RESEARCH ARTICLE

SPECIAL ISSUE

RSP Science Hub

International Research Journal on Advanced Science Hub
2582-4376
Vol. 05, Issue 05S May
www.rspsciencehub.com

Check for updates

http://dx.doi.org/10.47392/irjash.2023.S007

International Conference on intelligent COMPUting TEchnologies and Research (i-COMPUTER) 2023

Internet of Things (IoT) Device Investigative Analysis Using Machine-to-Machine (M2M) Framework

Phaneendra Kanakamedala[1]*, Yarra Harika*[1]*, Mamilla Krishnaveni*[1]*, Bhuvanesh Nallani*[1]
[1]*Lakireddy Balireddy College of Engineering, Mylavaram, India*

Emails: phanikanakamedala@gmail.com, yarraharika2002@gmail.com, mamillakrishnaveni8@gmail.com, bhuvaneshnallani89@gmail.com

Article History

Received: 23 February 2023
Accepted: 13 March 2023

Keywords:

Internet of things (IoT);
forensic analysis;
machinetomachine framework (M2M);
machine learning

Abstract

As we know that now a days the possibility of the uninterrupted attacks on the IOT devices are increasing. The less memory and the minute processing power of these appliances make it tough for the security analyst to store the records of the different attacks. The forensic analysis is used to evaluate the damage done on the devices due to numerous attacks. In this mechanism the attacks on the IOT devices are detects undoubtedly by using machine-to-machine (M2M) framework. In addition to the using machine-to-machine framework the machine learning algorithms also been used to identify various attacks automatically. Here we use the third-party logging server in order to issue. The execution will be studied in the form of accuracy, precision and the Random Forest gives the most accuracy.

1. Introduction:

When connected to the internet, IOT devices may safely gather and share data (Vishwakarma and Jain).The wide range of applications in it and provide the evolution of a number of innovations, such as wearable technology, smart cities, smart metering, smart thermostats, and smart homes (Yang et al.). The Internet of Things has simplified human lives (Javaid and Khan).

In spite of the reality that the applications of IoT are continuously increasing, IoT tool reliability stays a limitation (Hossain et al.). The manufactures of these devices are often engrossed with getting original appealing capabilities and modifying to improve the devices' intelligence and efficiency without increasing their price secured (Alladi et al.). In reality, There have been various cyberattacks on IoT devices in current as a result of years insufficient safety features (Almogren). The number of IoT devices and cyberattacks is each progressively growing (Sikder et al.).

Denial of service (DOS) is among the most familiar Infiltration of the IoT network. According to Cisco'sannualnet look at DDoS cyberattacks are expected to increase between 2018 and 2023.from the given diagram it compares the quantity of feasible DDoS assaults are every year (Hussain et al., "IoT DoS and DDoS Attack Detection using ResNet"). In addition, determined that IoT DoS attacks are constantly growing each day. It's far suggested by using the Palo Alto Networks Unit 42 studies crew 98% of IoT devices' traffic does not always encrypted, exposing the exclusive records network traffic and attacks on the network and systems at multiple levels (Stergiou et al.). It will increase the threat space for attackers, when these unprotected linked Internet of Things devices are on the network. In step with Kaspersky's Research, 1.5 billion assaults on IoT hardware has been mentioned within the initial half of 2021 (Hussain et al., "Towards a Universal Features Set for IoT Botnet Attacks Detection").

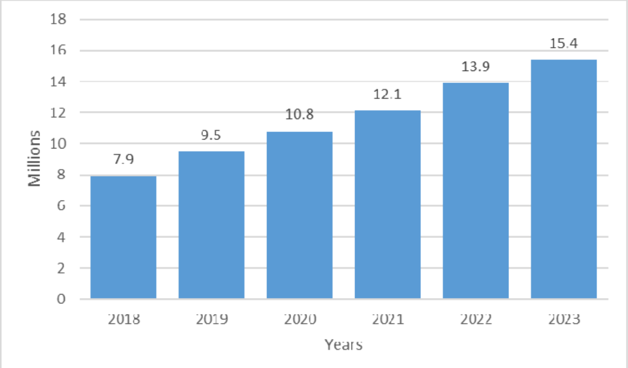


FIGURE 1. A year-by-year analysis of Intrusions

Moreover, IoT devices for smart homes which includes the various IoT devices, as smart cameras divide the 25% of the malware attacks in a botnet assault (Yousefnezhad, Malhi, and Främling). Through The Mirai attack takes use of default Credentials and obtained manipulate on hundreds million IoT devices and conducted a distributed denial of service (DDoS) assault against key systems (Tawalbeh et al.). HP additionally pronounced roughly 70% of machines are prone (Mariyanayagam, Shukla, and Virdee). Therefore, the security flaws for the tools need very secure (Gupta, R. Kumar, and A. Kumar). Security flaws is one of the weakness in devices which offers a prime target for hackers. Wrong component trying out, a scramble for price, as well as a scarcity of powerful rules are also the primary Reasons of IoT threats (Karabiyik and Akkaya). The structure is necessary to identify upon the assaults on various tools, store verification of those threats (Mazhar et al.). The vulnerabilities of devices can be mitigated by applying the forensic evaluation. Further, the assault and perpetrator may be clearly identified.

