Machine Learning for Human Intelligence
2024, Vol. 2, Issue 2

Research Article

Enhancing IoT Forensics with Machine Learning-Based Anomaly Detection

Muhammad Faheem Khan[1] and Muhammad Naveed[2,⋆]

[1,2]Department of Computer Science, TIMES University, 60000, Multan, Punjab, Pakistan.;
Email: faheem@t.edu.pk, naveed@t.edu.pk
⋆Corresponding author: Muhammad Naveed (naveed@t.edu.pk)

Article History

Academic Editor:
Dr. Muhammad Sajid
Submitted: January 21, 2024
Revised: March 1, 2024
Accepted: September 1, 2024

Keywords:
Cybersecurity, Node-to-Node, Forensic Analysis, Machine Learning, Cyber Attacks, Internet of Things (IoT)

Abstract

The adaptability and rapid expansion of IoT systems have heightened the likelihood of cyberattacks. Resource-constrained IoT devices present a difficulty for security handlers in tracking records of various attacks during forensic analysis. Forensic analysis is typically conducted on devices to assess the extent of damage incurred as a result of various attacks. The primary aim of this research is to establish a framework that enables security to do forensic analysis on resource-constrained IoT devices. This study proposes a framework that adeptly does forensic analysis and identifies various sorts of attacks on endpoints (IoT devices) via a node-to-node (N2N) architecture. This proposed system integrates many forensic tools and machine learning techniques to detect different sorts of attacks. The issue of evidence retrieval from the compromised endpoint is resolved by utilizing a third-party log server. We utilized the logs from the Security Onion forensic server to ascertain the type and impact of the attack. This framework is capable of autonomously identifying assaults through the application of several machine learning methods.

1 Introduction

The Internet of Things (IoT) is a network of interconnected devices that utilize shared resources to securely transmit and receive data when an internet connection is available. Regarding straight-through processes, the IoT surpasses traditional networks due to its scalable features and broader perspective. The Internet of Things (IoT) has enhanced human living standards through widespread application, leading to the creation of various inventions, including intelligent buildings, smart grid stations, wearable devices, smart appliances, and home automation systems.

It is a well-established fact that IoT devices are continuously improving at an exponential rate. Nonetheless, security continues to pose a difficulty overall. The producers are allocating increased time and resources towards enhancement of the development of functionalities and the introduction of new features to attract a client base, rather than prioritizing investment in security concerns. The absence of security attention has led to several cyberattacks [1]. Other primary reasons of vulnerabilities in IoT devices include inadequate quality assurance testing, haste in product delivery, and insufficient legislative measures [2].

The figure presents statistics for a single country (USA) on a weekly basis over the past five years [15]. According to a research by Symantec in May 2018, IoT attacks surged by 600% from 2016 to the end of 2017. The primary challenges in today's business landscape are customer privacy and

the Internet of Things (IoT) [3, 4]. Broaden attack surface, Regulatory oversight, Internet of Things Business process vulnerabilities, data ownership issues, and vulnerabilities. The integration of these susceptible devices into the IoT system's network amplifies the attacker's threat landscape. Kaspersky's analysis indicates that 1.5 billion such attacks occurred in the first half of 2021. HP has estimated that up to 70 percent of IoT devices are vulnerable and susceptible to breaches [5]. The resource-constrained nature of IoT devices presents a problem for security analysts in tracking various attack recordings during forensic analysis, compounded by the significant limitation of inadequate evidence acquisition [6]. A framework must be built to detect and store evidence of such attacks. To implement more effective and enhanced forensic methodologies, specialized methods and technologies are necessary to fortify and safeguard the IoT environment as shown in Figure 1.

