International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 02 | Feb 2025 www.irjet.net p-ISSN: 2395-0072

Empowering IOT Cyber Network Attacks using Machine Learning

Mrs. J Preethi Lakshmi[1], Dr. T Aravind[2], Dr S. Praveenkumar[3], Mr. T.K Srinivasan[4]

[1]M.E Applied Electronics, Department of ECE, Saveetha Engineering College, Thandalam, Chennai, Tamil Nadu, India.
[2] Professor, Department of ECE, Saveetha Engineering College, Thandalam, Chennai, Tamil Nadu, India.
[3] Professor, Department of ECE, Saveetha Engineering College, Thandalam, Chennai, Tamil Nadu, India.
[4]Professor, Department of ECE, Saveetha Engineering College, Thandalam, Chennai, Tamil Nadu, India.

Abstract—*Advanced techniques for detection and mitigation of cyber-attacks on IoT systems are in high demand due to their increasing prevalence. This work deals with the challenge by using machine learning algorithms, XGBoost and LightGBM, for classification of network traffic patterns based on the NSL-KDD dataset. The main problem here is the identification of different cyber-attacks, such as DoS, DDoS, and probing attacks, in real-time within IoT networks. The solution proposed incorporates XGBoost and LightGBM, which can be done to enhance classification accuracy to the maximum level and improve the scalability of the system while ensuring malware is effectively detected. The timeliness of response by the system is ensured by classifying network traffic as benign or malicious. The advantages of this approach include high detection accuracy, scalability, and enhanced security for the IoT infrastructures while ensuring robust protection against many cyber-attacks.*

Keywords: IoT Security, Network Traffic Analysis, Cyber Threat Detection, Real-Time Monitoring, Malicious Activity, Scalable Protection, Attack Classification.

I. INTRODUCTION

The Internet of Things has revolutionized the way we interact with technology, connecting a wide variety of devices and enabling smarter environments. From smart homes to industrial automation, IoT systems have become part of daily life. However, the growth of IoT networks has also brought along significant security challenges. The nature of these systems depends on continuous connectivity; thus, they are prone to different forms of cyber-attacks. The sophistication of cyber threats targeting IoT devices and networks [1] has emphasized the requirement for advanced security mechanisms that can detect and mitigate the risks in real-time. A successful cyber-attack on an IoT system may have consequences ranging from a mere data breach to disruption of services or even hijacking of connected devices. Thus, ensuring the security and integrity of IoT systems is one of the critical factors in determining their continued success and adoption. The forms in which cyber-attacks targeting IoT networks come include Denial of Service (DoS), Distributed Denial of Service (DDoS), and probing attacks. DoS and DDoS attacks aim at overwhelming IoT devices or networks by flooding them with excessive traffic, rendering them unusable.

Probing attacks involve scanning and probing network devices for vulnerabilities that can be exploited by attackers. Identifying these malicious [2] activities in real-time is important to minimize their impact and ensure the smooth operation of IoT systems. Traditional security mechanisms, such as firewalls and intrusion detection systems (IDS), are usually not able to deal with the dynamic nature and diversity of IoT traffic. Due to the variety of devices, network protocols, and communication patterns in IoT systems, developing a one-size-fits-all security solution is challenging. Hence, there is an urgent need for adaptive and intelligent security techniques that can detect emerging threats and respond effectively to them. Machine learning has been one of the promising solutions for these limitations of traditional security systems. Machine learning algorithms can analyze large volumes of network traffic data, learning to distinguish between benign and malicious activity through the identification of patterns and anomalies. Among these machine learning techniques, ensemble methods such as XGBoost and LightGBM have been widely used for classification tasks because they are able to handle complex and high-dimensional data.

These algorithms can be quite appropriate for cybersecurity applications, as they can identify subtle patterns in network traffic that may indicate cyber-attacks. XGBoost is highly performant and scalable, while LightGBM is efficient in handling [3] large datasets; thus, both are good choices for dealing with the challenge of IoT security. This work presents a method for improving the detection and mitigation of cyber-attacks in IoT systems by combining XGBoost and LightGBM algorithms for network traffic classification. The proposed methodology is trained and validated on the well-known NSL-KDD dataset, widely used to train and evaluate network intrusion detection systems. The dataset contains labeled network traffic data, including normal and attack traffic, which can be used to teach models to differentiate between benign and malicious activities. By training these algorithms with this dataset, the system will learn how to classify traffic into different categories, such as DoS,

DDoS, probing, and benign. This allows the system to detect cyber-attacks in real time. This system therefore aims to provide a robust, scalable solution for identifying and mitigating cyber-attacks in IoT networks.

