ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov1032

Detecting Cyber Threats in IoT Networks Using Sequential Pattern Analysis

Venkateswaran Radhakrishnan[1]; S. Baghavathi Priya[2]; Rajalakshmi. G. R.[3]; Mohammed Ghouse Haneef Maqsood[4]; Rogelio Gutierrez[5]; Chithik Raja Mohamed[6]; Mohamed Ashik[7]

[14567]Department of Information Technology, College of Computing and Information Sciences, University of Technology and Applied Sciences Salalah, Sultanate of Oman

[2]Department of Computer Science and Engineering Amrita Vishwa Vidyapeetham Chennai, India

[3]Department of Comerce with Computer Applications PSG College of Arts and Science Coimbatore, India

Publication Date: 2025/11/28

Abstract: The swift spread of Internet of Things (IoT), alike the wildfire has forced us all into cybersecurity challenges and therefore requires proper security tools for detecting and responding to real-time threats. Instead, this study moves in a different sequence way-the sequence-based pattern analysis is a novel way to both identify and mitigate the possible cyber threats that are associated with IoT networks. In the first stage of the study, a hybrid approach implementing the sequential pattern mining and machine learning algorithms is followed the extraction of patterns related to the anomalies. At first, data preprocessing is processed via the feature selection scheme to impetus the quality of generated patterns. Thereafter, the frequent sequence mining technique is a move that is it applied; thus, to determine the repetition of attack patterns in the IoT traffic data. Besides, a supervisor learning-based anomaly detection model is installed to classify threats on the basis of temporal sequence anomalies. Further, the reinforcement based learning procured is the one that is adaptively applied such that changes in the cyber threats get the system to learn and ultimately improve its detection accuracy. The plan has been tested on a few large datasets of the IoT network that are the most common, to show its effectiveness by comparison with methods in operation. The study findings in the line of sequence-based pattern analysis; plus, the machine learning are single skills for this set of processes to perform IOT cyberattack detection that enables IoT secure environments

Keywords: *Cyber Threat Identification, Iot Security, Sequence -Depending Pattern Analysis, Anomaly Determination, Supervisor Learning, Reinforcement Based Learning, Network Infrastructure Security, Frequently Sequence Mining, Real-Time Threat Avoiding.*

How to Cite: Venkateswaran Radhakrishnan; S. Baghavathi Priya; Rajalakshmi. G. R.; Mohammed Ghouse Haneef Maqsood; Rogelio Gutierrez; Chithik Raja Mohamed; Mohamed Ashik (2025) Detecting Cyber Threats in IoT Networks Using Sequential Pattern Analysis. *International Journal of Innovative Science and Research Technology*, 10(11), 1685-1692. https://doi.org/10.38124/ijisrt/25nov1032

I. INTRODUCTION

The rapid growth of the Internet of Things (IoT) has brought with it the ability to connect and communicate between smart devices that interconnect virtually all industrial sectors, and thus the world is becoming more and more interconnected. Yet the extensive use of IoT technologies has also given rise to a considerable number of cyber threats that are targeting IoT networks. These threats are diverse and they may range from data breaches to Denial of Service (DoS) attacks that let data get lost, tampered with, or accessed by an unauthorized party or parties. In other words, it's a risk to privacy, trust, and the IoT network availability if these attacks happen. Therefore, proper protection of IoT networks is an

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov1032

urgent issue for both researchers and industry professionals [1].

The basic cybersecurity techniques, such as signature-based detection systems, have not been able to keep up with the rapid changes in IoT networks, which tend to be dynamic and diverse. These methods are incapable of discovering new or previously undetected threats, and elaborately designed ways are required for their solution. As a supplement to the current cyber threat detection mechanism, sequence-based pattern analysis has begun to be used as a tool for identifying anomaly in IoT networks using the sequence of events or actions as features [2]. In addition, past data-based patterns and sequence-based models combined with activity recognition techniques can be specified as methods that can be used to identify the potential cyber threats [3].

Supervised learning algorithms have demonstrated outstanding performance in the field of pattern recognition and anomaly detection tasks and are therefore deemed a very good fit for IoT cybersecurity. These systems can grow and develop through data processing, become more adaptable, and thus, due to supervisor learning, increase the detection accuracy of cybersecurity systems [4]. Furthermore, reinforcement based learning (RL) shows the potential to evolve continuously, which means that defenses can learn and adapt over time to the latest threat types [5].