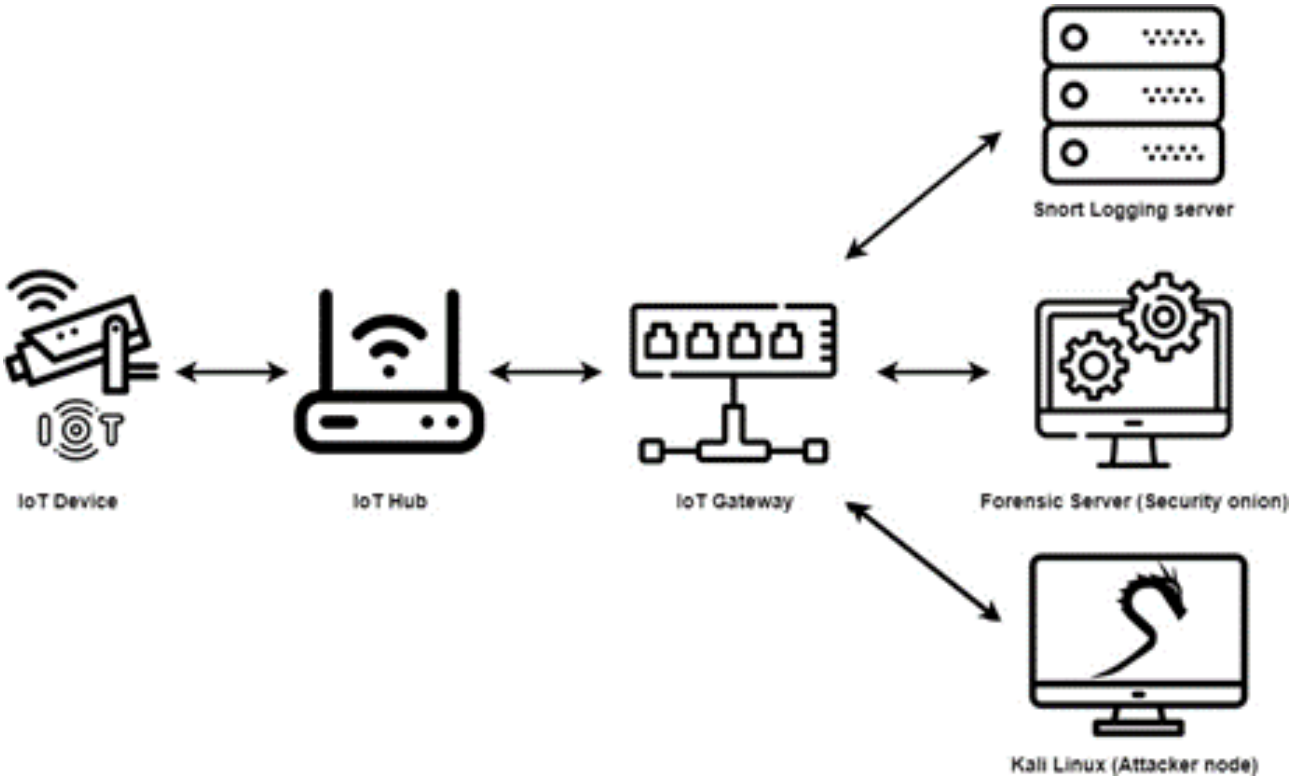

Figure 1: Designed framework.

We propose a forensic analysis system for IoT devices that automatically generates logs and issues alarms upon detecting threats. Forensic analysis is closely related to SIM, as it involves the comprehensive study of a crime after its occurrence to ascertain the causes, including the offender, motives, and intricate consequences of the security incident [7]. Forensic analysis is fundamentally distinct from network auditing; the former involves post-incident examination of security breaches to document actions taken and the timing of the violation, whilst the latter entails a proactive assessment of vulnerabilities inside a given network [8].

The suggested architecture addresses the limitation of data acquisition by utilizing a third-party server for logging purposes [9]. The data packets from IoT nodes are redirected to the specified machine, which stores files and produces alarms for malicious activity to be examined during forensic investigation. The history of these logs is retrieved from a designated forensic server and analyzed to obtain information regarding the perpetrators and the attacks. The machine learning technology is employed to autonomously identify assaults by supplying a dataset of logs.

The four fundamental processes of forensic analysis are data capture, assessment, analysis, documentation, and report preparation [10]. The primary issue encountered during data acquisition was the insufficient processing capability of the IoT devices [11]. We implemented a logging server in our suggested framework that employed Snort to identify assaults, maintain a record of malicious activity logs, and generate alerts. During the evaluation step, an examination of the acquired data is conducted

to extract pertinent information [13].

This suggested framework integrates forensic tools and machine learning methods. It also aids in establishing rules to identify attacks. The new regulations can then be incorporated into the proposed framework, facilitating the machine learning system's automatic detection of assaults. This subsequently produces multiple reports detailing the attack type and frequency, along with recommended measures for future reference. This offers a comprehensive overview of the assaults perpetrated by the assailants. We have employed various forensic tools and machine learning methods for the suggested system [14]. as shown in Figure 2. The research on identifying hostile activity in network traffic typ-

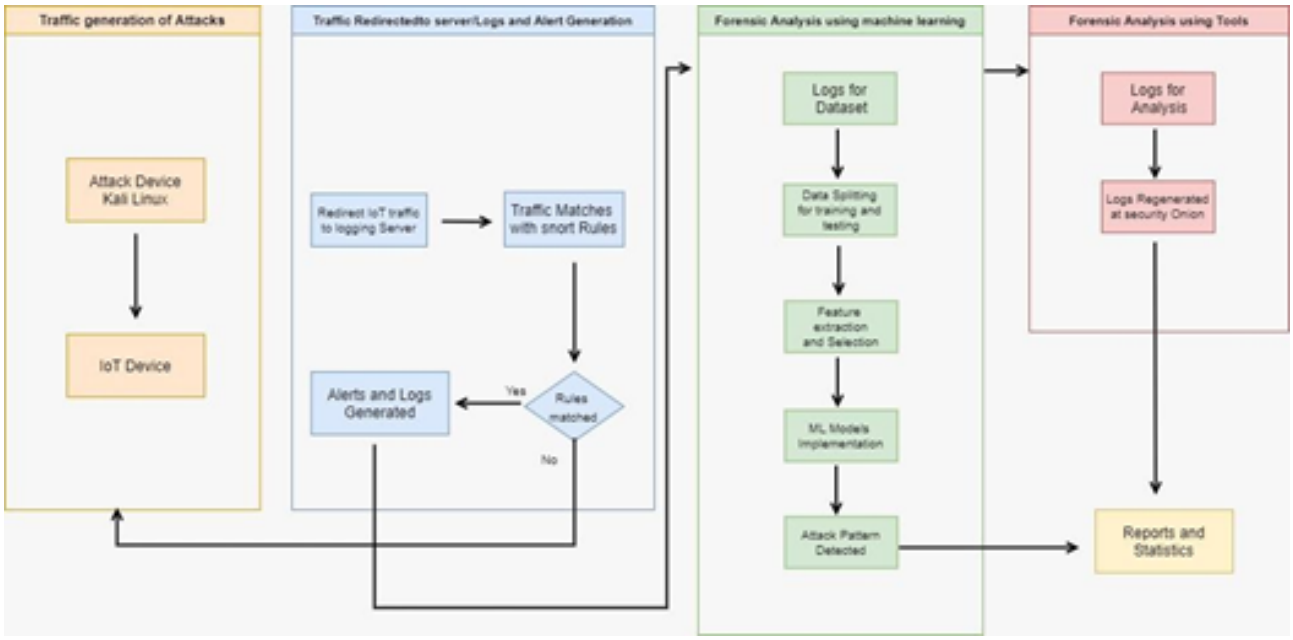

Figure 2: Proposed topology.

