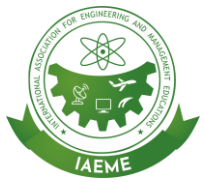
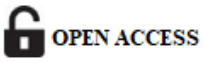
International Journal of Electrical Engineering and Technology (IJEET)
Volume 15, Issue 4, July-August 2024, pp. 1-15, Article ID: IJEET_15_04_001
Available online at https://iaeme.com/Home/issue/IJEET?Volume=15&Issue=4
ISSN Print: 0976-6545 and ISSN Online: 0976-6553
Impact Factor (2024): 18.11 (Based on Google Scholar Citation)





DEVELOPING ROBUST CYBER SECURITY PROTOCOLS FOR IOT NETWORKS USING AI

Harish Narne
Application Engineer, UiPath Inc., USA.

ABSTRACT

The exponential expansion of the IoT ecosystem has sparked major cybersecurity worries, despite the fact that it offers unmatched connectivity and ease. The inherent computational limits, extensive distribution, and the heterogeneity of IoT devices are a few of the elements that give rise to these challenges. It is critical to incorporate new technologies into the constantly evolving IoT landscape in order to address these difficulties. Concerning the security of the Internet of Things (IoT), the quickly developing field of machine learning (ML) holds great potential. The widespread use of Internet of Things (IoT) devices has increased cyber dangers in the modern digital age. The Internet of Things (IoT) presents a variety of security risks to these devices, such as encryption, malware, ransomware, and botnets. ttackers can compromise system integrity and demand ransom payments by exploiting and manipulating critical data, which these devices are vulnerable to. Building on lessons learnt from previous cyberattacks, strong cybersecurity protocols are critically important, especially in today's Smart Environments. Our research introduces a new methodology and framework for detecting and countering malware threats in the IoT ecosystem utilising AI approaches in a variety of dispersed contexts. Enhancing security measures in Smart Environments and making them more resilient against future threats, this unique technology proactively monitors network traffic data to detect potential dangers. In order to determine how effective our method was, we ran extensive performance and concurrency tests on the deep neural network (DNN) model that was running on IoT devices. The results showed that there was little effect on power consumption, CPU utilisation, physical memory usage, and network bandwidth, which was very encouraging. When we implemented the DNN model on some IoT gateways, we found that the network bandwidth increased by less than 30 kb/s and that the CPU consumption increased by barely 2%. In addition, the implemented model resulted in an average 13.5% increase in power consumption, even if the memory utilisation for Raspberry Pi devices stayed at 0.2 GB. Not only that, but our ML models showed off some rather impressive detection accuracy rates—roughly 93% accuracy on both datasets and an F1-score of 92%. Our technique successfully identifies dangers in Smart Environments, leading to improved cybersecurity in IoT ecosystems.

Keywords: Smart Environments, IoT ecosystems, cybersecurity.

Cite this Article: Harish Narne. Developing Robust Cyber Security Protocols for IoT Networks Using AI. International *Journal of Electrical Engineering and Technology (IJEET)*, 15(4), 2024, pp. 1-15.

https://iaeme.com/MasterAdmin/Journal_uploads/IJEET/VOLUME_15_ISSUE_4/IJEET_15_04_001.pdf

1. INTRODUCTION

The Internet has not altered your life, as Brendan O'Brien wisely pointed out. "Things are about to change drastically due to the Internet of Things!" [1]. This is true since the Internet of Things has indeed brought forth unprecedented connectivity. Improvements in sensor technology, wireless connectivity, and data analytics have led to an exponential growth in the number of connected devices. Connectivity is now easier and more pervasive than ever before thanks to the Internet of Things (IoT), which is sweeping across many sectors, towns, and homes. Actuators and sensors are the backbone of the IoT, as they gather information from the real world and transform it into digital signals.

The ability to monitor and operate several systems and processes in real-time is made possible by these little devices that collect a wide variety of data. Nevertheless, numerous security concerns have been introduced by the fast expansion and deep incorporation of IoT devices into daily life. The security and dependability of this growing ecosystem depend on these problems being thoroughly resolved. Internet of Things (IoT) devices come in all shapes and sizes, and their security features and protocols might be all over the place, creating a disjointed ecosystem full of potential entry points for hackers. Internet of Things devices are often vulnerable to breaches and exploitation because they put user ease and low cost ahead of security. Data breaches, Distributed Denial-of-Service (DDoS) assaults, and malware infections are just a few of the cyber dangers that these systems face.

The data these devices manage is extremely sensitive, and any security breach might have a major impact on privacy and important infrastructure systems. On top of that, security flaws might have a domino effect because hackers could use IoT devices as a foothold to access bigger networks. The safety of data transmissions between networks and Internet of Things devices is another major concern since a lot of these devices employ wireless communication protocols that can be easily intercepted or manipulated.

Some Internet of Things (IoT) devices may lack the resources to implement modern encryption and authentication methods, making these vulnerabilities much more severe. Managing security patches and upgrades becomes even more challenging due to the extensive deployment and lengthy lifespan of IoT devices, as many devices may not receive updates frequently or be impossible to reach for maintenance.

This could worsen security risks by increasing the number of devices that are obsolete or insecure [2].

Machine learning (ML) has arisen as a powerful tool for improving and strengthening IoT security in response to these security challenges.

Security measures need to be increasingly advanced to keep up with the growing complexity of IoT networks. Machine learning (ML) can provide the necessary intelligence by utilising complex algorithms and insights obtained from collected data.

It does this by constantly scanning the environment for trends, looking for unusual occurrences, and making predictions about impending danger. Because of this capabilities, we can respond proactively to security holes and incursions [3]. Figure 1 shows one example of this type of setup.

