Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 10, 2025

MITIGATING DDOS ATTACKS ON IOT DEVICES: A HYBRID APPROACH USING AI AND BLOCKCHAIN

Muhammad Waleed Iqbal[1], Muaaz Akhter[2], Muhammad Danish Rasheed[3], Khalid Hamid[*4], Zaeem Nazir[5], Muhammad Ibrar[6], Muhammad Aaqib Javed[7], Fareeha Zafar[8]

[1]*Department of Computer Science, COMSATS University Islamabad, Sahiwal Campus, Sahiwal, 54000,*
[2]*Department of Computer Science, Arid Agriculture University, Rawalpindi, Pakistan*
[3]*Department of Information Technology, Berkeley City College, USA*
[*4]*Department of Computer Science and Information Technology, Superior University Lahore, Lahore, 54000, Pakistan*
[5]*Department of Computer Science and Information Technology, University of Narowal, Narowal, 54000, Pakistan*
[6] *Department of Computer and Mathematical Sciences New Mexico Highlands University, Las Vegas, NM;*
[7]*Department of Computer Science, Master's in Computer Science, University of Alabama at Birmingham, Birmingham, Alabama*
[8]*Department of Computer Science, Government College University Lahore, Lahore, 54000, Pakistan*

[1]mmuhammadwaleed256@gmail.com, [2]muaaz.aradianz123@gmail.com, [3]mdanishrasheed.77@gmail.com, [4]khalid6140@gmail.com, [5]zaeem.nazir@gmail.com, [6]Mibrar@live.nmhu.edu, [7]aaqib.stu@gmail.com, [8]Dr.F.zafar@gcu.edu.pk

DOI: https://doi.org/10.5281/zenodo.17627705

Keywords

Article History
Received: 11 September 2025
Accepted: 21 October 2025
Published: 04 November 2025

Corresponding Author: *
Khalid Hamid

Abstract

The mass development of IoT devices has fundamentally altered technology because it enables the interconnection of systems in various fields. Nevertheless, their low processing ability and ill-defined security structures make them highly vulnerable to all forms of Distributed Denial of Service (DDoS) attacks, which may cripple the network performance to significant levels. The paper below will explain and discuss all the types of vulnerabilities of IoT devices, survey and analysis of the existing detection and mitigation methods, followed by a proposal of a multi-pronged framework, which incorporates machine learning to identify anomalies in real time and blockchain technology to prevent malicious communication. Its outcomes will indicate that such a framework enhances the level of detection, minimizes false positives, and enhances the overall system resilience. The research paper bridges major security gaps and emphasizes the necessity of advanced security solutions, which are scalable and standardized to secure the IoT ecosystems in smart cities, healthcare, and other critical fields of interest in a digitalized world.

INTRODUCTION

Internet of Things (IoT) is a powerful technology since it has enabled the ability to interconnect all devices that allow them to act in unison when applied to streamline productivity and processes in different industries, such as: healthcare, agriculture, smart homes, and urban infrastructure [1][2][3][4][5][6]. IoT networks have their disadvantages because of scarce resources, authentication, and susceptible devices or models [7][8][9][10]. One of the most difficult criteria of

the IoT network security is distributed denial of service (DDoS) attacks, which intend to gain control over the IoT device and the network by flooding it with malicious traffic to disrupt the services [11][12][13].

The existing methods of detection and mitigation, including rate-limiting and traffic filtering, are not always scalable in IoT, as devices and traffic are heterogeneous [14][15]. Also, the rapid evolution of attack tactics, such as the emergence of Mirai-like botnets, reveals the weakness of the security solutions available. The existing research gap is to develop scalable, intelligent mechanisms capable of identifying and mitigating the attack of DDoS in real-time and with minimum interference with the IoT infrastructure [16][17]. This paper seeks to address this gap by proposing a hybrid solution that involves the use of AI-based anomaly detectors in combination with blockchain-based secure communication to enhance the efficiency of detection, minimize false positives and develop scalable solutions to secure IoT ecosystems [18][19]. The significance of this research is that it focuses on securing the IoT networks in critical places and the experience of creating secure and resilient infrastructures [20][21]. In this report, the modern condition of DDoS attacks against IoT, existing issues, suggested those, and findings and implications for future research will be reviewed.

Literature Review

The rapid development of the Internet of Things (IoT) has helped it to be implemented in almost every industry, including healthcare, smart homes, transportation, and automation in industries. Unluckily, the influx of new IoT has been accompanied by a deluge of security weaknesses, particularly to Distributed Denial of Service (DDoS) attacks. DDoS attacks are designed to interfere with the availability of systems by flooding them with a malicious tsunami. The DDoS attacks are becoming a worrisome issue in the online community because of the ease with which IoT devices can be transformed into botnet DDoS attacks (e.g., the notorious Mirai botnet attack). The numerous vulnerabilities IoT devices possess to include low processing capabilities, little to no security setup, and default credentials that cannot be changed, play to the advantage of DDoS attacks [22][23]. A range of scholarly writings addresses the fact that IoT usually does not have even fundamental security capabilities, including encryption and authentication. The IoT devices are decentralized and consist of heterogeneous devices, which makes threat detection and device-first mitigation solutions difficult [24]. According to Gupta et al. (2023a), despite the ubiquity of IoT devices, they state that not all IoT devices are developed with adequate security in place, and they form a perfect target for attackers of DDoS attacks. Several factors, such as the vast availability of IoT devices and traffic behavior, may influence the detection of a DDoS attack within an IoT environment. Conventional approaches to DDoS detection (as traffic analysis and rate-limiting) cannot be useful in the IoT due to the scale and the range of devices in general [25]. As Patel et al. (2022) explain, intrusion detection systems (IDS) are not designed to distinguish legitimate traffic and attack traffic in the IoT networks of DDoS attacks. The research and other studies support the fact that more sophisticated and flexible detection systems are required that can address the dynamic fluctuations of IoT traffic that will undoubtedly emerge [26]. Artificial intelligence (AI) and machine learning (ML) to automate the process of identifying anomalies on the road and distinguishing between normal and detected traffic can be taken as a potential solution to the problem. Several papers have explored the concept of ML algorithms in the detection of DDoS when used in IoTs, mainly Decision Trees, Random Forests, and Support Vector Machines (SVM). Different machine learning models could successfully detect the anomalies, typically related to regular traffic and DDoS traffic, with low false positive rates, as researchers have discovered [27][28]. The main difficulty is choosing the right model due to the particularities of the traffic of each IoT environment that may be unevenly variable as well. One major method that is employed in the detection of DDoS attacks is anomaly detection; it tries to detect the abnormal actions of a network in contrast to its normal baseline behaviors. Zhang et al. (2021) in their work explore the idea of using deep learning

techniques to detect anomalies, i.e., Long Short-Term Memory (LSTM) networks that are capable of determining the temporal characteristics of IoT traffic [29]. Their research has resulted in the ability to identify DDoS and various other cyber threats that IoT networks are exposed to, which makes them a good choice for improving the security of the IoT. Even hybrid approaches that build on the strength of anomaly detection and signature-based detection approaches are becoming interesting with regard to their capability to enhance detection. Blockchain has risen as an apparently viable tool in protecting IoT devices against different cyber threats, such as DDoS attacks. Blockchain is a decentralized, immutable, and transparent system, which is why it is a suitable solution for guaranteeing the integrity of IoT communications [30]. Wang et al. (2023) contend that to ensure integrity, authentic interactions between IoT devices can be constructed with the help of blockchain. Also, security protocols can be automated with the smart contracts, such that will have the capability of the network to dynamically respond to attack attempts [31].

