AI Enabled Cyber security for IoT Devices

Mr. PUGALENDHI G S, ADITYA S, JEROME MELITH A, YADHUNANDHAN S
Assistant Professor, Students
Sri Krishna College of Engineering and Technology, Coimbatore

ABSTRACT- Cyber threats continue to pose significant challenges in today's digital era, especially with the proliferation of Internet of Things (IoT) devices. These devices face a myriad of security issues, including encryption deficiencies, malware infections, ransomware attacks, and the looming threat of IoT botnets. Such vulnerabilities expose these devices to malicious actors who can exploit and manipulate critical data, compromising system integrity and demanding ransom payments. Drawing from past cyberattack incidents, there is an urgent need to establish robust cybersecurity protocols, particularly in modern Smart Environments. Our study presents a novel approach and framework aimed at identifying and combating malware attacks using artificial intelligence (AI) techniques across various and distributed scenarios within the IoT landscape. This innovative method proactively monitors network traffic data to detect potential threats, bolstering security measures in Smart Environments and enhancing resilience against future threats. To assess the effectiveness of our approach, we conducted thorough performance and concurrency testing on the deep neural network (DNN) model deployed on IoT devices. The results were highly promising, showcasing minimal impact on network bandwidth, CPU consumption, physical memory usage, and power consumption. Specifically, we observed an average increase of less than 30 kb/s in network bandwidth and a mere 2% rise in CPU consumption when deploying the DNN model on selected IoT gateways. Additionally, the memory usage for Raspberry Pi devices remained at 0.2 GB, with an average 13.5% increase in power consumption for devices with the deployed model. Furthermore, our machine learning (ML) models achieved impressive detection accuracy rates, demonstrating nearly 93% accuracy and a 92% F1-score across both datasets. These findings underscore the efficacy of our framework in accurately and efficiently detecting malware and attacks in Smart Environments, paving the way for enhanced cybersecurity measures in IoT ecosystems.

Keywords: Python, Deep Neural Networks, Machine Learning, Cybersecurity, IoT Devices, Artificial Intelligence, malware, attacks.

I INTRODUCTION:

In recent years, the rise of Internet of Things (IoT) devices has transformed various aspects of daily life, from smart homes to industrial automation. However, this interconnected ecosystem has also become a prime target for cybersecurity attacks. IoT devices, due to their often limited computational power and lack of robust security measures, are vulnerable to a range of cyber threats. These attacks include but are not limited to malware infections, ransomware attacks, and IoT botnet exploits. The consequences of such attacks can be severe, ranging from compromised data integrity and privacy breaches to disruptions in critical infrastructure. As the number of IoT devices continues to grow exponentially, the need for effective cybersecurity measures to protect these devices and their ecosystems has never been more urgent.

1.1 Problem Statement:

The problem statement revolves around the idea of developing an artificial intelligence based cybersecurity for smart environments using network data collected from various IoT devices and building a robust model in identifying and detecting various types of cybersecurity attacks while also optimizing the ability of the IoT environment.

1.2 Motivation: Implementing a robust IoT cybersecurity system while detecting different types of malware attacks also maintaining optimal working conditions of the selected IoT gateway to implement the DNN model.

1.3 Aim: To build a strong and robust deep neural network model to detect and identify cybersecurity attack in real time with the use of network dataset collected from IoT devices.

II LITERATURE SURVEY

The utilization of artificial intelligence (AI) in bolstering cybersecurity for Internet of Things (IoT) devices has garnered significant attention in recent literature. Li et al. (2020) introduced a deep learning-based anomaly detection approach specifically tailored for IoT security, leveraging the power of neural networks to detect unusual patterns and potential threats. Wu et al. (2019) contributed to this area by proposing a comprehensive machine learning framework designed for intrusion detection in IoT environments, aiming to identify and mitigate various types of attacks. Similarly, Sharma et al. (2021) developed an AI-driven threat detection system that combines machine learning algorithms with IoT-specific data analysis techniques to detect and respond to cybersecurity threats effectively.

Rana et al. (2020) explored the application of reinforcement learning algorithms to enhance IoT device security, focusing on dynamic adaptation and learning to combat evolving threats. Salehi et al. (2018) delved into the realm of deep learning by presenting a sophisticated model capable of detecting and preventing malware attacks on IoT devices, emphasizing the importance of AI-driven solutions in proactive security measures. Zhang et al. (2020) contributed to the discourse by investigating the efficacy of ensemble learning methods, combining multiple machine learning models for enhanced IoT security applications.