IoT devices are able to reduce a constrained procedure for variety a set of specified instructions (Haider et al.). Correspondingly, among the IoT devices They are unable to acquire, interpret, or record, analyze connectivity. Because of the architecture of IoT device they are more complex for security analyst in case of store the data among the various attacks. Due to those constraints, the gathering of facts is a significant task in forensic analysis . To make IoT environment more secure and robust some of the special tools and approaches are required. In case of the research purpose the devices are Better appropriate analytical approaches should be developed and used.

The following mentioned issue is avoided along with assistance of forensic analysis approach. We provided a framework which executes the threats with detection, recognition and generate the records and warnings for these threats. This is focused with security Incident control (SIM) for recognizing security incidents are done at the computer network, after which proper precautions are taken and finished some constraints of security ideas which are harmed. Forensics analysis is distinct to network auditing as it is the pre-examination of a network's flaws while forensic analysis is the post-examination of security misfeasance that What happened to the document and when it happened.

Acquiring the data is one of the problem that is addressed by employing a third-party logging server. The traffic generated towards the devices are routed towards the server, in this forensic analysis is used to generate and store the logs and alerts of malicious attacks. to acquire data about the assaults and the perpetrators the previously saved records are recreated, and analyzed in a server. The detection of these machine learning is used to perform assaults using a dataset it built all these data.

The generalized forensic analysis procedure consists of four steps: data collection, evaluation, processing, verification and the report. [23]. In first step , the data according to a particular attack are gathered. Data acquisition is a major issue due to the limitation of IoT devices have limited computing power. In this case attacks with the evidences are not found . This issue can be handled by our intended system the log server is introduced to identify the threats and also the logs of malicious traffic are maintained, and warnings are generated. And the next step is to gathered information is analyzed to the different information which is pertinent. The traffic should be redirected in IoT devices are configured by using an IP table. The log server writes the logs related to the particular threats as well as embedding them into the detecting engine. In the process of traffic redirection related data is taken and other packets are removed. The obtained information is analyzed for the purpose of useful data. Server security onion gives the information related to when records are collected and regenerated. Security onion gives the information to identify the kind of assault and the assailants and the source and destination ports. Snort gives the alerts for these kinds of attacks. These kinds of attacks are inspected and gives the data help to identify the attacker and the extent of the harm caused by the threats. In the final step, the analytical findings are obtained.

2. Literature Survey

Various forensic tools and frameworks are designed for detecting the attacks in IoT devices.

Fagbola et al proposed a framework for smart digital forensic readiness (SIoTDFR). SIoTDFR includes six distinct stages, device connection, device identification, device monitoring, digital evidence gathering, digital evidence preservation and secure storage. It shows the tiniest PDE and when an incident occur it monitors the criminal activity easily.

Aslan et al. gives the idea on various malware detection techniques along with their advantages and disadvantages. To detect the both signature-based and heuristic-based detection methods have proven to be effective in detecting malware but to identify the detection method relying on known malware signatures has proven to be unsuccessful. Different approaches like behaviour based, Cloud-based methodologies exhibit strong performance in terms of efficiency complicated malware, some parts of the known and unknown malware are detected by using some approaches

Schedit et al introduced a system for recognizing IoT devices through the utilization of DNA has been devised. With the help the buyer's details and the unique identification number of the device were kept confidential DNA of IoT devices are created. By using the DNA, The signs of assaults on these devices can be quickly recognized through their distinct fingerprints. The Hybrid Forensic IoT server was introduced in order to help the present IoT forensic investigation process.

Shrivastava et al., Examined the threats and the utilization of machine learning algorithms on IoT devices was executed to improve their performance. To detect a malicious network traffic some of the classification-based are used, among all algorithms SVM gives the more accuracy. They examine some commands and identifies how the malicious activity is performed by the attackers.

Hegarty the authors tackled the intricate nature of digital forensics in the Internet of Things and suggested a cloud computing solution for conducting digital investigations.

An overall examination of suggested remedies and a blueprint of the system are included in the effort. Nonetheless, they lack a plan for implementing their idea.

Oriwoh et al These hypothetical situations were developed through a comprehensive examination of individuals who employed a novel approach in committing their digital offenses Upon evaluating and deducing insights from the research findings, a framework was established which utilizes regions as the basis for exploring the IoT ecosystem, and centers on three key elements.