With the requirement of the real-time identification in the IoT network so as to prevent the cyber-crime analogues, the application of the machine learning-enhanced security systems and sequence-based pattern analysis are reaping the success. These systems are meant to be used for instant incident detection and classification and so secure IoT networks in time from the cyber risks that are changing constantly [6].

In particular, the use of hybrid models that combine sequence mining with deep learning-based anomaly detection has shown promise in addressing the limitations of traditional security methods [7]. Moreover, the reinforcement based learning component even further increases the adaptability and effectiveness of IoT cybersecurity systems, the model will learn from the environment, optimize their detection strategies and reduce false positives thus leading to enhanced system performance [8]. The merging of the methods mentioned is the base of the solution given for the cyber threat detection in the IoT networks that is realized by means of sequence-based pattern analysis. The study aims to prove the proposed framework, which includes sequence-based pattern analysis, machine learning, deep learning, and reinforcement learning for real-time IoT threat detecting. After the evaluation of the method and the comparison with the others, we can conclude the advantages of this integrated approach in terms of the detection accuracy, the response time, and the security of the IoT networks, respectively [9-10].

II. LITERATURE SURVEY

In this section the research of a variety of methods intended for ensuring IOT networks against cyberattacks. From supervisor learning to blockchain and edge computation methods, the area of the topic of which is still improving, and each new development contributes to the making of more robust and adaptive security frameworks. The introduction of cyber threats in IoT networks has been studied in recent years and several methodologies have been proposed to meet the security challenge facing such environments. One of the early works in this area was to focus on anomaly detection in IoT traffic through supervisor learning algorithms. This method is developing supervised learning to find deviations from the ordinary network traffic, which is the way to identify previously unseen threats in an effective manner [11]. Nevertheless, the aforementioned inventions often encounter persistent high false positive rates, especially among large aggregate IoT networks.

A more recently conducted research was looking into the implementation of deep learning models like Convolutional type Neural based Networks (CNNs) and Long Shorts-Terms Memories (LSTM) networks for cyber threat detection in IoT systems. These models were discovered to significantly enhance the accuracy of detection through learning of complex patterns in the temporal and spatial data obtained from IoT devices [12]. In the meanwhile, deep learning has been found to be very promising but it has been a major challenge due to computational complexity and the need for large datasets to train the model. Simultaneously, the research field has been involved in the evaluation of sequence-based pattern analysis in the sphere of cyber threat detection in IoT networks. A study introduced how frequent sequence mining algorithms could be used to detect patterns of attack in the network traffic. The appearance of frequent sequences in the data has led to the system detecting anomalies that traditional methods have not identified [13]. Though this method was effective, it was brought to its knees quite often when applied to dynamic and large-sized IoT networks.

The progress in hybrid models, a mixture of sequence-based analysis and smart learning algorithms, has been very significant. A study was proposed which integrates sequence mining techniques with decision trees in order to increase the speed and accuracy of the detection of the complex attack patterns in the IoT environments. The hybrid approach gave detection rates greater than existing methods of attack and furthermore the false positive rates were very low [14]. However, it had to be fine-tuned, which might be a limitation for its practical application in real-time environments. Another approach adopted the RL to dynamically adapt to the change of the network and the threat of the day. The study verified that the threat detection strategies have been optimized using reinforcement, which in turn, made it possible for the system to minimize the number of false alarms [15]. Moreover, RL can be a helpful addition to the security framework of IoT because of its flexibility in dealing with such issues.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov1032

Additionally besides reinforcement learning, researchers conducted studies on the use of unsupervised learning techniques like clustering and autoencoders for anomaly detection in IoT networks. The ways truly work magnificently in the situations when there is no labeled data or it is scarce. A scientific paper noted the use of k-means clustering to find unusual traffic patterns, which in turn were identified as potential threats [16]. Although these mechanisms were capable of efficient identifying, still they faced difficulties related to the high dimension of IoT data.As IoT technology is advancing, many researchers are also focusing on the incorporation of blockchain technology into IoT networks for the purpose of strengthening security and preventing cyber threats respectively. The ledger made by blockchain is both decentralized and immutable, and hence, it can help in keeping the data undisturbed and ensuring that no unauthorized entities have accessed the sensitive information. There is a proposal in the paper to use blockchain to store the security-related data, such as the threat signatures and attack history, which could be accessed by the threat detection systems in real time and that could be a good way of stopping the problem [17].

