Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 3 (2023)

# Performance and security Evaluation of Ad Hoc Networking Technologies for IoT Environments

**[1]Neeraj Verma, [2]Pro. (Dr.) Awakash Mishra**

[1]Research Scholar, Department of Technology
Maharishi university of Information Technology, Lucknow , MUIT, Lucknow , Uttar Pradesh , India -226013
[2]Professor, Department of Computer Science Engineering, School of Engineering and Technology
Maharishi university of Information Technology, Noida
MUIT, Noida, G.B. Nagar, Uttar Pradesh, India -201304

E-mail-Id - [1]vermneeraj@gmail.com

*Co-author E-mail-Id - dean.research@muit.in

**Abstract:** A new age of unparalleled connectedness has been ushered in by the fast growth of Internet of Things (IoT) devices, allowing everything from smart homes and industrial automation to healthcare and agriculture. Ad hoc networking technologies play a pivotal role in facilitating communication among IoT devices, providing the flexibility and scalability required to support the diverse and dynamic IoT ecosystem. However, this connectivity comes with significant challenges related to both performance and security. This paper presents a comprehensive study focused on the performance and security evaluation of ad hoc networking technologies in the context of IoT environments. The need for enhancing security in ad hoc networking has seen a significant growth over the last decade. There are several security systems that prioritise the detection of assaults. Various machine learning mechanisms are taken into consideration for the purpose of identifying attacks. However, a significant concern associated with current research endeavours is to the constrained aspects of security and performance. There is still a need to improve the security of ad hoc networking. To accomplish this purpose, hybrid mechanisms have been devised. Advanced machine learning techniques are used to classify attacks such as man-in-the-middle attacks, denial of service attacks, and brute force attacks. In order to improve the precision of decisions and the categorization of assaults in ad hoc networks, the suggested research makes use of the Long Short-Term Memory (LSTM) model.

**Keywords:** Performance, security, Ad Hoc Networking, IoT Environments

## 1. Introduction

IoT is a game-changing concept that will eventually link together trillions of sensors and gadgets into one global network. IoT applications span a diverse array of domains, from smart cities and industrial automation to healthcare and agriculture. Central to the realization of this IoT vision are the networking technologies that enable devices to communicate with each other and with the broader internet. Among the various networking paradigms, ad hoc networking technologies have gained prominence for their ability to provide flexible and dynamic connectivity in IoT environments.

Ad hoc networking, characterized by decentralized, self-organizing networks, is well-suited to the dynamic and heterogeneous nature of IoT deployments. In this context, devices can autonomously establish connections, adapt to changing network conditions, and collaborate to exchange data, making ad hoc networking a cornerstone of IoT connectivity. However, harnessing the full potential of ad hoc networking technologies in IoT environments requires a deep understanding of their capabilities, challenges, and the intricacies of ensuring both performance and security.

This paper explores the role of ad hoc networking technologies within the context of IoT environments, shedding light on their significance and the unique challenges they address. We delve into the fundamental concepts that underpin IoT and ad hoc networking, emphasizing the convergence of these two domains. Our

objective is to provide a comprehensive overview of the intersection between ad hoc networking and IoT, highlighting the key considerations, opportunities, and research areas that define this exciting intersection.

### 1.1 IoT and Its Expanding Horizons:

IoT has evolved from a concept to a global phenomenon, encompassing an ever-expanding ecosystem of interconnected devices. These devices, ranging from sensors and actuators to smartphones and appliances, generate and consume vast amounts of data. The promise of IoT lies in its ability to leverage this data to drive efficiency, enhance decision-making, and create innovative services and applications.

### 1.2 The Role of Ad Hoc Networking in IoT:

Ad hoc networking technologies are instrumental in making IoT a reality. Unlike traditional network architectures, where devices rely on centralized infrastructure, ad hoc networks empower IoT devices to communicate directly with one another. They enable IoT deployments in remote and dynamic environments, where fixed infrastructure may be impractical or cost-prohibitive.

### 1.3 Challenges and Opportunities:

However, the marriage of ad hoc networking and IoT is not without its challenges. The dynamic nature of IoT environments, scalability concerns, energy constraints of IoT devices, and security considerations demand careful attention. Balancing performance, scalability, and security while optimizing resource utilization is a complex task.

In this study, we set out on a trip to investigate the varied ecosystem of ad hoc networking approaches for IoT settings. We delve into the architectural considerations, communication protocols, and security mechanisms that underpin this convergence. Furthermore, we examine real-world IoT use cases where ad hoc networking technologies play a pivotal role.

Our aim is to provide readers with a holistic understanding of the pivotal role that ad hoc networking technologies play in enabling the IoT revolution. We highlight the need for interdisciplinary collaboration, innovation, and research to address the evolving challenges and opportunities at the intersection of ad hoc networking and IoT, ultimately driving the continued growth and evolution of this transformative ecosystem.