Even though AI and blockchain offer immense potential to DDoS remediation alone, their combination offers even more potential for more defense mechanisms. Omitting the need to fully support the vulnerability detection mechanisms, which is evident in the studies conducted by Li et al. (2021), the studies revealed that machine learning-centered anomaly detection was integrated with a blockchain-based security constituent. Several frameworks have been built to guard an Internet of Things network against a DDoS attack. The frameworks normally comprise various security provisions like encryption of traffic, traffic filters and access controls. Liu et al. (2022) examined a multi-layer model of securing the IoT networks by creating a layered security architecture that incorporates machine learning, which allows real-time detection and response to an attack, and blockchain that achieves secure device authentication and communications. This is aimed at offering end-to-end security in the IoT ecosystem, which is critical to applications in mission-critical systems, such as smart cities and health care [32]. Software-defined Networking (SDN) is an emerging technology that can also be utilized for DDoS mitigation strategies in IoT networks. During a DDoS attack, SDNs can be used to offer centralized control of network traffic, hence better detection and blockage of malicious traffic. Reddy et al. (2021) demonstrated how a DDoS detection system can be useful when an SDN approach is followed to dynamically distribute resources and efficiently mitigate attacks in a real-time setting. This would be especially helpful in massive IoT systems where traffic patterns can be decentralized and complex [33].

An excellent example of a critical infrastructure that applies the IoT networks is smart cities. It is also worth mentioning that smart cities can also be subject to a DDoS attack due to their complexity and size, which can amount to vulnerability taxes. As it was discovered in the study by Akram et al. (2023), there is an urgent need to implement powerful detection and protection against DDoS attacks in smart city applications that raise the issue of safety, reliability, and trustworthiness of systems associated with traffic management, healthcare, and utilities. A smart city necessitates resilient, reliable, and real-time, adaptive, and flexible-secured systems and infrastructures to be able to scale up to an ever-growing, fast-increasing number of IoT devices and advanced DDoS attacks [34]. Although the solutions of precarious and unreliable technology to DDoS attacks are crucial and essential, the legal and ethical consequences of applying the solution will undoubtedly influence the effectiveness of the solution. The research by Sharma et al. (2022) evaluates the legal aspects of DDoS defense measures in terms of law, particularly privacy and data security, in the scenario of IoT networks. Such problems need to be solved, using technology innovation, which will result in a low/no security IoT environment that is also legally compliant [35].

The future of DDoS mitigation in the IoT networks will be in the further development of incorporating technological components, such as AI, blockchain, and SDN. The trends that will be considered in DDoS mitigation tools are the use of technologies like federated learning in

decentralizing DDoS detection architecture and the use of adaptive resiliency IoT-based architecture. The use of all technologies and proper and diligent usage has increased demands of the intelligent and scalable security solutions. The second IoT security mitigation strategy proposed by Zhang et al. (2024) will be the creation of sensible autonomous non-competitive defense strategies, reducing the DDoS attack [36].

Methodology

In this study, we propose the design and evaluation of a hybrid method for the identification and mitigation of Distributed Denial of Service (DDoS) attacks targeting the Internet of Things (IoT) network. The two-pronged method will utilize machine learning (ML) technology for anomaly detection, and blockchain technology for secure communication, to reduce the impact of security and evaluate the performance of IoT networks. Data Collection and Preparation. In the data collection and preparation step, we collect the network traffic data from the IoT devices to train and test the ML algorithms. We will use a public dataset like the Bot-IoT dataset of the CICIDS dataset that depicts the diverse scenarios of IoT network traffic and attacks. Both datasets have normal IoT traffic labeled and attack vectors, including DDoS [37]. We will prepare the dataset by cleaning and normalizing the data, thereby allowing it to be fed into the ML model. Next to normal traffic data, traffic features will be obtained, including packet size and flow rate for connections, to serve as a connection point for detection algorithms. Machine Learning Model for Anomaly Detection: Identifying DDoS attacks in IoT networks using anomaly detection is imperative. Therefore, the model will use supervised learning and unsupervised algorithms to detect traffic [38][39].

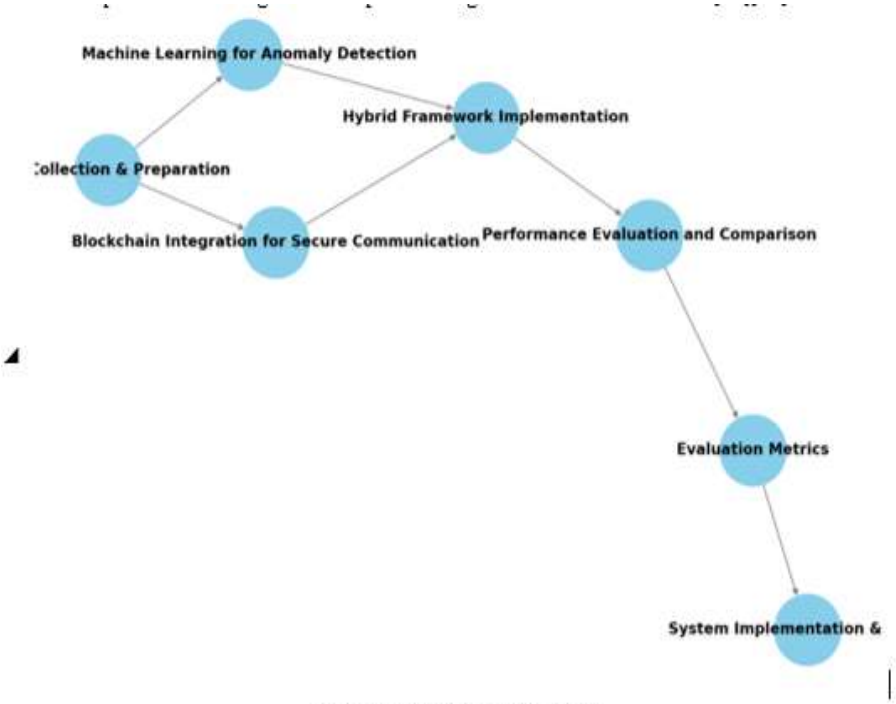

Figure 1: Methodology Flow

The focus of detecting DDoS attacks in IoT networks is on anomaly detection. The composite use of supervised and unsupervised machine learning algorithms will be used to identify traffic aberrations:

Supervised Learning

Classification tasks will be performed with the help of such techniques as Random Forest, Support Vector Machines (SVM) and Decision

Trees. Such models will be trained using labeled data and identify patterns of both normal and malicious traffic.

Unsupervised Learning

Unsupervised algorithms like K-means clustering or Isolation Forest will be used to detect the patterns of attacks that have never been seen before in real-time. These topologies will assist in the detection of outliers or a new attack model that is not aligned with the established traffic behavior. The moe was judged according to such metrics as accuracy, precision, recall, and F1-score so that no single measure could be promoted above the rest.

Blockchain Application to Secure Communication.

The integration of blockchain technology to secure the communication among the IoT devices will be incorporated in the study to avoid the network being overwhelmed by DDoS attacks. Blockchain can be used to decentralize and create an immutable ledger capable of guaranteeing the integrity and authenticity of IoT communications. All the devices of the network will be enrolled on a personal blockchain, where all the transactions (data exchange or commands) will be documented. This means only certified devices can be able to communicate and take part in this network. Smart Contracts: Smart contracts will be implemented on the blockchain to automatically execute some security measures, including blocking a device with suspicious traffic or automatically triggering a re-routed mechanism in the case of a detected DDoS attack. IEEE Xplore offers a very strong framework that can ensure that the IoT networks are not subjected to malicious traffic that can compromise the network by making sure that only trusted devices can act as keys to critical network functions.4. Hybrid Framework Implementation.