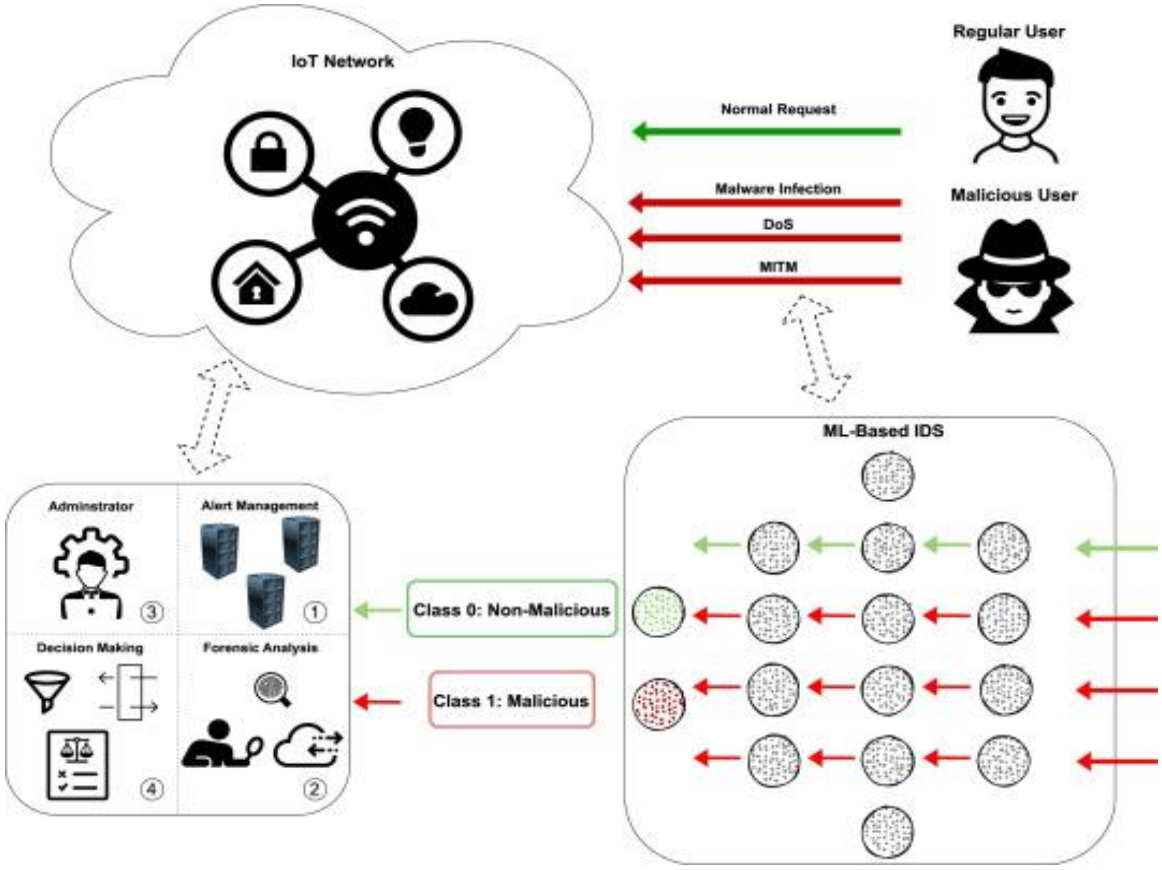


Fig. 1. Cyber threat detection using an environment based on machine learning.

Anomaly detection stands out among the several machine learning applications utilised to guarantee the security of the Internet of Things.

Through analysis of IoT device, network, and communication channel behaviour, machine learning algorithms seek out typical patterns of operation.

These algorithms can quickly identify suspicious activity by establishing a baseline for usual behaviour and then identifying any deviations or anomalies as possible security issues. The rapid detection and response capabilities of this technology enable the mitigation of severe damage caused by cyberattacks such as distributed denial of service (DDoS) or malware infections.

Another common approach that can be enhanced by incorporating ML algorithms is signature-based detection. This method provides an important initial barrier against known cyber dangers by relying on the detection of patterns or signatures of malicious activity or infection. One way that machine learning can improve signature-based detection is by automating the process of creating and updating signatures [4]. In order to create and continuously update signatures, ML algorithms can scour massive malware sample banks for distinct patterns and traits, even as new threats emerge and change. Thus, security systems can keep up with the changing threat landscape, which strengthens defences against both existing and new threats [5]. The massive amounts of data produced by IoT devices can also be better understood with the help of ML.

By doing so, security experts can uncover previously unseen correlations, spot patterns, and foresee potential dangers [6]. Accordingly, businesses can improve their security by making data-driven decisions and allocating resources wisely. By incorporating machine learning into IoT security operations, the aforementioned threats and difficulties can be better handled.

Thanks to this partnership, we have created an Internet of Things (IoT) environment that is more secure and robust, which is protecting our ever-more-connected world [7].

2. LITERATURE REVIEW

The Internet of Things concept allows for data transmission by integrating physical devices and sensors. Technology components in IoT networks have improved the efficiency of data collecting, analysis, reporting, and planning for the future. Detecting, analysing, and monitoring system consistency are all capabilities of multi-layered Internet of Things (IoT) systems. Basic configuration includes three tiers: application, network, and perception. The application layer is responsible for delivering user-specific programs and services. When it comes to the Internet of Things (IoT), the network layer is in charge of things like security, energy consumption, data capacity building, inter-device reliability, and connecting devices to other networks, equipment, and services. The environment is sensed by the perception layer through computational hardware, actuators, and sensors. Data transfer, encryption, and signal processing are all responsibilities of the physical layer, which also handles power consumption, security, and interoperability. In Figure 1 we can see the security holes and the organisations that are working to fix them at each level of the IoT.