Nisais Nimalasingam An effective approach to detecting IoT malware through forensic analysis is to focus on the most distinct network traffic features and combine them with the binary characteristics of various malware families. A massive collection of network traffic data was utilized, featuring various network traffic characteristics. As a result of the feature extraction process for each malware type, the proposed model demonstrated an impressive detection accuracy of nearly 96% during the experimentation stage of the research.

Ayush Kumar and Teng Joon Lim ML classification algorithms were used to offer EDIMA, a modular solution for the identification of network activity coming from IoT threats. Obtained features are collected from network traffic samples at the accessing gateway level and given target class. Several common machine learning (ML) techniques were trained using some of the selected features that have been retrieved, and the resulting ML models were again deployed to analyse data collected with their classification scores provided.

Meffert et al The challenges posed by IoT devices, such as the absence of a uniform standard, are emphasized as being numerous and complex. There are many different communication protocols used by different electronic devices, while some of these devices often use Real-Time Operating Systems

(RTOS), which often have very little storage space or none.

3. Methodology

As shown in Figure 2, the suggested architecture for analysis of devices during assault is composed of four components.. First, traffic generation attack is in charge of generating attacks from the Kali Linux system to the tools used in experimentation. second, there is a network redirection logging server where the warnings are provided in charge for routing traffic to the devices and the servers, analyses communication and provides records only the network matches with server rules. Third, analysis with the server is in charge of regenerating records obtained from the network. The records are rebuilt, the useful data about assault and the assailants is taken . Finally, the analysis in charge of detecting threats with the help various machine learning models.

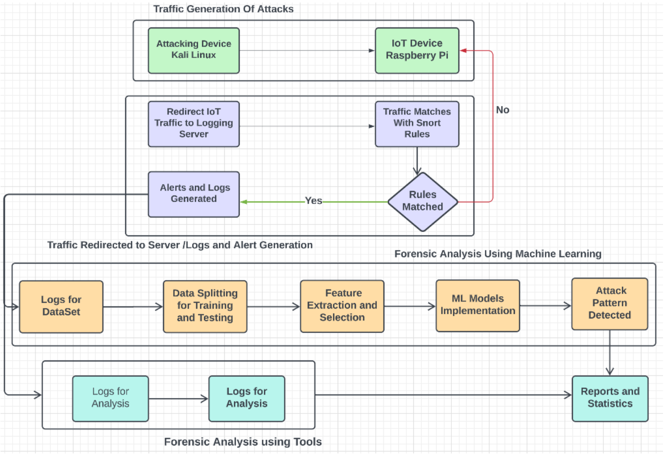

Traffic Generation Of Attacks
Attacking Device Kali Linux
IoT Device Raspberry Pi
Redirect IoT Traffic to Logging Server
Traffic Matches With Snort Rules
No
Alerts and Logs Generated
Yes
Rules Matched
Traffic Redirected to Server /Logs and Alert Generation
Forensic Analysis Using Machine Learning
Logs for DataSet
Data Splitting for Training and Testing
Feature Extraction and Selection
ML Models Implementation
Attack Pattern Detected
Logs for Analysis
Logs for Analysis
Reports and Statistics
Forensic Analysis using Tools

FIGURE 2. **Approach for forensic analysis of network.**

Different devices are used in our designed experimentation, like the The Raspberry Pi, utilized as an Internet of Things device, can be equipped with a Pi camera. , snort as a logging server , security onion as a forensic server , Kali Linux to produce assault possibilities. These devices are all linked to a common system. the given diagram depicts about device configuration.

3.1. Assault Network Generation

In this architecture the initial step involves using Kali Linux, to perform several assaults on the Raspberry Pi , which has an Ip address of 192.168.56.101. On the board, IoT devices are built with connectivity options Sensors, cameras, and other devices of various types are used. The Internet of Things board is built on an open-source platform. In this experiment, a Raspberry Pi is used as an IoT device, Ettercap, HPING3, NMAP, Metasploit, and Wireshark were among the Kali Linux tools we used. These are Raspberry Pi-based attacks.

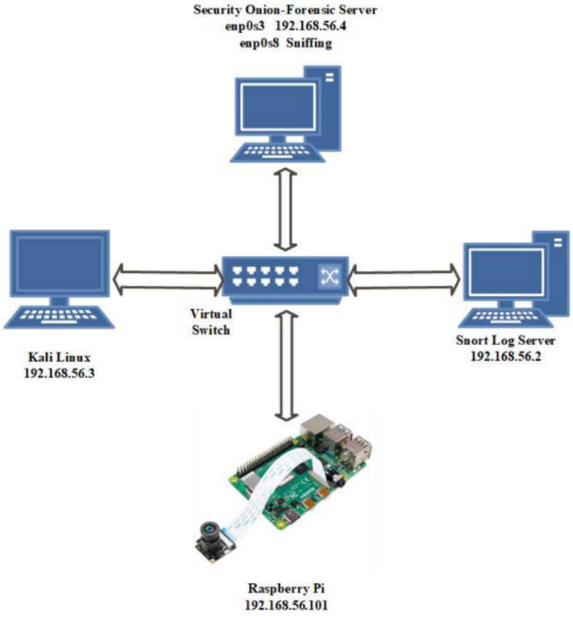


FIGURE 3. **Network diagram**

1. NMAP port scanning;
2. attack through brute force with Metasploit;
3. Synthetic flooding with DoS utilizing HPING3;
4. Via Ettercap, perform MITM ARP spoofing