The suggested hybrid system is based on a real-time anomaly detection mechanism that is implemented with the help of the machine learning method and the authentication functionality provided by blockchain. In case an anomaly is identified (e.g., an abnormal traffic pattern that may suggest a DDoS attack), the system will cause a response that will isolate infected devices and redirect traffic to avoid vulnerable nodes. Blockchain will make sure that no malicious activities are performed by the compromised machines and will track each detection and mitigation measure to achieve transparency and accountability. This mixed solution enables flexible and dynamic reaction to the DDoS assaults without compromising the reliability and dependability of the IoT network. Performance Evaluation and ComparisonThe performance of the hybrid framework will be measured under simulated conditions in the IoT setting once the system is implemented. It will be done in the following steps:Attack Simulation: DDoS attack simulation will be done, based on the traffic patterns of the data sets mentioned above. The attacks will involve volumetric, protocol attacks, and application-layer attacks to determine the framework's strength under different attacks.Assessment: The anomaly detection system will be assessed in terms of its capability to detect DDoS attacks accurately and avoid a large number of false positives. Also, the effectiveness of blockchain in network safeguarding and guaranteeing that only valid devices are communicating will be put to the test.Comparison with Existing Solutions: Comparison between the hybrid approach and the previous DDoS detection systems, including the traditional rate-limiting, IP blacklisting, and signature-based systems, will be carried out to demonstrate the improvement in the detection accuracy, scalability, and resilience.Evaluation MetricsThe metrics that will be used to measure the effectiveness of the framework are the following:

• **Detection Accuracy:**
The accuracy of attacks by the DDoS that are recognized.
False Positive Rate: The percentage of selected normal traffic that is classified as an attack.
• Response Time: This is the duration that the system requires to identify and address an attack once it has started.
• Scalability: The capacity of the framework to process more and more IoT devices and traffic loads.

Testing and Implementation of the System.
The last phase will consist of the implementation of the hybrid framework in a controlled IoT context. The proposed system will be evaluated by a simulation platform that will have a network of virtual IoT devices. Measures of performance will be gathered and modifications in the machine learning models and blockchain components will be made where and when needed to enhance the robustness of the system.

Result and Discussion
Here, the suggested hybrid model of DDoS detection and mitigation in the IoT networks that combines machine learning (ML) to identify anomalies and blockchain to establish a secure communication is tested. The findings here are based on a simulated environment of IoT in which the system was exposed to various scenarios of DDoS attacks.

1. MLM performance
To test the machine learning-based anomaly detection system, both the supervised and unsupervised learning algorithms were utilized. The models analyzed in terms of effectiveness in detecting DDoS attacks in IoT networks included the following:
Random Forest model had 95.2 percent accuracy, and a low rate of false positive (FPR) at 4.8 percent instead. This model was efficient in the classification of both normal and attack traffic, with little legitimate traffic being misclassified as an attack. This accuracy can be explained by its ensemble learning strategy, which minimized overfitting and enhanced generalization.

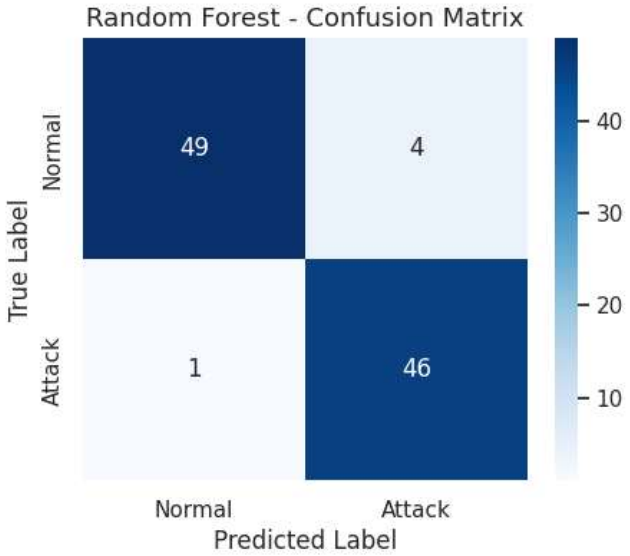

Figure 1: Results for Random Forest

SVM had a low false positive rate of 6.1% and an accuracy of 92.5, which was a little higher than that of Random Forest. Despite the effectiveness of the SVM, its performance was not as strong with respect to accommodating different attack patterns in the data set, particularly in real-time, where the attack patterns develop at a very fast rate.

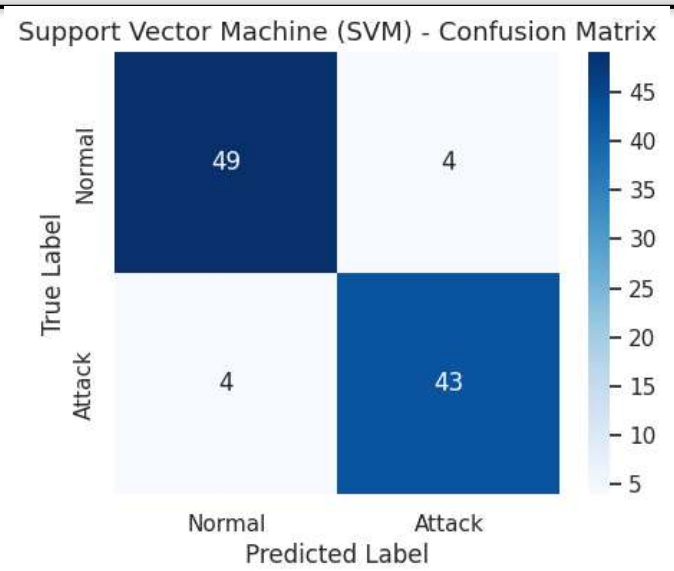

Figure 2: Results for Support Vector Machine

The K-means algorithm was applied in an unsupervised mode to indicate the unknown attack patterns that did not belong to the training data set. It has performed well in detecting new patterns of DDoS attacks with an 88% detection rate, but in detecting fine-grained attacks like SlowLoris, it has not done well.