Most Internet of Things (IoT) designs have three tiers, each of which stores a different kind of data, enabling functionality, and technical progress [8]. Due to the Internet of Things (IoT) network, users can process data more efficiently and with less effort and resources. As the IoT becomes more widespread and used, the number and severity of attacks against its systems are on the rise [10]. The IoT and its reliance on critical infrastructures are the targets of several cyberattacks.

The quick advancement of adversarial strategies has led to an increase in the complexity, tenacity, and intelligence of cyber threats. There is a pressing worldwide need to strengthen the cybersecurity of vital cyber facilities. Therefore, before implementing effective and strong cybersecurity treatments, it is essential to identify cyber dangers [9]. Devices, sensors, servers, actuators, protocols, cloud services, and applications are all part of the Internet of Things (IoT), as seen in Figure 2.

It is capable of freely communicating with both approved and unauthorised users. The user's interaction with an IoT network makes it hard to tell if the content is benign or harmful. Cyber threats posed by unauthorised users in IoT networks are a result of the absence of mandated security measures.

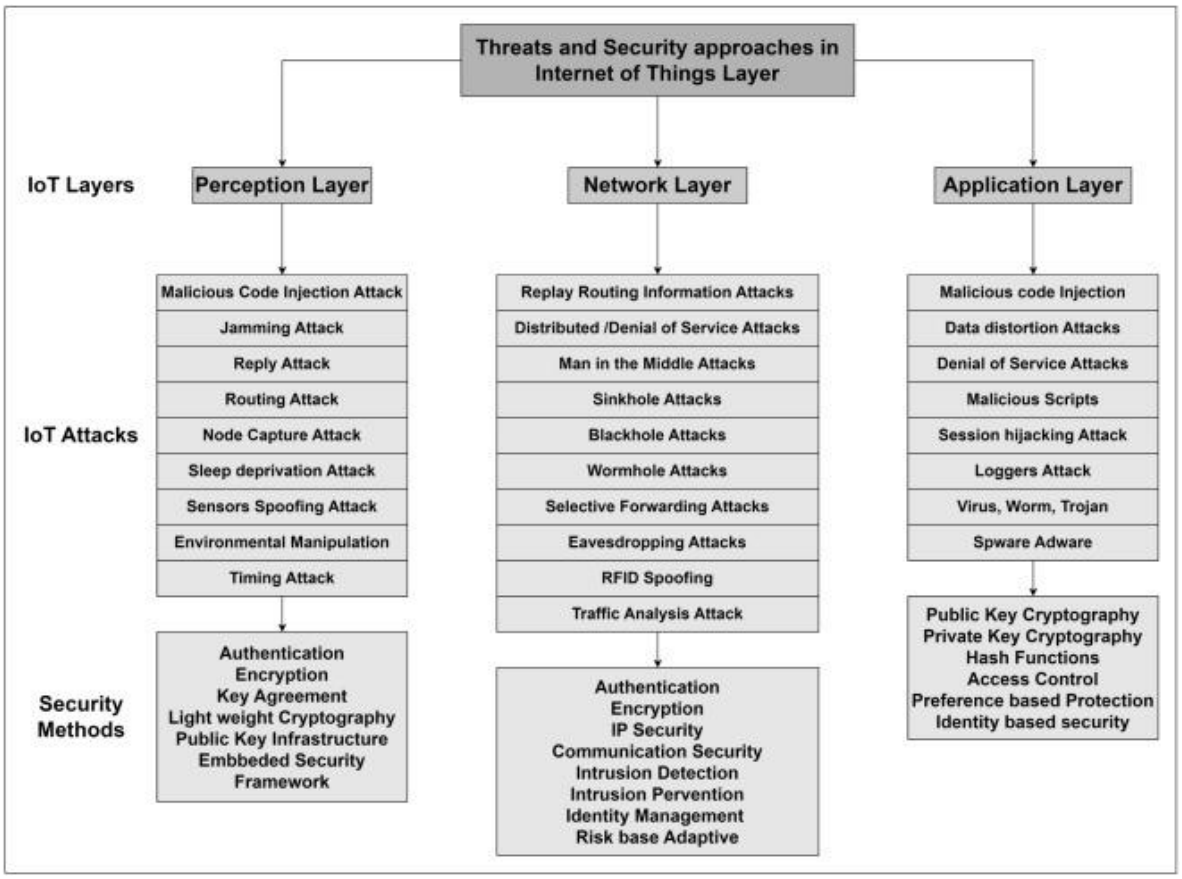


Fig. 1. Addressing security risks in Internet of Things layers

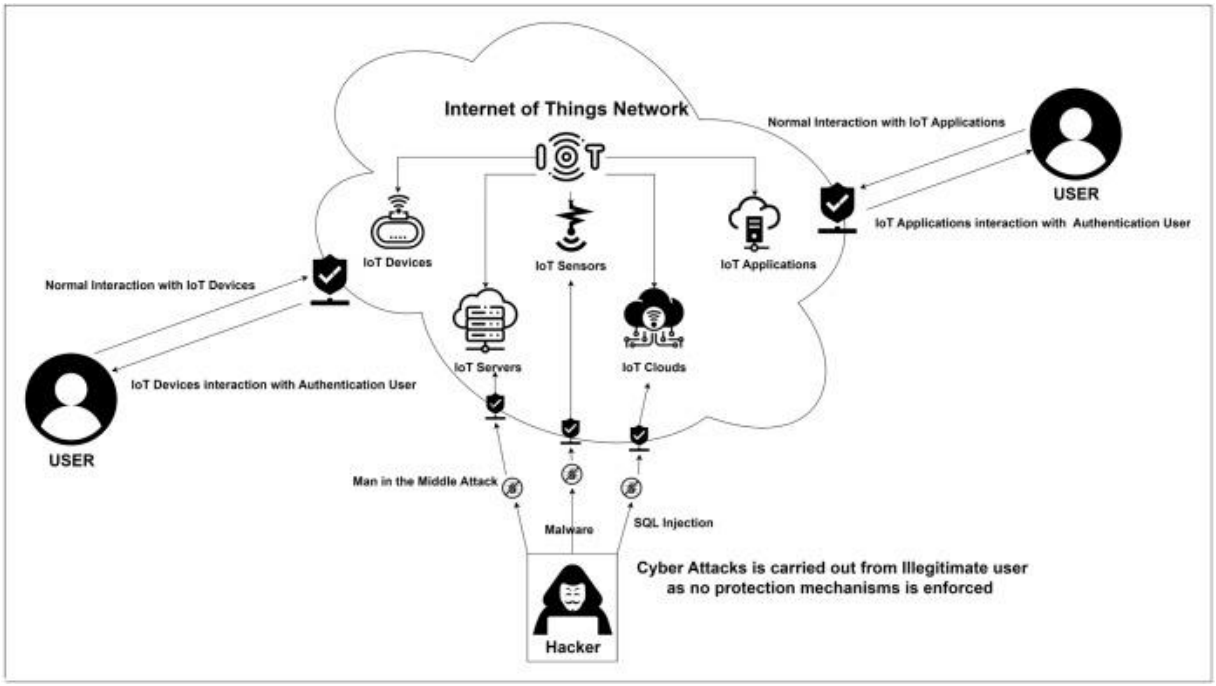


Fig. 2. Internet of Things networks do not have any safeguards in place to prevent communication with both authorised and unauthorised users.

The importance of Internet of Things security is paramount due to the increasing frequency and severity of cyberattacks and the proliferation of connected devices. The need of safeguarding the infrastructure supporting Internet of Things (IoT) devices is growing as their use spreads across several sectors, including households [11].

Inadequate security protections, little memory capacity, and restricted computing capabilities are common in IoT devices, leaving them open to attack. After breaking into a large number of susceptible IoT devices, hackers can create botnets—networks of infected devices that are linked together—and then cause significant delays by overwhelming the devices with network traffic. Unauthorised access can be achieved via manipulating Internet of Things (IoT) devices that have security flaws [12]. Because they collect and transmit personal information, data breaches are common in all Internet of Things devices. It opens the door for hackers to modify data in transit, introduce harmful commands into the communication channel, and intercept data transfers.