ically confounds investigators due to ignorance of traffic characteristics when training the suggested model. The identified research gap has prompted the authors to develop a forensic framework, which was evaluated against essential performance metrics [15]. A key feature of this architecture is its ability to compute, evaluate, and analyze extensive data sets without compromising the performance or quality of IoT devices. Any IoT-enabled company can utilize this technology to produce a dataset of IoT assaults, facilitating the observation and analysis of malicious activity. This framework maintains a record of cybercrimes, and the documented material can serve as evidence against the culprit in legal proceedings. Finally, security analysts can employ this integration of machine learning and forensic technologies to develop efficient systems for the detection of IoT intrusions [16].

This paper is structured as follows. Section II comprises a literature review that provides an overview of diverse attack vectors targeting IoT systems, forensic methodologies at both device and network levels, and intrusion detection technologies applicable to IoT. Section III delineates the approach via which our system attains optimal results. Section IV delineates the outcomes attained from the application of both forensics and machine learning models, demonstrating that their combined implementation yielded the anticipated results. Section V encompassed the conclusion of this research article and addressed prospective work pertaining to this subject.

2 Literature Review

Nisioti et al. evaluated the efficacy of current Intrusion Detection Systems against contemporary network threats. The study presented a classification of Intrusion Detection Systems based on Implementation, Architecture, and Detection methods. The significance of feature selection in training the core model for an IDS was underscored [17, 18]. This study concluded that an ideal selection for the core model may incorporate a combination of supervised and unsupervised models. Clustering

techniques that accommodate irregularly-shaped groups are superior to those designed for circular formations [19, 20]. The researchers asserted that Intrusion Detection Systems must evolve to incorporate correlation and attribution mechanisms to facilitate the forensic procedure. Ultimately, they suggested that IDS incorporate three more categories of traffic: data exfiltration, command and control communication, and ransomware, to enhance its efficacy in identifying malicious operations [21, 22]. Moreover, honeynet solutions are undervalued by researchers as ineffectual, despite their capability to obtain bot binaries and valuable insights on botnet communication patterns [23, 24].

Traditional forensic systems are deemed ineffective due to constrained hardware resources, rendering them obsolete as we go into the era of digital transformation. As hardware and software evolve, attackers are employing sophisticated techniques to compromise digital systems, vital infrastructure, and servers. Consequently, the forensic methodologies exhibit inefficiency due to the interconnectivity of all devices, resulting in a very limited volume of evidence. There is a necessity to allocate time to the development of advanced, efficient, and automated forensic analysis methods or techniques [25].

Another author [26] examines various virus observation techniques, highlighting their merits and potential misuses. Attitude-based observation involves the use of many technologies to assess the behavior of malware systems. Specific elements are acquired and addressed utilizing machine learning methodologies. Heuristic-based observations encompass human experience and diverse machine learning methodologies, enabling the detection of zero-day attacks; yet, they are incapable of tracing contemporary complicated malware. Model examination relies on procedures that involve analyzing behaviors and aggregating files exhibiting similar patterns, which can be classified as malware.

Artificial intelligence can be employed for malware detection through deep learning techniques [27], [28], [29]. These rely on multiple processes, including aspect extraction and neural network layer identification, with findings analyzed to detect malware. Cloud-based identification encompasses the transmission and storage of files in the cloud, with malware detection reliant on behavioral analysis and saved signatures. Mobile device identification techniques are employed in malware detection, particularly for diverse Android smartphones, which utilize several aspects to provide input to machine learning. IoT nodes are more susceptible to assaults since adequate security mechanisms are not developed due to the resource limitations of the devices.

3 Methodology

The suggested framework for conducting forensic investigation of attacked IoT nodes comprises four modules. The designed framework facilitates interconnection across all components of the IoT nodes. The IoT node is capable of bi-directional communication with all other components via the IoT hub and gateway.

The initial module involves traffic production for the attack, utilizing the Kali Linux operating system along with various exploitation tools to execute an attack on the IoT nodes for experimental purposes, hence producing the attacker's traffic. Authors have concentrated on the examination phase of large data, despite the fact that the distributed environment can also facilitate other phases. An illustration of massive data preservation with snapshots is provided by [30].

Conversely, a more adaptable paradigm is the Device-to-Cloud model, wherein devices link directly to a Cloud service provider for data storage or instruction reception. This paradigm enables the end-user to access their device via a web interface or smartphone application, allowing them to examine reports from data collection or modify the device's state [30]. This facilitates data aggregation and provides the user with the flexibility to transfer their data between cloud providers.

For experiments, we utilized several devices, including Raspberry Pi as the IoT endpoint [31], Snort for logging server [32, 33]. The attacker's communication is initially sent towards the IoT device, with received traffic then routed to the logging server. In this server, Snort rules identify malicious traffic and generate logs, which are subsequently turned into datasets and processed through machine learning using the Security Onion server. The final results were produced by the integration of machine learning and forensic onion server analysis as shown in Figure 3.