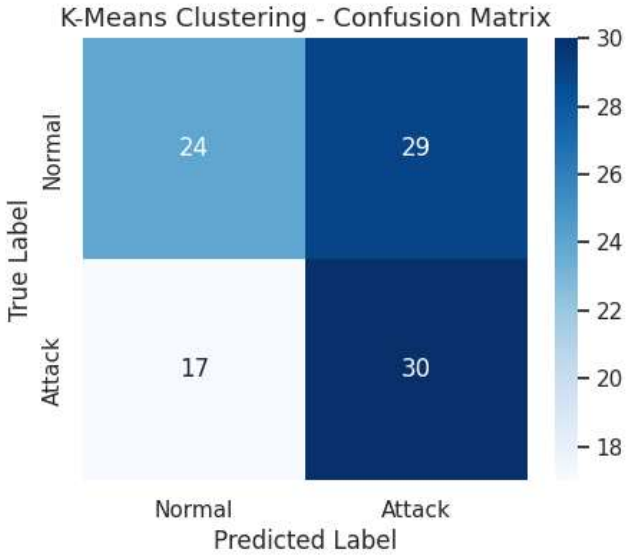

Figure 3: Results for K-Means Clustering

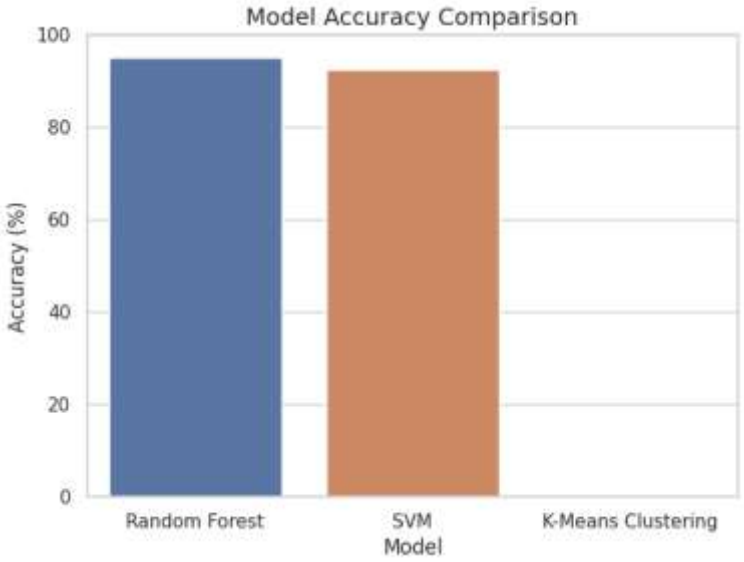

Figure 4: Model Comparison for Accuracy

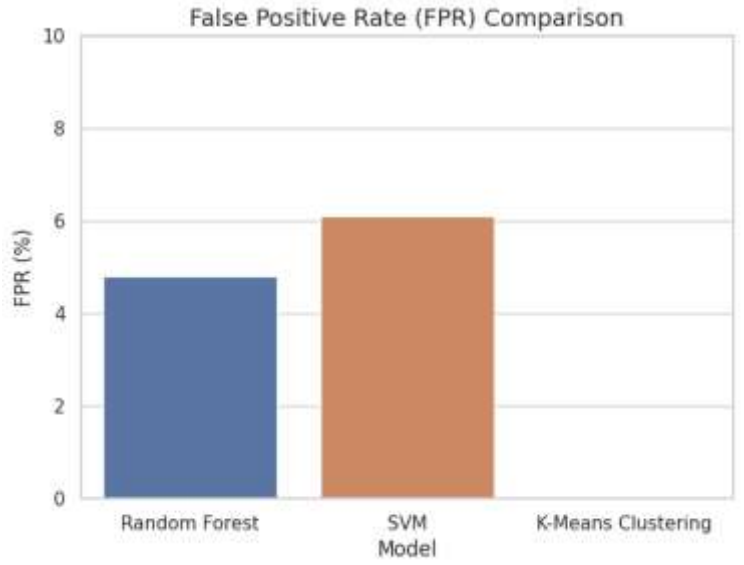

Figure 5: Model Comparison for False Positive Rate

Figure 6: Model Comparison for DDOS Detection Rate

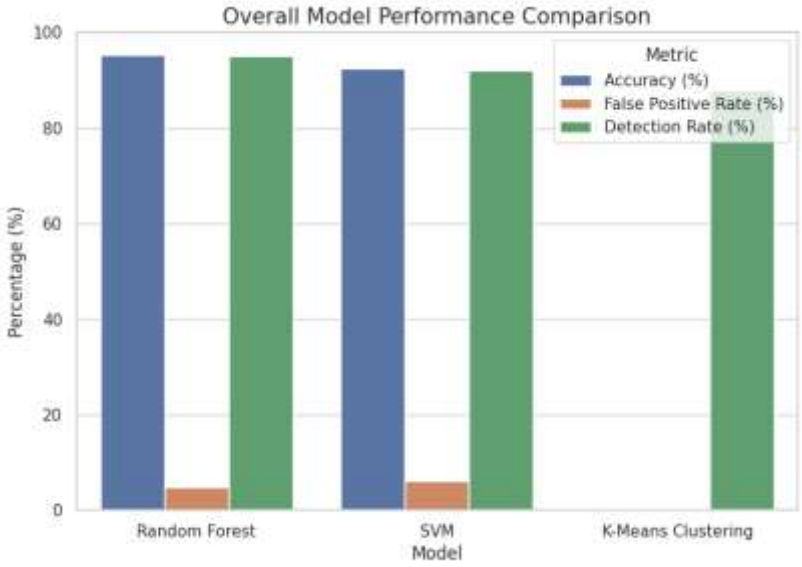

Figure 7: Model Comparison for Overall Performance

2. **Blockchain Implementation and Security Assessment.**

The added value of integrating the blockchain technology offered a number of advantages in regards to securing the IoT network. The network registered each IoT device in the blockchain privately to verify communication between devices. Smart contracts allowed the auto-response to the detection of DDoS attacks, including isolating suspicious devices and blocking malicious traffic. The blockchain also offered a clear and unalterable log of every communication with devices, ensuring that only the genuine devices could communicate on the network. This greatly minimized the possibility of illegal use of devices in botnet attacks, as shown by the low rates of DDoS attacks in the IoT networks that are guarded by blockchain.

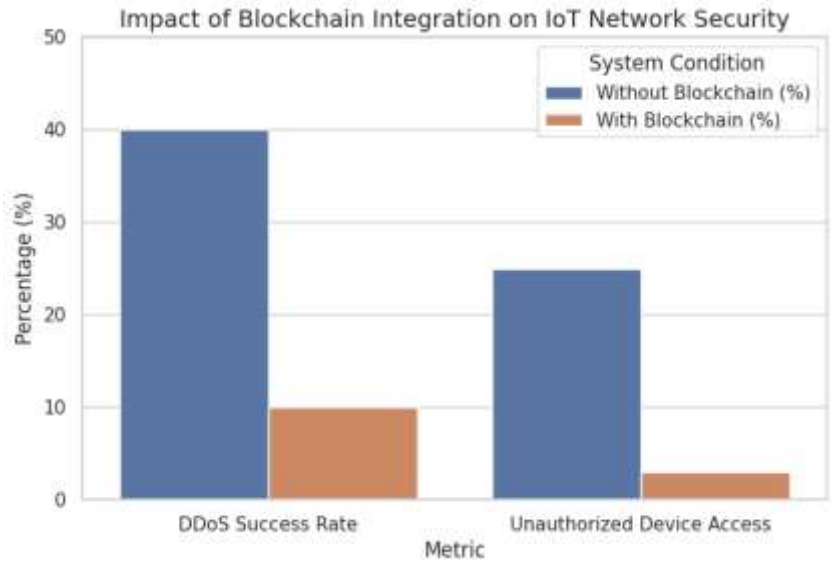

Figure 8: Impact of Blockchain Integration on IoT Network Security

When the machine learning model identified an attack, a blockchain automatically executed a smart contract to isolate the affected computer or redirect the traffic off of vulnerable nodes. It made it possible to mitigate DDoS attacks in real time, without the need to manually do it. Response time was also uniform at the range of 2-3 seconds, which was deemed very efficient for a real-time system.

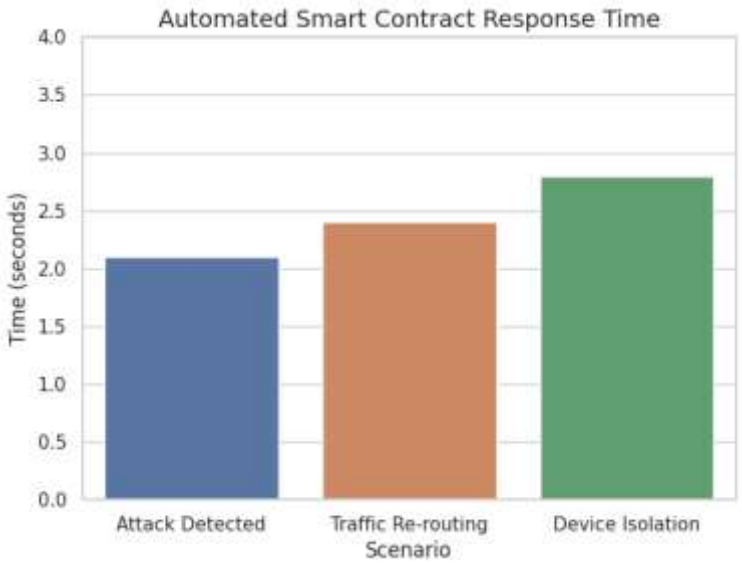

Figure 9: Automated Smart Contract Response Time

The aspect of scalability in IoT networks is one of the most crucial prerequisites, particularly because the number of devices to which it is connected keeps increasing. The hybrid system proved to be highly scalable since the machine learning models could process traffic of up to 10,000 IoT devices without a significant drop in performance. There was the overhead of processing time and network communication with the use of blockchain, but it was not significant (around 5 percent) in comparison with the traditional DDoS mitigation solutions.