The capacity to evade detection for extended periods poses a threat to security [13]. Internet of Things (IoT) devices equipped with microphones or cameras pose a threat of unauthorised data transfer. Since this is an IoT network, both users and devices connected to it must use robust authentication measures [14].

Any unlawful behaviour that compromises the security, availability, or confidentiality of information in any way is considered an intrusion into the Internet of Things (IoT) ecosystem. Virtual private networks (VPNs) allow users to set up encrypted communication channels, protecting the privacy and authenticity of any data sent [15]. When authorised users are unable to use computer services due to an attack blocking their access, this is called an incursion. Installing an Intrusion Detection System (IDS) is standard procedure for protecting computer systems. Software, hardware, or a combination of the two could form the basis of this system. Network traffic must be monitored by Intrusion Detection and Prevention Systems (IDPS) in order to identify any suspicious activity that could indicate a security violation [16].

Since a conventional firewall is unable to detect malicious network traffic or unauthorised computer activity, intrusion detection systems (IDS) are implemented. There are two primary kinds of intrusion detection systems: SIDS, which is based on signatures, and AIDS, which is based on anomalies [17].

Table 1 displays various intrusion detection methods. One rapidly growing area of study is the use of deep learning frameworks for intrusion detection in networks. Despite the abundance of surveys covering this emerging field of study, there is a need in the literature for a fair evaluation of various deep learning models, particularly in view of recent developments in intrusion detection datasets [18]. Cybersecurity is an important issue in the modern world. For instance, intrusion detection systems (IDS) search for signs of hostile activity, while firewalls have been used to safeguard critical data. Anomaly detection and pattern recognition are only two of the many techniques that have benefited greatly from the fast growth of AI research [19]. To combat cybersecurity risks and guarantee safety, AI is an encouraging approach [20]. Figure 3 shows the architecture that contains the IoT components: servers, clouds, sensors, devices, and applications. To protect these networks, an Anomaly-based Intrusion Detection System (IDS) can be set up.

Table 1. Approaches to intrusion detection methods for the Internet of Things.