### 1.4 Performance Evaluation:

The performance evaluation component of this study encompasses the following aspects:

1. **Throughput and Scalability:** We investigate the ability of ad hoc networking technologies to handle increasing number of IoT devices & resulting data traffic. Throughput and scalability are critical factors in ensuring uninterrupted data flow.
2. **Latency and Delay:** Low-latency communication is crucial for real-time IoT applications. We assess the latency and delay characteristics of different ad hoc networking solutions under varying network loads.
3. **Energy Efficiency:** IoT devices are often constrained by limited battery capacity. We examine the energy consumption of ad hoc networking protocols and their impact on device longevity.
4. **Quality of Service (QoS):** Many IoT applications require specific QoS guarantees. We analyze the ability of ad hoc networks to meet these requirements and maintain a high level of service quality.

### 1.5 Security Evaluation:

The security evaluation component of this study addresses the following security concerns in IoT ad hoc networks:

1. **Authentication and Access Control:** IoT devices are susceptible to unauthorized access. We assess the effectiveness of authentication and access control mechanisms in preventing unauthorized device entry.
2. **Data Confidentiality and Integrity:** Ensuring the confidentiality and integrity of IoT data is paramount. We evaluate encryption and data integrity solutions to protect sensitive information.

3. **Resilience to Attacks:** IoT networks are vulnerable to various attacks, including DoS and intrusion attempts. We analyze the resilience of ad hoc networking technologies against these threats.
4. **Trust and Privacy:** IoT devices often collect and transmit personal and sensitive data. We investigate the establishment of trust relationships and mechanisms for preserving user privacy.
5. **Key Management:** Effective key management is essential for securing communications in IoT ad hoc networks. We assess the key distribution and management strategies employed by different technologies.

## 2. Literature Review

We uncover various important studies and research articles that have added to our knowledge of this crucial junction of technology when doing a literature study on the performance and security assessment of ad hoc networking technologies in IoT contexts.

Protection Strategies for IoT Devices: A DL and ML Approaches Analysis (M. A. A.-Garadi et al., 2020). The widespread use of networked technologies has spawned fresh security worries. Possible future applications of ML/DL methods to IoT security are then examined, along with their pros and cons. The use of ML/DL to strengthen IoT security is examined, along with its benefits and drawbacks. These potential opportunities and roadblocks might spark new areas of investigation. [1] QIANG LIU et al.(2018) looked at the risks of data-driven machine learning and possible countermeasures. The urgency with which the potential dangers to ML and their solutions must be explored prompted this study. In detail research by D. J. Miller (2020) examined countermeasures to adversarial learning in DNN categorization. They also investigate potential privacy issues with regards to training data. Then, they demonstrate how effective different precautions are at preventing TTE, RE, and backdoor DP attacks on images by means of common industrial practises. Many new fields have benefited from the recent developments in ML, such as data analytics, autonomous systems, and security diagnostics. N. Papernot et al. (2018) looked at the state of privacy and security in ML to see where we are at the moment [3]. In 2019, Chaoyun Zhang and colleagues investigated the use of deep learning to mobile and wireless networks. [4]. With the hope of inspiring additional cross-disciplinary work, this essay gives a comprehensive analysis of the shared ground between DL and mobile and wireless networking. [5] In the period of adversarial ML, Adnan Qayyum et al. were interested in how to best protect connected and autonomous automobiles. This article takes a look at CAVs through the prism of adversarial ML attacks and suggests a method for protecting against them in different scenarios. AI was employed by Marwa Mamdouh et al. (2018) to safeguard IoT and wireless sensor networks. ML is increasingly being used as the foundation for security measures against threats to WSNs and the Internet of Things. Both the dangers facing the Internet of Things and WSN, & ML methods being employed to combat them, are discussed in this article.Junfeng Xie et al. (2019) [7] investigated the problems and obstacles encountered in studying and implementing machine learning strategies to SDN. They provide a comprehensive review of studies using SDNs and other forms of machine learning. They start out with a quick rundown of the canon and the works that belong in it. Time estimates for tasks in cloud-based workflows were reported by T. Pham et al. (2020) using a two-stage machine learning approach. To predict how long it would take to finish tasks in cloud-based workflows, we provide a novel two-stage machine learning approach. High-quality prediction is achieved by our method's usage of two iterations of prediction and parameters that account for runtime data. T. K. Rodrigues et al. explore edge and cloud computing at the crossroads of ML, computation, and communication control in their soon-to-be-published paper [9]. The purpose of this article is to shed light on the present status of research in MEC systems by providing a comprehensive introduction to the usage of ML in these systems. It was also pointed out which MEC issues may be addressed by ML solutions, which algorithms are now preferred in cutting-edge ML research, and so on, all of which was helpful information. The secret sharer was introduced by N. Carlini et al. (2018) [10] as a way to evaluate how likely it was that neural networks would remember and extract secrets unintentionally. Our research offers a method for assessing whether or not a generative sequence model, a common kind of ML model, would erroneously remember out-of-the-ordinary sequences from its training data. [11] Threats to ML for network security are examined by O. Ibitoye et al. (2019). Chinese learning models have improved the speed, accuracy, and efficiency of many decision-support systems. Potential benefits of DL for mobile and wireless networks were investigated by C. Zhang et al. (2019) in [12]. The authors of this paper [13] go further into the intersection of DL with wireless and mobile networking.