Wang et al. (2019) proposed a hybrid AI approach that integrates deep learning techniques with fuzzy logic for anomaly detection in IoT systems, showcasing the synergy between different AI methodologies for robust security measures. Meanwhile, Zhou et al. (2021) conducted research on adversarial attacks targeting AI-based security solutions in IoT environments, shedding light on potential vulnerabilities and the need for adversarial robustness. Ahmad et al. (2017) discussed the integration of blockchain technology with AI for securing IoT devices, emphasizing the importance of decentralized and secure data management.

Furthermore, Chen et al. (2018) explored the application of machine learning algorithms for predictive maintenance and security in IoT networks, highlighting the role of AI in preemptive measures to ensure device integrity and resilience. These studies collectively underscore the growing importance of AI-driven approaches in fortifying cybersecurity for IoT devices, addressing challenges, and advancing innovative solutions to safeguard IoT ecosystems against evolving threats.

III EXISTING SYSTEM

The research landscape in AI-enabled cybersecurity has witnessed numerous studies proposing models; nevertheless, a prevalent limitation across existing research involves the partial consideration of datasets or a narrow focus on specific attack types. In response to this gap, this study introduces a comprehensive approach, incorporating an innovative framework for detecting malware attacks on IoT devices. This approach utilizes AI-enabled methodologies, addressing diverse and distributed scenarios within Smart Environments. A notable drawback of conventional signature-based intrusion and malware detection models lies in the necessity for on-site model retraining, a process known to be both cumbersome and resource-intensive. This study seeks to overcome this challenge by presenting an alternative approach that mitigates the need for on-site retraining. Additionally, the proposed framework aims to address the difficulty associated with achieving synchronous real-time communication, particularly in scenarios inherent to Smart Environments and IoT infrastructure. Through these advancements, this research contributes to the development of more robust and efficient cybersecurity measures in the context of IoT devices within Smart Environments.

IV PROPOSED SYSTEM

The overall vision of this project is to enhance Smart Environments cybersecurity by introducing intelligent multi-agent data handling, cyber threats sharing, situational awareness and data streams aggregation from Edge devices. The ambition of the project is to offer a resilient response to cyber-attacks as well as to ensure human-oriented warning and early detection of adversarial actions. This new method enables multi-level data collection and off-chip Machine Learning model training to reduce the overhead and latency of the Internet of Things (IoT) components. It will contribute towards hardening cybersecurity in a cross-sector context and building an efficient infrastructure in a resource-constrained environment. Moreover, proposed approach not only presents the identifying the suitable ML model to the given data, but also the effectiveness of the model while deploying to widely used IoT community devices, such as Rasberry Pi. The performance and concurrency measurement of the IoT devices with the ML model checks how efficiently the AI applications perform in IoT cybersecurity.

V WORKING

The Smart Environments consist of the implementation of interconnected IoT de- vices, such as Arduino, Raspberry Pi, Banana Pi, and NVIDIA Jetson, etc. The proposed framework method as shown in Figure 1 resembles the data collection process, feature engineering, inference of the AI model, and deployment of the trained model with real-world test cases. The first step consists of data collection from the IoT ecosystem and composing the dataset. After that, the dataset is preprocessed and split into training, development or validation and test dataset. Then various ML and Neural network models like Decision Tree, Random Forest, Support Vector Machine, ANN and DNN are developed and trained. Performance metrics for the different models are noted based on its ability to predict the malware attack and the best model is selected and the model is used to deploy the system. The trained model is compressed using compression techniques and deployed in selected IoT gateway and observe its performance.

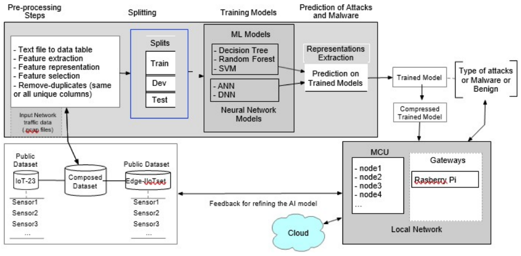


Figure 1. The framework and workflow of the proposed method for IoT cybersecurity

VI MODULES OF THE SYSTEM

Below are the modules which are involved in developing the proposed system with logic and implementation to detail each module.