Detection method	**Signature based intrusion detection system**	**Anomaly based intrusion detection system**
	It detects known dangers by analysing attack signatures. These identifiers have the potential to reveal potential threats in system or network behaviour.	Additionally, it has the capability to identify zero-day attacks. It finds typical patterns of attack and highlights any changes from that baseline.
	A decrease in false positives is achieved by the use of attack signatures.	It might lead to the discovery of fresh attacks.
	Since it doesn't need processing or analysis, it responds rapidly to recognised dangers.	Novel attacks without signatures may be detected. It can detect irregularities even if the assault is unknown.
	Step one is to connect the intrusion detection system (IDS) to a signature database. Step two is to keep an eye on system logs or network traffic.	Insider threats can be caught by IDS when authorised users commit crimes or abuse their skills.
Benefits	Signature databases enhance SIDS by providing numerous signatures for recognised attack patterns and vulnerabilities.	To improve its detection accuracy, it can learn from system behaviour or changes in the network and adjust its baseline accordingly.
	Database signatures are the only known threats it can counter. It is unable to detect newly-developed attack techniques or zero-day attacks.	It might mistakenly alert you when there's an abnormality. Security staff could become weary from false positives.
	Its effectiveness against encrypted attacks is diminished because it is unable to detect them.	It has the potential to confuse normal and pathological growths. Strange occurrences could be a sign of behavioural or security problems.
	A false negative can occur while trying to identify a signature because the database does not have the most recent version or variant of the attack.	Computingly demanding and hardware-specific analyses of system records or network traffic for baseline, deviation may be necessary.
	Regular updates to the signature database are necessary for its proper operation. The database's signatures must be updated to reflect new attack patterns.	It may be vulnerable to attacks that go undetected because it cannot decipher encrypted packets.
Drawbacks	Problems with scalability arise when network traffic grows.	A computer system that is always evolving makes it challenging to create a standard profile.

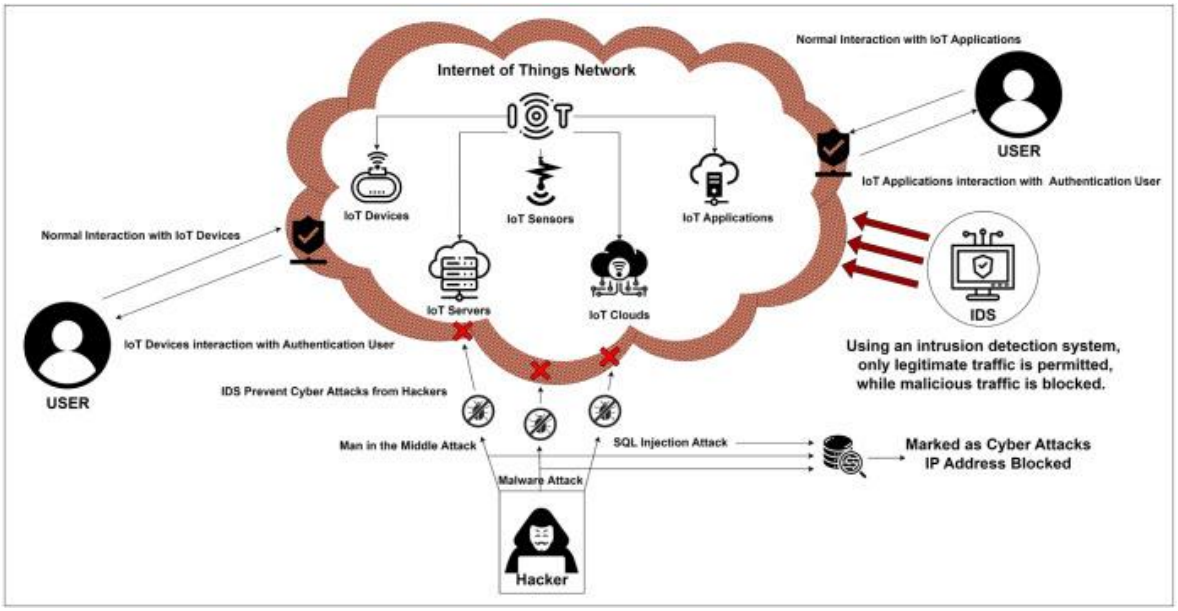


Fig. 3. Preventing intrusions on the Internet of Things network

In light of the foregoing, scientists have adjusted the architectures of neural networks in an effort to improve IDS. Data classification using predefined criteria is made possible by Deep Neural Networks (DNNs), which employ computer resources to sift through mountains of data in search of patterns and connections [21]. An interesting possibility in IoT security is the use of a well-trained DNN for intrusion detection based on anomalies. This paper lays the groundwork for an IoT intrusion detection system by demonstrating how to employ Deep Neural Networks to spot data anomalies in real-time [22]. A key objective of this project is to develop an Intrusion Detection System (IDS) for the Internet of Things (IoT) that combines models from Feed Forward Neural Networks (FFNN), Long Short-Term Memory (LSTM), and Random Neural Networks (RandNN). With the aim of integrating cyber security measures and enhancing intrusion detection performance, this study lays out the framework for deploying DL-IDS, a Deep Learning approach, inside IoT networks [23]. The main goal of this project is to create an Intrusion Detection System that can use a multi-layered Neural Network to detect many prevalent Internet of Things attacks.

3. PROPOSED SYSTEM

Incorporating intelligent multi-agent data handling, cyber threat sharing, situational awareness, and data stream aggregation from Edge devices is the overarching goal of this project to improve the cybersecurity of Smart Environments. Providing a robust reaction to cyber-attacks, along with human-oriented warning and early identification of hostile activity, is the project's objective. To lessen the burden and delay of IoT components, our novel approach permits multi-level data collecting and off-chip Machine Learning model training. Stronger cybersecurity in a multi-sector setting and more efficient infrastructure construction under limited resources are two outcomes. Not only does the suggested method show how to find the best ML model for the provided data, but it also shows how well the model works when deployed to popular IoT devices like Rasberry Pi. We use the ML model to measure the concurrency and performance of the IoT devices, which helps to guarantee that AI applications are effective in IoT cybersecurity.