## 3. Problem Statement

Performing a comprehensive performance and security evaluation of ad hoc networking technologies in IoT environments involves addressing a range of critical issues. These issues are essential to ensure the efficiency, reliability, and security of IoT deployments. Here are some key issues that should be considered:

**Performance Evaluation Issues:**

1. Scalability: Assessing how ad hoc networking technologies scale as number of IoT devices in network grows. Understanding limits & trade-offs of scalability is crucial for large-scale IoT deployments.
2. Throughput and Bandwidth Management: Measuring the network's data transfer capacity and evaluating how different ad hoc networking protocols manage and optimize bandwidth utilization.
3. Latency and Delay: Analyzing communication delay and latency, especially in real-time IoT applications such as industrial automation and autonomous vehicles.
4. Energy Efficiency: Evaluating the energy consumption of ad hoc networking technologies, as IoT devices are often battery-powered and energy-efficient communication is critical for their longevity.
5. Quality of Service (QoS): Assessing the ability of ad hoc networks to meet QoS requirements for various IoT applications, such as healthcare monitoring or video surveillance.
6. Mobility Management: Examining how ad hoc networks handle mobility of IoT devices, including handovers, seamless connectivity, and routing adaptability.

**Security Evaluation Issues:**

1. Authentication and Access Control: Evaluating the effectiveness of authentication mechanisms in preventing unauthorized access to IoT devices and networks. Assessing access control policies and their enforcement.
2. Data Confidentiality and Integrity: Analyzing the encryption methods employed to protect data in transit and at rest. Ensuring data integrity and confidentiality, especially for sensitive IoT data.
3. Resilience to Attacks: In the context of Internet of Things deployments, determining how secure ad hoc networking solutions are against typical threats like denial of service, intrusion, and jamming.
4. Trust and Identity Management: Examining how trust relationships are established between IoT devices and evaluating identity management solutions for secure device authentication.
5. Key Management: Evaluating the key distribution and management mechanisms used in ad hoc networks to ensure secure and efficient cryptographic operations.
6. Privacy Preservation: Ensuring that user privacy is maintained by assessing mechanisms for anonymizing data and protecting personally identifiable information (PII).
7. Secure Firmware Updates: Investigating secure methods for updating IoT device firmware to patch vulnerabilities and enhance security without compromising the network.
8. Compliance and Standards: Ensuring that ad hoc networking technologies align with industry and regulatory standards for IoT security.
9. Attack Surface Assessment: Identifying the attack surface of IoT devices and ad hoc networking protocols to proactively address potential vulnerabilities.
10. Security Incident Response: Developing and evaluating strategies for detecting, mitigating, and responding to security incidents in IoT ad hoc networks.
11. End-to-End Security: Ensuring that security measures span the entire IoT ecosystem, from edge devices to cloud services, to prevent weak links in the security chain.
12. Secure Boot and Hardware-Based Security: Exploring hardware-based security solutions, including secure boot processes and trusted execution environments, to protect IoT devices from physical attacks.
13. Ethical Considerations: Addressing ethical issues related to data privacy, consent, and responsible IoT practices within the context of security evaluations.

A comprehensive performance and security evaluation of ad hoc networking technologies for IoT environments should encompass these issues to provide a thorough understanding of capabilities & limitations of these technologies and to ensure the robustness and security of IoT deployments.

## 4. Proposed Work

In recent years, there has been a growing need for enhanced security measures to be included in Ad Hoc Networking. Various security systems persist, with a major focus on the identification and detection of potential threats. Various machine learning algorithms are considered while endeavoring to identify assaults. However, a significant limitation of the existing work is in its restricted focus on security and performance considerations. Continued enhancements to the security of the Ad Hoc Networking remain imperative. The use of hybrid mechanisms is crucial to achieve this objective. In order to classify potential attacks such as man-in-middle attacks, DSN, & BF attacks, an advanced ML method is used. The proposed study makes use of LSTM model to improve judgement and speed up the categorization of Ad Hoc Networking attacks.