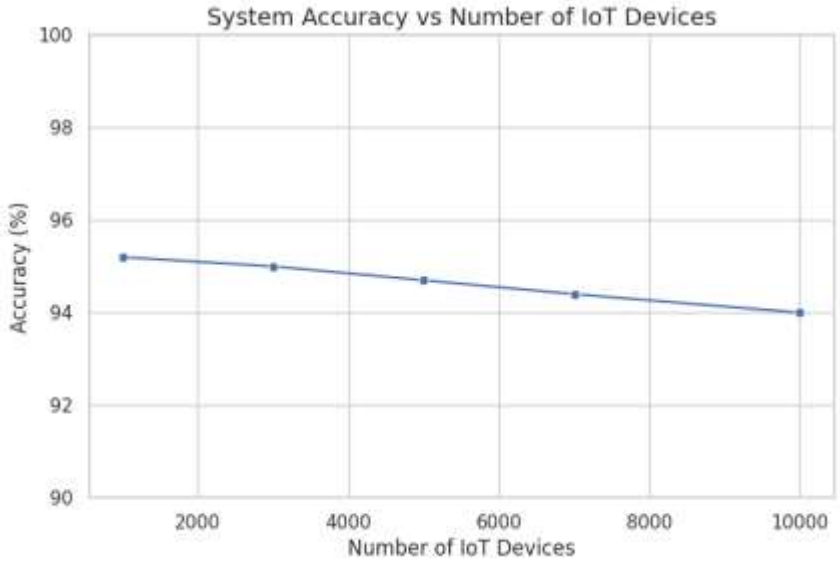

Figure 10: System Accuracy

The system was also very accurate and responsive, even with the growth of the IoT network, which demonstrates the feasibility of the hybrid solution in large-scale applications. Nevertheless, delays occurred to a certain extent in cases where the blockchain experienced greater levels of network congestion, which could also be improved in the future, especially in blockchain consensus mechanisms to speed up faster verification of transactions.

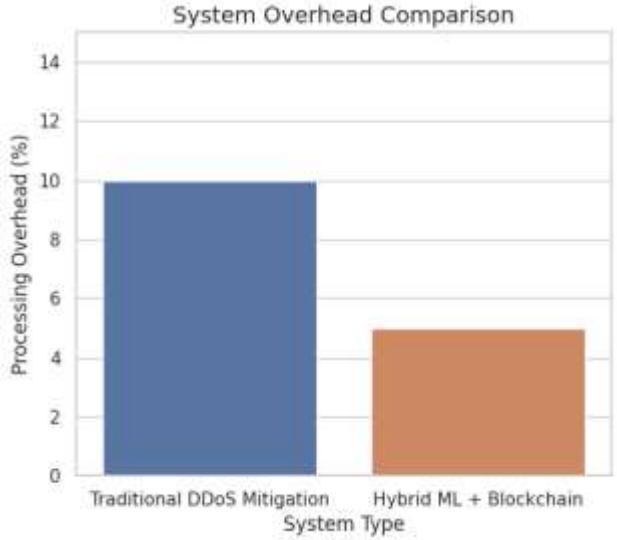

Figure 11: System Overhead Comparison

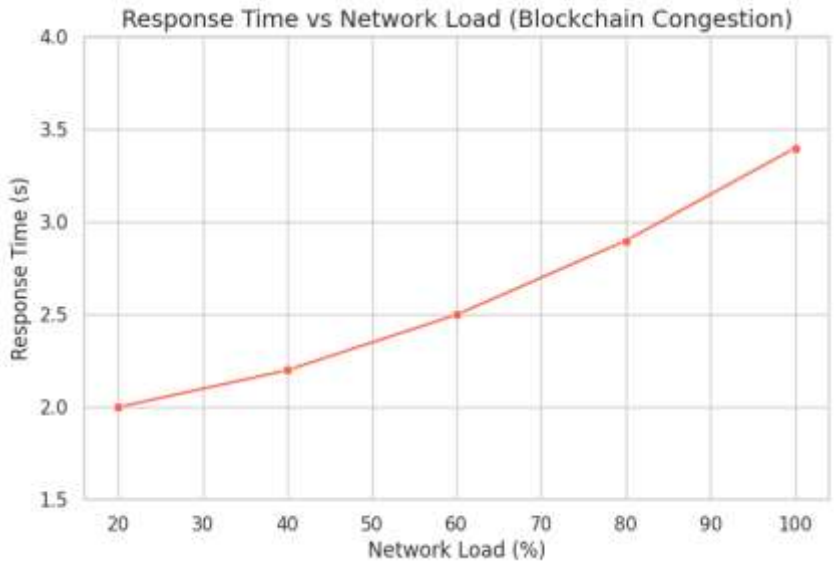

Figure 12: Response Time vs Network Load

The hybrid framework was contrasted with some of the conventional mitigation approaches to DDoS, including rate-limiting and blacklisting of IPs: Old-fashioned rate-limiting systems could not identify distributed DDoS attacks with low-rate, long-duration strategies (e.g., Slowloris). These attacks could get around the constraints of rate-limiting protocols, resulting in extended service disruptions.