3.2. Diversion of communication & creation of intrusion records and signals

Under this architecture the traffic from the devices is diverted to a server, additional records were produced. To prevail the limitations of IoT device traffic is forwarded to a server at 192.168.56.2 as its IP address. Every device has an M2M connection and can communicate with one another directly. Regarding server-side record archiving, It was done using a tracking interface (WAZUH) .A third-party server is used. However, the Raspberry Pi's ARM architecture does not support it. The network traffic is then routed through IP tables towards a snort gateway, which has the address of 192.168.56.2. Snort is installed on the logging server. Snort guidelines are created and added to the setup file for certain attacks. Snort examines a network arriving at the device ,compares towards a snort guideline. When the server's identification finds it is match, then threats were detected by a snort alert, & records are kept in the server. Otherwise, packets are outmoded. Snorts generates attack logs in pcaps format. The open-source CIC flow metre these pcaps files are transformed to CSV files using program . These machine learning models are utilized using a CSV file of records because ML can't be performed to pcap files.

3.3. Analytical Approaches Using Security Onion

Logs are saved for analysis after snort detects an attack. These network files included details on the kind of threats, source & destination address, and additional information. Security onion have two network cards and an IP address of 192.168.56.4. The first is used for management, and the second sniffs network packets to find illegal activity on the network. The logging server record solve a problem of evidence acquisition. Security onion includes a number of built-in tools for analysing logs, including squil and squert. Sguil is the graphical user interface for snort, a command-line tool. As we have captured the log, to gather details about assaults and assailants, these logs are periodically created.

3.4. Machine learning for forensic analysis

Machine learning algorithms are used to detect attacks on IoT devices. Automatic detection using Snort is not possible in which We utilize IDS to various threats each time. Through an artificial assault prediction system, ML by using various types of classifiers and labelling generates CSV-formatted logs. This information was split into training and testing groups after pre-processing. After extracting the features, we developed ML models and evaluated them using real-time traffic and the testing dataset.

3.4.1. Data Labelling and Flow Aggregation

Because PCAP files cannot be used by machine learning models, To transform into CSV format a CIC flow meter is utilized . Traffic behaviour ,some analytical traits are taken out. after that ,Those attributes catered to machine learning model, which detects threats to devices. Information is labelled to identify standard and anomalous behaviour, shown in Table 3.

TABLE 1. Analysis and Configuring possibilities

Category	Type	Symbol
Normal	Normal	0
Anomaly	Dos	1
	Brute force	2
	Attack	3
	Shell Code	4
	Backdoors	

3.4.2. Data Pre-processing

To guarantee data reliability, integrity , and stability we eliminate irrelevant fields and any attributes which encrypt qualitative features, can never aid to categorization, & scale properties of numerals between 0 and 1. In order to prevent model efficiency deterioration and source bias, previously labelled fields such as category of threat and IP & port address must be removed. Various strategies are applied to eliminate anomalies and incomplete data.

3.4.3. Dividing the Dataset for Training & Testing

Furthermore, the dataset is divided as two subsets: training and testing. With the use of trained data, the model is developed and tested. Thirty percent of the dataset is used for testing, and 70% for training.

3.4.4. Identification and Analysis of Attributes

A machine learning algorithm's recognise effectiveness is decreased by related attributes. To select attributes, Backward elimination , k-best , and attribute value were utilized.. We chose k-best for feature extraction. As shown in Table 4, K = 10 yields the best accurate results.

TABLE 2. Test config settings

Selected	Features
10	Flow_Byts/s,Pkt_Len_Var,Flow_Pkts/s, Fwd_Pkts/s,Bwd_Pkts/s, Bwd_IAT_Max,Src_Port, Bwd_IAT_Mean,Bwd_IAT_Tot, Flow_Duration

3.4.5. Model development and evaluation

After the feature extractor extracts the features from the inputs, within the learning phase, inputs and labels are supplied to machine learning algorithms. The optimal model is built using a combination of machine learning methods. Each model operates differently due to the multiple domains on which input is trained During the testing step, input usually passed to the pattern generator to acquire the features. They are provided to extract the labels, into predefined classifier models predictions. We labelled our data as before. As a result, the threat is deduced & predicted from the model. Figure 4 depicts a typical representation of the training and testing stage. They made utilize of certain assessment criteria. to determine effectiveness of predictions, including the using confusion matrix's F1 score, recall, accuracy, and precision. The trained models are evaluated using the testing dataset. Efficiency and other metrics won't accurately depict the actual fault when we only utilise the training dataset. Additionally, during training, cross-validation is utilised to fine-tune the models and enhance the performance measures. On the basis of their accuracy, precision, F1 score, and recall, our models were assessed.

