEEE Transactions on Services Computing, 1111–1116. https://doi.org/10.1109/BigData47090.2019.9006011 ...

Jindal, A., Aujla, G. S., & Kumar, N. (2019). SURVIVOR: A blockchain-based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment. Computer Networks, 153, 36–48. Khoramshahi, M., & Billard, A. (2019). A dynamical system approach to task adaptation in physical human-Network interaction. Autonomous Networks, 43(4), 927–946.

Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024

Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023

M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.

Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018

Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (Al) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power loT Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.

H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.

S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

Fatima, M., Ali, A., Ahmad, M., Nisa, F. U., Khan, H., & Raheem, M. A. U. ENHANCING THE RESILIENCE OF IOT NETWORKS: STRATEGIES AND MEASURES FOR MITIGATING DDOS ATTACKS. Cont.& Math. Sci., Vol.-19, No.-10, 129-152, October 2024 https://jmcms.s3.amazonaws.com/wp-content/uploads/2024/10/10072102/jmcms-2410025-ENHANCING-THE-RESILIENCE-OF-IOT-NETWORKS-MF-HK.pdf

Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.

Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

Mustafa, M., Ali, M., Javed, M. A., Khan, H., Iqbal, M. W., & Ruk, S. A. (2024). Berries of Low-Cost Smart Irrigation Systems for Water Management an IoT Approach. Bulletin of Business and Economics (BBE), 13(3), 508-514.

Hassan, A., Khan, H., Ali, A., Sajid, A., Husain, M., Ali, M., ... & Fakhar, H. (2024). An Enhanced Lung Cancer Identification and Classification Based on Advanced Deep Learning and Convolutional Neural Network. Bulletin of Business and Economics (BBE), 13(2), 136-141.

Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.

Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, “An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning”, Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

Zaheer, M., Azeem, M. H., Afzal, Z., & Karim, H. (2024). Critical Evaluation of Data Privacy and Security Threats in Federated Learning: Issues and Challenges Related to Privacy and Security in IoT. Spectrum of Engineering Sciences, 2(5), 458-479.

Khan, H., Usman, R., Ahmed, B., Hashimi, U., Najam, Z., & Ahmad, S. (2019). Thermal-aware real-time task schedulabilty test for energy and power system optimization using homogeneous cache hierarchy of multi-core systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

Mumtaz, J., Rehman, A. U., Khan, H., Din, I. U., & Tariq, I. Security and Performance Comparison of Window and Linux: A Systematic Literature Review. Securing the Digital Realm, 272-280.

Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

Asghar, M. A., Aslam, A., Bakhet, S., Saleem, M. U., Ahmad, M., Gohar, A., & Khan, H. (2025). An Efficient Integration of Artificial Intelligence-based Mobile Robots in Critical Frames for the Internet of Medical Things (IoMTs) Using (ADP2S) and Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 160-183.

Khan, H., Ali, A., & Alshmrany, S. (2023). Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs. Computers, Materials & Continua, 75(1).

Ali, R., Khan, H., Arif, M. W., Tariq, M. I., Din, I. U., Afzal, A., & Khan, M. A. Authentication of User Data for Enhancing Privacy in Cloud Computing Using Security Algorithms. In Securing the Digital Realm (pp. 187-200). CRC Press.

Noor, H., Khan, H., Din, I. U., Tarq, M. I., Amin, M. N., & Fatima, M. (2025). 12 Virtual Memory Management. Securing the Digital Realm: Advances in Hardware and Software Security, Communication, and Forensics, 126.

Ayub, N., Iqbal, M. W., Saleem, M. U., Amin, M. N., Imran, O., & Khan, H. (2025). Efficient ML Technique for Brain Tumor Segmentation, and Detection, based on MRI Scans Using Convolutional Neural Networks (CNNs). Spectrum of Engineering Sciences, 3(3), 186-213.

Ali, I., Saleem, M. U., Khan, A. A., Naz, A., Nawaz, M., & Khan, H. (2025). An Enhanced Artificial Intelligence Generated Virtual Influencer Framework: Examining the Effects of Emotional Display on User Engagement based on Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 184-209.

Ayub, N., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). Forecasting Multi-Level Deep Learning Autoencoder Architecture (MDLAA) for Parametric Prediction based on Convolutional Neural Networks. Engineering, Technology & Applied Science Research, 15(2), 21279-21283.

Mumtaz, J., Rehman, A. U., Khan, H., Din, I. U., & Tariq, I. Security and Performance Comparison of Window and Linux: A Systematic Literature Review. Securing the Digital Realm, 272-280.