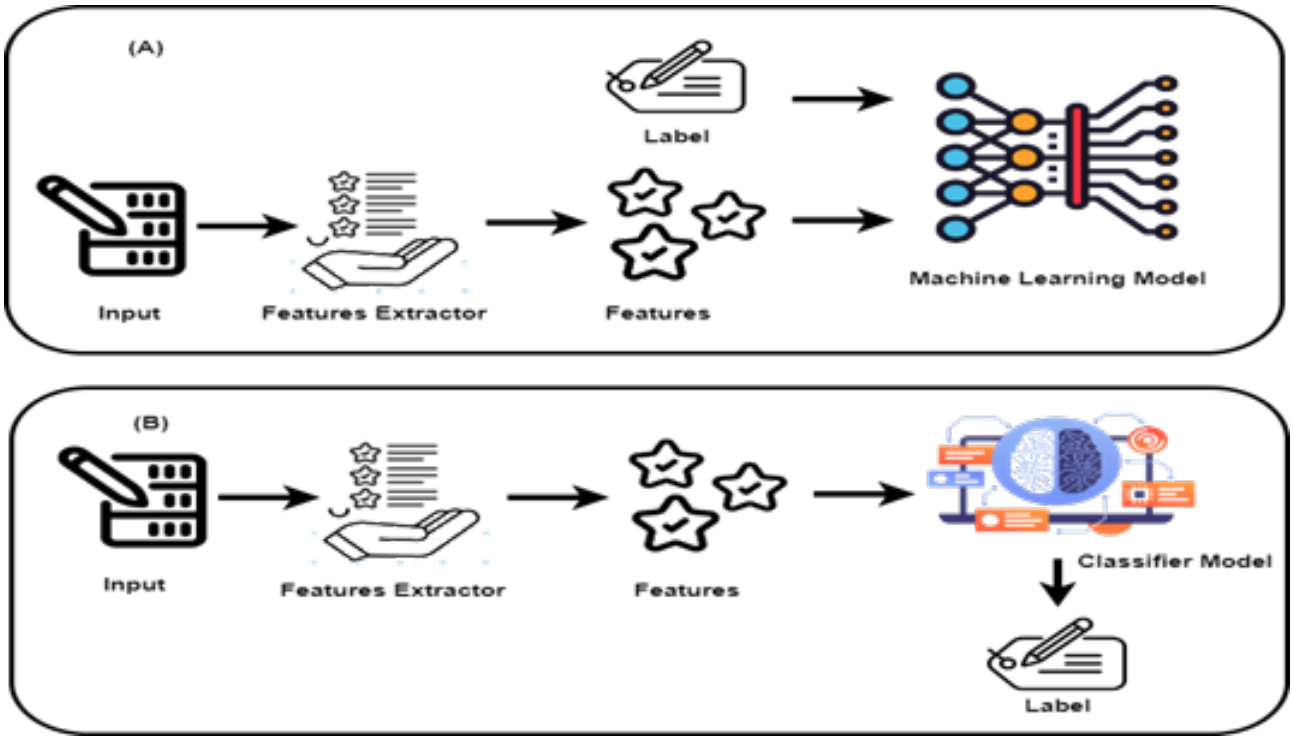

Figure 3: Training ML Model.

3.1 Traffic Generation for Attack

Network assaults, including ICMP Flood, TCP Synchronization Attack, and UDP Attack, represent some of the most critical challenges confronting contemporary web users. They are not only harmful to novice Internet users, but they also adversely affect huge organizations with extensive network workforces. It is categorized into two kinds of various network assaults: application-level attacks and network-level attacks. Network packet header information is typically examined to identify network-level attacks and ascertain if packets exhibit indicators of an attack.

3.2 Traffic Rerouting and Log/Alert Generation

We have developed a digital forensic framework for cloud crime investigation, consisting of five distinct phases. All phases encompassed by this framework operate analogously to established frameworks, with the exception of the third phase [34]. This phase, characterized by investigation and partial analysis, will be pivotal in the evaluation and interpretation of data generated by the cloud environment. After identifying the various phases required for cloud criminal investigation, we developed a generic control flow process for conducting digital forensics in the cloud. [35].

3.3 Forensic Server

The Security Onion virtual machine comprises two network interfaces; one facilitates server functionality, while the other is employed for packet sniffing to identify malicious activity. This entire system for keeping logs at the logging server resolves the issue of evidence acquisition. Security Onion incorporates a forensic server within our proposed framework, featuring an array of integrated tools, including Sguil, a log analysis application that serves as a graphical user interface for Snort. To obtain information regarding the attacks, we recreate the logs, having previously recorded them using the Snort IDS. Subsequent to the training of this machine learning model on the training dataset, it is evaluated using both the training and real-world data as shown in Figure 4.

Ultimately, data is categorized and tagged according to its nature to identify legitimate and harmful behavior, as illustrated in Table 1.