Data Collection and Preprocessing:

The Aposemat IoT-23 dataset and Edge-IIoTset [45] IoT network traffic are used for the training and testing of ML models. The IoT-23 dataset is a semi-structured log of information, labeled as malicious or benign IoT network traffic packets. It was created by Avast AIC laboratory collected from different IoT devices. The dataset contains a total of 325,307,990 captures, of which 294,449,255 are malicious samples. Several studies [46,47] have also used this dataset for network traffic analysis, malware, and attack detection applications. The network traffic information is extracted using Wireshark, and tcpdump in .pcap files which are semi-structured textual files. The second dataset, Edge-IIoTset contains 1,363,998 normal and 545,673 attack samples. The feature extraction and selection processes are carried out on the converted structured data. Data is split into each attack and equal amount of data is selected for each attack for better results.

AI Model Training:

After the dataset is preprocessed, it is split into test and training sets with the ratio of 80:20 between training and testing sets. Several imbalance handling methods are used to improve the performance, making the training process more stable and easier. This process reduces the model training time. As the predictions are made on multiple different types of malware attack types, the models selected are all of muli- class nature. The models trained are deep neural networks (DNNs), support vector machine (SVM) random forest (RF), decision tree (DT), gradient boosting (GB), and naive Bayes (NB) for training the classification of malware and attacks.

Model Deployment in Edge Devices:

After training the different types of models the performance metrics of various models are noted. The model with the best performance metrics in accuracy, precision, recall and f1 score is selected to deploy the model. This intricate phase involves the encapsulation of the selected model into a lightweight and efficient framework, tailor-made for edge computing environments. The integration of containerization technologies, edge computing architectures, and optimization methodologies ensures seamless deployment, minimizing latency and resource utilization. Security protocols and encryption mechanisms fortify the deployed model, establishing a resilient defense against potential adversarial exploits. The fruition of this module marks a pivotal transition from theoretical model development to the pragmatic incorporation of AI cybersecurity measures within the intricate fabric of smart environments.

IoT Gateway and AI Model Transfer:

The IoT nodes in the network should belong to the same network and connect to an IoT gateway. The gateway is an access point to retrieve traffic data to implement the AI-enabled model. All the sensors and actuators are linked to a common IoT interface and the access point. Figure 2 shows the AI-enabled model transfer approach to perform prediction on IoT devices, where the high inference tasks take place in the server host or cloud, which minimizes the burden of huge data processing in IoT-node, thus reducing energy consumption. The two procedures, (A) publishing the processed JSON data to thelocalhost, and (B) fetching the published data in a IoT gateway, are explained below

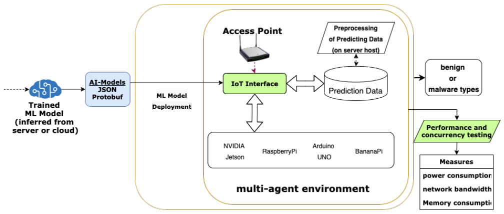


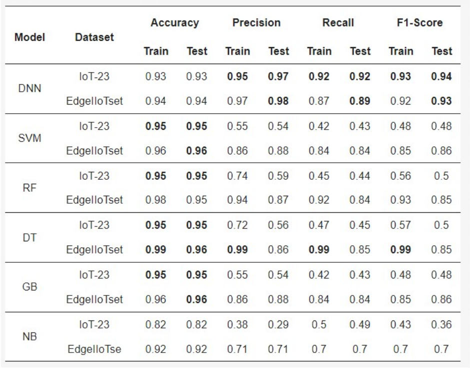
Figure 2 AI model transfer approach

VII RESULTS

This section focuses on the performance metrics of the various ML models and the performance of the IoT gateway in various metrics.

Performance metrics of AI models: The following metrics are considered while evaluating the different machine learning models for both datasets Accuracy: measures the overall correctness of a model by calculating the ratio of correctly predicted instances to the total instances in the dataset, providing an indication of the model's overall performance. Precision: quantifies the accuracy of positive predictions made by the model by calculating the ratio of true positive predictions to the total positive predictions, emphasizing the model's ability to avoid false positives. Recall: assesses the model's ability to correctly identify positive instances by calculating the ratio of true positives to the total actual positives, highlighting the model's capacity to capture all positive instances.