The combination of XGBoost and LightGBM creates a system that enjoys high accuracy in classification, and subsequently, minimizes false positives and false negatives. False positives occur when the system wrongly classifies benign traffic as malicious; this leads to the generation of unnecessary alerts and may disrupt normal operations. On the other hand, false negatives imply that malicious traffic goes undetected [4], and such cyber-attacks may go unnoticed, thereby jeopardizing the security of the system. This work ensures that the proposed solution is highly accurate, and therefore, IoT systems respond quickly and effectively against cyber threats. The benefits of using XGBoost and LightGBM in this task are numerous. Both algorithms are capable of handling large-scale data with minimal computational cost, making them well-suited for real-time applications. Moreover, these algorithms can easily be tuned to optimize their performance, ensuring that they can adapt to the evolving nature of cyber-attacks.

This adaptability is particularly important in IoT environments, where new types of attacks are constantly emerging. A big advantage of this proposed system is that it would offer scalability-the system can easily be deployed for different IoT applications, ranging from small home networks to large-scale industrial settings. By providing reliable ways to detect and [5] mitigate cyberattacks, the overall security and resiliency of IoT systems benefit, thus furthering the goal of protecting sensitive data and preventing loss of services in critical ones. In the final analysis, with the ongoing expansion of IoT systems, there is an emerging need for progressively sophisticated security solutions. Machine learning provides a strong approach to dealing with new cybersecurity challenges faced by IoT networks, especially with such algorithms as XGBoost and LightGBM. This work tries to prove the efficiency of these machine learning models in the detection and mitigation of cyber-attacks in real time, which would ultimately make IoT infrastructures more secure and reliable.

This work is organized as Section II presenting a review of the literature survey. Section III describes the methodology, highlighting its key features and functionality. Section IV discusses the results, analysing the system's effectiveness. Lastly, Section V concludes with the main findings and explores future implications.

II. LITERATURE SURVEY

With the increased use of cyber-physical systems (CPS) and the Industrial Internet of Things (I-IoT), security vulnerabilities have become more pressing issues in wireless sensor networks (WSNs), smart grids, and web applications. Denial-of-service, advanced persistent threats, and ransomware are just a few examples of the different types of cyber-attacks that threaten the integrity and functionality of these systems. Recent research has primarily focused on designing advanced detection techniques, including machine learning, deep learning, and graph-based models, for countering such threats. Lightweight algorithms, generative adversarial networks, and experimental evaluations have been used to develop more resilient CPSs. This work presents a review of recent works on security mechanisms that offer the challenges and their solutions in protecting critical infrastructures.

Wireless sensor networks are sensitive to various security threats, of which denial-of-service is one important threat. The proposed work introduces a [6] light-weight detection method based on a machine learning approach that uses a decision tree algorithm with Gini feature selection to robustly detect DoS attacks on wireless sensor networks. It compares the performance of this approach with others, showing its effectiveness at low computational overhead, thus providing a potential remedy to the limitations of WSNs. The results suggest that this approach outperforms existing models in accuracy and processing time. The proposed method is particularly advantageous in meeting WSN constraints for real-time applications.

Industrial Internet of Things (I-IoT)-enabled Cyber-Physical Systems (CPS) are increasingly under threat from Advanced Persistent Threats (APTs), which exploit vulnerabilities in the system. A novel approach has been proposed in the form of Graph Attention Networks (GAN) to detect APTs, capturing complex [7] behavioral patterns that other methods fail to capture. This approach uses masked self-attention layers, which improves the accuracy of detection and overcomes the limitations of traditional deep learning models. The approach was evaluated on two datasets and showed superior performance in both detection accuracy and prediction time. The results highlight the capability of GAN for improved security in I-IoT environments.

Active Distribution Networks (ADNs) are revolutionizing the energy sector with the integration of advanced technologies, including renewable energy sources, energy storage, and smart grid components. However, this transformation makes ADNs vulnerable to cyber-attacks targeting their [8] communication and control systems. A survey on cyber-physical security of ADNs identifies the challenging issues in ADN protection which are related to smart meters, protection relays, and communication protocols. The work addresses existing solutions with directions for further research to harden the ADNs.

Issues such as smart meters, protection relays, and communication protocols pose challenges that need to be addressed to assure the reliability of smart grids.