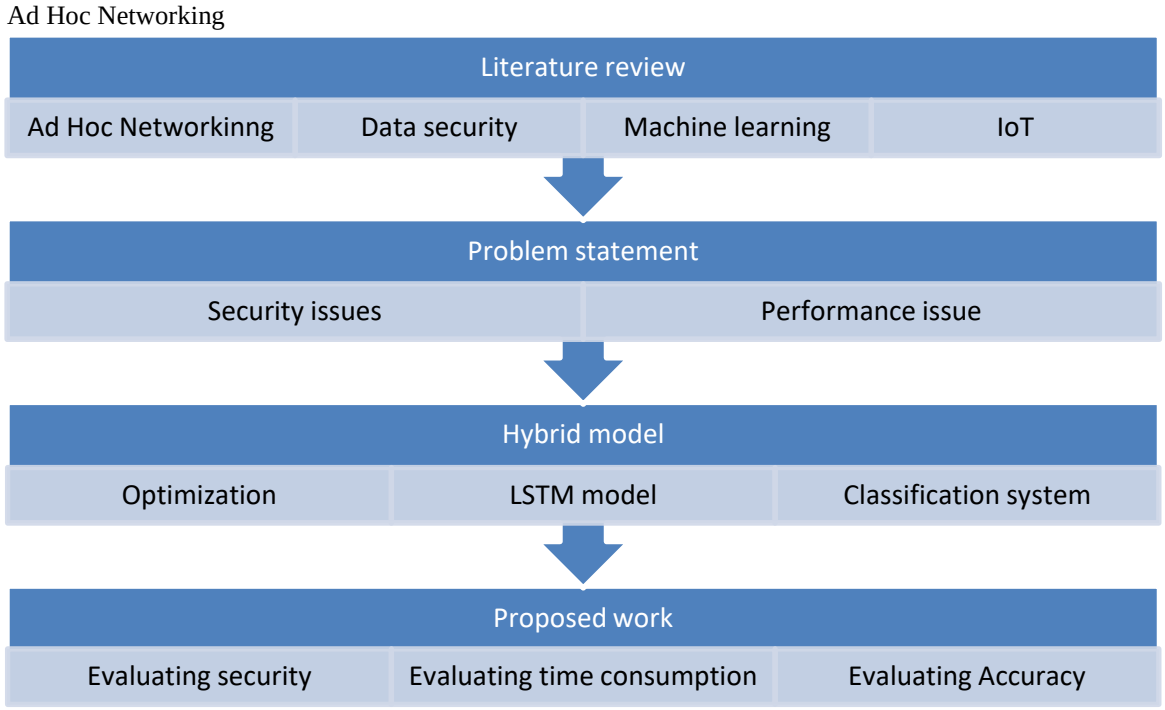


**Fig 4:** Process flow of proposed work

## 5. Result and Discussion

The proposed research makes use of a ML model to examine a dataset consisting of several trades. In this way, different forms of cyber dangers may be recognised and classified. Two different scenarios—one with the use of dataset filtering and the other without—have been simulated. Improved detection and classification performance is anticipated when an optimizer is used to filter the dataset. In Table 1, we can see the many configurations that were employed throughout the investigation.

**Table 1:** Configuration Parameter

| Parameters | Value |
|---|---|
| Number of epochs | 500 |
| Batch size | 16 |
| Optimizer | Adam |
| Classification model | LSTM |

### 5.1 Confusion matrix in case of conventional model

**Table 2:** Confusion matrix of conventional classification model

| | Denial-of-Service | Denial-of-Detection | Unfair use or resources |
|---|---|---|---|
| **Denial-of-Service** | 3419 | 109 | 142 |
| **Denial-of-Detection** | 132 | 3500 | 153 |
| **Unfair use or resources** | 149 | 91 | 3405 |

**Results**

TP: 10324

Overall Accuracy: 93.01%

Table 3 displays the derived accuracy metrics after applying accuracy, precision, recall, and F1-score to table 2.

**Table 3:** Accuracy of Confusion matrix of unfiltered dataset

| Class | n (truth) | n (classified) | Accuracy | Precision | Recall | F1 Score |
|---|---|---|---|---|---|---|
| 1 | 3700 | 3670 | 95.21% | 0.93 | 0.92 | 0.93 |
| 2 | 3700 | 3785 | 95.63% | 0.92 | 0.95 | 0.94 |
| 3 | 3700 | 3645 | 95.18% | 0.93 | 0.92 | 0.93 |

### 5.3.2 Confusion matrix of filtered dataset

The filtered dataset's Confusion matrix is considered in Table 4.

**Table 4:** Confusion matrix of filtered dataset

| | Denial-of-Service | Denial-of-Detection | Unfair use or resources |
|---|---|---|---|
| **Denial-of-Service** | 3447 | 117 | 113 |
| **Denial-of-Detection** | 98 | 4612 | 101 |
| **Unfair use or resources** | 32 | 31 | 2593 |

**Results**

TP: 10603

Overall Accuracy: 95.52%

Accuracy, precision, recall, and F1-score were applied to Table 4 to obtain accuracy metrics shown in Table 5.

**Table 5:** Accuracy of Confusion matrix of filtered dataset

| Class | n (truth) | n (classified) | Accuracy | Precision | Recall | F1 Score |
|---|---|---|---|---|---|---|
| 1 | 3700 | 3650 | 97.03% | 0.96 | 0.95 | 0.96 |
| 2 | 3700 | 3733 | 97.07% | 0.95 | 0.96 | 0.96 |
| 3 | 3700 | 3717 | 96.95% | 0.95 | 0.96 | 0.95 |

### 5.4 Comparative Analysis

In Table 6, we can see the outcomes of comparing the actual and expected output of Classes 1, 2, and 3. The proposed work has been verified to be correct when compared to the reference model.

**1. Accuracy**

**Table 6:** Comparison Analysis of Accuracy

| Class | Conventional model | Proposed model |
|---|---|---|
| **1** | 95.21% | 97.03% |
| **2** | 95.63% | 97.07% |
| **3** | 95.18% | 96.95% |

Using the information in table 6, we can evaluate how well the new model matches up to the gold standard in fig. 5.