Sultan, H., Rahman, S. U., Munir, F., Ali, A., Younas, S., & Khan, H. (2025). Institutional dynamics, innovation, and environmental outcomes: a panel NARDL analysis of BRICS nations. Environment, Development and Sustainability, 1-43.

Hussain, M., Ahmed, H. A., Babar, M. Z., Ali, A., Shahzad, H. M., Rehman, S. U., ... & Alshahrani, A. M. (2025). An Enhanced Convolutional Neural Network (CNN) based P-EDR Mechanism for Diagnosis of Diabetic Retinopathy (DR) using Machine Learning. Engineering, Technology and Applied Science Research, 15(1), 19062-19067.

Yousaf, M., Khalid, F., Saleem, M. U., Din, M. U., Shahid, A. K., & Khan, H. (2025). A Deep Learning-Based Enhanced Sentiment Classification and Consistency Analysis of Queries and Results in Search Using Oracle Hybrid Feature Extraction. Spectrum of Engineering Sciences, 3(3), 99-121.

Jabeen, T., Mehmood, Y., Khan, H., Nasim, M. F., & Naqvi, S. A. A. (2025). Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), 143-161.

Hussain, S., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). An Enhanced Random Forest (ERF)-based Machine Learning Framework for Resampling, Prediction, and Classification of Mobile Applications using Textual Features. Engineering, Technology & Applied Science Research, 15(1), 19776-19781.

Ahmad, I., Nasim, F., Khawaja, M. F., Naqvi, S. A. A., & Khan, H. (2025). Enhancing IoT Security and Services based on Generative Artificial Intelligence Techniques: A Systematic Analysis based on Emerging Threats, Challenges and future Directions. Spectrum of engineering sciences, 3(2), 1-25.

Khan, A. K., Bakhet, S., Javed, A., Rizwan, S. M., & Khan, H. (2025). Framework for Predicting Customer Sentiment Aware Queries and Results in Search Using Oracle and Machine Learning. Spectrum of Engineering Sciences, 3(2), 588-617.

Khawar, M. W., Salman, W., Shaheen, S., Shakil, A., Iftikhar, F., & Faisal, K. M. I. (2024). Investigating the most effective AI/ML-based strategies for predictive network maintenance to minimize downtime and enhance service reliability. Spectrum of Engineering Sciences, 2(4), 115-132.

Ahmad, J., Salman, W., Amin, M., Ali, Z., & Shokat, S. (2024). A Survey on Enhanced Approaches for Cyber Security Challenges Based on Deep Fake Technology in Computing Networks. Spectrum of Engineering Sciences, 2(4), 133-149.

Khan, H., Imtiaz, M. A., Siddique, H., Rana, M. T. A., Ali, A., Baig, M. Z., ... & Alsaawy, Y. (2025). An Enhanced Task Migration Technique Based on Convolutional Neural Network in Machine Learning Framework.

Fawy, K. F., Rodriguez-Ortiz, G., Ali, A., Jadeja, Y., Khan, H., Pathak, P. K., ... & Rahman, J. U. (2025). Catalytic exploration metallic and nonmetallic nano-catalysts, properties, role in photoelectrochemistry for sustainable applications. Reviews in Inorganic Chemistry, (0).

Liaqat, M. S., Sharif, N., Ali, A., Khan, H., Ahmed, H. N., & Khan, H. (2024). An Optimal Analysis of Cloud-based Secure Web Applications: A Systematic Exploration based on Emerging Threats, Pitfalls and Countermeasures. Spectrum of engineering sciences, 2(5), 427-457.

Abdullah, M. M., Khan, H., Farhan, M., & Khadim, F. (2024). An Advance Machine Learning (ML) Approaches for Anomaly Detection based on Network Traffic. Spectrum of engineering sciences, 2(3), 502-527.

Hashmi, U., & ZeeshanNajam, S. A. (2023). Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

SU J W, VASCONCELLOS D V, PRASAD S, et al. 2018 Lightweight classification of IoT malware based on image recognition[C]//HIRONORI K. 2018 IEEE 42nd annual computer software and applications conference(COMPSAC). Piscataway: IEEE, 664–9.

Mohurle S, Patil M. A brief study of wannacry threat: ransomware attack 2017. Int J Adv Res Comput Sci. 2017;8(5):1938–40.

Shaukat K, Rubab A, Shehzadi I, et al. A socio-technological analysis of cyber crime and cyber security in Pakistan. Transylv Rev. 2017;1:84.

Shaukat K, Alam T M, Hameed I A, et al. A review on security challenges in internet of things (IoT)[C]//2021 26th international conference on automation and computing (ICAC). IEEE, 2021: 1–6.