



Internet of Thing Hacking

Dissertation

Abstract

Internet of thing hacking might be regret by developing cyber security implementation through Kali Linux ethical hacking penetration testing to secure smart home IOT devices, various smart home devices are vulnerable due to insecure WIFI connection, since cyber security fail to investigate the IOT security solution, due to inappropriate machine learning method so there is needs to improve the machine learning methodology to enhance the cyber security issues in internet of thing device. Since the cyber security issues has been suggested Kali Linux security solution to secure home devices from hacking attack. Kali Linux is most powerful security solution which secure all internet of thing system from hacking attack. Secondary data collected from Kaggle and Google scholars & IEEE Sites. Machine learning model developed to improve the previous past model which enhance the IOT in more organized manner.

Student

Dharmendra

Contents

Abstract.....	0
List of Figure & Table	5
Chapter # 1: INTRODUCTION INTERNET OF THINGS HACKING	6
Smart Home Security.....	6
Machine Learning based solution for Security of internet of things (IOT)	6
Machine learning approach for webshell detection in internet of things devices	7
Machine learning method internet of things designed.....	7
Lightweight Cryptography of Internet of Things System	8
Big data Privacy Preserving in Multi-Access Edge Computing.....	8
Testing the Security ESP32 Internet of things devices	8
Intrusion detection system enhance network security using RaspberryPI Honeypot in Kali Linux	8
Kali Linux Honeypot Cybersecurity.....	8
Kali Linux Binwalk Firmware Security	9
Security verification in IOT devices Firmware.....	9
SVM based intrusion detection identification of GRID device Firmware	9
Large-Scale firmware function security based on SImhash	9
Research Aim & Objective	10
Research Considerations.....	10
Chapter 2 Literature Review	11
Related Work	11
Blockchain Strengthen the Internet of thing	12
Penetration testing tool for internet of thing System	12
IOT Forensic digital investigation framework for IOT System	12
Security and privacy challenges in internet of things	12
Building ethical hacking site for learning and student engagement	13
Ethical hacking the need for cybersecurity.....	13
Ethical Hacking for Boosting IOT Vulnerability management.....	13
Enabling Trust and Security TIP for IOT IEEE.....	13
Consumer IOT Security Vulnerabilities Case Studies and Solution.....	14
Eavesdropping attack.....	14
Social Engineering Attack.....	15

Healthcare IOT Benefits, Vulnerabilities and Solutions	15
Checksum code	15
API Information Extraction.....	15
Survey on Security and Privacy Issues in Edge computing assisted in IOT	15
Classification security and privacy attack	16
Intrusion detection system	17
Cryptography Method.....	17
Securing Fog Computing of Internet of thing Applications Challenges and Solutions	17
Security in Internet of thing challenges and solution and Future direction	18
Secure Protocols for IOT	18
Layers of IOT System	18
Security Methods to Protect IOT	19
Machine learning based IDPS enhancement with complementary features for IOT home Networks ..	19
SDN based predictive alarm manager for security attack detection at IOT Gateways.....	19
Blockchain-aided edge framework for cybersecurity for internet of thing	20
Deep Intrusion detection system in Lambda architecture based on edge cloud computing for IOT.....	20
Internet of thing security requirements issues related to sensor	21
DEEP LSTM approach for intrusion detection in IOT device for smart home.....	21
Secure User authentication for rapid smart home IOT Management.....	21
IOT Security for Smart Home Issues and Solutions.....	22
Hyperledger Fabric framework with 5G network blockchain based security IOT Smart home	22
IOT enables smart Energy Grid	22
Conclusion of Literature Review	22
Research Methods:	23
Research Gap	23
Chapter 3: Methodology.....	24
Introduction	24
Research Philosophy	24
Shortcomings in the Literature	24
Research Strategy	24
IOT DOS and DDOS Dataset	25
Dataset Features.....	25
Python Libraries for preprocessing	25

Machine Learning Programming.....	25
Logistic Regression Model	25
Random Forest Classifier	25
SVC (Support Vector Classifier)	26
Decision Tree.....	26
Gaussian Naïve Bays Algorithm	26
Result	26
Ethical Hacking Kali Linux Hacking tools to Secure IOT.....	26
Ethical Hacking on IOT Device Penetration Testing.....	27
Mitigating Security Risk and Threats	27
Analysis	28
Ethical Concern	28
Chapter 4: Result & Analysis	29
Python Machine learning programming.....	29
Dataset information.....	29
Network Traffic IOT dataset.....	29
Python libraries	29
Network traffic IOT DATA	30
Wireshark PCAP FILE Network	31
Data Preprocessing in Python Notebook.....	31
Dataset Head.....	32
Checking Missing values in dataset.....	32
Dataset information.....	33
Decision tree classifier	33
Feature Selection	34
Decision tree classifier to Detect IOT attack libraries.....	34
Outcome	35
Decision Tree Classification report	35
Naïve Bays Model to DETECT IOT Attack	35
Print data columns	36
Naïve Bays Modeling.....	36
Training and testing the dataset	37
Naïve Bays Classification report.....	38