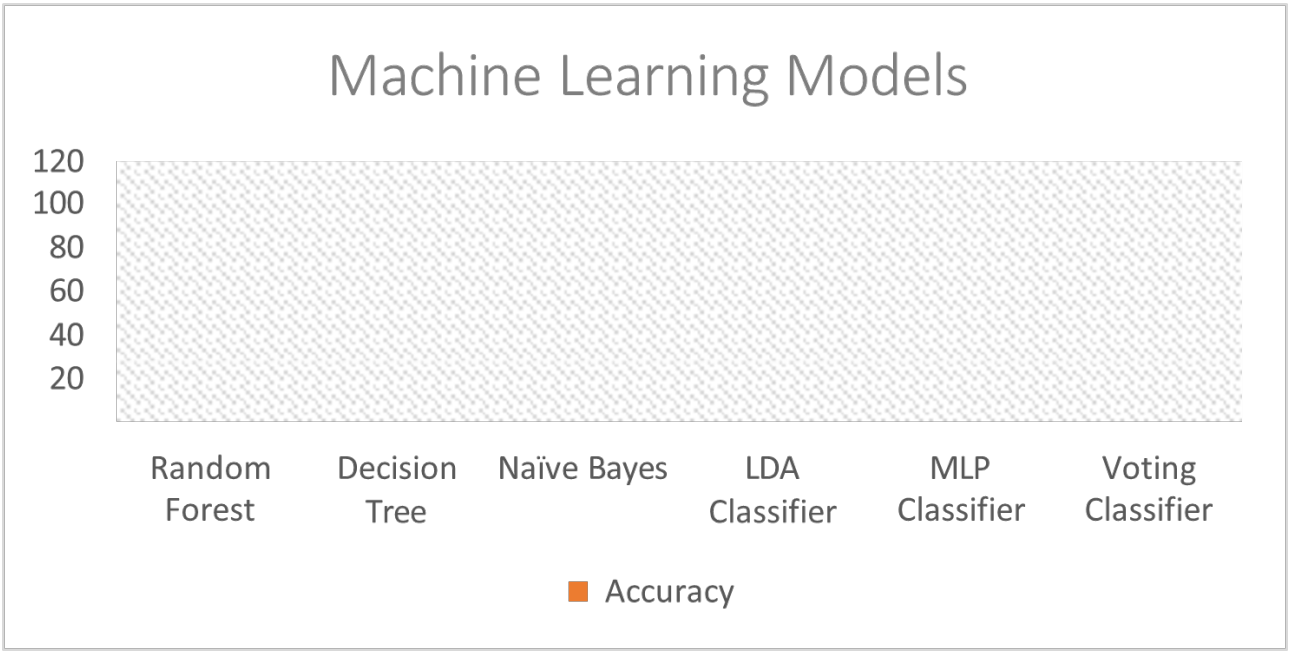

Figure 4: Accuracy comparison.

Table 1: Machine Learning Data Annotation

Category	**Classification**	**Identifiers**
Authentic	Standard	0
Malevolent	DDoS SYN Flood	1
Malevolent	Brute Force	2
Malevolent	Man-in-the-Middle ARP Spoofing	3
Malevolent	Port Scan	4

Data preparation primarily aims to enhance the performance of predictive machine learning models. Extraneous fields that do not aid in classification have been eliminated from the dataset, and the numerical features have been normalized to a range between zero and one. Fields formerly utilized for data labeling must be eliminated, as this will compromise the data's integrity and degrade performance.

Dataset Division: The machine learning model is trained using the training set, while the test set is employed to evaluate the correctness of the learned model. The ratio for splitting is 7:3, for training and testing, respectively.

The training of the machine learning model involves utilizing inputs derived from previously extracted features. Diverse techniques are employed to execute machine learning approaches, including optimal installation. The efficacy of machine learning predominantly relies on pre-trained data collected using diverse methodologies. The operation of machine learning relies on many steps: (1) initially providing raw data to extract the necessary features, and (2) thereafter forwarding these characteristics to a trained model for label predictions, as previously conducted with our data. Consequently, an attack that transpires can be readily identified from these anticipated labels.

Our primary focus is to enhance node-to-node interaction based on the IoT device. The protocol of our concept assigns specialized IP addresses to IoT devices, while the other machines operate within a constrained architecture. The objective of creating a domain that emphasizes forensic analysis based on IoT architecture leveraging node-to-node connectivity. In this context, many assaults are executed on IoT devices [37], [38], [39]. A pre-trained dataset is employed to assess this proposed solution for machine learning. The discovery of attack enhancement is more successful and timely when utilizing the combined functionality of machine learning and forensic models. Following the implantation of these

measures, a comprehensive ledger is created detailing the attacks, their frequency, and recommended actions for implementation. The report enables us to delineate the entire attack script and facilitates communication with the perpetrators. as shown in Figure 5.