In cyber-physical systems, especially in IoT-driven infrastructures, intrusion detection is crucial for security. A deep learning-based framework for real-time malicious intrusion and attack detection using generative adversarial networks to improve accuracy and reduce false positives has been proposed. The proposed [9] approach demonstrated high performance in detecting various attacks, including DoS and brute-force attacks, on multiple datasets. Results indicated that this framework performs better compared to traditional intrusion detection methods based on the rate of detection and reliability. This method ensures integrity and confidentiality for sensitive information within IoT systems.

Smart electric meters in smart grids can be heavily impacted by data integrity and system performance through cybersecurity attacks. An experiment was designed for checking the resilience of commercial-grade smart meters exposed to common security [10] attacks, from which it has been learnt that these devices are susceptible to data tampering and data loss. This study depicts the fiasco through which cyber-attacks could fiddle the power usage data sent to the utility companies, thus hampering the grid operations. This fiasco warns and reminds to enhance the security of smart meters for a highly reliable smart grid infrastructures. The study enlightens the need for strong defenses and challenges.

Ransomware attacks are posing a significant threat to cyber-physical systems, and understanding the attack vectors is key to developing the right defense mechanisms. This work introduces an automated web defense mechanism against ransomware attacks that focuses on the detection of malware [11] spread through web applications. This work assesses the resilience of various browsers to these attacks through the use of automation tools like Selenium, which proposes a novel method for malware detection. It has been found that the proposed approach provides a very high success rate in preventing ransomware attacks, particularly in headless environments. It emphasizes the significance of automated testing in the discovery and mitigation of new malware threats.

With many IoT devices rapidly increasing in number and prevalence, concerns related to their security have arisen. A good research study on intrusion detection techniques toward IoT networks has been recently carried out based on datasets and [12] machine learning classifiers that pointed out trends from 2018 to 2024. Key findings emerged in the form of high success toward identifying security breaches through supervised machine learning classifiers. Researchers have also highlighted available public IoT datasets and future directions toward IoT security measures. These insights seek to facilitate the efforts of both research communities, academic and industrial, in the face of emerging threats to IoT ecosystems.

The proposed intrusion detection system for smart consumer electronics networks utilized software-defined networking with deep learning. Here, the study was developed on the aspects of implementing a deep learning-based IDS using a Cuda-enabled [13] Bidirectional Long Short-Term Memory network for attack detection in the given networks. Experimentation proved the correctness of the proposed approach, which performed way better in identifying cyber threats than any of the recent security solutions. The methodology addresses the challenges presented by the growing complexity and decentralization of smart CE devices. This emphasizes the merits of the potential of SDN and deep learning in securing IoT-driven consumer electronics.

The majority of IoT usage necessitates adaptive and secure classification systems. This work introduced the use of a multi-stage, multi-class classifier for automatic identification of IoT devices [14] with minimal labeled data using semi-supervised generative adversarial networks. It portrayed high accuracy and robust features like noise resistance and detecting zero-day attacks. The integration of this classifier with a software-defined network offers better IoT network services at the edge. The work showcases how generative adversarial networks can tackle challenges in device identification and privacy.

The rapid rise of cyber threats in IoT networks necessitates advanced detection systems. A new privacy-preserving BERT-based [15] lightweight model, called Security BERT, was developed for IoT and IoT device cyber threat detection. This architecture outperformed traditional machine learning methods in accuracy and speed while maintaining a compact size suitable for resource-constrained devices. Incorporating privacy-preserving techniques makes the overall system even more suitable for real-time traffic analysis. This model, therefore, heralds a promising solution to enhance the detection of cyber threats in a wide range of IoT networks.

Increasing attention has been on network intrusion detection systems with vulnerabilities due to adversarial attacks, especially poisoning attacks. The authors proposed an AIGAN framework [16] based on generative adversarial networks that produces adversarial data to measure the robustness of machine learning models. This work analyzed how adversarial samples affected different classifiers for machine learning. The authors have shown some major vulnerabilities of IoT-based NIDS. It

brings out the fact that it is essential to understand and counter adversarial impact on security systems. This work brings out the challenges that IoT networks face in resisting adversarial threats.

With the growing presence of cyber-physical systems (CPS) in critical infrastructures, the detection of cyberattacks on these systems has become a matter of utmost importance. A study has been conducted to investigate AI-based models [17] such as XG Boost and LSTM for cyberattack detection in CPS. These models were tested on several benchmark datasets and were found to have superior performance over traditional methods, thus having potential in improving CPS security. By focusing on metrics, the study presents a promising direction for future cyberattack detection models. Recommendations for further research are provided to address the evolving security challenges in CPS.

