2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME) | 978-1-6654-1262-9/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICECCME52200.2021.9590959

Implementation of Cyber Threat Intelligence Platform on Internet of Things (*IoT*) using TinyML Approach for Deceiving Cyber Invasion

Abir Dutta
PhD. Scholar
Research and Technology Development Center,
Sharda University, Gr. Noida
abir_wbsetcl@yahoo.com

Shri Kant
Center of Cyber Security and Cryptology
Deptt. of Computer Sc. and Engg,
Sharda University
shrikant.ojha@gmail.com

***Abstract*- In recent past years' application of Internet of Things (IoT) technology has been radically enhanced in various domain across the sphere. Due to less computational capabilities and non-applicability of conventional security protocol, both wired or wireless communication channel of IoT devices are facing major security issues and challenges in cyber security landscape. Enforcement of upgraded Tactics, Technology and Procedure (TTPs) by the modern cyber criminals turns the traditional signature based threat detection mechanism inefficient for implementation of resilient as well as comprehensive security measures in IoT artifacts. In this backdrop, integration of Cyber Threat Intelligence (CTI) platform and machine learning approach [1], with the conventional security mechanism assists us to develop an effective, robust and secure framework for the smart devices to combat all current and futuristic security concerns and develop an automated, responsive security architecture pertaining to the IoT devices. This paper focuses on the various security issues and challenges along with layer wise security protocols applicable for the IoT devices. Furthermore, author designed a TinyML based framework using Tensorflow module, amalgamated with CTI platform for predicting potential threat propagated to the smart devices employing Naïve Bayes supervised ML classifier and the final solution is predicting threat accurately 96.8% and 96.3% for training and test dataset respectively.**

***Keywords:* Internet of Things (IoT), Machine Learning, Artificial Intelligence, Cyber Threat Intelligence.**

I. Introduction

According to the recent survey conducted by the Norton, US, by 2025 more than 21 billion things will be connected to the Internet [2], with significantly high rate of growth for use of IoT devices in compared to the connected IoT devices in 2016. There is multiple definition of IoT, however, best comprehensive explanation of these devices was coined by Haller et al "A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business process". Exponential expansion of IoT ecosystem also amplifies the window of attack surface and as consequence aggressive monitoring and upgradation of combat technique are mandatory for safe keeping of data and things from the malicious attack.

Crucial aspect of things over the Internet is, plenty utilization of such devices in house hold sectors, such as smart TV, Mobile, Sensor watch and many more, which are prone to be attacked due to less security measures implemented in domestic sector. Additionally, heterogeneity and versatile application of smart things becomes a lucrative choice for the invaders. IoT devices are composed of several embedded microcontrollers, thus these devices are limited in terms of resources namely, memory and processing capabilities, power consumption module.

In the aforementioned backdrop, traditional security system might not be the suitable solution for smart devices as they demand higher resource allocation to be high-yielding in the respective cyberspace. Existing signature based or anomaly based detection systems are highly dependent on the signature or on the baseline behavioral analysis of the threat. Integration of Machine learning and Deep learning [3] with the existing security solution enhance the prediction of adversary significantly at the same time the overall architecture becomes more complicated, time consuming as well as higher memory and storage is required to accommodate the automated and model driven alert triggering facility.

IoT devices are mostly affected by Bot-IoT attack [4] and DoS attack [5] and these attacks can be arrested by detection of attack well in advance. Cyber threat intelligence is an evidence-based knowledge about the malicious activity for arresting the attack in cyberspace. Association of AI and ML with cyber threat intelligence generates an automated, resilient framework to extract intelligence from various sources and blending this actionable threat intelligence to existing security mechanism of IoT eco space in order to perform quickly, accurately, effectively and efficiently despite of the resource constraints.

However, to mitigate several issues such as high power consumption ratio, higher in-build memory capacity, higher time required to respond against the alert of the existing threat detection models, author proposed CTI-TinyML based security

Authorized licensed use limited to: PES University Bengaluru. Downloaded on February 10,2023 at 05:01:20 UTC from IEEE Xplore. Restrictions apply.

architecture for cyber threat detection which take mW or even below power consumption with few MB memories required to implement the proposed model in order to predict the attacks more promptly and accurately. This model will be designed by implementing Tensorflow Lite Keras high level API in Tiny ML platform for diminishing False Positive alert and focusing only on the True security alerts.