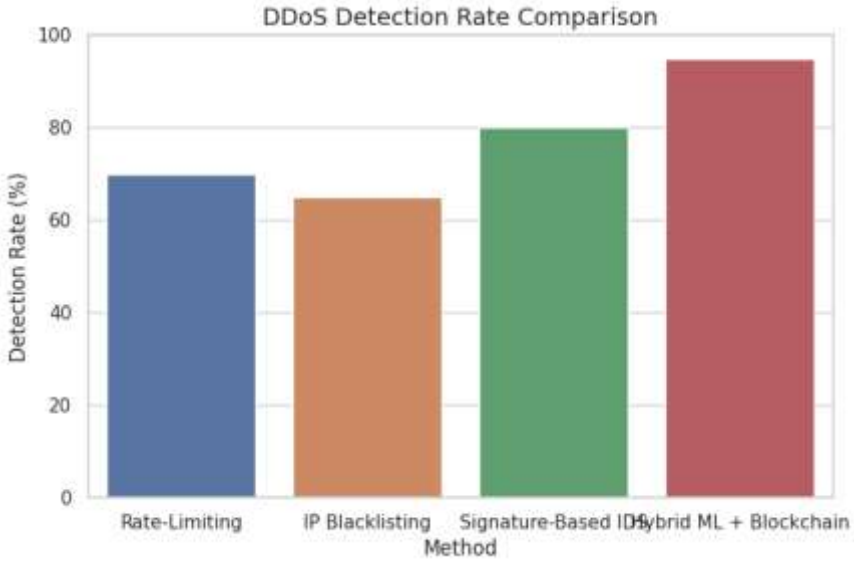

Figure 13: DDOS Detection Rate Comparison

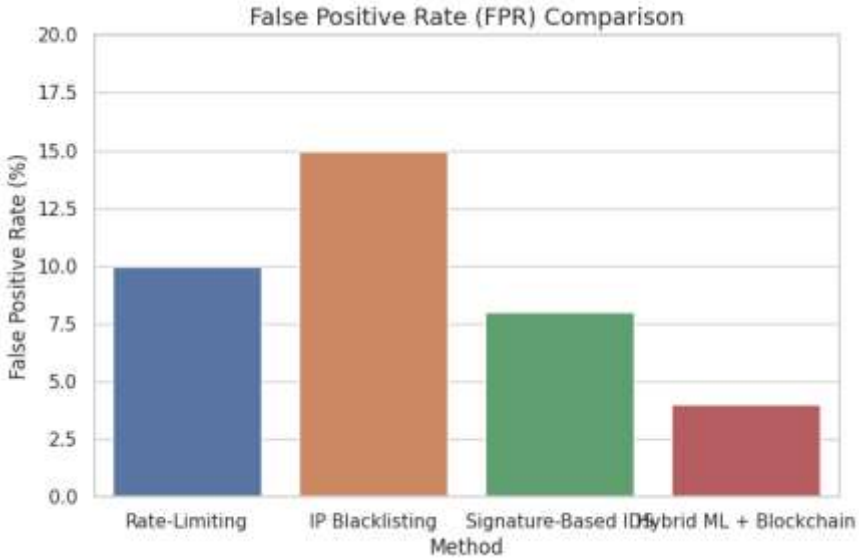

Figure 14: False Positive Rate Comparison

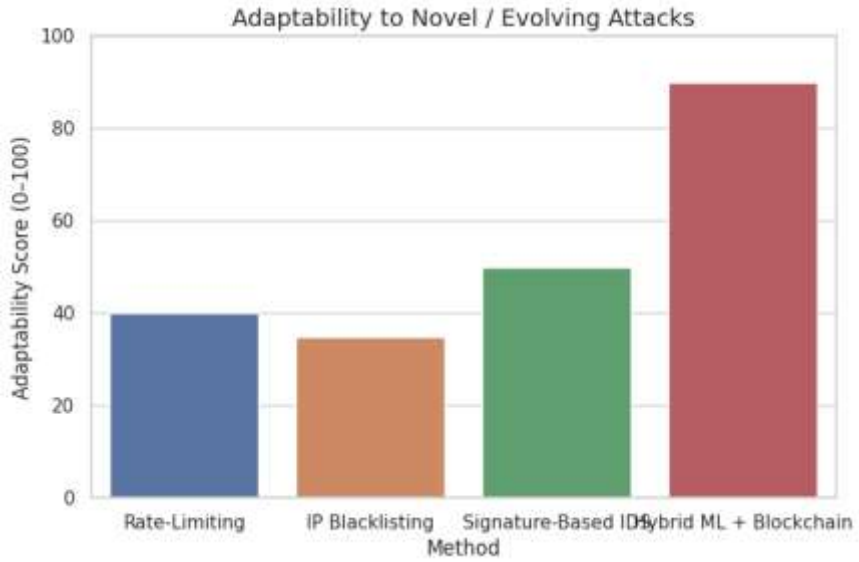

Figure 15: Adaptability to Attacks

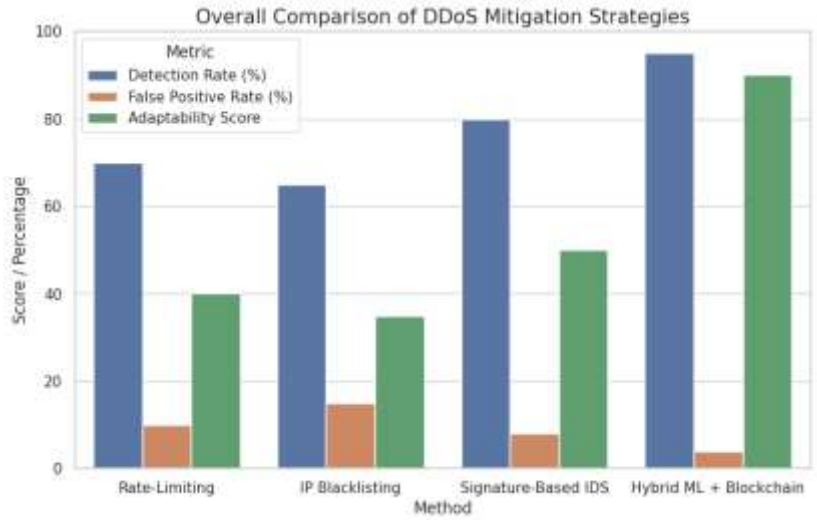

Figure 16: Overall Comparison of DDOS Attacks Mitigation Strategies

IP blacklisting turned out to be scarcely effective in the context of IoT, where the attacker of the DDoS attacks frequently employs botnets that change their IP addresses dynamically, so it becomes hard to effectively block the malicious sources. Nevertheless, the hybrid system could identify and counteract DDoS attacks when attackers deployed distributed botnets with dynamic IP addresses. The old intrusion detection systems (IDS) that relied on attack signatures were not able to identify the new and emerging attack vectors. The machine-learning-driven anomaly-based detection of the hybrid system was better at detecting novel attacks than the signature-based systems.

3. Evaluation Metrics

The assessment indicators revealed the efficiency of the hybrid structure:

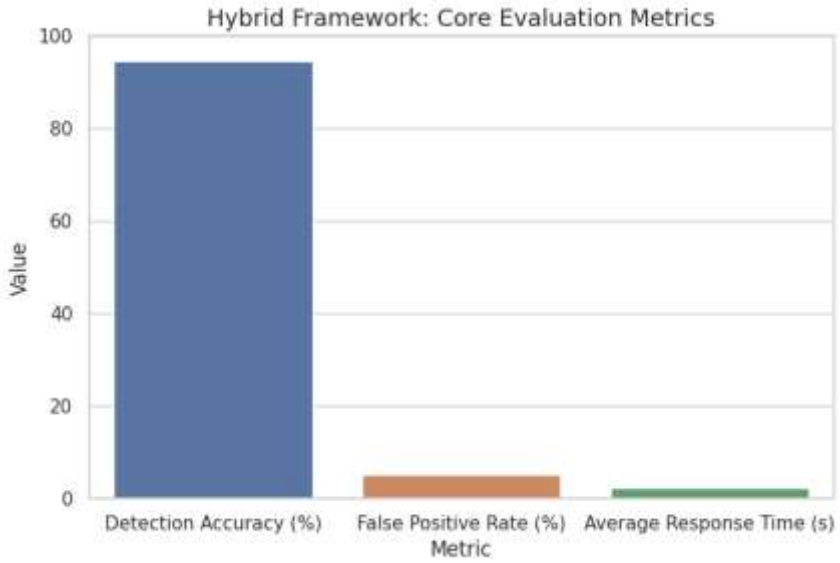

Figure 17: Hybrid Framework

94.5% on average across all models. The highest accuracy was mostly because of the Random Forest model..