Data Collection and Preprocessing:

Using the Edge-IIoTset IoT network traffic and the Aposemat IoT-23 dataset, we train and test ML models. The IoT-23 dataset is a semi-structured data set that labels packets of IoT network traffic as malicious or benign. Data from several Internet of Things devices was used to develop it by the Avast AIC lab. Among the 325,307,990 captures included in the collection, 294,449,255 are malicious samples. Network traffic analysis, virus, and attack detection applications have also made use of this dataset in multiple studies. The information about the network traffic is collected from semi-structured text files (.pcap files) using Wireshark and tcpdump. An additional 1,363,998 normal samples and 545,673 attack samples make up the Edge-IIoTset dataset. The transformed structured data is then used to perform the feature extraction and selection operations. For optimal outcomes, data is divided amongst all attacks and an equal amount of data is chosen for each.

AI Model Training:

After preprocessing, the dataset is split into two parts: a training set and a test set, with a ratio of 80:20.

The training process is made more stable and easy by using various imbalance handling approaches to boost performance. Model training time is decreased using this method. The chosen models are all of a multi-class character because predictions are based on several forms of malware attacks. Classification of malware and attacks is accomplished by the training of neural networks (DNNs), support vector machines (SVMs), decision trees (DTs), gradient boosting (GBs), and naive Bayes (NBs).

Model Deployment in Edge Devices:

After the various models have been trained, we take note of their performance indicators. When deciding which model to deploy, we look at how well it performs across several measures, including accuracy, precision, recall, and f1 score. At this complex stage, the chosen model is encapsulated into a framework that is optimised for efficiency and lightness, specifically for use in edge computing settings. Seamless deployment with minimal latency and resource utilisation is achieved through the combination of optimisation approaches, edge computing architectures, and containerisation technologies. A robust defence against possible adversarial attacks is established by the deployment model using security protocols and encryption techniques. A significant step forward from conceptual model building to the practical integration of AI cybersecurity measures into the complex web of smart environments is signalled by the completion of this module.

IoT Gateway and AI Model Transfer:

Connected to an IoT gateway, the network's IoT nodes should all be part of the same network. In order to put the AI-enabled model into action, the gateway must be able to access data about traffic. The access point and a shared Internet of Things interface connect all the actuators and sensors. Figure 4 depicts an AI-enabled model transfer method for making predictions on IoT devices; in this method, the server host or cloud handles the high-inference activities, relieving the IoT-node of the burden of processing massive amounts of data and so lowering energy usage. We will explain the two steps below: First, transferring the JSON data that has been processed to a localhost; second, getting that data from an Internet of Things gateway.

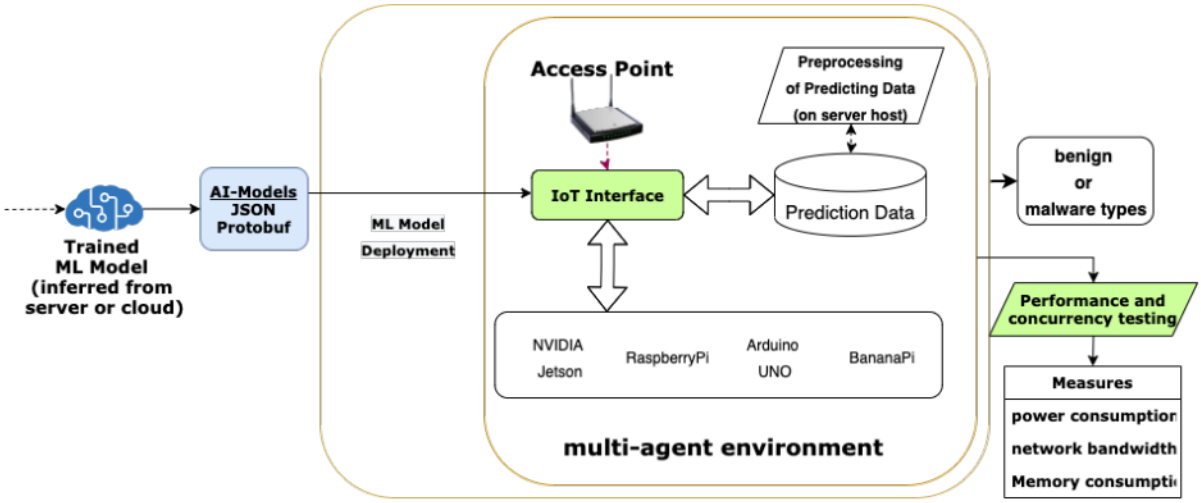


Figure 4. AI model transfer approach.

4. RESULTS

Metrics for the IoT gateway's and the different ML models' performance are the main emphasis of this section.

Performance metrics of AI models:

When comparing the various ML models on the two sets of data, the following metrics are taken into account: Accuracy, as a proportion of all examples in the dataset for which the model produced a true prediction, is one approach to assess a model's performance. The accuracy metric evaluates the model's ability to prevent false positives by counting the number of correct positive predictions compared to the total number of positive predictions. Recall measures the ability of the model to detect positive instances and compares them to the number of genuine positives. It emphasises the model's accuracy in capturing all positive occurrences.

F1 score: It evaluates the model's performance in a fair manner by considering both false positives and false negatives. This makes it suited for imbalanced datasets and offers a full 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 5. Performance Metrics of ML Models

Hardware Performance Testing:

One kind of resource utilisation testing is hardware performance testing, which examines the model's executable system's response to a specified load and set of environmental conditions. To standardise the deployment process for IoT systems and test hardware performance, many metrics are used. (a) Network Bandwidth: This metric takes into account the total data transfer rate of all the Internet of Things devices' physical network ports. Devices such as lo, VPNs, network bridges, intermediate functional blocks, bond interfaces, etc. are not encompassed in the measurement. Before the ML model is run on the Raspberry Pi, the sent and received bandwidth varies between 0 and 4.7 kb/s and 0 to −4.0 kb/s, respectively, as illustrated in Figure 6. whereas the ML model is operational, the receiving bandwidth ranges from zero to eighty kbps, whereas the sending bandwidth falls within the same range but with a negative sign.