Rest of this paper is organized as- Section 1 illustrate potential network security protocols pertinent to the IoT security layers along with various security attacks relevant to the smart devices. Section 2 refers the role of cyber threat intelligence in the IoT cyber security domain. Section 3, represents embedding of tiny ML based model in a microcontroller based architecture. Section 4 describe the benefits of Integration of AI and ML with Cyber Threat Intelligence platform. Section 5 demonstrate a proposed model which is able to detect threats, using a trained supervised TinyML oriented model based on the actionable threat intelligence platform. Finally, Section 6 specify the conclusion of this research work.

II. An overview of IoT Architecture

A. Security Protocols

IoT landscape is defined as the large scale of heterogeneous devices connected over the Internet, which form an IoT ecosystem. IoT architecture primarily consists of Four layers- Application, Network, Perception and Physical. Mapping of functionalities and the concerned protocol [6] of these layers is depicted (TABLE I)

TABLE I. Layer wise Protocols for IoT ecosystem

Network Layer	***Functionality***	***Protocols***
Physical Layer	Physical Access Control	DSL, USB, Ethernet, 4G/5G, ZigBee, VSAT
Perception Layer	• Sensor • Nodes • Smart System Devices • Used Frequency-low Radio Frequency (LoRa)	PLC, GPS, WSN
Network Layer	• Big data analysis • Connectivity • Encryption of Data • Used Frequency-Wi-Fi, Bluetooth, Short range	ICMP, IGMP, IPv4/v6, OSPF, TCP/UDP, SLIP, RLP, ROLL, TLS
Application Layer	• Mobile and web app based devices • Cloud app based devices • Enterprise app device tools	MQTT, HTTP, DDS, SSH, NTP, AMQP, XML, JSON, CoAP, XMPP, REST

B. Attack Types in IoT devices

Physical damage of a smart device which may be referred as physical attack, is equivalent threatening as other active and passive attack. Nowadays attack surface which includes clouds, physical Things, web application, Network also enhanced many fold due to colossal use of IoT devices worldwide. Different active attacks [7] like, spoofing, MITM, DoS, tampering of data etc. can leads to impersonate the user credential, compromise of authentication and repudiation and attacks the CIA triad of security directly. On the other side, passive attacks such as traffic analysis [8] can affect the privacy of a user.

III. Role of cyber threat intelligence in the IoT cyber security domain

Rapid shifting of attack technology placed the traditional signature based threat detection mechanism of IoT appliances, into severe challenging position, which generates the necessity of combining of cyber threat intelligence platform and existing communication methodology. Unlike conventional security approach, CTI platform allows to detect attacks well in advance depend on the evidence based knowledge as fed to the security appliances which are integrated with in the Things over the Internet. Although framework for real-time dataset generation [9], Network Intrusion detections system [10] and IoT Based Smart Grids [11] are potential solution for threat detection of smart devices but CTI based security measures facilitates detection of 0-Day vulnerabilities potentially compared to the signature based anomaly detection technique.

Implementation of actionable threat data feed collected from CTI platform is used to enhance the security system of software defined networks (SDN) [12]. In cyber threat intelligence platform STIX format has been extended [13] to facilitate the interpretation of critical patterns. Extension of STIX allows marking the feature of an object and these features represents relationship among various objects. Intelligence information can be presented in graph that could support threat detection mechanism provided by the conventional security system. Comprehensive assessment model of CTI in user perspective assists to evaluate intelligence in multi-dimension with quantitative index system.

A. Classification of Threat Intelligence:

Strategic threat intelligence gives a broader overview about "how" threats and attacks are changing day by day in threat landscape. Strategic TI includes chronological trends and motivations of the attacker along with the awareness about "who" and "why" behind the attack, which facilitates clues regarding their future scope of operations and tactic. This allows security analysts to adopt appropriate defensive measurements in an efficient and effective manner. Operational threat intelligence provides the perception of threat actors about their methodology and discloses potential threat. It includes- 1) artefacts, tools and infrastructure used by the threat community 2) technique and procedure used by the group 3) upcoming TTPs- emerging exploits and phishing methodology. Tactical threat intelligence is meant for archival document related cyber-attacks, cater as a corpus of evidence (for compliance, law enforcement, investigations, legal purposes, etc.).

B. Technical Threat Intelligence (TTI):

The defender must be cautious about the data fundamentals in addition to the threat actors, to combat cyber-attacks often referred as indicator of compromise (IoC). IoC yields intelligence, is very synonymous to TTI. IoC is collected from various sources namely inner sources (log, network traffic information, honeynet, etc.), nation nominated sources (law enforcement, compliance, etc.), corporate sources, open Source (i.e., public forums) and in house intelligence collection (attacker forums, Facebook, etc.).