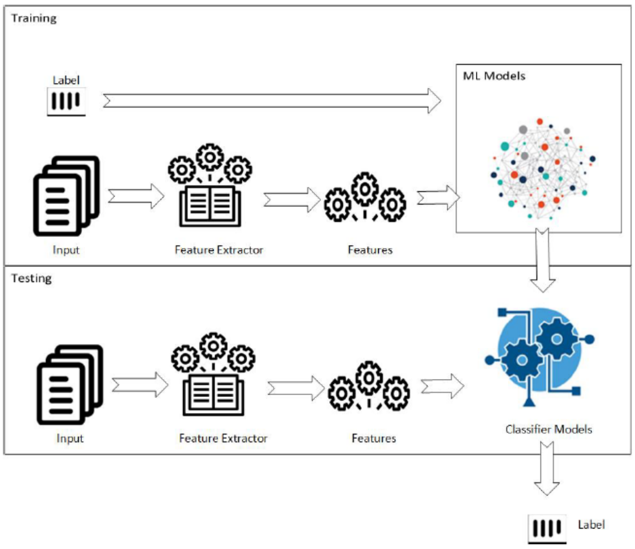


FIGURE 4. **Training and testing of ML models**

3.5. Analysis and Report

The proposed research design is intended for Machine-To-Machine (M2M) communication using IoT devices. IoT devices and other devices are given unique IP addresses. A private network is a collection of machines. The goal of creating the vicinity is to thoroughly investigate during analytics of device communication via M2M connectivity. Several attacks on IoT devices were carried out in this environment. The entire network Traffic via Iot systems is redirected to the Snort monitoring server. The analytical system security onion retrieves the records from the server, where network packets are created & examined. To automate this proposed model, ML models are applied with the dataset. When Cyberattack detection seems to be more accurate when forensic tool analysis and machine learning study are combined.

4. Existing state-of-the-art methods for forensic analysis of IoT devices include:

Digital Forensic Investigation of Internet of Things Devices: This method involves analyzing the digital artifacts on IoT devices to identify evidence of cybercrime incidents. The method uses traditional forensic techniques, such as data carving and analysis of file system metadata.

Network Forensics Analysis for Internet of Things: This method involves analyzing the network traffic between IoT devices and other devices or services to identify evidence of cybercrime incidents. The method uses network traffic analysis tools to capture and analyze the traffic.

Accuracy:

Accuracy is a statistical metric that is commonly used to evaluate the performance of a model, classifier, or algorithm. It is defined as the ratio of the correctly predicted instances to the total number of instances in each dataset.

$$Accuracy = (TP + TN)/ (TP + FP + TN + FN) \qquad (1)$$

TP-True Positive, TN-True Negative, FP-False Positive, FN-False Negative.

Equation (1) represents the proportion of correct predictions among all predictions made.

Recall :

Recall is a statistical metric used to evaluate the performance of a classification model or algorithm in correctly identifying the positive instances. It is also known as sensitivity or true positive rate (TPR). The formula to calculate Recall is:

$$Recall = (TP)/(TP + FN) \qquad (2)$$

Equation (2) represents the proportion of true positives among all actual positive cases.

Precision :

Precision is a commonly used performance metric in machine learning and information retrieval that measures the proportion of true positives among the instances predicted as positive. It is calculated using the following formula:

$$Precision \ = \ (True \ positives)/ \ ((True \ positives + False \ Positives)) \tag{3}$$

Equation (3) represents the proportion of true positives among all positive predictions made.

F-Score :

The F-score (also called F1-score) is a statistical measure that combines precision and recall into a single value. It is used to evaluate the performance of a classifier or model in binary classification problems.

The formula to calculate the F-score is:

$$F1 - score \ = (2 * (precision * recall))/ \ ((precision + recall)) \tag{4}$$

Equation (4) represents the harmonic mean of precision and recall, which gives a balanced score that takes both precision and recall into account.