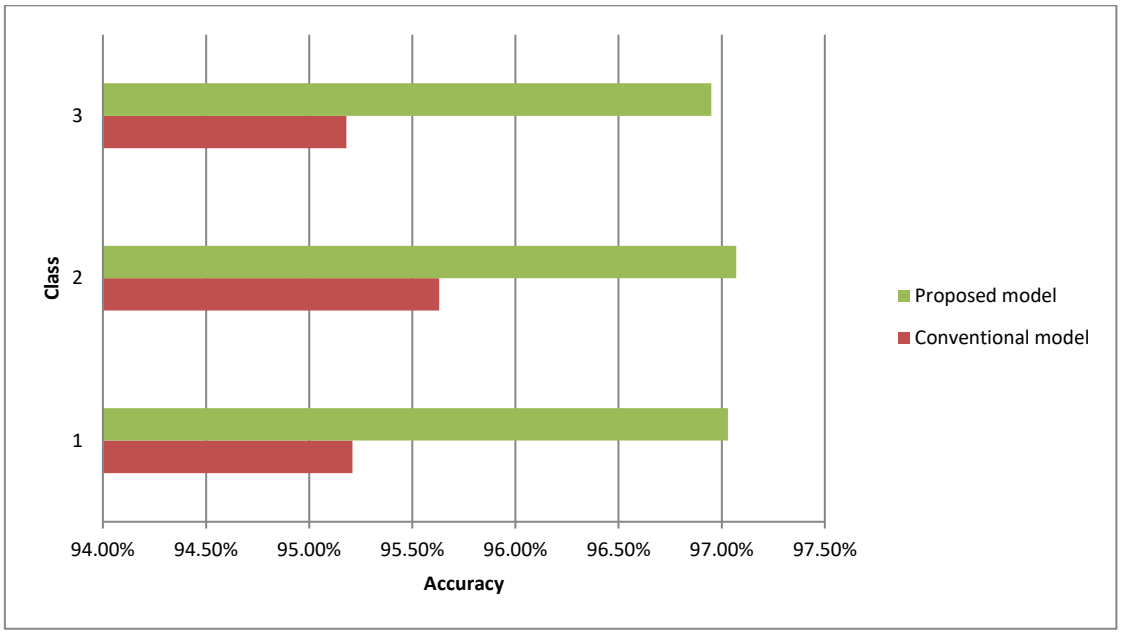


**Fig 5:** Comparison Analysis of Accuracy

Table 7 shows the results of a reliability analysis between completed and anticipated tasks for Grades 1-3. The proposed model has been shown to be more accurate than the current paradigm.

**2. Precision**

**Table 7:** Comparison Analysis of Precision

| Class | Conventional model | Proposed model |
|---|---|---|
| 1 | 0.93 | 0.96 |
| 2 | 0.92 | 0.95 |
| 3 | 0.93 | 0.95 |

Based on the results of table 7, we create figure 6 to demonstrate the suggested model's higher accuracy over the baseline model.

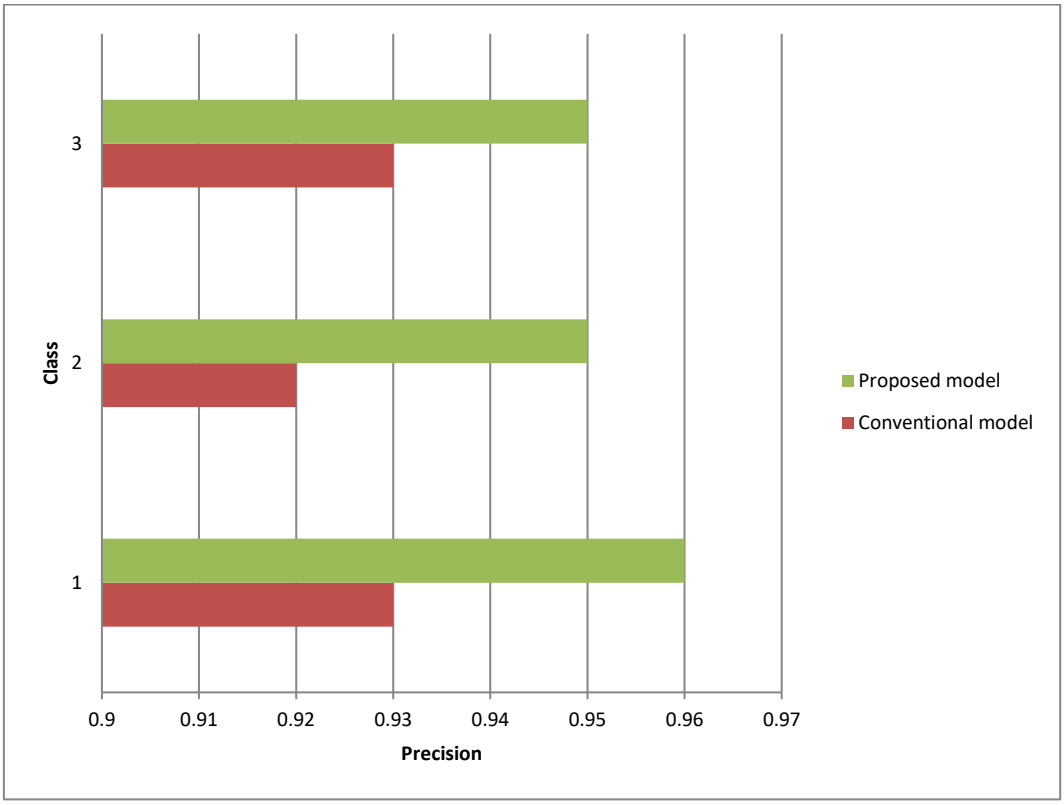


**Fig 6:** Comparison Analysis of Precision

Table 8 shows outcomes of a comparison between recall values of old & new work for classes 1, 2, & 3. Recall value for proposed model is greater than that of baseline model.