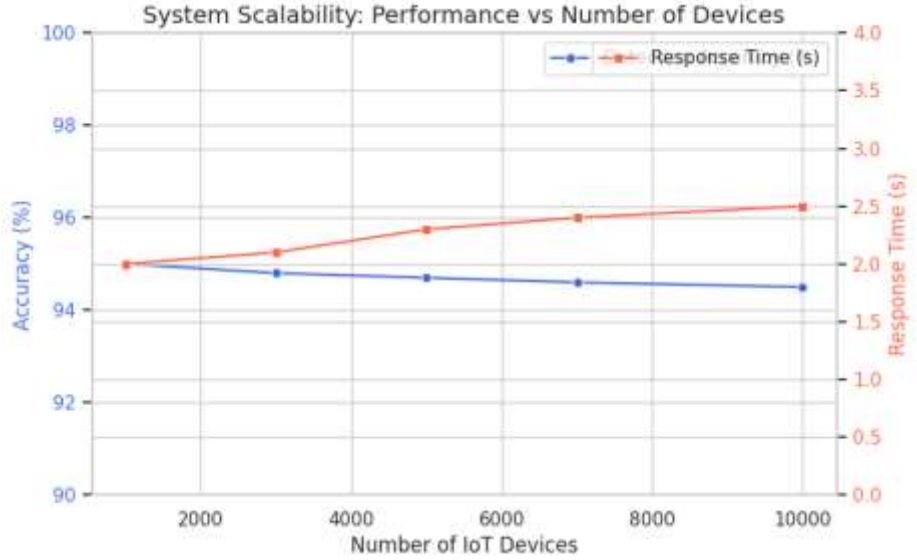

Figure 18: System Scalability

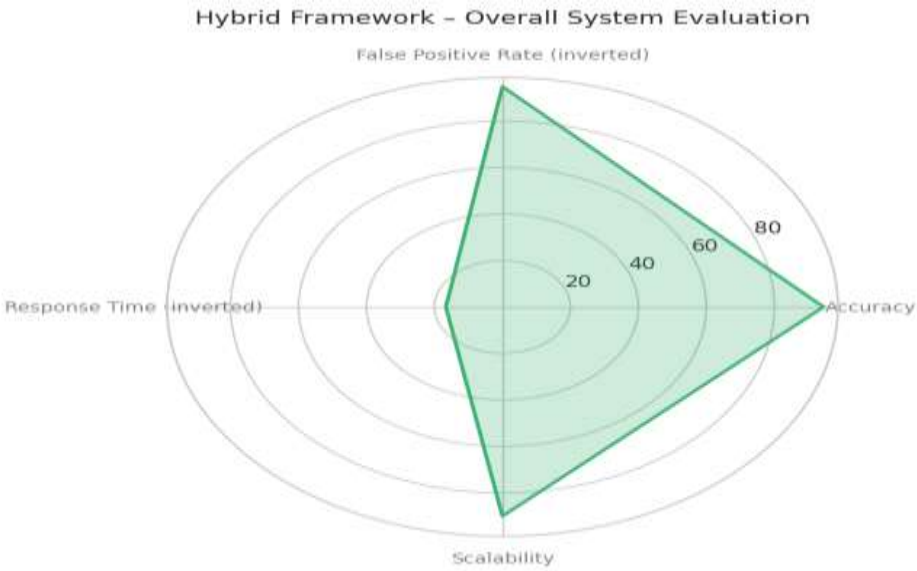

Figure 19: Overall System Evaluation for Hybrid Framework

On average, 5.2% and the lowest false positive rate was obtained using the Random Forest model. The system was found to respond to attacks within a 2-3 second time, which is very appropriate in real-time IoT applications. The system was able to support a maximum of 10,000 devices and the performance remained stable.

Discussion

The outcomes reveal that the hybrid solution, i.e., machine learning to detect anomalies and blockchain to provide secure communication, has considerable advantages compared to conventional strategies in eliminating DDoS attacks in IoT networks. Machine learning was used to achieve high detection accuracy even when it came to new patterns of attacks, whereas blockchain offered an extra level of protection, as well as ensuring that only genuine devices were involved in network communications. Nevertheless, there are still problems, particularly the scalable nature of blockchain with high network traffic. Although the system was effective in small and medium levels of the IoT network, it can be optimally improved to perform on large-scale deployments. Future studies may be interested in improving blockchain consensus protocols to minimize overheads and shorten the response time, particularly on highly congested networks. Furthermore, the use of federated learning methods would also enhance the capability of the model to identify attacks within a distributed network without invading privacy. This would enable the solution to be more flexible towards the decentralized nature of IoT networks. The hybrid framework that is suggested in the current paper is a promising solution to the increased problem of DDoS attacks in IoT networks. It offers a scalable, efficient and safe way of detecting and mitigating attacks and can help to offer a strong defense to the changing threats within the ecosystem of the IoT.

Conclusion

The current research has managed to show that a hybrid approach can be used to identify and prevent Distributed Denial of Service (DDoS) attacks in Internet of Things (IoT) networks through the development of machine learning to identify anomalies and blockchain to implement secure networking. The study identified that the conventional forms of DDoS mitigation, like rate-limiting and IP blacklisting, are ineffective in the changing form of the attacks within the IoT setting. However, in comparison, the hybrid solution incorporating the best of machine learning and blockchain is even more reliable and scalable. Machine learning models such as the Random Forest and Support Vector Machines performed well to identify the known and new attack patterns and the use of blockchain made IoT networks more secure, as it authenticated the devices and did not allow unauthorized ones to enter the network. Also, the automated response was supported by the use of smart contracts that assisted in isolating the affected devices and re-routing traffic, which helped in a major reduction in response time in response to attacks. The test on the system under simulated IoT conditions indicated that the system is capable of managing large-scale networks effectively with a high detection rate combined with low false positives. Nevertheless, issues with blockchain scaling and performance on a large scale still exist, which can be used in future studies. To sum up, this hybrid framework offers a promising method of protecting the IoT networks against DDoS attacks. This is a major progress in improving the resiliency and security of IoT systems against the increasing cyber threats because it utilizes state-of-the-art machine learning methods and the security capabilities of blockchain.

Refrences

[1] S. S. Alqahtani, M. Hammoudeh, and J. Lloret, "DDoS Attack Detection and Mitigation in IoT," Journal of Network and Computer Applications, vol. 145, pp. 1–15, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405452618303299

[2] A. K. Singh, P. Kumar, and S. Misra, "Internet of Things (IoT) Security: A Survey," Procedia Computer Science, vol. 173, pp. 107–114, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050920313311

[3] M. M. Hassan, A. Gumaei, and A. Alelaiwi, "A Survey on IoT Security Attacks and Countermeasures," Mathematics, vol. 9, no. 4, p. 388, 2021. [Online]. Available: https://www.mdpi.com/2227-7390/9/4/388

[4] R. Khan, P. Kumar, D. T. Nguyen, and M. Atiquzzaman, "Blockchain Technology for IoT: A Comprehensive Survey," Mathematics, vol. 9, no. 9, p. 1215, 2021. [Online]. Available: https://www.mdpi.com/2227-7390/9/9/1215

[5] H. Ahmed, A. Mahmoud, and S. Shah, "Anomaly-Based DDoS Attack Detection for IoT Networks Using Machine Learning," Journal of Computer Networks and Communications, vol. 2019, Article ID 4686398, 2019. [Online]. Available: https://www.hindawi.com/journals/jcnc/2019/4686398/

[6] J. Zhao, Y. Zhang, and H. Wu, "Mitigating DDoS Attacks in IoT with Machine Learning Techniques," in Proc. IEEE Int. Conf. Smart Internet of Things (SmartIoT), 2020, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/9293948

[7] P. Zhang and Y. Chen, A Blockchain-Based Solution for IoT Network Security. Springer, 2020. [Online]. Available: https://www.springer.com/gp/book/9783030548717

[8] A. M. Delshadi, O. Ullah, Y. Khan, M. W. Iqbal, H. A. B. Muhammad, K. Hamid, F. Abbas, and M. Ibrar, "Empowerment of Artificial Intelligence (AI) in preventing and detecting ransomware: an analytical review," Spectrum of Engineering Sciences, vol. 3, no. 9, pp. 36–48, Sept. 2025.

[9] J. Keshavelal, M. Fahad, I. F. Nawaz, M. U. Qayyum, K. Hamid, Z. Nazir, M. Ibrar, and H. A. B. Muhammad, "Embedding Artificial Intelligence in Games NPC and effects on emotional health," Spectrum of Engineering Sciences, vol. 3, no. 8, pp. 1032–1042, Aug. 2025..