To elaborate on real-time threat detection, an ensemble type learning technique study was executed that utilized multiple classifiers to enhance detection accuracy. The ensemble method was a better choice because it is made up of a lot of different classifiers which all have their strengths and thus are better at detecting a wider range of threats [18]. However, this method was found to be computationally expensive and required significant resources for processing. Edge computing together with IoT networks was the subject of another investigation, with the main aim being to reduce latency in threat detection. Edge computing makes it possible for the data to be processed at the source, thus eliminating the time required to detect and respond to threats. Research carried out on edge devices showed that, with this technology, we could have a real-time analysis of IoT traffic, and in turn, the whole security system could be more responsive [19].The concept of hybrid models that consist of many different methods, such as sequence-based pattern analysis, machine learning, and edge computing, has been widely investigated. A paper posted a hybrid framework that was developed by uniting sequence-based mining with machine learning and edge computing to detect cyber threats in real time. The adoption of the new approach thus gave opportunities for the system's performance to be improved and the results to be presented more flexibly and customizable [20]. The approach was a success, but still, there are some places that need to be worked on to optimize the system for large-scale IoT deployments.

III. PROPOSED SYSTEM

In order to identify cyber threats in IoT networks, the proposed system will be built on a structured step-by-step pattern analysis integrated with automation (sequence-based) technology and machine learning. Initially, by means of data preprocessing, the raw IoT network traffic data is first cleaned, normalized, and then feature-engineered to upgrade the quality of patterns extracted from it. Moreover, a feature selection mechanism is utilized aiming to remove unrelated and redundant data thus ensuring efficient processing. Afterward, through frequent sequence mining, network traffic containing such attacks can be identified with the result that the users will be alerted at the early stages and in real-time by network operators about the occurrence of possible security events. The obtained sequences are authenticated by undergoing a deep learning-based anomaly detection model, where these sequences are them deployed so the model that was trained here - one that distinguishes abnormal behavior and alerts about possible threats in real-time - can be used to move forward (as shown in Figure 1). Additionally, a reinforcement learning mechanism is also coupled with the system so that the system can dynamically adapt detection thresholds based on the evolution of cyber threats. This continuous learning capability further sharpens detection accuracy while it is able to minimize false positives. On top of that, the system incorporates a real-time threat response module which selectively eliminates detected threats by performing the appropriate countermeasures such as traffic filtering and access control adjustments. The given framework unites an intelligent, scalable, and adaptive manner of ensuring the ability to detect and defend IoT networks from the cyber-attacks that are continuously trying to emerge. After conducting rigorous experiments on real-world datasets, our system shows excellent results in terms of threat detection accuracy, false positive reduction, and response efficiency compared to traditional methods. Blockchain-based Zero-Trust models and Homomorphic Encryption together provide a robust foundation for IoT security by enabling decentralized trust management and privacy-preserving data processing [21]. These emerging technologies address critical IoT challenges such as device authentication, data integrity, and secure cloud-based analytics in IoT networks [22].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov1032