### 3. Recall Value

**Table 8:** Comparison Analysis of Recall Value

| Class | Conventional model | Proposed model |
|---|---|---|
| **1** | 0.92 | 0.95 |
| **2** | 0.95 | 0.96 |
| **3** | 0.92 | 0.96 |

Figure 7 was created using data from table 8 to illustrate the superior recall of the proposed model over the baseline.

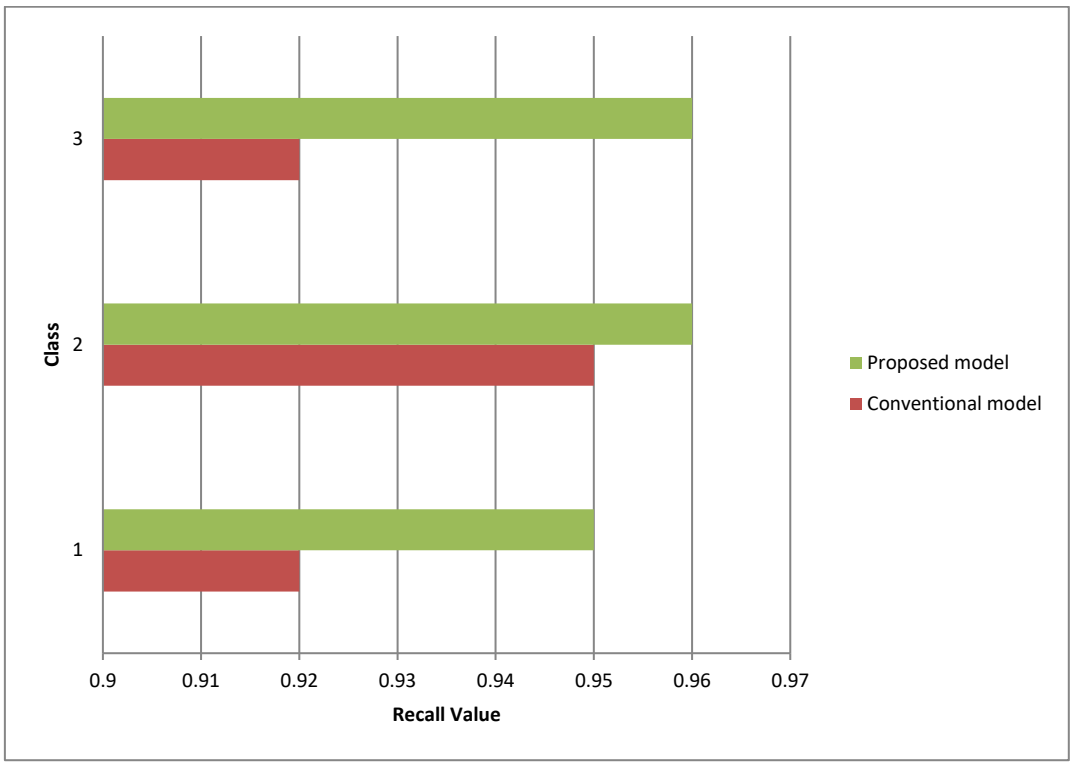


**Fig 7:** Comparison Analysis of Recall Value

Table 9 shows F1-scores for projects in classes 1, 2, and 3 that have been completed or are in the planning stages. The F1-Score of the recommended procedure vs the gold-standard procedur.

## 4. F1-Score

**Table 9:** Comparison Analysis of F1-Score

| Class | Conventional model | Proposed model |
|---|---|---|
| **1** | 0.93 | 0.96 |
| **2** | 0.94 | 0.96 |
| **3** | 0.93 | 0.95 |

Table 9 shows F1-Score for recommended model compared to baseline model, & Figure 8 provides a visual depiction of this data.