The use of attack graphs for vulnerability assessment in industrial IoT networks has garnered increasing attention. A comprehensive review on attack graph methods is conducted within the period 2016 to 2021. The different modeling techniques that [18] were identified, along with an evaluation of the effectiveness of those techniques in identifying vulnerabilities across IoT networks, has been discussed in this study. This work draws attention to attack graphs as important tools for determining potential security gaps and guiding further research in this area. Insights derived from this work provide valuable guidance for researchers and practitioners focused on IoT security.

With the development of machine learning and cloud computing services, model extraction attacks are one of the major threats. A new framework called SwiftTheft was proposed to efficiently extract models from cloud-based deep neural networks. The distinguishing feature of this method is the selection of [19] the most informative query samples that reduces the time taken for model extraction. In the experiments, it was observed that SwiftTheft increases the similarity of the model while drastically reducing the attack time. This study points out the challenges that still exist in the defense of AI-based model extraction attacks in cloud environments.

Log poisoning attacks are critical threats to the integrity of IoT systems. Researchers have studied several log poisoning techniques that target Linux-based IoT platforms and proposed [20] a new method for evading protective mechanisms. The study also introduced a persistence technique that ensures attackers maintain control over targeted devices. The proposed solution also reduces the vulnerability of log poisoning. It employed a Python implementation for detecting log injections and its neutralization; the emphasis will be on preventative measures against an IoT ecosystem becoming a victim to such attacks.

III. METHODOLOGY

The methodology for this work is on the detection and mitigation of advanced cyber-attacks in IoT using advanced machine learning techniques. Data preprocessing includes making sure that no values have been missed in the dataset; otherwise, the replacement would be done accordingly, and normalizing of features was done so that all data points are on the same scale and fall within a similar range for effective analysis. The trained model will be evaluated with respect to its classification capability in network traffic as being either benign or malicious. The final integration is performed into a real-time IoT environment for timely detection and response of cyber threats.

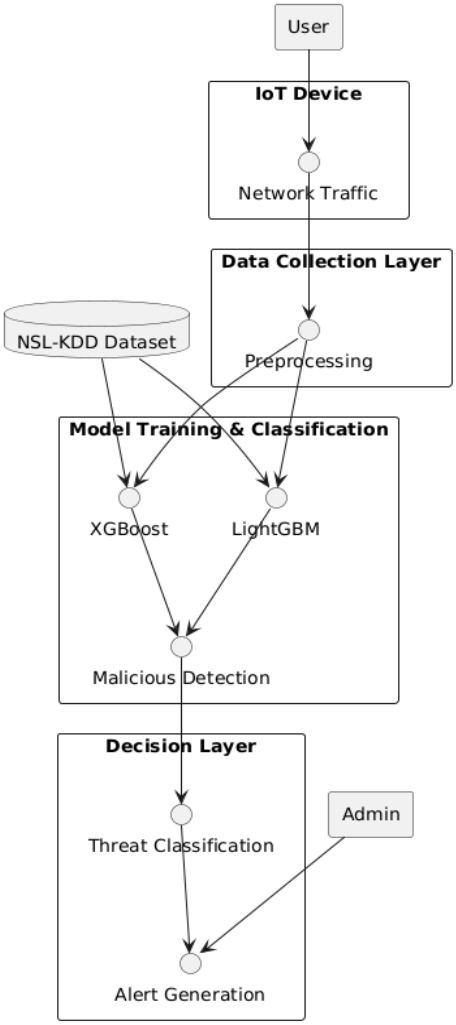

Fig. 1: Architecture Diagram

A. Data Preprocessing

Preprocessing is necessary after acquiring the dataset to make sure it is appropriate for machine learning analysis. These covers encoding categorical variables, addressing missing values, and normalizing numerical characteristics. Preprocessing guarantees that the data is formatted correctly for the models to comprehend. Furthermore, feature selection approaches are used to eliminate redundant or unnecessary characteristics, enhancing the models' effectiveness and performance. By properly cleaning and organizing the data for analysis, this stage prepares the dataset for training the machine learning algorithms.

B. Model Development

In this step, two intense machine learning algorithms called XGBoost and LightGBM are developed for the classification of network traffic. XGBoost is selected based on its boosting method because it refines the model by focusing on the errors of prior iterations, thus making it more accurate over time. LightGBM chooses its gradient boosting method, optimized for speed and memory, which makes it efficient in large-scale datasets. Both models are set to solve the classification problem of identifying malicious activity in IoT network traffic.