Authorized licensed use limited to: PES University Bengaluru. Downloaded on February 10,2023 at 05:01:20 UTC from IEEE Xplore. Restrictions apply.

C. Gathering of Threat Intelligence:

Security system of an enterprise can be made more robust and reliable if appropriate intelligence is amalgamated with the traditional security system, which can be achieve by integrating threat intelligence with the existing safety appliances. These actionable threat intelligences can be gathered from various available sources which are further categorized as structured and unstructured data source.

a) *Structured data sources:* Now-a-days various “open source intelligence” (OSINT) is available which are responsible for generating continuous flow of intelligence periodically. Few of the structured data source of intelligence generation are, “Structured Threat Information Expression” (STIX) [14], Mitre’s “Common Vulnerabilities and Exposures” (CVE) [15], Mitre’s “Common Weakness Enumeration” (CWE) [16], “Cyber Observable eXpression” (CybOX), “Trusted Automated eXchange of Indicator Information” (TAXII) etc. which provides up-to-date source of actionable threat intelligence that can be utilized by the organizations to know the motivation and strategies of threat actors well in advance.

b) *Unstructured data source:* Intelligence can be generated from other various sources such as IoT devices log, blacklisted IPs, IoT hacker’s forum (including other languages apart from English), social media community, even from the in-house raw data (logs containing attack signature of various security appliances of the organization).

D. Challenges in Cyber Threat Intelligence:

This is crucial to identify issues and challenges associated with cyber threat intelligence [17], and this section summarizes few challenges-

a) *High Voluminous Threat Intelligence data degrade the quality of Threat Intelligence:* Threat intelligence data feeds accumulated from free source, open source or closed source leads to rapid growth rate of threat data feed and an overwhelming threat intelligence data feed limits the decision support system of security personnel.

b) *Non- sharing Threat Intelligence:* According to the survey of European Union Agency for Network and Information Security (ENISA), it is obvious that, majority of the organizations are unwilling to disclose and share their threat intelligence publicly. Additionally, organizations are afraid of negative publicity, legal rules and regulation quality of threat information budget, unaware of being attacked.

c) *Heterogeneous nature of Threat data feed:* Intelligence collected from various sources is in different format and generate an interoperability concern. MITRE generates three standards to overcome this heterogeneous nature of Intelligence data feed namely, Structured Threat Information Expression (STIX), Cyber Observable Expression (CYBOX) and Trusted Automated Exchange of Indicator Information (TAXII).

In view of the above challenges which generate hindrances towards implementation of threat intelligence by the organizations integration of AI and ML [18-20] with the CTI platform becomes indispensable in recent cyberspace. As a consequence, it develops a resilient, sustainable, organized and reliable intelligence repository for the organizations in automated fashion. At the same time this approach migrates the security paradigm into reactive to proactive mechanism.

IV. TinyML Model description

TinyML is one of the fastest-growing areas of Deep Learning. In a nutshell, it’s an emerging field of study that explores the types of models you can run on small, low-power devices like microcontrollers. TinyML can be defined as “subset of machine learning architecture, techniques, tools and approaches capable of performing on-device analytics for a variety of sensing modalities (vision, audio, motion, identification etc.) at mW (or below) power range targeting predominately battery operated devices”.

TinyML is a subset domain of Deep Learning inspired by "OK Google". This field is focused on the interference not on the training only. Model developed by TinyML performs with highly accuracy in terms of prediction, speed, with lesser parameter to train the system as well as in hardware optimized paths. TinyML models can be easily accommodate with in small microcontroller with few MB of RAM and few KB in storage and these targeting models are works smoothly with reduced battery power consumption with "mW" (milli Watt) range of power only [30] Tiny ML has significant data mining and analytics capabilities and numerous cases and verticals. Comprehensive definition of TinyML is "Running machine learning on embedded devices at an average of less than one mill watt in power". Here the power management is crucial as it handles the devices running on battery as well and without manual intervention or remains unattended state. TinyML models are deployed on the microcontroller (MCU) which possess the characteristics like- On-Chip Memory, Essentially self-contained, Generally bare metal or Real time operating system deployment, Containers are not supported by the microcontrollers. MCU can perform wide range of tasks such as predictive maintenance, simple speech recognition, person detection using camera, gesture recognition using accelerometer etc. Arduino is one of most popular IDE to design a TinyML model. Choice of embedded IDE highly depends on MCU choice. MCU language supports typically include assembler, C and C++. ML models may be embedded as source code or as data to be executed by embedded inference engine. However, lots of vendor like ST Micro, NXP, CEVA and many others have their own libraries optimized for TinyML platform.