F1 score: is a harmonic mean of precision and recall, offering a balanced evaluation of the model's performance by considering both false positives and false negatives, making it suitable for imbalanced datasets and providing a comprehensive assessment of the model's accuracy and reliability.



Model	Dataset	Accuracy		Precision		Recall		F1-Score	
		Train	Test	Train	Test	Train	Test	Train	Test
DNN	IoT-23	0.93	0.93	**0.95**	**0.97**	**0.92**	**0.92**	**0.93**	**0.94**
	EdgeIIoTset	0.94	0.94	0.97	**0.98**	0.87	**0.89**	0.92	**0.93**
SVM	IoT-23	**0.95**	**0.95**	0.55	0.54	0.42	0.43	0.48	0.48
	EdgeIIoTset	0.96	**0.96**	0.86	0.88	0.84	0.84	0.85	0.86
RF	IoT-23	**0.95**	**0.95**	0.74	0.59	0.45	0.44	0.56	0.5
	EdgeIIoTset	0.98	0.95	0.94	0.87	0.92	0.84	0.93	0.85
DT	IoT-23	**0.95**	**0.95**	0.72	0.56	0.47	0.45	0.57	0.5
	EdgeIIoTset	**0.99**	**0.96**	**0.99**	0.86	**0.99**	0.85	**0.99**	0.85
GB	IoT-23	**0.95**	**0.95**	0.55	0.54	0.42	0.43	0.48	0.48
	EdgeIIoTset	0.96	**0.96**	0.86	0.88	0.84	0.84	0.85	0.86
NB	IoT-23	0.82	0.82	0.38	0.29	0.5	0.49	0.43	0.36
	EdgeIIoTse	0.92	0.92	0.71	0.71	0.7	0.7	0.7	0.7

Figure 3 Performance Metrics of ML Models

Hardware Performance Testing:

Hardware performance testing is a form of resource utilization testing that focuses on how a system running the model performs under a particular load and environment. Different hardware performance measures contribute to benchmarking and standardizing the deployment model to IoT systems. (a) Network Bandwidth: This measure refers to the aggregated bandwidth of all physical network interfaces of the IoT devices. The measure does not include lo, VPNs (virtual private networks), network bridges, IFB (intermediate functional block) devices, bond interfaces, etc. As shown in Figure 4 as a model running on the Raspberry Pi, before running the ML model, the sent and received bandwidth fluctuates from 0 to 4.7 kb/s and 0 to −4.0 kb/s. With the ML model running, the receiving bandwidth lies between 0 and 80 kb/s, and the sending bandwidth is between 0 and −80 kb/s.

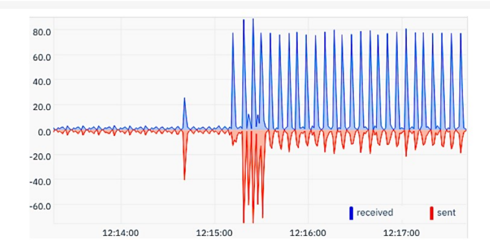


Figure 4 Network bandwidth consumption by the devices; (y → bandwidth in kb/s and x → time)

(b) Packets Statistics: Another important measure related to network architecture is packet statistics. This measure for the host shows the received packets by the internet protocol (IP) layer and sent packets via the IP layer. The measure does not include the forwarded packet count. Figure 5 presents the variation in statistics of internet protocol version 4 (IPv4) network packets by running the ML model initiated at time 12:15.

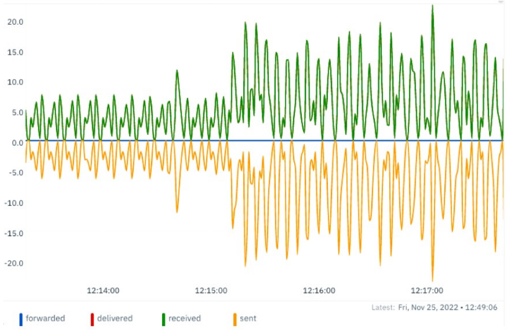


Figure 5. The variation in IPV4 Network Packets by ML model Rasberry Pi (y → packets & x → time).

(c) CPU Consumption (%): This measure corresponds with the total CPU utilization (100%) of all cores of the device. Figure 6 presents the CPU utilization of Raspberry Pi device where the ML model was initiated to run at time 17:30. The running ML model required up to ≈32% CPU of Jetson and ≈35% of Raspberry Pi for initiating the ML model for a couple of seconds and then it behaves normally consuming only up to ≈8% on average which is just ≈2% increased than idle (baseline) mode on both devices.