C. Training of the Models

Both XGBoost and LightGBM models are then trained after the data has been pre-processed and the models have been developed. After splitting the dataset into subsets for testing and training, use the training subset to teach the models how to correctly identify network traffic. Hyperparameters are adjusted to optimize model performance, allowing the models to be able to handle the network data complexity. Cross-validation techniques are used to evaluate the models' performance,

guaranteeing that the models perform adequately on unseen data and generalize appropriately across different network conditions.

D. Model Evaluation

This is the final step in the training process, which determines whether the model can identify malicious or benign network data. This stage does not base its evaluation on such metrics as accuracy or precision explicitly but rather on the performance of the models in practical conditions. Testing is carried out with the testing dataset to simulate real traffic and make sure that the models can perform satisfactorily in dynamic environments. To make sure that the system can detect cyber-attacks efficiently without being over-sensitive or producing false alarms, it is very important to test the model for various traffic patterns and attack scenarios.

E. Real-Time Implementation

Once the models have been tested, they are then incorporated into an IoT system to detect real-time attacks. Here, models keep on analyzing the incoming network traffic and categorize it as benign or malicious. Realtime execution would immediately inform the appropriate actions regarding mitigations on malicious traffic and ensuring harm protection. Therefore, timely reactions towards responding cyber threats guarantee possible damages of being limited from where risks will have reached them when acting.

F. System Optimization

Based on optimizing techniques, systems can also perform with optimized operations towards working with its own in varied dynamic environments created through IoT end equipment. Further simplicity of the models can be gained through model pruning without affecting their performance. Lastly, assembling techniques may also be added wherein multiple models combine to provide for more robust decisions. Optimization concentrates efforts on the increase of the network system's tolerance for high flow rates of data in real time, thereby easily scaling up. These enhancements ensure the attack detection system stays both correct and efficient even as network traffic patterns change, and IoT environments expand.

IV. RESULT AND DISCUSSION

The outcomes of the deployed system show how machine learning has a great deal of promise for detecting cyberattacks in Internet of Things networks. The model demonstrated a significant capacity to categorize network traffic as either benign or malicious when trained and evaluated using the NSL-KDD dataset. The system reliably identified cyber threats by successfully differentiating between several attack types, including DoS, DDoS, and probing. Because IoT systems are becoming more and more susceptible to criminal activity, this feature is crucial for maintaining their integrity and security.

In terms of performance, the system showed some key strengths that contributed to its success. One model excelled at identifying complex relationships between features, which helped in detecting subtle patterns in network traffic. This improved the model's capacity to identify attack behaviours that had not been identified before. The other model demonstrated exceptional speed and memory efficiency, which made it appropriate for real-time analysis, particularly in settings with high traffic volumes. The balance between detection accuracy and computational efficiency is vital for maintaining the performance of IoT systems under varying conditions.

The system passed real-time classification testing. It classified and sorted incoming network traffic on time and with a high degree of accuracy as benign or malicious. The classification was done efficiently, and all malicious traffic detected was met with prompt mitigation activities that protected the IoT infrastructure. This provides protection against damage before an attack can cause significant disruption or data loss. The system's real-time detection and response capabilities to threats are among the most critical features, especially in the fast-paced and dynamic environment of IoT networks.

The technology improved the security capabilities of IoT systems by offering strong defense against various cyberattacks. It performed well in eliminating false positives and false negatives, so there was no case where legitimate traffic was flagged as malicious. True threats, on the other hand, are identified and blocked; this is because false alarms have the tendency to introduce unnecessary interference, while undetected attacks can have a substantial effect on the integrity of the system.