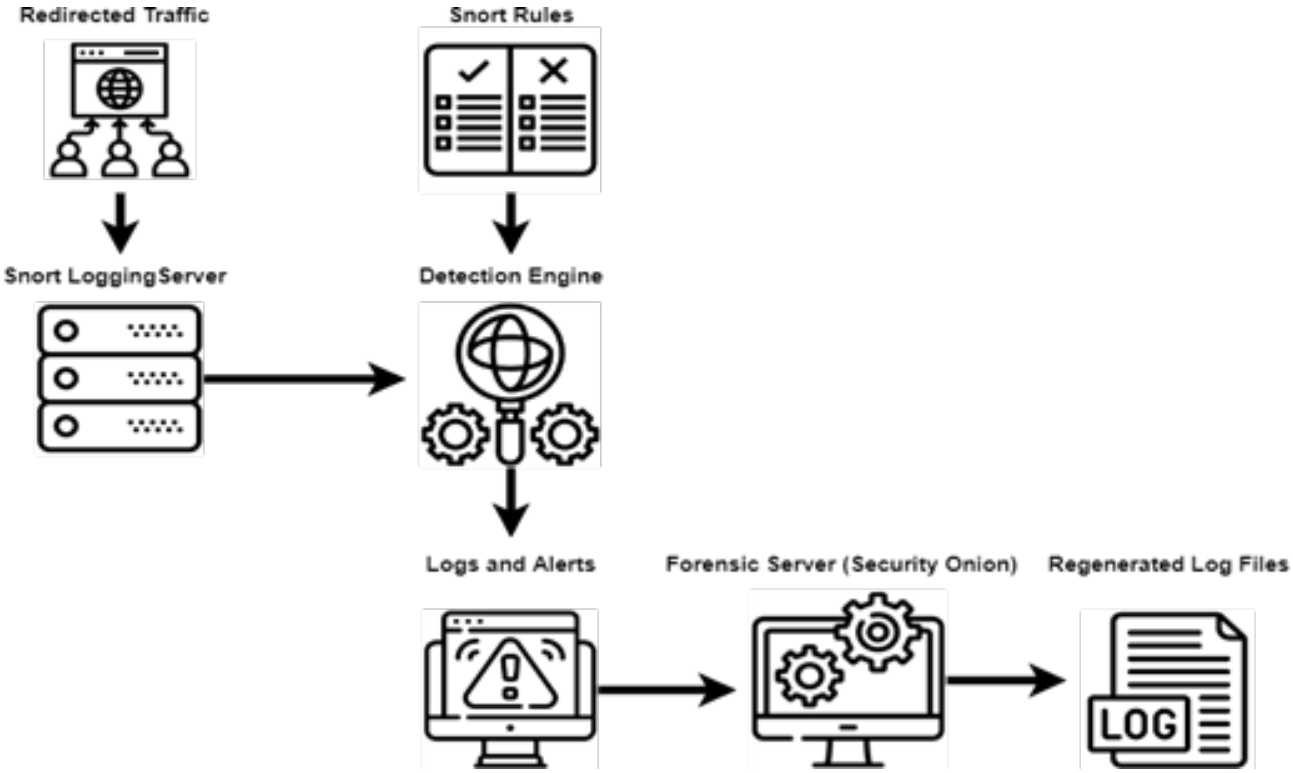

Figure 5: Architecture of forensic.

3.4 Forensic Server Analysis

For the forensic analysis, we utilized Security Onion, a Linux-based operating system. This operating system has security tools designed for log management, intrusion detection system features, and monitoring capabilities. Log interpreter tools facilitated the visualization of log files. Even when delving far into the logs, these tools assist us in analyzing the various sorts of attacks by separating them through a color system. Squert is utilized for analyzing DDoS attack logs, quantitatively indicating the frequency of SSH requests started by the attacker, while also demonstrating that the attacker does not want to establish a connection, but rather to inundate the endpoint. The generated logs indicate that the attacker attempted port scanning for open ports, as well as the acquisition of information regarding the operating system, MAC address, and SSH key.

3.5 Machine Learning Algorithm Performance

Machine learning algorithms are employed for the automated identification of assaults on IoT nodes. To achieve this objective, we employed multiple machine learning techniques on the dataset derived from the logs collected by the logging server. Decision Trees have superior performance compared to other machine learning algorithms, achieving an accuracy of 97.29 percent. The accuracy comparison of the employed ML model, illustrated in Figure 6, elucidates the design of the forensic and logging server. The incoming traffic to the IoT device is redirected to the Snort logging server, which is configured with Snort rules, thereby creating a comprehensive detection engine. Based on established rules, it classifies traffic as either malicious or regular, generating logs and alarms for malicious traffic, which are forwarded to the forensic server, resulting in the creation of regenerated log files for examination.

Various types of categorization machine learning models have been employed to differentiate between legal and malicious packets, achieving an accuracy of 88 percent with the presented models. In

contrast, our suggested methodology, which combines forensic server logs generated with forensic server tools as a dataset alongside machine learning algorithms, yields an accuracy of 97.29 percent. These machine learning algorithms have already attained state-of-the-art outcomes for various problems [40], [41], [42], [43], [44], [45], [46].

4 Conclusion

Forensic investigation is the meticulous examination of a crime scene conducted to ascertain the underlying causes of the offense. Our suggested system efficiently tackles the challenges of limited memory and storage in IoT devices. The suggested framework functions inside a straight-through process context, enhancing its efficiency and reliability. Network traffic is transmitted to logging servers with ongoing communication between devices. Regulations are established at the logging server to compare and subsequently analyze network traffic. The records of malicious traffic are securely stored and can be accessed through multiple methods at the forensic server. Subsequent reports detailing the sorts of attacks, their frequency, and recommended actions were produced. This data will facilitate the tracing of attackers by providing a comprehensive overview of the assault footprints. This article will broaden its scope by incorporating a high rate of assault along with the division of categories and sub-classifications. The utilized data set consists of prevalent attacks on IoT devices, rendering it a constrained collection of data. The attributes of this model can be enhanced through the implementation of more sophisticated procedures. The dataset of everyday utilized IoT devices can also be incorporated to enhance the scope of ML-based forensic investigation.

References

[1] Sikder, A., Petracca, G., Aksu, H., Jaeger, T., & Uluagac, A. (2021). A study on sensor-related threats and attacks targeting smart devices and applications. *IEEE Communications Surveys & Tutorials*, *23*(2), 1125-1159.

[2] Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). Challenges and solutions in IoT privacy and security. *Applied Sciences*, *10*(12), 4102.

[3] Hussain, F., Abbas, S. G., Husnain, M., Fayyaz, U. U., Shahzad, F., & Shah, G. A. (2020, November). Detection of IoT DoS and DDoS attacks via ResNet. In *2020 IEEE 23rd International Multitopic Conference (INMIC)* (pp. 1-6). IEEE.