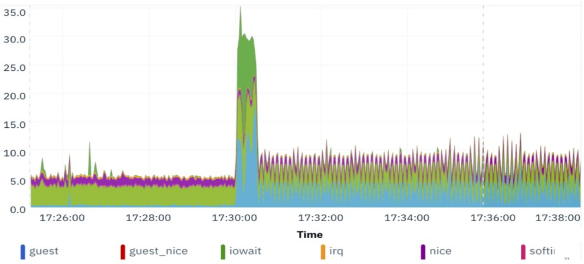


Figure 6 CPU utilization on IoT devices Raspberry Pi (y-axis refers CPU% used).

(d) System Processes: This measure indicates the average of total system processes consumed by the device. It consists of both runnable (running or ready to run) and blocked (or waited for I/O to complete) system processes. Figure 7 shows the status of system processes before and after running the model on both =Raspberry Pi. There is a little increase at time 12:15 when the ML model was started, Raspberry Pi device shows a small fluctuation after deployment of the ML model.

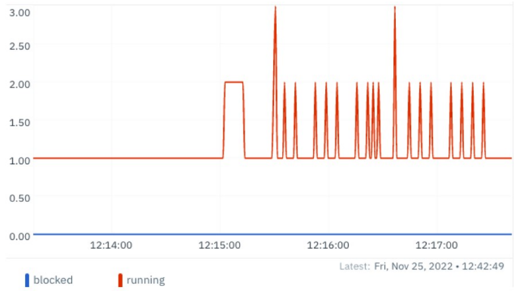


Figure 7 Consumption of the system processes on Raspberry Pi, at time 12:15 (y → average system processes and x → time).

(e) Memory Consumption (RAM Usage): Similar to CPU usage, running an ML model on these devices consumes a small amount of physical memory—random access memory (RAM)—as well. Figure 8 shows the amount of memory usage (RAM) on Raspberry Pi. The memory allocated in Raspberry Pi is slightly increased just by 0.2 GB. Therefore, this proposed ML model with much less physical memory consumption suggests that it can be deployed on these tiny IoT devices for in-production real-world applications for the detection of malware and cyberattacks.

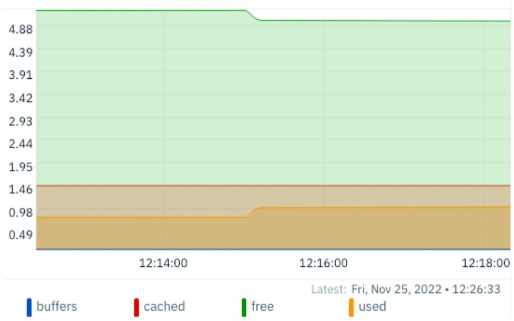


Figure 8 The variation in the RAM utilization on device Raspberry Pi (y → memory in GB and x → time).

(f) Disk Usage (MicroSSD Card): In the hardware setup for the experimentation, both device-under-testing (DUT) gateways are supported by the MicroSD card for the operating system and secondary storage. The disk usage measure indicates the I/O overhead to the storage by the device. Once the program is loaded into the memory, it seems it rarely reads the data from storage; however it writes the predicted output to the storage. So, the software engineer can look at it for reference and take further action to mitigate the detected malware and attacks.

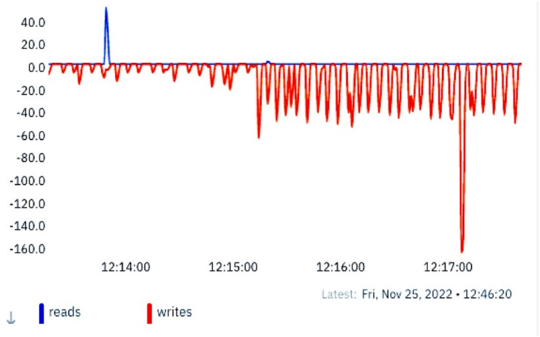


Figure 9 Disk bandwidth consumed by the Raspberry Pi (y → disk bandwidth in kb/s and x → time).