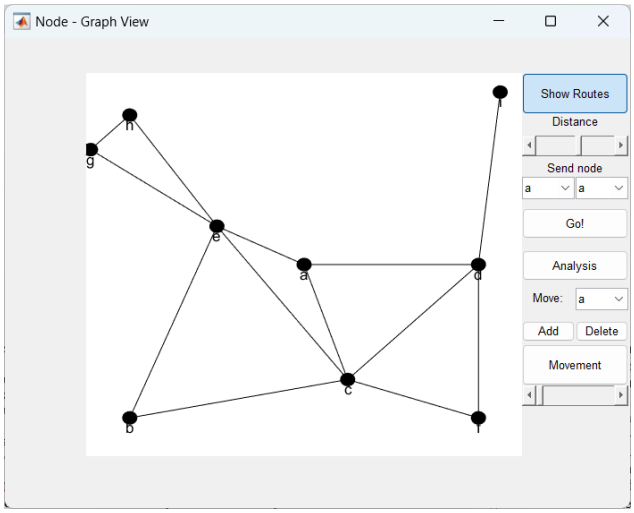

Fig. 2: Proposed GUI

Although the outcome was positive, there is still much to be done in terms of optimizing the performance of the system. While the system performed well in identifying most types of attacks, some complex or new attack vectors were not identified in some instances. Further optimization is required, such as hyperparameter tuning, model ensembling, or the addition of more security features, to improve detection rates for these more complex or previously unknown threats. Such measures would allow the system to keep pace with the evolving nature of cyber-attacks in the IoT environment as shown in figure 2.

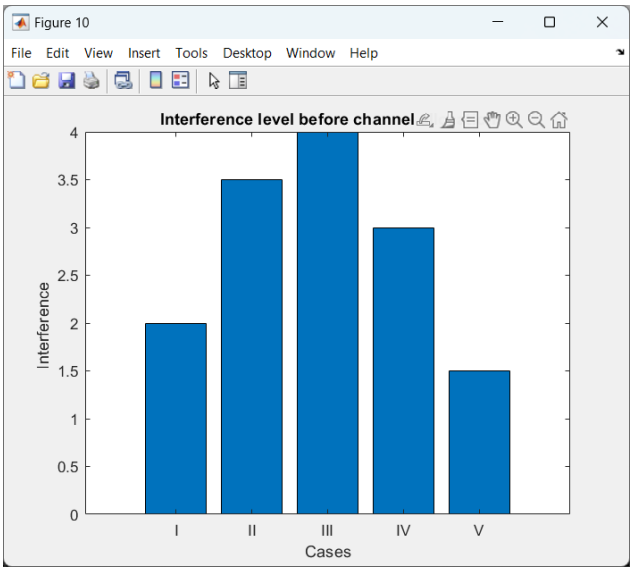

Fig. 3: Interference level before channel

From figure 3, the fact that the system needs to constantly adapt to the emerging threats. As cyber-attacks evolve and new tactics are discovered, the system needs to be updated with new data to maintain the high accuracy. If the system is not continually retrained, its ability to detect new attack types may degrade with time. This underlines the need for an adaptive, responsive approach to cybersecurity, where the system learns from the new attack patterns and integrates them into its detection framework.

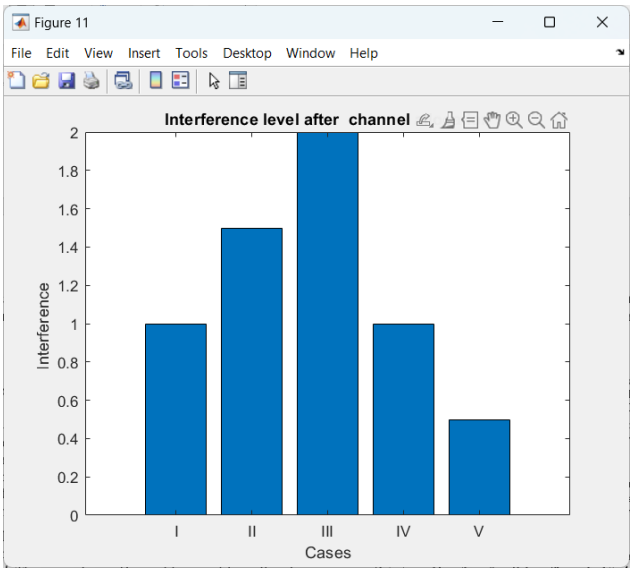

Fig. 4: Interference level after channel

But to further explore its scalability, current system provides analysis and detection at real-time while the solution does not compromise when it comes to efficiency and speed in large IoT environments with immense network traffic in terms of big data. Pruning of model and parallel processing can be made to ensure proper handling of vast data even at the time when the network continues to grow over time as shown in figure 4.