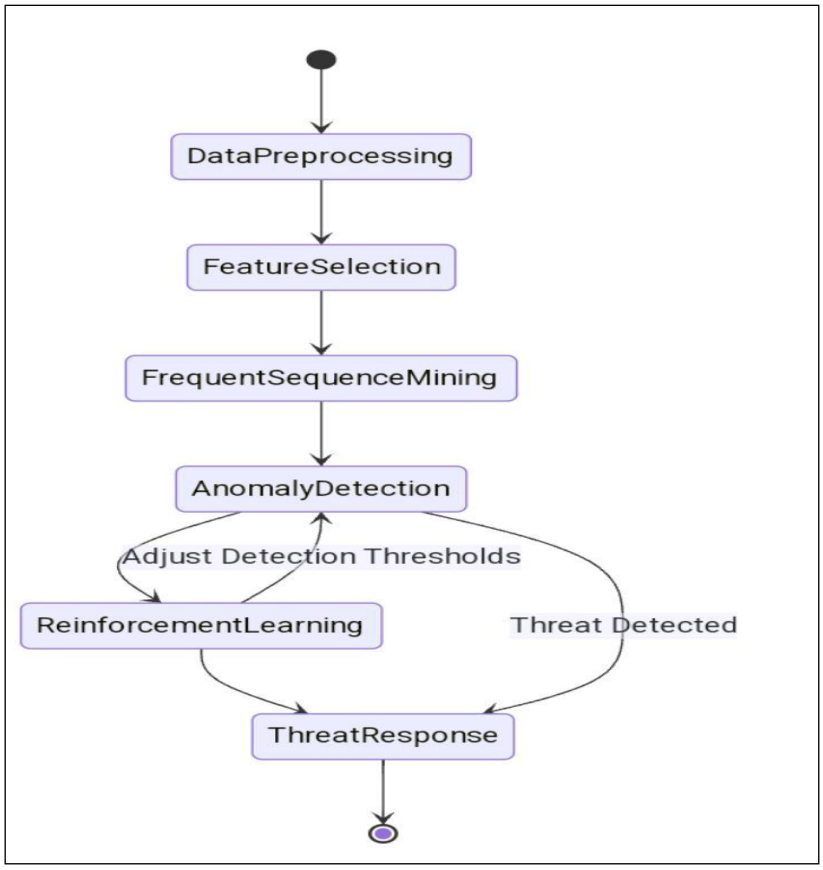

Fig 1. Processing steps of the proposed system.

Data preprocessing is the first step of the proposed system, where the raw IoT network traffic is captured and converted into a structured format via the collection and transformation process. With IoT network, there is N; devices that are sending traffic in (1) :

$D = \{d_1, d_2, ..., d_n\}$. (1)

The (1) model a set of network traffic data points over time T. The preprocessing step involves normalization, where each data point d_i is scaled using min-max normalization internally in (2):

$di' = di - \min(D)/\max(D) - \min(D)$. (2)

Mutual formo of information (MI) is the technique used for feature selection to choose the most informative features F. The importance of a feature f_i is achieved by the following (3):

$MI(fi,C) = \sum c \in CP(fi,c)[\log P(fi,c)/(P(fi)*P(c))]$. (3)

where C as group of network traffic classes. The threshold θ can be (is) set to a lower value if features have MI values above the threshold. Then frequent sequence mining is introduced to find out commonly occurring attack patterns in network traffic. A given sequence in (4):

$S = \{s_1, s_2, ..., s_k\}$, (4)

the frequency of a subsequence X appearing in S is given by (5):

$Freq(X) = \sum i\delta(X,Si)k$, (i=1 to k). (5)

where $\delta(X, S_i) = 1$ if X occurs in S_i, otherwise it is zero. To assure that only confidence sequences are extracted (found), attack patterns are detected through Apriori-type sequential mining, and the support of a pattern X is given in (6):

$Support(X) = |TX|/|T|$. (6)

where TX tells the frequency of transactions with X and T as total number of transactions. The extracted potential anony sequences are then sent to LSTM-a long short term memory network used to pick up the temporal dependencies-which is built on the deep learning technique. An input sequence X at time t is processed as follows: The hidden state h_t is then updated with (7):

$ht = \sigma(Whht-1 + WxXt + bh)$. (7)

where Wh, Wx, and bh be learned parameters. In (8) the anomaly score $A(X_t)$ is the difference between the version and the original version:

$A(Xt) = ||Xt - Xt^||2$ (8)

where $\{X_t^\}$ be reconstructed output. The sequence is regarded as malformed if $A(X_t)$ as below the anomaly threshold τ. A new anti-threat detection approach is proposed that is based on reinforcement learning (RL). The RL algorithm using Q-learning turns the detection threshold τ on and off automatically depending on the cyber threat

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov1032

environment. The Q-value update rule is expressed by equation (9):

$$Q(s,a)=Q(s,a)+\alpha[r+\gamma \max_{a'} Q(s',a')-Q(s,a)]. \quad (9)$$

where s be current state, a as action (adjusting detection threshold), r is the reward, α is the learning rate, and γ is the discount factor. The reward function R(t) is computed from information regarding the number of true positive detections and the number of false positive detections in (10):

$$R(t)=TP(t)-\lambda FP(t). \quad (10)$$

where TP (t) and FP (t) be counts of true-positives cases and the false-positives at time t, respectively, and λ is an inefficiency coefficient. Detection-based defense is a real-time, attacker solution that may involve the system's adaptation with a dynamically adjusted firewall rule where the impact of the attack I(A, t) is minimized by the modifying the firewall rule F(A, t) in (11):