[4] Over fifty percent of IoT devices are susceptible to significant attacks. (2022). Retrieved September 29, 2022, from https://threat-post.com/half-iot-devices-vulnerable-severe-attacks/153609/

[5] O'Donnell, A. L., & O'Donnell, L. Over fifty percent of IoT devices are susceptible to significant attacks. *Threatpost*. Retrieved from https://threatpost.com/half-iot-devices-vulnerable-severe-attacks/153609/

[6] Asif, S., Ambreen, M., Muhammad, Z., ur Rahman, H., & Iqbal, S. Z. (2022). Cloud computing in healthcare: Examination of threats, vulnerabilities, future challenges, and mitigation strategies. *LC International Journal of STEM*, *3*(1), 63-74.

[7] Rughani, P. H. (2017). Acquisition of IoT evidence—challenges and issues. *Advancements in Computational Sciences and Technology*, *10*(5), 1285-1293.

[8] Karabiyik, U., & Akkaya, K. (2019). Digital forensics for Internet of Things and wireless sensor networks. In *Mission-oriented sensor networks and systems: Art and science* (pp. 171-207). Springer.

[9] Forensic Analysis - A comprehensive overview. *ScienceDirect Topics*. Retrieved from https://www.sciencedirect.com/topics/chemistry/forensic-analysis

[10] Lord, N. (2018). What constitutes security incident management? The cybersecurity incident management process: Examples, best practices, and additional insights. *Digital Guardian's Data Insider*.

[11] Rahman, H., Arshad, H., Mahmud, R., & Mahayuddin, Z. R. (2017, October). A framework for breast cancer visualization employing augmented reality x-ray vision techniques in mobile technologies. In *AIP Conference Proceedings* (Vol. 1891, No. 1, p. 020116). AIP Publishing LLC.

[12] Haider, S. K., Jiang, A., Almogren, A., Rehman, A. U., Ahmed, A., Khan, W. U., & Hamam, H. (2021). Energy-efficient UAV flight path model for cluster head selection in next-generation wireless sensor networks. *Sensors*, *21*(24), 8445.

[13] Horsman, G. (2022). A sequence of data collection for digital forensic investigations. *Journal of Forensic Sciences*, *67*(3), 1215-1220.

[14] Ghabban, F. M., Alfadli, I. M., Ameerbakhsh, O., AbuAli, A. N., Al-Dhaqm, A., & Al-Khasawneh, M. A. (2021, June). Comparative analysis of network forensic technologies and techniques in network forensics. In *2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)* (pp. 78-83

[15] Zia, Z. U. R., Rahman, H. U., Malik, M. H., & Jahngir, A. (2020). Technical challenges in achieving ultra-reliable & low latency communication in 5G cellular-V2X systems. *LC International Journal of STEM*, *1*(3), 89-95.

[16] Abbas, M., Arshad, M., & Rahman, H. (2020). Detection of breast cancer using neural networks. *LC International Journal of STEM*, *1*(3), 75-88.

[17] Hameed, S., Khan, F. I., & Hameed, B. (2019). Understanding security requirements and challenges in Internet of Things (IoT): A review. *Journal of Computer Networks and Communications*, *2019*.

[18] Arıs, A., Oktug, S. F., & Voigt, T. (2018). Security of internet of things for a reliable internet of services. In *Proceedings of the 2018 International Conference on Internet of Things (ICIoT)*.

[19] Kasinathan, P., Pastrone, C., Spirito, M. A., & Vinkovits, M. (2013, October). Denial-of-Service detection in 6LoWPAN based Internet of Things. In *2013 IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob)* (pp. 600-607). IEEE.

[20] Kasinathan, P., Costamagna, G., Khaleel, H., Pastrone, C., & Spirito, M. A. (2013, November). An IDS framework for internet of things empowered by 6LoWPAN. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (pp. 1337-1340).

[21] Oh, D., Kim, D.,& Ro, W. W. (2014). A malicious pattern detection engine for embedded security systems in the Internet of Things. *Sensors*, *14*(12), 24188-24211.

[22] Fagbola, F. I., & Venter, H. S. (2022). Smart digital forensic readiness model for shadow IoT devices. *Applied Sciences*, *12*(2), 730.

[23] Koroniotis, N., Moustafa, N., & Sitnikova, E. (2020). A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework. *Future Generation Computer Systems*, *110*, 91-106.

[24] Scheidt, N., & Adda, M. (2020, August). Identification of iot devices for forensic investigation. In *2020 IEEE 10th International Conference on Intelligent Systems (IS)* (pp. 165-170). IEEE.

[25] Patil, A., Banerjee, S., Jadhav, D., & Borkar, G. (2022). Roadmap of Digital Forensics Investigation Process with Discovery of Tools. In *Cyber Security and Digital Forensics* (pp. 241-269).

[26] Aslan, Ö. A., & Samet, R. (2020). A comprehensive review on malware detection approaches. *IEEE Access*, *8*, 6249-6271.

[27] Wahab, M. A. A., Surin, E. S. M., Nayan, N. M., & Rahman, H. (2021). MAPPING DEFORESTATION IN PERMANENT FOREST RESERVE OF PENINSULAR MALAYSIA WITH MULTITEMPORAL SAR IMAGERY AND U-NET BASED SEMANTIC SEGMENTATION. *Malaysian Journal of Computer Science*, 15-34.