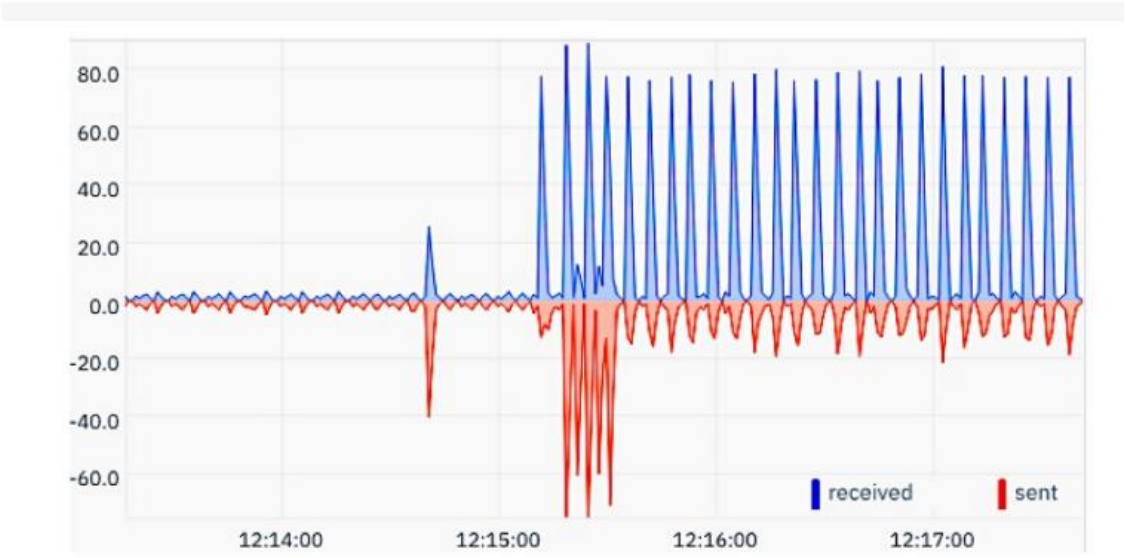


Figure 6. The bandwidth in kb/s and the duration represent the network bandwidth that the devices consume.

(b) Statistics on Packets: Packet statistics are another crucial metric in the realm of network architecture. The host's packet reception and packet transmission statistics as measured by the internet protocol (IP) layer. The packets that have been sent are not accounted for in this metric. By executing the ML model that was started at 12:15, Figure 7 shows the variance in statistics of IPv4 network packets.

Figure 7. The variance in IPV4 network packets as predicted by the Rasberry Pi ML model, where y represents packets and x represents time.

(c) Percentage of CPU Usage: This metric lines up with the device's total CPU utilisation, which is 100% of all cores. The CPU utilisation of the Raspberry Pi device, where the ML model was

started to run at 17:30, is shown in Figure 8. For the first few seconds, the running ML model used up to around 32% of Jetson's CPU and about 35% of Raspberry Pi's CPU to get it started. After that, it performs normally, consuming an average of about 8% of CPU, which is just about 2% more than idle operation on both devices.

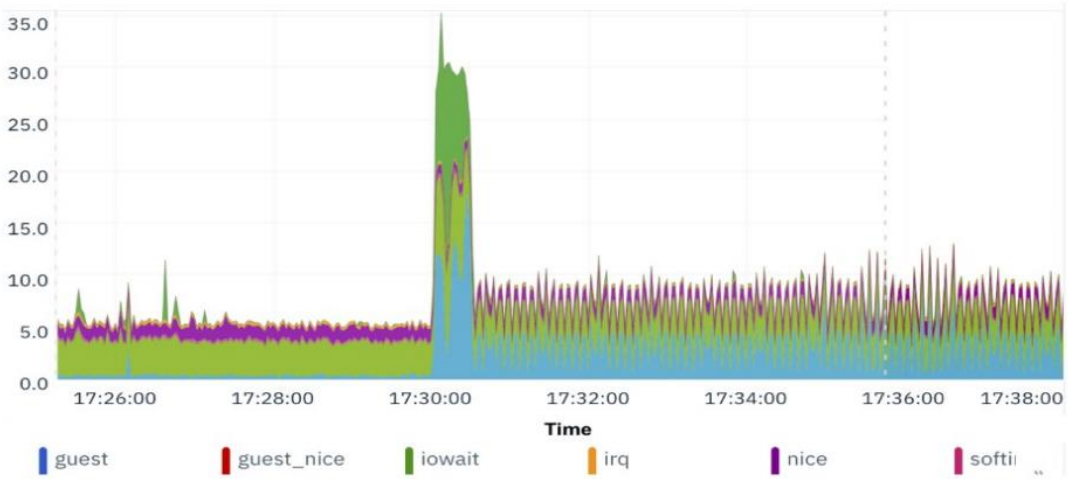


Figure 8. CPU usage on Internet of Things devices Raspberry Pi charts showing the percentage of CPU time consumed.

(d) System Processes: The average of all system processes that the device uses is shown by this metric. It is made up of system processes that are either runnable (ready to run) or blocked (waiting for I/O to finish). Before and after the model was performed on both =Raspberry Pi, the status of system processes is shown in Figure 9. The Raspberry Pi device exhibits a slight variation following the deployment of the ML model; there is a slight uptick around 12:15, the moment at which the model was begun.

Figure 9. The Raspberry Pi system processes' consumption at 12:15 (y → average system processes and x → time).