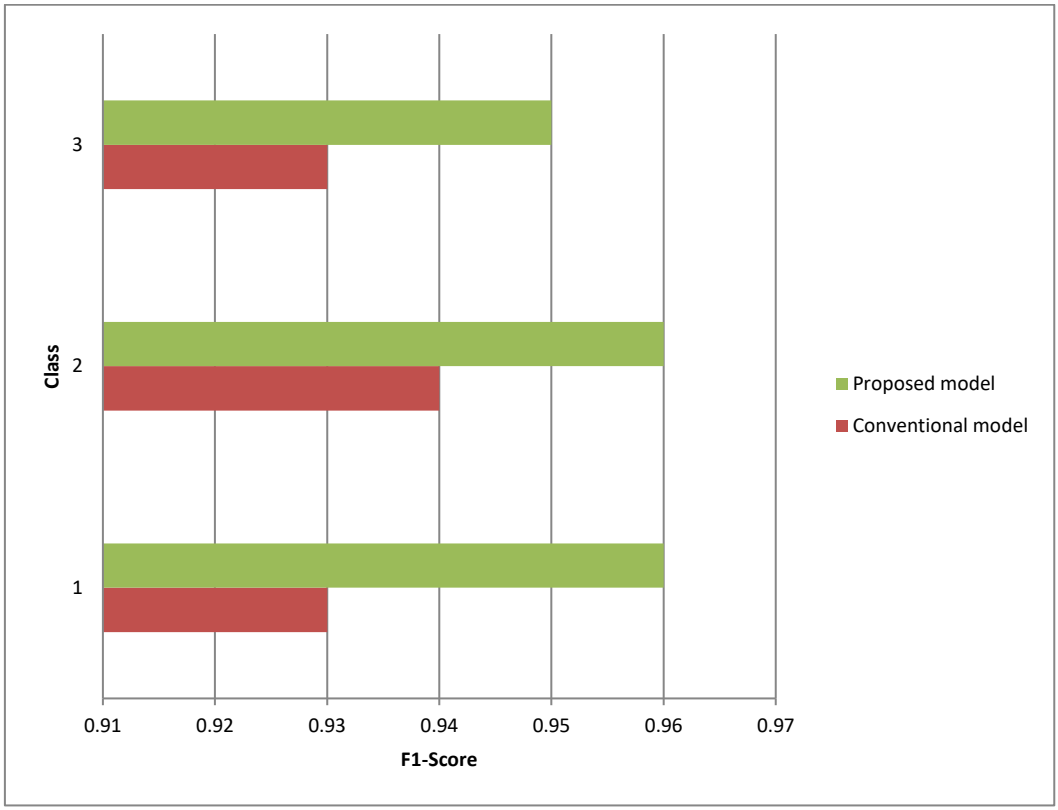


**Fig 8:** Comparison Analysis of F1-Score

## 6. Conclusion

The simulation findings suggest that the offered study has shown more accuracy than earlier techniques that relied on a machine learning methodology. The proposed method shows potential for reducing wasted time and improving accuracy. Additionally, improvements in accuracy, recall value, precision, and F1 Score have resulted from using the classification strategy throughout the process of attack categorization. There has been a rising need over the last decade for better security in ad hoc networking. There are still several security systems available, all of which focus primarily on the identification of potential dangers. When trying to identify assaults, several machine learning approaches are considered. However, existing solutions only address partial security and performance issues. When it comes to security, ad hoc networking can still be made better. This can only be achieved by using hybrid techniques. Attacks including man-in-the-middle attacks, denial-of-service assaults, and brute-force attacks are all categorised using a cutting-edge machine learning method. To better classify attacks against ad hoc networks and improve the reliability of decisions, the LSTM model has been included in the proposed study.

## 7. Future Scope

The future scope of performance and security evaluation for ad hoc networking technologies in IoT environments is poised for significant expansion and innovation. As the Internet of Things continues to permeate various aspects of our lives, from smart cities to industrial automation and healthcare, the demand for robust, efficient, and secure communication infrastructure is paramount. One key avenue for future exploration lies in the integration of emerging technologies, such as 5G networks and edge computing, into ad hoc networking solutions, offering the potential for enhanced performance and lower latency. Moreover, the looming threat of quantum computing underscores the importance of developing quantum-safe networking protocols, making research in this area essential for long-term security. The convergence of machine learning and AI with ad hoc networking presents opportunities for adaptive threat detection and performance optimization. As IoT devices diversify and energy efficiency becomes increasingly crucial, research into green IoT and energy harvesting techniques will shape the future of ad hoc networking. Additionally, the evolving regulatory landscape and growing privacy

concerns necessitate investigations into privacy-preserving protocols and compliance with data protection standards. Interoperability, standardization, and real-world testbeds remain vital areas of study to ensure seamless integration and practical applicability. In summary, the future scope of performance and security evaluation in IoT ad hoc networking is dynamic and multidimensional, driven by the need to navigate evolving challenges while harnessing the potential of emerging technologies to shape a more connected and secure IoT landscape.

**Reference**

[1] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (iot) security," IEEE Communications Surveys & Tutorials, 2020.

[2] Q. Liu, P. Li, W. Zhao, W. Cai, S. Yu, and V. C. Leung, "A survey on security threats and defensive techniques of machine learning: A data driven view," IEEE Access, vol. 6, pp. 12 103–12 117, 2018.

[3] D. J. Miller, Z. Xiang, and G. Kesidis, "Adversarial learning targeting deep neural network classification: A comprehensive review of defenses against attacks," Proceedings of the IEEE, vol. 108, no. 3, pp. 402–433, 2020.

[4] N. Papernot, P. McDaniel, A. Sinha, and M. P. Wellman, "SoK: Security and privacy in machine learning," in Proc. 2018 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2018, pp. 399–414.

[5] C. Zhang, P. Patras, and H. Haddadi, "Deep learning in mobile and wireless networking: A survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2224–2287, Third Quarter 2019.

[6] A.Qayyum, M. Usama, J. Qadir, and A. Al-Fuqaha, "Securing connected & autonomous vehicles: Challenges posed by adversarial machine learning and the way forward," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 998–1026, 2020.

[7] M. Mamdouh, M. A. I. Elrukhsi, and A. Khattab, "Securing the Internet of Things and wireless sensor networks via machine learning: A survey," in Proc. 2018 International Conference on Computer and Applications (ICCA), Aug 2018, pp. 215–218.