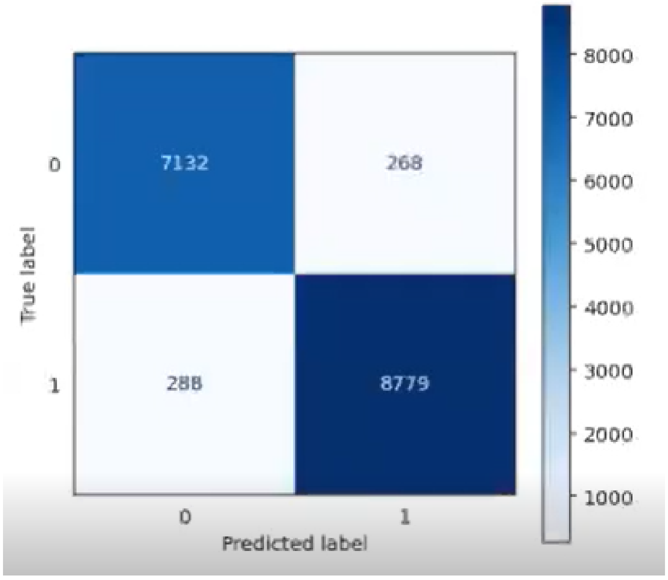


FIGURE 5. Random ForestConfusion Matrix

Random Forest Confusion Matrix : It shows the performance of a Random Forest classification model on a set of test data. It summarizes the number of correct and incorrect predictions made by the model for each class, organized by true and predicted labels.

Decision tree confusion matrix:

It summarizes the performance of a Decision Tree classification model on a set of test data. It shows the number of correct and incorrect predictions made by the model for each class, organized by true and predicted labels.

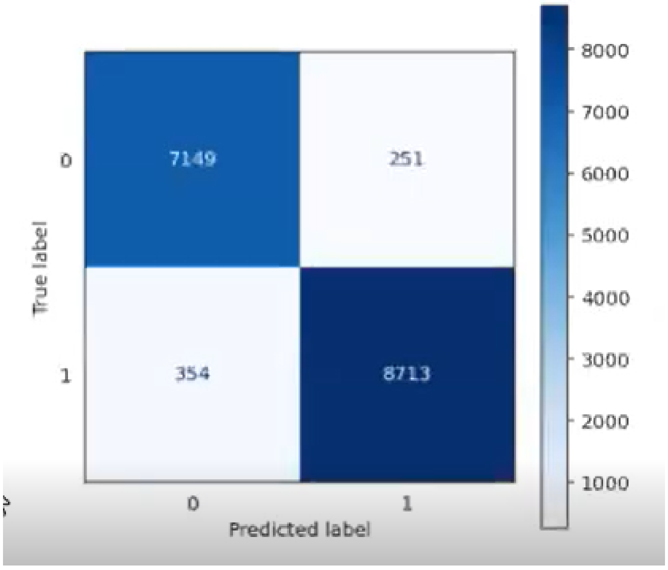


FIGURE 6. Decision tree confusion matrix

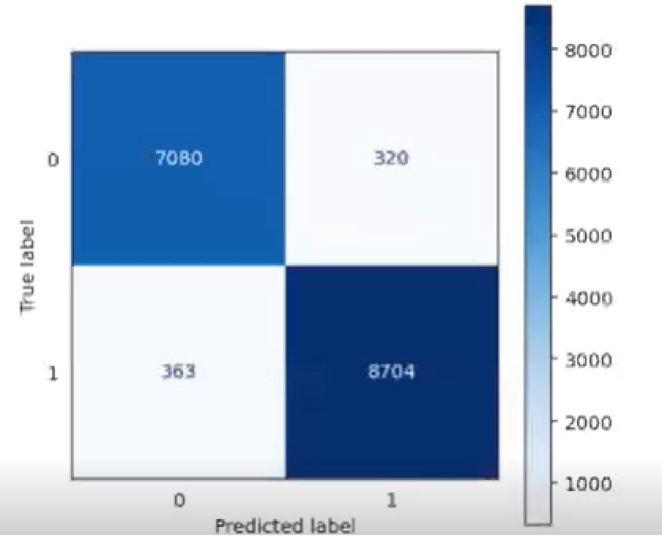


FIGURE 7. Extra trees confusion matrix

Extra trees confusion matrix :

It summarizes the performance of an Extra Trees classification model on a set of test data. It shows the number of correct and incorrect predictions made by the model for each class, organized by true and predicted labels.

MLP Confusion Matrix :

It summarizes the performance of an MLP classification model on a set of test data. It shows the number of correct and incorrect predictions made by the model for each class, organized by true and predicted labels.