V. Integration of AI and ML with Cyber Threat Intelligence platform

Integration of machine learning in IoT security domain helps to build a superior and reliable model [21-28] pertaining to the malware detection, spam classification and network intrusion identification. Implementation of artificial intelligence at various phase of cyber threat intelligence like tactical intelligence and operational intelligence [29] described that, tactical threat intelligence is suitable for “Multi-Agent” system where as operational CTI is applicable for “Recurrent Neural

Authorized licensed use limited to: PES University Bengaluru. Downloaded on February 10,2023 at 05:01:20 UTC from IEEE Xplore. Restrictions apply.

Network". Automation of operational CTI can be achieved by integrating artificial Intelligence with CTI. TU-Sofia researcher have proposed the design of the system in phases 1) Network Activity Measurement- to identify opponent's intension network traffic monitoring is performed in this stage by using various packet capture tools. 2) Data Pre-processing- collected data are needed to be cleansed in order to extract essential attributes of the packet. 3) Feature Extraction- In this stage, only selected relevant features are extracted to conduct the experiment. 4) Classification: Set of features is grouped into one class and the associated algorithms are called "classifier". 5) Application or commands are aggregated with the behavioral state to monitor the model. To transform the overwhelming threat intelligence generated by structured and unstructured sources to actionable data feed is an utmost crucial aspect of CTI perspective. At the same time eradication of spurious threat intelligence is also expected for building an effective and accurate intelligence platform. Supervised machine learning approach performs significantly in order to extract relevant threat intelligence from various unstructured sources.

VI. Detailed Methodology of proposed Model

In this experiment our primary focus is to extract actionable threat intelligence from various data source. To obtain the relevant threat intelligence we adopt the approach of natural language processing, as NLP is a powerful tool to translate human languages to the intelligence suitable for machine. Outline of our proposed model architecture (Fig. 1) will be-

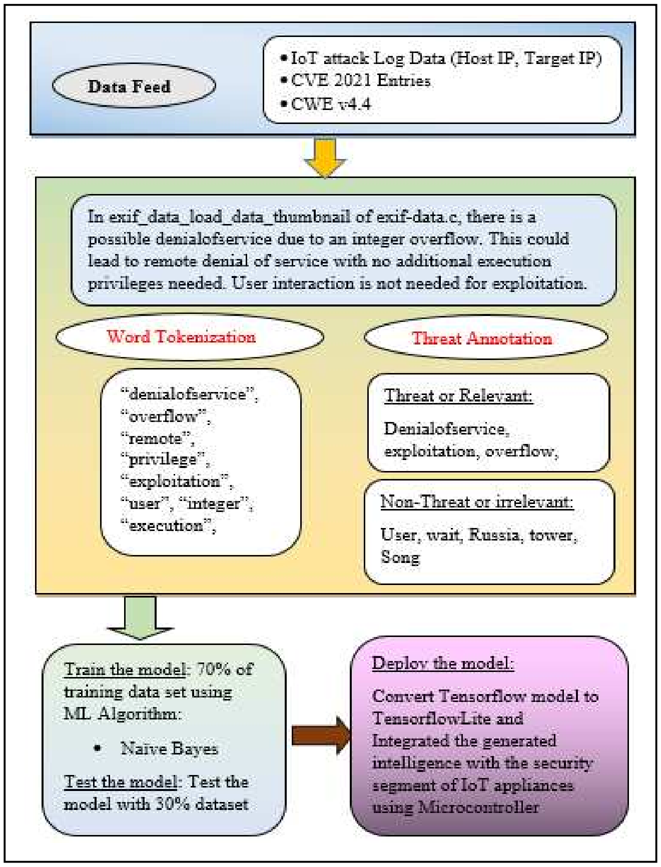

Data Feed
• IoT attack Log Data (Host IP, Target IP)
• CVE 2021 Entries
• CWE v4.4
In exif_data_load_data_thumbnail of exif-data.c, there is a possible denialofservice due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.
Word Tokenization
Threat Annotation
"denialofservice", "overflow", "remote", "privilege", "exploitation", "user", "integer", "execution",
Threat or Relevant:
Denialofservice, exploitation, overflow,
Non-Threat or irrelevant:
User, wait, Russia, tower, Song
Train the model: 70% of training data set using ML Algorithm:
• Naïve Bayes
Test the model: Test the model with 30% dataset
Deploy the model:
Convert Tensorflow model to TensorflowLite and Integrated the generated intelligence with the security segment of IoT appliances using Microcontroller