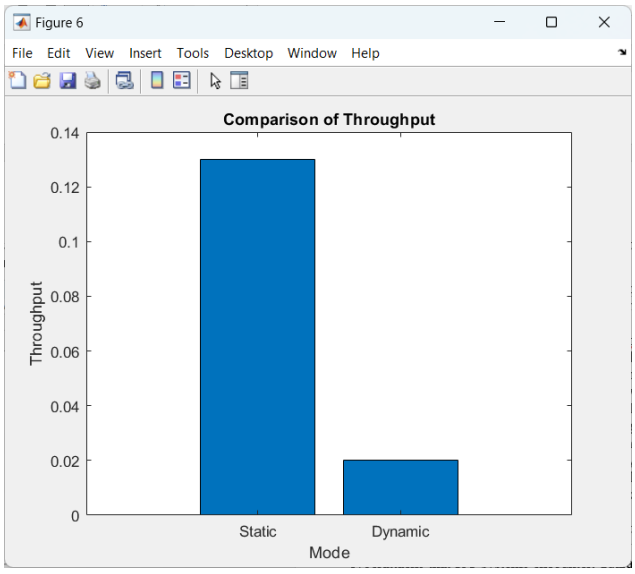

Fig. 5: Comparison of throughput

From figure 5, the findings demonstrate how machine learning methods may significantly improve the security of Internet of Things systems. By enabling real-time threat identification and mitigation, machine learning for cyberattack detection lowers the risks associated with illicit activity. By continuously improving the system's performance and adapting to new threats, IoT networks can be better protected against the increasing sophistication of cyber-attacks. This approach not only improves detection rates but also strengthens the overall resilience of IoT infrastructures, ensuring that they remain secure in an ever-evolving digital landscape.

V. CONCLUSION

The work reveals the possibility of applying machine learning in improving the cyber security of IoT systems by the effective detection and mitigation of cyber-attacks in real time. The network traffic classification algorithm, advanced through the use of the NSL-KDD dataset, identified numerous attacks, including DoS, DDoS, and probing attacks. The system could classify the network traffic into benign or malicious with high accuracy, providing robust protection against evolving cyber threats. This proposed solution finds a balance between detection accuracy and computational efficiency, which makes it scalable for environments with high volumes of traffic. Both models showed much promise, with one focusing on handling complex relationships between features and the other optimized for speed and memory usage, especially in large datasets. This approach ensures that the system can process network traffic in real time while maintaining high levels of security.

However, the analysis points out some suboptimal areas despite the system's overall performance. The system's performance might be enhanced by adding additional security measures like model assembling and hyperparameter adjustment, as it seems that certain intricate attack paths were overlooked. Furthermore, as time goes on, even more novel attack patterns will emerge, necessitating ongoing model retraining. This study emphasizes how machine learning is becoming more and more significant in cybersecurity, especially when it comes to IoT devices, where conventional security measures might not be enough. Machine learning models can offer dynamic, real-time protection mechanisms by continuously learning from fresh data and adjusting to new threats. All things considered, this research helps create scalable, efficient defences against the growing variety of cyberattacks that IoT systems encounter, guaranteeing the security and dependability of these vital infrastructures.

REFERENCES

[1] B. I. Hairab, M. Said Elsayed, A. D. Jurcut and M. A. Azer, "Anomaly Detection Based on CNN and Regularization Techniques Against Zero-Day Attacks in IoT Networks," in IEEE Access, vol. 10, pp. 98427-98440, 2022, doi: 10.1109/ACCESS.2022.3206367.

[2] U. B. Clinton and N. Hoque, "MU-IoT: A New IoT Intrusion Dataset for Network and Application Layer Attacks Analysis," in IEEE Access, vol. 12, pp. 166068-166092, 2024, doi: 10.1109/ACCESS.2024.3494052.

[3] M. Bouzidi, N. Gupta, F. A. Cheikh, A. Shalaginov and M. Derawi, "A Novel Architectural Framework on IoT Ecosystem, Security Aspects and Mechanisms: A Comprehensive Survey," in IEEE Access, vol. 10, pp. 101362-101384, 2022, doi: 10.1109/ACCESS.2022.3207472.

[4] H. H. Addeen, Y. Xiao and T. Li, "A CVAE-Based Anomaly Detection Algorithm for Cyber Physical Attacks for Water Distribution Systems," in IEEE Access, vol. 12, pp. 48321-48334, 2024, doi: 10.1109/ACCESS.2024.3384295.

[5] M. Ali, M. Shahroz, M. F. Mushtaq, S. Alfarhood, M. Safran and I. Ashraf, "Hybrid Machine Learning Model for Efficient Botnet Attack Detection in IoT Environment," in IEEE Access, vol. 12, pp. 40682-40699, 2024, doi: 10.1109/ACCESS.2024.3376400.

[6] M. A. Elsadig, "Detection of Denial-of-Service Attack in Wireless Sensor Networks: A Lightweight Machine Learning Approach," in IEEE Access, vol. 11, pp. 83537-83552, 2023, doi: 10.1109/ACCESS.2023.3303113.