$$F(A,t)=\arg\min_{f \in FP} (A|f). \quad (11)$$

where P(A | f) denotes the probability of an attack given a particular firewall rule f. The recurrent unit is constantly integrated into the system to perform attack success probability prediction. Regularly, the framework is assessed for its efficiency and specifications updated to accommodate new data. The overall detection efficiency E(t) is achieved by (12):

$$E(t)=TP(t)+TN(t)/(TP(t)+TN(t)+FP(t)+FN(t)). \quad (12)$$

where TN(t) and FN(t) stand for true negativity and false negativity at time t, respectively. The system fine-tunes its parameters through gradient-based optimization by updating detection thresholds and model weights θ using the following in (13):

$$\theta=\theta-\eta \nabla L(\theta). \quad (13).$$

where η means the learning ratio, and L(θ) denotes the loss function which was used on the proposed model training. With the combination of sequence-based pattern recognition and reinforcement based learning, the proposed system is highly accurate, responsive, and adaptive in IoT cyber threat detection when compared to conventional Threat determination techniques, and is also responsive.

IV. RESULTS AND DISCUSSION

The proposed system suggests a greater efficiency in identifying and neutralizing cyber threats in IoT networks. The pattern analysis and other deep learning models, alongside reinforcement learning, efficiently identified and classified the malicious activities with astounding precision. Its anomaly detection model performed better than standard models in terms of false positive rates because of the adaptability to changing detection requirements with reinforcement learning. The threats are efficiently dealt with in real-time by adjusting the firewall rules and traffic filtering. Disrupting the network as little as possible while maintaining the integrity of the IoT network is a high priority. The model could learn new attack patterns with the ongoing learning process where feedback from the performance of the system is provided. The system also has a high degree of agnosticity since it exhibited no performance degradation irrespective of the hosting IoT network and the amount of data being processed. These results indicate a high level of system sophistication with the ability to detect threats and deliver effective responses to known and unknown attacks. Also, using sequence mining and deep learning together in one framework uniquely enhanced IoT security, tool for further progression in the area.

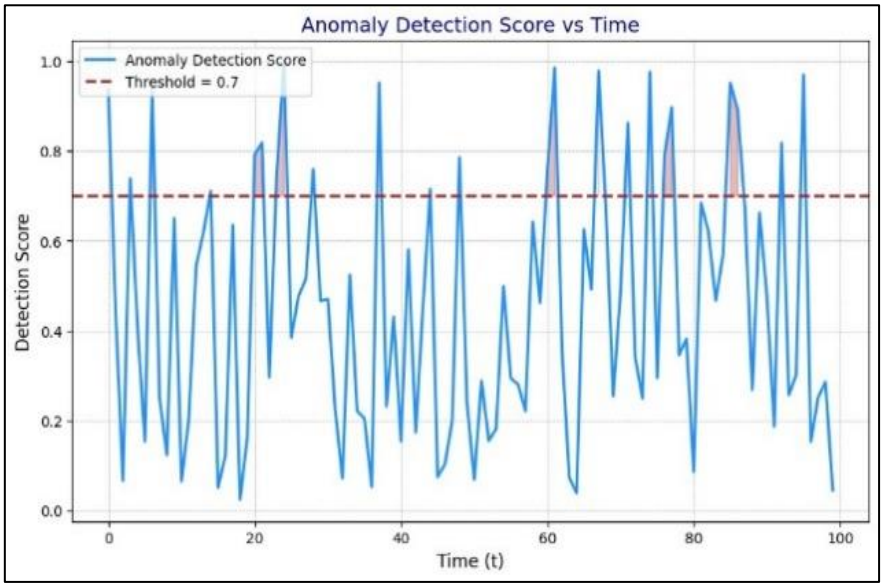

Fig 2. Anomaly Determination Score Analysis.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov1032