Fig. 1. Outline of the Proposed model

A. Data Gathering

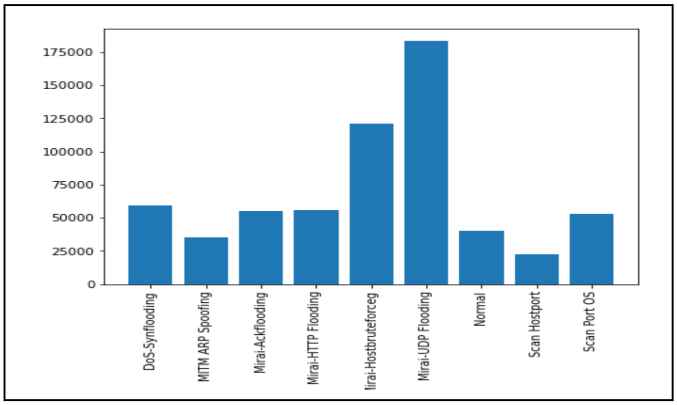


Fig. 2. Distribution of various attack types relevant for IoT

Proper dataset for building a model is the crucial aspect of research paradigm. In this approach we have considered the data source from various indigenous sources like structured and unstructured sources. To consider the suspicious IP address that are responsible for attack at different port with the vulnerability DNS over HTTPS (DoH) as listed RFC8484 by The Internet Engineering Task Force (IETF), we adopted IoT malware set of data from GitHub [37] which consists of multiple features such as 'Src_IP', 'Src_Port', 'Dst_IP', 'Dst_Port', 'Protocol', 'Label', 'Cat', 'Sub_Cat' with 9 types of attack category as depicted above (Fig. 2) -

Moreover, we consider existing vulnerabilities [31] that are identified and organized in CVE2021 and software as well as hardware weakness that are structured in CWE v4.4 are also included for construction of dataset. Lastly, we also collected some "Benign" malware set collected from 'Kaggle' web portal. As we collected data from different sources, in order to construct a single, consolidated .csv file, we need to employ the feature extraction approach to build the requisite dataset. Perhaps, IoT malware segment contain the affected IP address whereas CVE 2021, CWE4.4 and Benign dataset requires separate treatment to extract the adversary keywords.

However, we prepend all the aforementioned four datasets to produce our final consolidated dataset which contains over 10,000 relevant tuples and in this experiment we have reserved 30 % of entire dataset for testing purpose and remaining 70 % dataset are utilized to train the model in order to predict the invasion based on the threat keyword, malicious IP address or port address, hashes etc.

B. Data Cleansing and Data Preparation

Collected data are heterogeneous in nature hence relevant feature extraction is one of the crucial aspect prior to design the extraction model. Here we have extracted the Src_IP, Description as the feature and then we perform data cleansing in order to build the effective and accurate model for prediction of threat. Here, we used "tensorflow.keras.preprocessing.text" package to perform word tokenization, word lemmatization, removal of duplicate words on the dataset and prepare a vector of word using count vectorization and bag of word approach of natural language processing which is implemented on the platform of python language using "nltk" and panda package.

Authorized licensed use limited to: PES University Bengaluru. Downloaded on February 10,2023 at 05:01:20 UTC from IEEE Xplore. Restrictions apply.

For instance, description as collected from a dataset are tokenized to yields tokens like, “keylogger”, “DDoS”, “Spain” “BufferOverflow”, “injection”, “team”, “Nobel” etc.

Now, annotation or labelling plays a significant role in terms of accurate prediction as well as identification of threat. In this experiment we will implement the “Tableau Desktop” tool to label the tokenized keyword based on “threat” keyword or infected IP addresses (Such as - exploitation, overflow, 176.103.130.130) and “Non-threat” keyword (e.g.- Russia, music, Allen Solley etc.). Post tokenization we enforce the Tensorflow embedding technique [33] to the clean dataset which is the numerical representations of text information and we use Word2Vec methods for calculating word embedding.

C. Machine Learning classifier to build the model:

Naïve Bayes algorithm is used for classification problem especially for text classification. In our proposed model, one feature is independent of existence of another feature i.e. each feature contributes to the prediction without having correlation. At the same time Zero-day vulnerability is a domain of uncertainty and Naïve Bayes classifier is one of the potential classifier for detecting known as well as unrevealed threats. In context of smart devices, we presume an underlying set of association among entities which are responsible for events generation.