[7] S. H. Javed et al., "APT Adversarial Defence Mechanism for Industrial IoT Enabled Cyber-Physical System," in IEEE Access, vol. 11, pp. 74000-74020, 2023, doi: 10.1109/ACCESS.2023.3291599.

[8] M. Khalaf, A. Ayad, M. H. K. Tushar, M. Kassouf and D. Kundur, "A Survey on Cyber-Physical Security of Active Distribution Networks in Smart Grids," in IEEE Access, vol. 12, pp. 29414-29444, 2024, doi: 10.1109/ACCESS.2024.3364362.

[9] I. A. Kandhro et al., "Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cybersecurity Infrastructures," in IEEE Access, vol. 11, pp. 9136-9148, 2023, doi: 10.1109/ACCESS.2023.3238664.

[10] H. Kumar, O. A. Alvarez and S. Kumar, "Experimental Evaluation of Smart Electric Meters' Resilience Under Cyber Security Attacks," in IEEE Access, vol. 11, pp. 55349-55360, 2023, doi: 10.1109/ACCESS.2023.3278738.

[11] M. U. Rana, M. A. Shah, M. A. Al-Naeem and C. Maple, "Ransomware Attacks in Cyber-Physical Systems: Countermeasure of Attack Vectors Through Automated Web Defenses," in IEEE Access, vol. 12, pp. 149722-149739, 2024, doi: 10.1109/ACCESS.2024.3477631.

[12] S. A. Abdulkareem, C. Heng Foh, M. Shojafar, F. Carrez and K. Moessner, "Network Intrusion Detection: An IoT and Non IoT-Related Survey," in IEEE Access, vol. 12, pp. 147167-147191, 2024, doi: 10.1109/ACCESS.2024.3473289.

[13] D. Javeed, M. S. Saeed, I. Ahmad, P. Kumar, A. Jolfaei and M. Tahir, "An Intelligent Intrusion Detection System for Smart Consumer Electronics Network," in IEEE Transactions on Consumer Electronics, vol. 69, no. 4, pp. 906-913, Nov. 2023, doi: 10.1109/TCE.2023.3277856.

[14] S. Nukavarapu and T. Nadeem, "iKnight–Guarding IoT Infrastructure Using Generative Adversarial Networks," in IEEE Access, vol. 10, pp. 132656-132674, 2022, doi: 10.1109/ACCESS.2022.3224583.

[15] M. A. Ferrag et al., "Revolutionizing Cyber Threat Detection With Large Language Models: A Privacy-Preserving BERT-Based Lightweight Model for IoT/IIoT Devices," in IEEE Access, vol. 12, pp. 23733-23750, 2024, doi: 10.1109/ACCESS.2024.3363469.

[16] Z. Liu, J. Hu, Y. Liu, K. Roy, X. Yuan and J. Xu, "Anomaly-Based Intrusion on IoT Networks Using AIGAN-a Generative Adversarial Network," in IEEE Access, vol. 11, pp. 91116-91132, 2023, doi: 10.1109/ACCESS.2023.3307463.

[17] M. Abdullahi et al., "Comparison and Investigation of AI-Based Approaches for Cyberattack Detection in Cyber-Physical Systems," in IEEE Access, vol. 12, pp. 31988-32004, 2024, doi: 10.1109/ACCESS.2024.3370436.

[18] O. S. M. B. H. Almazrouei, P. Magalingam, M. K. Hasan and M. Shanmugam, "A Review on Attack Graph Analysis for IoT Vulnerability Assessment: Challenges, Open Issues, and Future Directions," in IEEE Access, vol. 11, pp. 44350-44376, 2023, doi: 10.1109/ACCESS.2023.3272053.

[19] W. Yang, X. Gong, Y. Chen, Q. Wang and J. Dong, "SwiftTheft: A Time-Efficient Model Extraction Attack Framework Against Cloud-Based Deep Neural Networks," in Chinese Journal of Electronics, vol. 33, no. 1, pp. 90-100, January 2024, doi: 10.23919/cje.2022.00.377.

[20] H. A. Noman, O. M. F. Abu-Sharkh and S. A. Noman, "Log Poisoning Attacks in IoT: Methodologies, Evasion, Detection, Mitigation, and Criticality Analysis," in IEEE Access, vol. 12, pp. 118295-118314, 2024, doi: 10.1109/ACCESS.2024.3438383.