[28] Abid, I., Almakdi, S., Rahman, H., Almulihi, A., Alqahtani, A., Rajab, K., ... & Shaikh, A. (2022). A convolutional neural network for skin lesion segmentation using double U-Net architecture. *Intelligent Automation and Soft Computing*, *33*(3), 1407-1421.

[29] Rahman, H., Bukht, T. F. N., Imran, A., Tariq, J., Tu, S., & Alzahrani, A. (2022). A deep learning approach for liver and tumor segmentation in CT images using ResUNet. *Bioengineering*, *9*(8), 368.

[30] Pal, M. (2005). Random forest classifier for remote sensing classification. *International Journal of Remote Sensing*, *26*(1), 217-222.

[31] Jagannathan, G., Pillaipakkamnatt, K., & Wright, R. N. (2009, December). A practical differentially private random decision tree classifier. In *2009 IEEE International Conference on Data Mining Workshops* (pp. 114-121). IEEE.

[32] Feng, X., Li, S., Yuan, C., Zeng, P., & Sun, Y. (2018). Prediction of slope stability using naive Bayes classifier. *KSCE Journal of Civil Engineering*, *22*(3), 941-950.

[33] Balakrishnama, S., & Ganapathiraju, A. (1998). Linear discriminant analysis-a brief tutorial. *Institute for Signal and Information Processing*, *18*(1998), 1-8.

[34] Windeatt, T. (2006). Accuracy/diversity and ensemble MLP classifier design. *IEEE Transactions on Neural Networks*, *17*(5), 1194-1211.

[35] Ruta, D., & Gabrys, B. (2005). Classifier selection for majority voting. *Information Fusion*, *6*(1), 63-81.

[36] Pajankar, A. (2021). *Practical Linux with Raspberry Pi OS*. Apress.

[37] Krishna, G. S., Kiran, T. S. R., & Srisaila, A. (2021). Testing performance of Raspberry Pi as IDS using SNORT. *Materials Today: Proceedings*.

[38] Heenan, R., & Moradpoor, N. (2016, May). Introduction to security onion. In *The First Post Graduate Cyber Security Symposium*.

[39] GitHub. (2022). *GitHub - ahlashkari/CICFlowMeter: CICFlowmeter-V4.0 (formerly known as ISCXFlowMeter) is an Ethernet traffic Bi-flow generator and analyzer for anomaly detection that has been used in many Cybersecurity datsets such as Android Adware-General Malware dataset(CICAAGM2017), IPS/IDS dataset(CICIDS2017), Android Malware dataset (CICAndMal2017) and Distributed Denial of Service (CICDDoS2019)*. [online] Available at: https://github.com/ahlashkari/CICFlowMeter [Accessed 29 September 2022].

[40] Rahman, H., Arshad, H., Mahmud, R., Mahayuddin, Z. R., & Obeidy, W. K. (2017). A framework to visualize 3d breast tumor using x-ray vision technique in mobile augmented reality. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, *9*(2-11), 145-149.

[41] Salleh, S., Mahmud, R., Rahman, H., & Yasiran, S. S. (2017). Speed up robust features (SURF) with principal component analysis-support vector machine (PCA-SVM) for benign and malignant classifications. *Journal of Fundamental and Applied Sciences*, *9*(5S), 624-643.

[42] Obeidy, W. K., Arshad, H., Yee Tan, S., & Rahman, H. (2015, November). Developmental analysis of a markerless hybrid tracking technique for mobile augmented reality systems. In *International Visual Informatics Conference* (pp. 99-110). Springer, Cham.

[43] Tariq, J., Alfalou, A., Ijaz, A., Ali, H., Ashraf, I., Rahman, H., ... & Rehman, S. (2022). Fast intra mode selection in HEVC using statistical model. *Computers, Materials and Continua*, *70*(2), 3903-3918.

[44] Mahmood, T., Li, J., Pei, Y., Akhtar, F., Imran, A., & Yaqub, M. (2021). An automatic detection and localization of mammographic microcalcifications ROI with multi-scale features using the radiomics analysis approach. *Cancers*, *13*(23), 5916.

[45] Imran, A., Nasir, A., Bilal, M., Sun, G., Alzahrani, A., & Almuhaimeed, A. (2022). Skin cancer detection using combined decision of deep learners. *IEEE Access*.

[46] Imran, A., Li, J., Pei, Y., Akhtar, F., Mahmood, T., & Zhang, L. (2021). Fundus image-based cataract classification using a hybrid convolutional and recurrent neural network. *The Visual Computer*, *37*(8), 2407-2417.

[47] Imran, A., Li, J., Pei, Y., Akhtar, F., Yang, J. J., & Dang, Y. (2020). Automated identification of cataract severity using retinal fundus images. *Computer Methods in Biomechanics and Biomedical Engineering: Imaging & Visualization*, *8*(6), 691-698.

[48] Imran, A., Li, J., Pei, Y., Akhtar, F., Yang, J. J., & Wang, Q. (2019). Cataract detection and grading with retinal images using SOM-RBF neural network. In *2019 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 2626-2632). IEEE.

[49] Imran, A., Li, J., Pei, Y., Mokbal, F. M., Yang, J. J., & Wang, Q. (2019). Enhanced intelligence using collective data augmentation for CNN based cataract detection. In *International Conference on Frontier Computing* (pp. 148-160). Springer, Singapore.

[50] Bilal, A., Sun, G., Mazhar, S., Imran, A., & Latif, J. (2022). A transfer learning and U-Net-based automatic detection of diabetic retinopathy from fundus images. *Computer Methods in Biomechanics and Biomedical Engineering: Imaging & Visualization*, 1-12.