We proposed to employ the Naïve-Bayes classifier MultinomialNB() for extracting high level threat intelligence from the dataset, considering 75% data for training dataset and 25% data forecast dataset with the parameter value as- alpha : 1.0 , fit prior: True and class prior: None. Text vector is the data feed for this model to train the model, followed by testing the model to evaluate the performance of the model in terms of performance metrics [36] as-

$$\text{Accuracy}= \frac{TP+TN}{TP+FP+FN+TN} \qquad \text{Precision}= \frac{TP}{TP+FP}$$

$$\text{Recall}= \frac{TP}{TP+FP} \qquad \text{F-measure}= \frac{2*\text{Precision}*\text{Recall}}{\text{Precision} + \text{Recall}}$$

Where, TP=True Positive, TN=True Negative, FP=False Positive, FN=False Negative

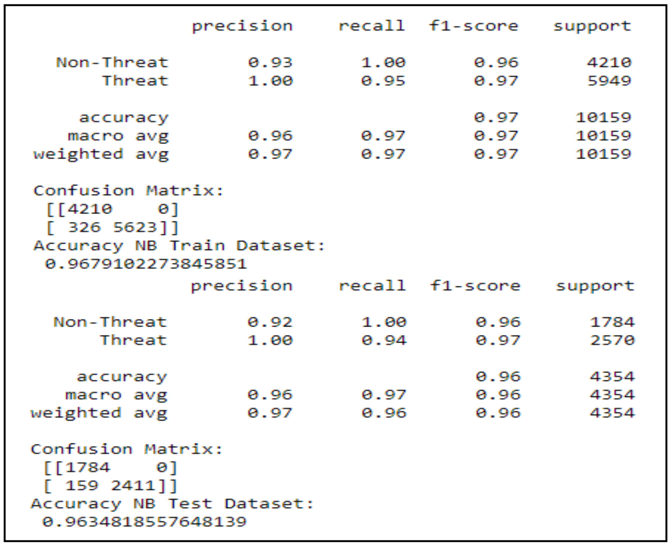
Support vector machine (SVM), convolutional neural network (CNN) also perform significantly [32], for extracting intelligence from renounced hacker’s community. However, aforementioned classifiers perform outstandingly for the homogeneous dataset. Presently, we are supposed to conduct our experiment on such a composite dataset which is heterogeneous in nature and comprises of malicious attack type, threat keyword, IP address, port number etc. and we expect Naïve Bayes algorithm will perform remarkably for such kind of heterogeneous dataset. In this ambit, we would like to extend our experiment implementing SVM, CNN as well in addition to the NB algorithm and a comparison may be drawn among these three classifiers against the performance metrics. Finally, all three model are need to be tested by feeding the 30% dataset for predicting malicious activities and triggering alerts against the threat.

D. Deploy the model into microcontroller:

After designing and subsequent testing the model is capable to generate actionable intelligence data feed and these data feed can be integrated into the various security appliances Post designing of the model we need to convert it into a form ready to be deployed on the microcontroller in the form of an array of bytes that the TF interpreter will read to recreate the model. Array of bytes are allocated on the read only program memory of device in the form of C or C++ byte array. These MU are integrated within the IoT devices to trigger alert for the True Positive cases promptly even for zero days’ vulnerabilities. In our proposed model any 32-bit microcontroller with 48 MHz clock speed with in-built Wi-Fi or Bluetooth facility will be suitable for embedding into the device. Among various variant available in market we recommended to choose Arduino Nano 33 BLE Sense or Adafruit Edge Badge MU kit for our proposed model.

E. Result of the Experiment

We have evaluated various metrics related to the performance of the trained model for both the dataset i.e. train and test dataset. We have measured the accuracy, precision and f1-score of the model (Fig. 3) it is obvious that the model is accurately predicting threats for train and test dataset as 96.8% and 96.3 % respectively. In our experiment it is obvious that, 93% proportion of positive identifications was actually correct for non-threat keyword also.



```
              precision    recall  f1-score   support

  Non-Threat       0.93      1.00      0.96      4210
      Threat       1.00      0.95      0.97      5949

    accuracy                           0.97     10159
   macro avg       0.96      0.97      0.97     10159
weighted avg       0.97      0.97      0.97     10159

Confusion Matrix:
 [[4210    0]
 [ 326 5623]]
Accuracy NB Train Dataset:
 0.9679102273845851
              precision    recall  f1-score   support

  Non-Threat       0.92      1.00      0.96      1784
      Threat       1.00      0.94      0.97      2570

    accuracy                           0.96      4354
   macro avg       0.96      0.97      0.96      4354
weighted avg       0.97      0.96      0.96      4354

Confusion Matrix:
 [[1784    0]
 [ 159 2411]]
Accuracy NB Test Dataset:
 0.9634818557648139
```