Gradient Boosting Classifier :

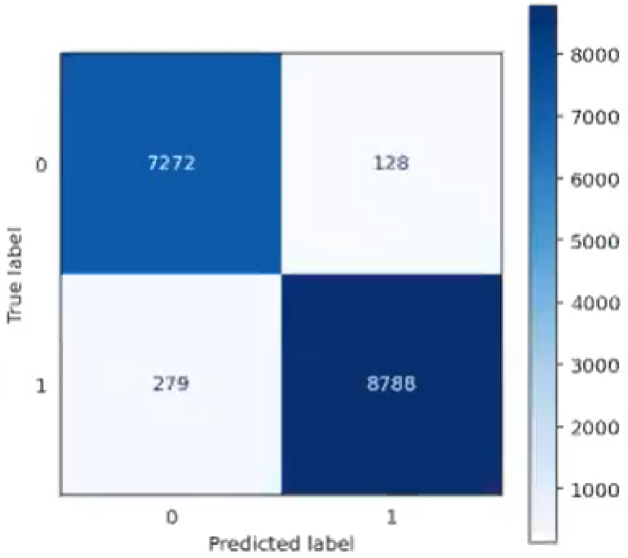


FIGURE 8. MLP Confusion Matrix

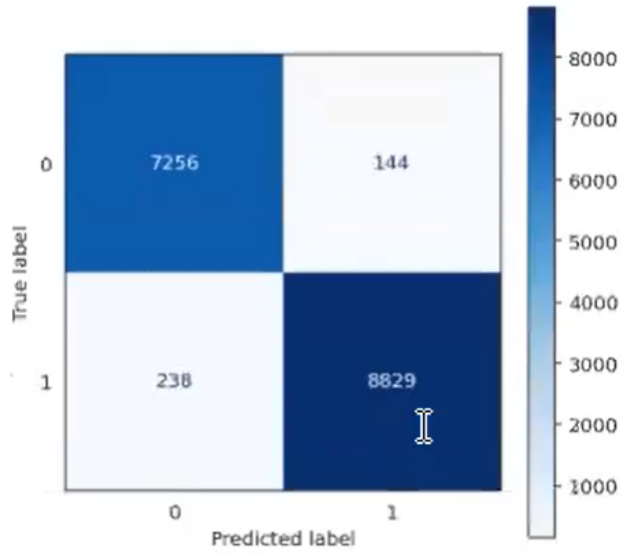
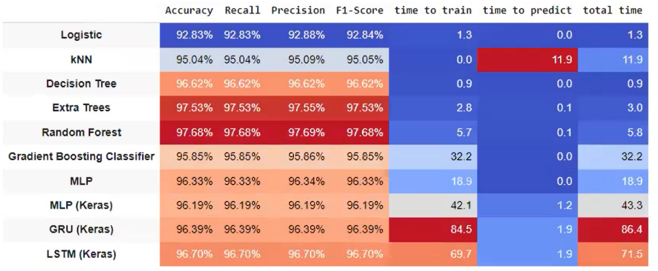


FIGURE 9. Gradient Boosting Classifier

It used for classification tasks. It is an ensemble learning method that combines multiple weak prediction models to create a strong classifier. The algorithm builds the model in a step-by-step manner by minimizing the error in each iteration.

Various machine learning models are applied to the dataset obtained from records gathered by the logging server. We employed strategies like component significance, k-best, and backward elimination to identify & choose features. We utilised the k-best feature extraction and selection approach to choose the most optimal characteristic in the database while executing several tests. This information is separated as 70% for training and 30% for testing. We assessed the performance of the models by taking into account various parameters, including accuracy, recall, precision, and F1-score.Table 3 compares the efficiency of ML algorithms. Among all the algorithms random forest gives the more accuracy.



	Accuracy	Recall	Precision	F1-Score	time to train	time to predict	total time
Logistic	92.83%	92.83%	92.88%	92.84%	1.3	0.0	1.3
kNN	95.04%	95.04%	95.09%	95.05%	0.0	11.9	11.9
Decision Tree	96.62%	96.62%	96.62%	96.62%	0.9	0.0	0.9
Extra Trees	97.53%	97.53%	97.55%	97.53%	2.8	0.1	3.0
Random Forest	97.68%	97.68%	97.69%	97.68%	5.7	0.1	5.8
Gradient Boosting Classifier	95.85%	95.85%	95.86%	95.85%	32.2	0.0	32.2
MLP	96.33%	96.33%	96.34%	96.33%	18.9	0.0	18.9
MLP (Keras)	96.19%	96.19%	96.19%	96.19%	42.1	1.2	43.3
GRU (Keras)	96.39%	96.39%	96.39%	96.39%	84.5	1.9	86.4
LSTM (Keras)	96.70%	96.70%	96.70%	96.70%	69.7	1.9	71.5

FIGURE 10. Compares the efficiency of ML algorithms

5. Future scope:

As the Internet of Things (IoT) continues to grow and become more prevalent in our daily lives, the need for forensic analysis on IoT devices using machine-to-machine (M2M) frameworks is becoming increasingly important. Here are some potential future developments and applications in this field like Increased complexity of IoT devices,Improved security,Increased demand for forensic analysis andCross-disciplinary collaboration

6. Conclusion:

The proposed system is aimed at detecting attacks on IoT devices through the implementation of machine learning techniques like Random Forest, Decision Tree, Extra Trees, Gradient Boosting Classifier, MLP. A confusion matrix is a useful tool for evaluating the performance of different classifiers used on a test dataset where the true values are already known. It presents the number of true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN) for each classifier. The true positives are the number of correctly classified positive instances, while true negatives are the number of correctly classified negative instances. False positives are the number of negative instances that are mistakenly classified as positive, and false negatives are the number of positive instances that are mistakenly classified as negative. A confusion matrix allows us to compare the classification results of different models and assess their overall accuracy.