CONCLUSION AND FUTURE WORK

In conclusion, malware and multi-level attacks in Smart Environments are found by the AI-enabled detection approach. This innovative approach actively searches for malicious software and assaults in the data broadcast from the network. Taking into account all of the samples, deep neural networks (DNNs) generally outperform other options when it comes to malware identification and classification on the IoT-23 and Edge-IIoTset datasets. Hardware engineers can support the efficient deployment of AI-models in Smart Environments with the provided precise power consumption measurements and concurrency testing. The proposed technique appears to be efficient for in-production deployment due to its high f1-score, accuracy, and precision, as well as its low impact on CPU utilisation (2% increase), current consumption, and network bandwidth (30 kb/s on average). Additionally, the study's results imply that the model efficiently and accurately detects malware and assaults in IoT devices. By automating the detection process and reducing the need for manual analysis, this technology helps identify infected IoT devices and saves money on malware assessments.

REFERENCES

[1] A. Djenna, S. Harous, D.E. Saidouni, Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure, Appl. Sci. 11 (10) (2021) 4580.

[2] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, M. Gidlund, Industrial internet of things: Challenges, opportunities, and directions, IEEE Trans. Ind. Inform. 14 (11) (2018) 4724–4734, http://dx.doi.org/10.1109/TII.2018.2852491.

[3] L.S. Vailshery, Statista, 2022, [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/, Accessed on May 20, 2023.

[4] Y. Lu, L. Da Xu, Internet of things (IoT) cybersecurity research: A review of current research topics, IEEE Internet Things J. 6 (2) (2018) 2103–2115.

[5] A.R. Khan, M. Kashif, R.H. Jhaveri, R. Raut, T. Saba, S.A. Bahaj, Deep learning for intrusion detection and security of Internet of things (IoT): current analysis, challenges, and possible solutions, Secur. Commun. Netw. 2022 (2022).

[6] I. Ullah, Q.H. Mahmoud, Design and development of RNN anomaly detection model for IoT networks, IEEE Access 10 (2022) 62722–62750, http: //dx.doi.org/10.1109/ACCESS.2022.3176317.

[7] P. Sethi, S.R. Sarangi, Internet of things: architectures, protocols, and applications, J. Electr. Comput. Eng. 2017 (2017).

[8] N. Abosata, S. Al-Rubaye, G. Inalhan, C. Emmanouilidis, Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications, Sensors 21 (11) (2021) 3654.

[9] M. Burhan, R.A. Rehman, B. Khan, B.-S. Kim, IoT elements, layered architectures and security issues: A comprehensive survey, Sensors 18 (9) (2018) 2796.

[10] S. Bajpai, K. Sharma, B.K. Chaurasia, Intrusion detection framework in IoT networks, SN Comput. Sci. 4 (4) (2023) 350.

[11] M.H.P. Rizi, S.A.H. Seno, A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city, Internet Things (2022) 100584.

[12] D. Nanthiya, P. Keerthika, S. Gopal, S. Kayalvizhi, T. Raja, R.S. Priya, SVM based ddos attack detection in IoT using IoT-23 botnet dataset, in: 2021 Innovations in Power and Advanced Computing Technologies (I-PACT), IEEE, 2021, pp. 1–7.

[13] M. Ibrahim, A. Continella, A. Bianchi, AOT-Attack on Things: A security analysis of IoT firmware updates, in: 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P), 2023.

[14] T. Suleski, M. Ahmed, W. Yang, E. Wang, A review of multi-factor authentication in the Internet of Healthcare Things, Digit. Health 9 (2023) 20552076231177144.

[15] M.I. Zakaria, M.N. Norizan, M.M. Isa, M.F. Jamlos, M. Mustapa, Comparative analysis on virtual private network in the internet of things gateways, Indones. J. Electr. Eng. Comput. Sci. 28 (1) (2022) 488–497.

[16] A. Javadpour, P. Pinto, F. Ja'fari, W. Zhang, DMAIDPS: A distributed multi-agent intrusion detection and prevention system for cloud IoT environments, Cluster Comput. 26 (1) (2023) 367–384.

[17] A. Khraisat, A. Alazab, A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges, Cybersecurity 4 (2021) 1–27.

[18] A. Awajan, A novel deep learning-based intrusion detection system for IoT networks, Computers 12 (2) (2023) 34.

[19] N. Yadav, S. Pande, A. Khamparia, D. Gupta, Intrusion detection system on IoT with 5G network using deep learning, Wirel. Commun. Mob. Comput. 2022 (2022) 1–13.

[20] M. Abdullahi, Y. Baashar, H. Alhussian, A. Alwadain, N. Aziz, L.F. Capretz, S.J. Abdulkadir, Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review, Electronics 11 (2) (2022) 198.

[21] T. Saba, A. Rehman, T. Sadad, H. Kolivand, S.A. Bahaj, Anomaly-based intrusion detection system for IoT networks through deep learning model, Comput. Electr. Eng. 99 (2022) 107810.

[22] H. Asgharzadeh, A. Ghaffari, M. Masdari, F.S. Gharehchopogh, Anomaly-based intrusion detection system in the Internet of Things using a convolutional neural network and multi-objective enhanced capuchin search algorithm, J. Parallel Distrib. Comput. (2023).

[23] S.M. Kasongo, A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework, Comput. Commun. 199 (2023) 113–125.

Citation: Harish Narne. Developing Robust Cyber Security Protocols for IoT Networks Using AI. International Journal of Electrical Engineering and Technology (IJEET), 15(4), 2024, pp. 1-15.

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/IJEET/VOLUME_15_ISSUE_4/IJEET_15_04_001.pdf

Abstract Link:
https://iaeme.com/Home/article_id/IJEET_15_04_001

✉ **editor@iaeme.com**