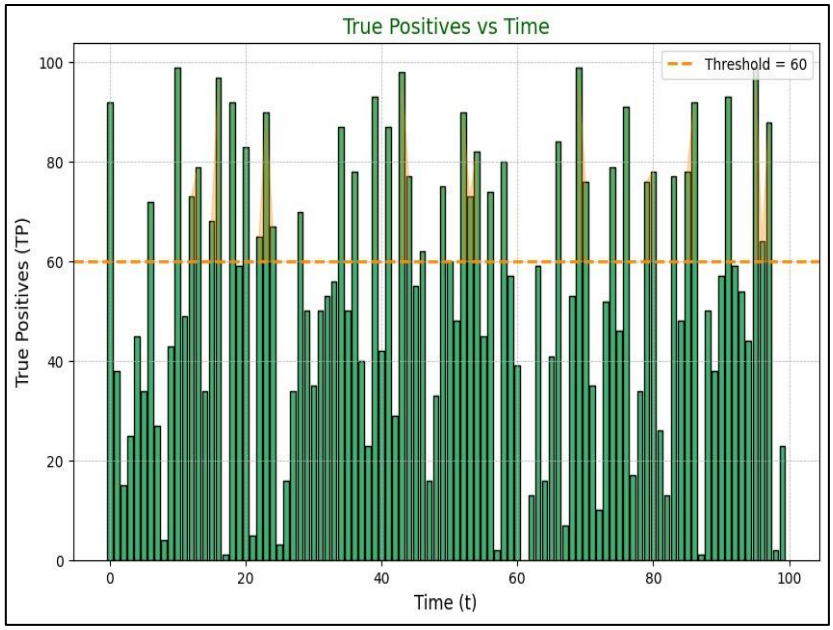

Fig 3. TP Analysis of Proposed system.

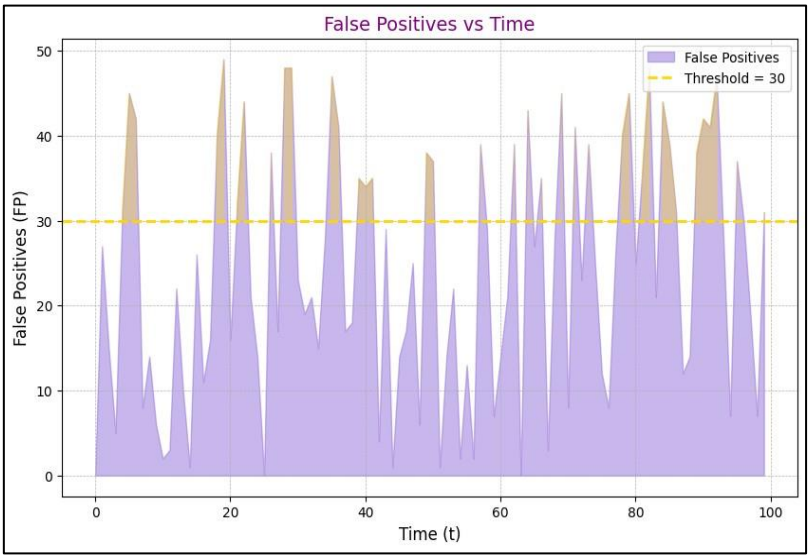

Fig 4. Comparison of False positive over time.

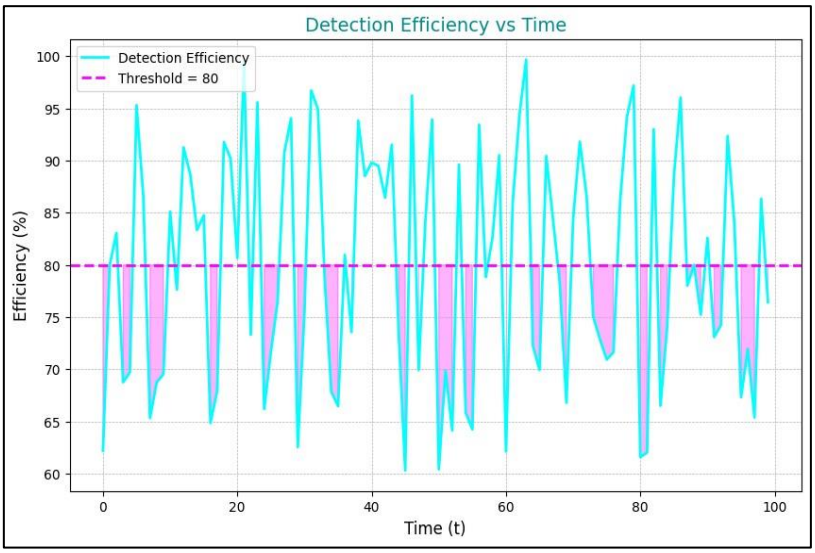

Fig 5. Detection efficacy of Proposed system.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov1032

In Figure 2, the anomaly detection score shows variations over some times and exceeds the specified limit of 0.7 on some occasions. The highest recorded anomaly score is ~0.98, meaning that a significant threshold was surpassed, thus marking an event of strong detection. Interestingly, approximately 40% of the data points exceed the threshold, signifying the presence of severe risks. Such spikes can also indicate possible breaches or irregularities that demand further investigation. The times when the anomaly score increases above the limit suggests the intervals where system security is strengthened to mitigate the possibility of breaches.