Fig. 3. Outcome of the experiment

VII. CONCLUSION

IoT is the future of global things and this technology empowered the entire globe to be connected with each other very convenient way virtually. However, increasing growth of utilization of these devices also attracts immense challenges [34-35] to retain the security aspects intact without being breached. CTI and ML based security solution can shield the things in automated manner and also significant for arresting the zero days’ vulnerabilities for the IoT devices as well. Additionally, if we design the threat predicting model using TinyML platform then the integration in microcontroller and subsequently in the

Authorized licensed use limited to: PES University Bengaluru. Downloaded on February 10,2023 at 05:01:20 UTC from IEEE Xplore. Restrictions apply.

smart devices will seamless and less power consuming framework.

We have designed a model based on machine learning approach employing Naive Bayes classifier to extract the potential threat intelligence from heterogeneous data source and the model is able to predict the threat incidents accurately up to 96.3%. As size of the smart devices are constraints so we the entire threat predicting as well as alert triggering module are embedded in a microcontroller which will be integrated within the IoT devices for detecting threat well in advance based on the earlier fed intelligence.

References

[1] R. Montasari et al., 2021, “Application of Artificial Intelligence and Machine Learning in Producing Actionable Cyber Threat Intelligence”, Springer Nature Switzerland AG 2021. Page- 47-64. *(references)*

[2] Norton, The future of IoT: 10 predictions about the Internet of Things, Accessed on: 30th June, 2021, Available: https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html

[3] T. Taleb, M. Bagaa, J.B. Bernabe and A. Skarmeta, 2020, “A Machine Learning Security Framework for IoT Systems”, IEEE Access, Volume 4.

[4] M. Shafiq, Z. Tian, Y. Sun and D. Xiaojiang, 2020, “Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city”, Elsevier Future Generation Computer Systems 107, pp 433–442.

[5] ThreatPost, More Than Half of IoT Devices Vulnerable to Severe Attacks, Accessed on: 02nd July 2021, Available: https://threatpost.com/half-iot-devices-vulnerable-severe-‘attacks/153609.

[6] B. Kumar, B. Mohanta, D. Jena, U. Satapathy and S. Patnaik , 2020, “Survey on IoT Security: Challenges and Solution using Machine Learning, Artificial Intelligence and Blockchain Technology”, Elsevier B.V.- Internet of Things Volume 11, September 2020, 100227.

[7] S.M. Tahsie, H. Karimipour and P. Spachos, 2020, “Machine learning based solutions for security of Internet of Things (IoT): Asurvey”, Elsevier Journal of Network and Computer Applications 161 (2020) 102630.

[8] S. Bhatt, Rachit, and P.R Ragiri, 2020, “Security trends in Internet of Things: a survey”, Springer Nature Appl. Sci. 3, 121.

[9] Y. Al-Hadhrami and F.K. Hussain 2020, “Real time dataset generation framework for intrusion detection systems in IoT”, Elsevier Future Generation Computer Systems 108, 414–423.

[10] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki, 2018, “Network Intrusion Detection for IoT Security based on Learning Techniques”, IEEE communications surveys and tutorials, 2896380, NOVEMBER 2018.

[11] X.C. Yin, Z.G. Liu, L. Nkenyereye and B. Ndibanje, 2019, “Toward an Applied Cyber Security Solution in IoT-Based Smart Grids: An Intrusion Detection System Approach”, Published: 14 November 2019, MDPI Sensors 2019, 19, 4952; doi:10.3390/s19224952.

[12] C.R. Banbury et al, 2020, “Benchmarking TinyML Systems: Challenges and Direction”, Proceedings of the 3rd ML Sys Conference.

[13] H. Doyu, R. Morabito and J. Höller, 2020, “Bringing Machine Learning to the Deepest IoT Edge with TinyML as-a-Service”, Published on IEEE IoT Newsletter - March 2020.

[14] STIX, “Structured Threat Information eXpression (STIX™) 1.x Archive Website”, Accessed on 05th July 2021. Available: https://stixproject.github.io/’

[15] MITRE, “Common Vulnerabilities and Exposures, Accessed on: 28th January 2021. Available: https://cve.mitre.org.

[16] MITRE, Common Weakness Enumeration, Accessed on: 28th January 2021 Available: https://cwe.mitre.org/about/index.html

[17] Md. S. Abu, S.S Rahayu, A Ariffin and Y. Robiah, 2018, “Cyber Threat Intelligence – Issue and Challenges”, Indonesian Journal of Electrical Engineering and Computer Science · April 2018, vol. 10(1):371-379.