[8] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, C. Wang, and Y. Liu, "A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges," IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 393–430, First Quarter 2019.

[9] T. Pham, J. J. Durillo, and T. Fahringer, "Predicting workflow task execution time in the cloud using a two-stage machine learning approach," IEEE Transactions on Cloud Computing, vol. 8, no. 1, pp. 256–268, Jan. 2020.

[10] T. K. Rodrigues, K. Suto, H. Nishiyama, J. Liu, and N. Kato, "Machine learning meets computation and communication control in evolving edge and cloud: Challenges and future perspective," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 38–67, 2019.

[11] N. Carlini, C. Liu, J. Kos, Ú. Erlingsson, and D. Song, "The secret sharer: Measuring unintended neural network memorization & extracting secrets," arXiv preprint arXiv:1802.08232, 2018.

[12] O. Ibitoye, R. Abou-Khamis, A. Matrawy, and M. O. Shafiq, "The threat of adversarial attacks on machine learning in network security–a survey," arXiv preprint arXiv:1911.02621, 2019.

[13] C. Zhang, P. Patras, and H. Haddadi, "Deep learning in mobile and wireless networking: A survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2224–2287, Third Quarter 2019.

[14] Aazam, M., Huh, E. N., & Khan, I. (2021). A survey of mobile edge computing: Promises, issues and challenges. IEEE Access, 9, 2972-2989.

[15] Abbas, S., & Merabti, M. (2020). Scalability and Performance Evaluation of LPWAN Technologies for the Internet of Things. In Proceedings of the 4th International Conference on Cloud Computing and Artificial Intelligence (pp. 65-76).

[16] Abomhara, M., & Koien, G. M. (2020). Security and privacy for cloud-based IoT: Challenges. IEEE Internet of Things Journal, 7(7), 6353-6369.

[17] Ahmed, T., & Hu, J. (2021). A comprehensive survey of network virtualization in cloud computing. Journal of Network and Computer Applications, 173, 102993.

[18] Alcaraz, C., & Zeadally, S. (2021). A survey on the security of IoT technologies. IEEE Access, 9, 8943-8970.

[19] Ansari, M. S., & Islam, S. H. (2020). Security and privacy challenges in fog computing: A review. Journal of Network and Computer Applications, 168, 102714.
[20] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., ... & Thomas, K. (2021). The rise of shadow IoT. ACM Transactions on Privacy and Security (TOPS), 24(1), 1-25.
[21] Aziz, M. W., & Zainal, A. (2020). Security attacks and solutions in IoT networks: A review. Journal of King Saud University-Computer and Information Sciences.
[22] Bhargava, B., & Kumar, P. (2020). Performance analysis of wireless communication protocols for Internet of Things (IoT) using NS-3 simulator. Procedia Computer Science, 167, 72-79.
[23] Bouhafs, F., Qureshi, K., & Qaisar, S. (2021). Security and privacy in fog and edge computing: Challenges and solutions. Future Generation Computer Systems, 121, 82-85.
[24] Dinh, T. T. A., & Lee, C. (2020). Secure communication for the Internet of Things: A survey. IEEE Internet of Things Journal, 7(1), 9-41.
[25] Elhoseny, M., Yuan, X., Hu, Z., & Hossain, M. S. (2020). Fog computing for the Internet of Things: Security and privacy issues. IEEE Internet of Things Journal, 8(3), 1846-1854.
[26] Farooq, M. O., Kunz, T., & Parizi, R. M. (2020). A survey of emerging M2M/IoT wireless communication technologies. IEEE Access, 8, 19715-19733.
[27] Farooq, M. O., & Kunz, T. (2020). Performance analysis of IoT networks using LoRa, Sigfox, and NB-IoT. IEEE Access, 8, 26022-26032.
[28] Haque, A., Rahman, M. A., & Haque, M. E. (2021). Secure data communication in IoT: Challenges and solutions. Computers & Security, 106, 102275.
[29] Kaddoum, G., Rida, A., & Taha, S. (2020). Internet of Things (IoT) security: Current status, challenges and prospective measures. In 2020 IEEE/ACS 17th International Conference on Computer Systems and Applications (AICCSA) (pp. 1-8).
[30] Kim, H., & Kim, S. (2021). A comprehensive survey of blockchain-based secure IoT systems. Journal of Network and Computer Applications, 184, 102953.
[31] Liu, Y., Zhao, K., Wang, Y., Zhang, L., Zhao, H., Wang, L., & Liu, Y. (2020). A survey of security challenges in industrial Internet of Things. Future Generation Computer Systems, 107, 332-346.
[32] Mahmood, A. N., & Hu, J. (2020). Security and privacy in mobile cloud computing: Challenges and future research directions. Future Generation Computer Systems, 108, 714-719.
[33] Miao, X., Ma, M., & Xia, Z. (2020). A survey of fog computing in wireless sensor networks: Concepts, frameworks, applications, and issues. IEEE Access, 8, 41670-41685.
[34] Misra, P., Suman, S., & Odelu, V. (2020). IoT security: A survey of vulnerabilities, threats, and countermeasures. IEEE Access, 8, 17782-17809.
[35] Nabeel, M., & Gani, A. (2020). A survey of big data architectures and machine learning algorithms in healthcare. Journal