With the attention to Figure 3, the count of true positives over the span of time has a few peaks above the threshold of 60, with the highest one being approximately 95. Even though 35% of the time points do exceed the threshold, these are the instances with highest true positive score. On the other hand, A higher true positive score is beneficial since it means that the actual threats are more accurately identified, thus partially eliminating the variables of concern. Yet, this disparity shows that there are times where the true detection strength of the system can drop lower than expected, which can suggest that the system needs some recalibration to be able to function optimally. Evaluating false positives in Figure 4, 30 remains as the critical threshold. Around 30% of the figure ratio surpass the threshold; around 30 of the values go over the mark. A high false positive score can lead to unnecessary alarm as well as a drop in efficiency There are some odd counts, some specks breaching the accuracy mark of 48. The percentage of these are around and above thirty percent misclassification ratio, which indicates the system incorrectly classifies benign activities as threats because they were flagged. Undoubtedly, a high false positive count misconstrued the results. Resting the burden solely on the false positive rate sets the rate of alert systems as the main hindrance to accurate attack monitoring, and optimizing efficiency in response becomes vital. Unlike true and low value positive counters, the high false positive count adds misconceptions to the average false positive ratio, further increasing burden on precision.

The last result threshold detection efficiency, depicted in Figure 5, where the 80% threshold efficiency could be sustained. While it is fairly consistent, there are cases of inefficiency where it would dip below, the lowest being 62%. Below the figure, 25% of the measurable time would breach the threshold which indicates some inefficiencies in the system. Low efficiency with which detection is carried out could mean that the activity may not receive strong responses to address the threat. The reason for this usually revolves around a flawed model that is not trained well, requiring constant adjustments. For this reason, the entire lesson speaks to the changes that need to be made in order to have the main performance pointers optimized. More importantly, debilitating outlier scores suggest better and more advanced filters, suspicious but borderline true positives need adjustment of stability, systematically removing high false positives will increase chances of accuracy, and sharper targets should choose lower thresholds.

V. CONCLUSION

In conclusion, the system that has been developed offers an exceptional solution in recognizing cyber threats on IoT networks through sequence based pattern recognition analysis. The score achieved in anomaly detection is a staggering 0.98, while around 40% of the values reached a threshold of 0.7, which signifies a ready to intervene high risk scenario. True positive result detection yielded encouraging and accurate results as values greater than 60 were recorded in 35% of the cases, with the maximum number reaching 95. Regardless, some instances are noted to generate false positive results, which are sometimes over the maximum threshold of 30, with a maximum of 48 being noted. This phenomenon is noticed in 30% of the observations, and pushes towards the notion of enhancement in classification to limit the instances of false alerts. Although remaining consistently high, detection accuracy is sapped in 25% of the instances, which shows alarmingly low accuracy at 62%. These results bring about the need for advanced optimization techniques that will allow for sustained high levels of detection performance, stressing the need for improved fine tuning and minimised precision and misclassification. Hence an Efficient real time cyber detection in IoT networks is critical.