References

Alladi, Tejasvi, et al. “Consumer IoT: Security Vulnerability Case Studies and Solutions”. *IEEE Consumer Electronics Magazine* 9.2 (2020): 17–25. 10.1109/MCE.2019.2953740.

Almogren, Ahmad S. “Intrusion detection in Edge-of-Things computing”. *Journal of Parallel and Distributed Computing* 137 (2020): 259–265. 10.1016/j.jpdc.2019.12.008.

Gupta, Deena Nath, Rajendra Kumar, and Ashwani Kumar. “Federated Learning for IoT Devices”. *Federated Learning for IoT Applications*. Ed. Yadav, et al. Springer International Publishing, 2022. 19–29.

Haider, Syed Kamran, et al. “Energy Efficient UAV Flight Path Model for Cluster Head Selection in Next-Generation Wireless Sensor Networks”. *Sensors* 21.24 (2021): 8445–8445. 10.3390/s21248445.

Hossain, Eklas, et al. “Application of Big Data and Machine Learning in Smart Grid, and Associated Security Concerns: A Review”. *IEEE Access* 7 (2019): 13960–13988. 10.1109/ACCESS.2019.2894819.

Hussain, Faisal, et al. “IoT DoS and DDoS Attack Detection using ResNet”. *2020 IEEE 23rd International Multitopic Conference (INMIC)*. IEEE, 2020. 1–6.

Hussain, Faisal, et al. “Towards a Universal Features Set for IoT Botnet Attacks Detection”. *2020 IEEE 23rd International Multitopic Conference (INMIC)*. IEEE, 2020. 1–6.

Javaid, Mohd and Ibrahim Haleem Khan. “Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic”. *Journal of Oral Biology and Craniofacial Research* 11.2 (2021): 209–214. 10.1016/j.jobcr.2021.01.015.

Karabiyik, Umit and Kemal Akkaya. “Digital Forensics for IoT and WSNs”. *Mission-Oriented Sensor Networks and Systems: Art and Science*. Ed. Ammari and H. Springer International Publishing, 2019. 171–207.

Mariyanayagam, Dion, Pancham Shukla, and Bal S Virdee. “Bio-Inspired Framework for Security in IoT Devices”. *Intelligent Sustainable Systems*. Ed. Nagar, et al. Springer Nature Singapore, 2022. 749–757.

Mazhar, Muhammad Shoaib, et al. “Forensic Analysis on Internet of Things (IoT) Device Using Machine-to-Machine (M2M) Framework”. *Electronics* 11.7 (2022): 1126–1126. 10.3390/electronics11071126.

Stergiou, Christos, et al. “Secure integration of IoT and Cloud Computing”. *Future Generation Computer Systems* 78 (2018): 964–975. 10.1016/j.future.2016.11.031.

Tawalbeh, Lo’ai, et al. “IoT Privacy and Security: Challenges and Solutions”. *Applied Sciences* 10.12 (2020): 4102–4102. 10.3390/app10124102.

Vishwakarma, Ruchi and Ankit Kumar Jain. “A survey of DDoS attacking techniques and defence mechanisms in the IoT network”. *Telecommunication Systems* 73.1 (2020): 3–25. 10.1007/s11235-019-00599-z.

Yang, Geng, et al. “IoT-Based Remote Pain Monitoring System: From Device to Cloud Platform”. *IEEE Journal of Biomedical and Health Informatics* 22.6 (2018): 1711–1719. 10.1109/JBHI.2017.2776351.

Yousefnezhad, Narges, Avleen Malhi, and Kary Främling. “Security in product lifecycle of IoT devices: A survey”. *Journal of Network and Computer Applications* 171 (2020): 102779–102779. 10.1016/j.jnca.2020.102779.

Embargo period: The article has no embargo period.

To cite this Article: Kanakamedala, Phaneendra, Yarra Harika, Mamilla Krishnaveni, and Bhuvanesh Nallani. "**Internet of Things (IoT) Device Investigative Analysis Using Machine-to-Machine (M2M) Framework**." International Research Journal on Advanced Science Hub 05.05S May (2023): 50–59. http://dx.doi.org/10.47392/irjash.2023.S007