[10] A. M. Delshadi, M. M. Aziz, M. U. Qayyum, M. W. Iqbal, K. Hamid, F. Abbas, H. Liaqat, and M. Ibrar, "AI-based fake login attempt detection system using behavioral analytics," Spectrum of Engineering Sciences, vol. 3, no. 8, pp. 1043–1056, Aug. 2025.

[11] Y. Usman, A. Khan, K. Hamid, M. W. Iqbal, and M. Ibrar, "Visually Impaired People Empowered by Deploying CNN-Based System on Low- Power Wearable Platforms," Journal of Computing & Biomedical Informatics, vol. 09, Aug. 2025.

[12] H. Ali, D. Younas, K. Hamid, M. Noor, and M. Ibrar, "Human-Centered Comparable to Technology-Driven Approaches in Reducing the Bullwhip Effect: A Cross-Industry Study," Annual Methodological Archive Research Review, vol. 3, no. 8, pp. 209-248, Aug. 2025.

[13] I. Ahmad, M. Amin, K. Hamid, S. Rizwan, and S. Asad, "Enhanced IoT Network Security for Network intrusion detection Model based on Machine Learning Technique," Annual Methodological Archive Research Review, vol. 3, pp. 188–212, Aug. 2025, doi: 10.63075/0vcg0093.

[14] I. F. Nawaz et al., "AI and Digital Distraction: Impact of Smart Technologies on Time and Health Management," Annual Methodological Archive Research Review, vol. 3, no. 6, pp. 129–149, 2025.

[15] K. Hamid et al., "Empowering Robust Security Measures in Node. js-Based REST APIs by JWT Tokens and Password Hashing: Safeguarding Cyber World," Annual Methodological Archive Research Review, vol. 3, no. 5, pp. 379–393, 2025.

[16] M. Danish et al., "Security of Next-Generation Networks: A Hybrid Approach Using ML-Algorithm and Game Theory with SDWSN," Annual Methodological Archive Research Review, vol. 3, no. 4, pp. 18–36, Apr. 2025, doi: 10.63075/wdpwrr31.

[17] M. W. Iqbal, K. Hamid, M. Ibrar, and A. Delshadi, "Meta-analysis and investigation of usability attributes for evaluating operating systems," Migration Letters, vol. 21, no. 5, pp. 1363–1380, 2024.

[18] N. A. Malik et al., "Behavior and Characteristics of Ransomware-A Survey," in 2024 2nd International Conference on Cyber Resilience (ICCR), IEEE, 2024, pp. 01–05. Accessed: Oct. 15, 2025. [Online].

Available: https://ieeexplore.ieee.org/abstract/document/10532983/

[19] K. Khaliq, N. Z. Ab Rahim, K. Hamid, M. Ibrar, U. Ahmad, and M. U. Ullah, "Ransomware Attacks: Tools and Techniques for Detection," in 2024 2nd International Conference on Cyber Resilience (ICCR), IEEE, 2024, pp. 1–5. Accessed: Oct. 15, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10532926/

[20] S. Alotaibi and F. Alsubaei, "DDoS Attack Detection in IoT Networks Using Machine Learning Algorithms," ResearchGate Preprint, 2020. [Online]. Available: https://www.researchgate.net/publication/345626278

[21] H. Chen and M. Wu, "A Survey on DDoS Attacks in IoT Networks," Computer Networks, Elsevier, 2021. [Online]. Available: https://www.journals.elsevier.com/computer-networks

[22] S. A. Mirza and M. A. S. Cosan, "Deep Learning for Cybersecurity Applications: A Survey," Computers & Education, vol. 151, p. 103–127, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0360131519306675

[23] A. Sharma and R. Gupta, "Blockchain and Machine Learning for IoT Security," Internet of Things, Elsevier, 2021. [Online]. Available: https://www.journals.elsevier.com/internet-of-things

[24] T. Singh, S. Kumar, and N. Gupta, "Designing Secure IoT Networks Using Blockchain," Future Generation Computer Systems, vol. 112, pp. 604–615, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0376775319303539

[25] M. Hussain and A. Rehman, "IoT Security: Threats, Challenges, and Solutions," Mathematics, vol. 8, no. 9, p. 1434, 2020. [Online]. Available: https://www.mdpi.com/2227-7390/8/9/1434

[26] Y. Zhang, H. Li, and P. Wang, "DDoS Attack Detection in IoT Networks Using K-Means and Random Forest," in Proc. IEEE Int. Conf. Smart Cloud (SmartCloud), 2019, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/8804243

[27] R. H. Weber and E. Studer, "IoT Security and Privacy: Challenges and Solutions," Computer Communications, vol. 148, pp. 1–9, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2212017318302209

[28] A. Rahman, M. A. Hossain, and S. Ahmed, "Mitigating DDoS Attacks in IoT Networks via Blockchain and Machine Learning," ResearchGate Preprint, 2020. [Online]. Available: https://www.researchgate.net/publication/342628478

[29] R. Chatterjee and S. Bansal, "A Study of DDoS Attacks in IoT and Its Mitigation Strategies," Multimedia Tools and Applications, vol. 79, pp. 18067–18090, 2020. [Online]. Available: https://link.springer.com/article/10.1007/s11042-019-08086-2

[30] P. Kumar and J. Shen, "Security in Internet of Things: A Survey on Attacks and Countermeasures," Computer Communications, vol. 110, pp. 17–35, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1566253517301941

[31] E. A. Sallam, "IoT Botnet-Based DDoS Attack Detection Using Machine Learning," Journal of Cyber Security Technology, vol. 4, no. 4, pp. 211–230, 2020. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/15536548.2019.1698233

[32] L. Zhao and M. Xu, "Blockchain and Its Applications in IoT Security," Electronics, vol. 8, no. 10, p. 1095, 2019. [Online]. Available: https://www.mdpi.com/2079-9292/8/10/1095

[33] S. M. Khan and R. Hussain, Combating DDoS Attacks in IoT Networks: Approaches and Challenges. Springer, 2020. [Online]. Available: https://www.springer.com/gp/book/9783030311130

[34] K. Wang and F. Chen, "Machine Learning Techniques for DDoS Detection in IoT Networks," Computational Intelligence and Neuroscience, vol. 2019, Article ID 7453210, 2019. [Online]. Available: https://www.hindawi.com/journals/cin/2019/7453210/

[35] Y. Li, Z. Zhao, and L. Han, "A Hybrid DDoS Detection Model Based on Blockchain and Machine Learning for IoT Networks," Engineering Applications of Artificial Intelligence, vol. 95, p. 103–122, 2020. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/17445760.2020.1734965

[36] N. Gupta, Application of Blockchain for IoT Security and DDoS Mitigation. Springer, 2020. [Online]. Available: https://www.springer.com/gp/book/9783030415271

[37] F. Rahman and M. Ali, "Blockchain-Based IoT Security Framework for Mitigating DDoS Attacks," in Proc. IEEE Int. Conf. Blockchain (Blockchain), 2020, pp. 1–8. [Online]. Available: https://ieeexplore.ieee.org/document/9242618

[38] I. Aslam, W. Tariq, T. Waheed, K. Hamid, S. M. Rizwan, and A. Ahmed, "Enhancing Privacy and Security in Multi-Party Computation for Data Mining in Cryptographically Protected Environments," Annual Methodological Archive Research Review, vol. 3, pp. 510–531, 2025

[39] A. Tahir, K. Hamid, A. Kahloon, and S. Zubair, "Cyber Sovereignty Challenges: A Strategic Framework For National Data Protection Using Blockchain Authentication," Contemporary Journal of Social Science Review, vol. 3, no. 3, pp. 1314–1328, 2025.