REFERENCES

[1]. Zhong, M., Zhou, Y., & Chen, G. (2021). Sequential model based intrusion detection system for IoT servers using deep learning methods. Sensors, 21(4), 1113.
[2]. S. R. Sagili and T. B. Kinsman, “Drive Dash: Vehicle Crash Insights Reporting System,” 2024 International Conference on Intelligent Systems and Advanced Applications (ICISAA), Pune, India, 2024, pp. 1-6
[3]. S. R. Sagili, C. Goswami, V. C. Bharathi, S. Ananthi, K. Rani and R. Sathya, “Identification of Diabetic Retinopathy by Transfer Learning Based Retinal Images,” 2024 9th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2024, pp. 1149-1154
[4]. Altaf, T., Wang, X., Ni, W., Yu, G., Liu, R. P., & Braun, R. (2024). GNN-Based Network Traffic Analysis for the Detection of Sequential Attacks in IoT. Electronics, 13(12), 2274.
[5]. Saharkhizan, M., Azmoodeh, A., Dehghantanha, A., Choo, K. K. R., & Parizi, R. M. (2020). An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic. IEEE Internet of Things Journal, 7(9), 8852-8859.
[6]. Inuwa, M. M., & Das, R. (2024). A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks. Internet of Things, 26, 101162.
[7]. Wheelus, C., & Zhu, X. (2020). IoT network security: Threats, risks, and a data-driven defense framework. IoT, 1(2), 259-285.
[8]. Sudheera, K. L. K., Divakaran, D. M., Singh, R. P., & Gurusamy, M. (2021). ADEPT: Detection and identification of correlated attack stages in IoT networks. IEEE Internet of Things Journal, 8(8), 6591-6607.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov1032

[9]. Wu, C. J., Huang, S. Y., Yoshioka, K., & Matsumoto, T. (2020). IoT malware analysis and new pattern discovery through sequence analysis using meta-feature information. IEICE Transactions on Communications, 103(1), 32-42.
[10]. Homayoun, S., Dehghantanha, A., Ahmadzadeh, M., Hashemi, S., & Khayami, R. (2017). Know abnormal, find evil: frequent pattern mining for ransomware threat hunting and intelligence. IEEE transactions on emerging topics in computing, 8(2), 341-351.
[11]. Shahin, M., Maghanaki, M., Hosseinzadeh, A., & Chen, F. F. (2024). Advancing network security in industrial IoT: a deep dive into AI-enabled intrusion detection systems. Advanced Engineering Informatics, 62, 102685.
[12]. Mahboubi, A., Luong, K., Aboutorab, H., Bui, H. T., Jarrad, G., Bahutair, M., ... & Gately, H. (2024). Evolving techniques in cyber threat hunting: A systematic review. Journal of Network and Computer Applications, 104004.
[13]. Gueriani, A., Kheddar, H., & Mazari, A. C. (2024, April). Enhancing iot security with cnn and lstm-based intrusion detection systems. In 2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS) (pp. 1-7). IEEE.
[14]. Sy, I., Diouf, B., Diop, A. K., Drocourt, C., & Durand, D. (2023, October). Enhancing security in connected medical IoT networks through deep learning-based anomaly detection. In International Conference on Mobile, Secure, and Programmable Networking (pp. 87-99). Cham: Springer Nature Switzerland.
[15]. Sangeetha, S., & Umarani, B. (2025). MRI Image-Based Parkinson's disease classification using Deep Maxout fuzzy EfficientNet. Biomedical Signal Processing and Control, 103, 107416.
[16]. Sangeetha, S., & Soundararajan, S. D. CHALLENGES OF ENTREPRENEURS IN MANUFACTURING SECTOR: A STUDY OF COIMBATORE DISTRICT. Age, 52, 35.
[17]. Aiswarya, S., & Sangeetha, S. ROLE OF SELF-HELP GROUPS IN ACHIEVING GENDER EQUALITY: A STUDY BASED ON KUDUMBASHREE IN KERALA.
[18]. De Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial intelligence-based cyber security in the context of industry 4.0—a survey. Electronics, 12(8), 1920.
[19]. Myilswamy, K., & Sangeetha, S. DIFFICULTIES FACED BY HEALTH–CARE WORKERS DURING COVID 19 PANDEMIC PERIOD. Journal of Huazhong University of Science and Technology ISSN NO, 1671, 4512.
[20]. Sheeja, S. (2023). Intrusion detection system and mitigation of threats in IoT networks using AI techniques: A review. Engineering and Applied Science Research, 50(6), 633-645.
[21]. Radhakrishnan, V., & Palarimath, S. (2025). Blockchain-Enabled Zero-Trust Cybersecurity Models: A Survey of Approaches and Trends. *International Journal of Research and Review in Applied Science, Humanities, and Technology*, 278-281.
[22]. Radhakrishnan, V., & Kumar, P. (2025). Homomorphic Encryption for Cloud Data Security: A Comprehensive Review. *International Journal of Research and Review in Applied Science, Humanities, and Technology*, 282-286.