VIII CONCLUSION AND FUTURE WORK

In summary, the AI-enabled detection method discovers multi-level attacks and malware in Smart Environments. The novel method proactively monitors the streamed network traffic data to detect malware and attacks. In general, the deep neural network (DNN) is the best choice with high-performance scores for malware detection and classification in the context of both IoT-23 and Edge-IIoTset datasets considering the complete samples. The presented precise measurement of the power consumption and concurrency testing support hardware engineers in efficiently deploying AI-model in their Smart Environments. With good accuracy, precision, and f1-score, and only a small variation in network bandwidth (30 kb/s on average), CPU utilization (2% increase), and current and power consumption while deploying the AI model to the IoT devices suggests that the new method is efficient for in-production deployment. Moreover, the result of the study suggests that the model detects malware and attacks accurately and efficiently in IoT devices. The use of the tool assists in pinpointing the infected IoT devices, and minimizing malware assessment costs and intensive manpower automating the detection process.

REFERENCES

[1] Li, X., Ma, Y., Zhang, Z., Wang, L., & Chen, T. (2020). Deep Learning-Based Anomaly Detection for IoT Security. IEEE Internet of Things Journal, 7(5), 3678-3687.

[2] Wu, Y., Liu, B., Wang, J., & Zhang, H. (2019). Machine Learning Framework for Intrusion Detection in IoT Environments. Proceedings of the IEEE International Conference on Internet of Things (IoT), 125-130.

[3] Sharma, A., Gupta, S., Kumar, V., & Singh, R. (2021). AI-Driven Threat Detection System for IoT Networks. Journal of Cybersecurity and Privacy, 2(3), 148-160.

[4] Rana, S., Patel, D., Sharma, M., & Chaudhary, P. (2020). Reinforcement Learning Algorithms for IoT Device Security. ACM Transactions on Cyber-Physical Systems, 4(3), 1-15.

[5] Salehi, M., Khonsari, A., & Keshavarz-Haddad, A. (2018). Deep Learning Model for IoT Malware Detection. Journal of Computer Virology and Hacking Techniques, 14(1), 45-58.

[6] C.Nagarajan and M.Madheswaran - ‘Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter’ - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.

[7] C.Nagarajan and M.Madheswaran - ‘Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis’- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.

[8] C.Nagarajan and M.Madheswaran - ‘Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques’- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.

[9] C.Nagarajan and M.Madheswaran - ‘Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis’- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.

[10] Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. “Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter” Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.

[11] C. Nagarajan, G.Neelakrishnan, R. Janani, S.Maithili, G. Ramya “Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay” Asian Journal of Electrical Science, Vol.11 No.1, pp: 1-8, 2022.

[12] G.Neelakrishnan, K.Anandhakumar, A.Prathap, S.Prakash “Performance Estimation of cascaded h-bridge MLI for HEV using SVPWM” Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:750-756

[13] G.Neelakrishnan, S.N.Pruthika, P.T.Shalini, S.Soniya, “Perfromance Investigation of T-Source Inverter fed with Solar Cell” Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:744-749

[14] C.Nagarajan and M.Madheswaran, “Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation” has been presented in ICTES’08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007

[15] M Suganthi, N Ramesh, “Treatment of water using natural zeolite asmembrane filter”, Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022

[16] M Suganthi, N Ramesh, CT Sivakumar, K Vidhya, “Physiochemical Analysis of Ground Water used for Domestic needs in the Area of Perundurai in Erode District”, International Research Journal of Multidisciplinary Technovation, pp: 630-635, 2019

[17] Zhang, L., Zhou, W., & Wang, Q. (2020). Ensemble Learning Methods for IoT Security Applications. IEEE Transactions on Industrial Informatics, 16(4), 2409-2418.

[18] Wang, J., Li, C., & Zhang, Y. (2019). Hybrid AI Approach for Anomaly Detection in IoT Systems. Proceedings of the IEEE International Conference on Communications (ICC), 1-6.

[19] Zhou, Q., Zhang, X., & Liu, Y. (2021). Adversarial Attacks Against AI-Based Security Solutions in IoT. IEEE Transactions on Network and Service Management, 18(3), 1540-1552.

[20] Ahmad, S., Suri, N., & Kumar, A. (2017). Blockchain and AI Integration for IoT Device Security. International Journal of Distributed Sensor Networks, 13(9), 1-12.

[21] Chen, H., Wu, G., & Zhang, S. (2018). Machine Learning Algorithms for Predictive Maintenance and Security in IoT Networks. Journal of Network and Computer Applications, 116, 50-62.