[18] R. Trifonov, O. Nakov and V. Mladenov, 2018, “Artificial Intelligence in Cyber Threats Intelligence”, IEEE, 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC), pp.1-4.

[19] N. Kaloudi and J. Li, 2020, "The AI-Based Cyber Threat Landscape: A Survey", ACM Computing Surveys, Volume 53, Issue 1.

[20] A. Ibrahim, D. Thiruvady, J.G Schneider and M. Abdelrazek, 2020, “The Challenges of Leveraging Threat Intelligence to Stop Data Breaches”, Frontiers Computer Sci., Vol. comp.2020.0003, Accepted on: 28 August 2020.

[21] Md. A. Garadi, A. Mohamed, K.A. Abdulla, D. Xiaojiang and M. Guizani, 2020, “A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security”, COMST IEEE 1553-877X (c) 2020.

[22] P. Karthika, R.G. Babu and A. Nedumaran , 2019, “Machine Learning Security Allocation in IoT”, Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS 2019), IEEE Xplore Part Number: CFP19K34-ART; ISBN: 978-1-5386-8113-8.

[23] J. Cañedo and A. Skjellum, 2016,” Using Machine Learning to Secure IoT Systems”, 2016 14th Annual Conference on Privacy, Security and Trust (PST), IEEE, Pg No- 219 – 222.

[24] L. Xiao, X. Wan, X. Lu, Y. Zhang and D. Wu, 2018, “IoT Security Techniques Based on Machine Learning”, IEEE Signal Processing Magazine, Pg. No- 053-5888 (2018), IEEE.

[25] S. Zeadally and M. Tsikerdekis (2019), “Securing Internet of Things (IoT) with machine learning”, International Journal for communication system, Willey Publication, Volume33, Issue 1.

[26] N. Khurana, S. Mittal, A. Piplai and A. Joshi , 2019, “Preventing Poisoning Attacks on AI Based Threat Intelligence Systems”, 2019 IEEE 29th International Workshop on Machine Learning for Signal Processing, pp. 1-6.

[27] M. Landauer, F. Skopik, M. Wurzenberger, W. Hotwagner and A. Rauber, 2019, “A Framework for Cyber Threat Intelligence Extraction from Raw Log Data”, 2019 IEEE International Conference on Big Data (Big Data).

[28] H. Griffioen, T. Booij and C. Doerr, 2020, “Quality Evaluation of Cyber Threat Intelligence Feeds”, Springer Nature Switzerland AG 2020, LNCS Vol. 12147, pp. 277–296.

[29] R. Montasari et al., (2021), “Application of Artificial Intelligence and Machine Learning in Producing Actionable Cyber Threat Intelligence”, Springer Nature Switzerland AG 2021. Page- 47-64.

[30] The tinyML Summit 2020, Accessed on: 30th June 2021. Available: https://www.tinyml.org/summit/

[31] T. Alladi, V. Chamola, B. Sikdar and K.K.R. Choo, 2020, “Consumer IoT: Security Vulnerability Case Studies and Solutions”, Published by the IEEE Consumer Electronics Society, 2019 Pg. No- 2162-2248.

[32] I. Deliu, C. Leichter and K. Franke , 2017, “Extracting Cyber Threat Intelligence From Hacker Forums: Support Vector Machines versus Convolutional Neural Networks”, 2017 IEEE International Conference on Big Data (BIGDATA).

[33] R. David et al, 2020, “TensorFlow Lite Micro: Embedded Machine Learning on TinyML Systems”, Published on arXiv, 20 Oct 2020.

[34] F. Hussain, R. Hussain, S. A. Hassan and E. Hossain¸ 2020, “Machine Learning in IoT Security: Current Solutions and Future Challenges”, COMST IEEE 1553-877X (c) 2020.

[35] M.A. Khan and K. Salah (2018), “IoT security: Review, blockchain solutions, and open challenges”, Elsevier Future Generation Computer Systems 82 (2018) 395–411.

[36] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido and M. Marchetti, 2018, “On the effectiveness of machine and deep learning for cyber security”, Conference: 2018 10th International Conference on Cyber Conflict (CyCon), Accepted May 2018.

[37] Github, “IoT Malware”, Accessed on: 11th August 2021. Available: https://github.com/ifding/iot-malware.

Authorized licensed use limited to: PES University Bengaluru. Downloaded on February 10,2023 at 05:01:20 UTC from IEEE Xplore. Restrictions apply.