Support Vector Machine modeling.....	38
SVM Classification Report	39
Kali Linux IOT Ethical Hacking Analysis:	39
Firmware	39
Bootloader	39
Why examines the Firmware	40
Features in firmware.....	40
Security issues in IOT devices.....	40
Static and Dynamic Analysis.....	40
Static Analysis	40
Dynamic Analysis	41
Binwalk.....	41
Binwalk Entropy Calculation	41
Firmware analysis in Kali Linux	41
Firmadyne	44
Firmware Analysis Toolkit	44
Firmware analysis toolkit directory	45
Machine Learning VS Ethical Hacking for IOT Security	47
Critical Analysis Ethical Hacking to Secure IOT devices	47
Chapter # 5: Discussion & Conclusion.....	48
Critical Discussion	48
Investigating the robustness of IOT security cameras against cyberattack.....	48
Wireshark VS CSV.....	48
Machine learning VS Kali Linux	49
Kali Linux Security Solution	49
Penetration testing in IOT System	49
References	50

List of Figure & Table

<i>Figure 1 : list of IOT security attack</i>	7
<i>Figure 2: eight common physical attack on the physical IOT security layer</i>	14
<i>Figure 3: IOT Layard Approach</i>	18
<i>Figure 4: SDN based predictive alarm manager</i>	20
<i>Figure 5: Adaptive model</i>	21
Figure 6: the four stages of penetration testing	27
Figure 7: data output	29
Figure 8 : python libraries	29
Figure 9: network traffic data outcome	30
Figure 10 Wireshark file	31
Figure 11 python data preprocessing	31
Figure 12 data head	32
Figure 13 data heatmap	32
Figure 14: data information	33
Figure 15: Decision tree classifier	33
Figure 16: feature selection training & testing	34
Figure 17: decision tree classifier library	34
Figure 18 : prediction analysis	34
Figure 19: outcome of prediction decision tree	35
Figure 20: classification report decision tree	35
Figure 21: Naïve Bays modeling	35
Figure 22 print data columns	36
Figure 23 data transformation naïve bays	36
Figure 24 training testing naïve bays model	37
Figure 25: printing the model	37
Figure 26: printing the model validate result	37
Figure 27 naïve bays classification report	38
Figure 28 support vector machine libraries	38
Figure 29 model printing	38
Figure 30 SVM report classification	39
Figure 31: Firmware Kali Linux analysis	40
Figure 32: Firmware Kali Linux analysis security checking IOT hardware	41
Figure 33: Firmware Kali Linux analysis security checking IOT hardware	42
Figure 33: searching URL	43
Figure 34: searching encoded IP address	44
Figure 35: searching open SSL	44
Figure 36: searching malicious user	44
Figure 37 firmware directory toolkit	45
Figure 38: defensive security FAT IOT analysis	45
Figure 39: security execution	46
Figure 40: check web URL hacker user	46

Chapter # 1: INTRODUCTION INTERNET OF THINGS HACKING

Internet of things widely used for designing smart home systems with control of smart internet control. Internet of thing which is recognized as IOT devices, monitor and management of smart home solutions. Smart home solutions based on various IOT control system, hence smart energy control management organized energy with organize manner which provides cost effective solution. By employing devices such as motion sensors with smart plugs hence smart home system enables the user to turn their lights, fan, and Air conditioning system with smart energy planning. Hence it reduces the cost and minimizing energy waste.

Smart Home Security

(Manhas, J. and Kotwal, S., 2021) smart home solutions related with each other to manage the smart electric system in organized manner. Smart home solution based on sensor technology and alarm which detects house changes condition from smoke development the opening, closing of doors and windows. If the smart IOT system detects any vulnerabilities it instantly notify the user. Implementation of intrusion detection system based on machine learning programing to detect malicious activity to mitigate cyber-attack, like phishing, hacking, snooping etc. hence the security methods still not works perfectly hackers still exploits the security breaches and capture sensitive information. Machine learning intrusion detection system proposed by various researchers in the literature, which critically analyze the working of machine learning detection activity. Machine learning approach proposed on KNN, decision tree, naïve bays and support vector machine evaluated the implementation of intrusion detection network. The machine learning classification approach proposed on four measuring accuracy to detect any vulnerability in real time which measures through the precision score and Recall score.

Machine Learning based solution for Security of internet of things (IOT)

(H. and Spachos, P., 2020) internet of things system implemented and deployed to manage home energy system which minimize the energy cost and enable them to manage the electronic appliances which organize the various solution on smart phone. Internet of things system facing security issues & challenges due to inappropriate and insecure internet WIFI connection. Internet WIFI connection easily hacked and spoil by hacker. Since the machine learning approach organized the various solution which possible challenged them to view the objectives of security, since machine learning approach is not reliable approach. Machine learning possible solution trying to impressed the internet of things system to secure them from hacking attack.

Internet of things layer architecture discussed in literature review sections in details, since internet of things devices hardware developments needs review, which needs development according to the requirement of cybersecurity system. (Tsikerdekis, M., 2020) securing internet of things devices with machine learning technique approach, advance machine learning methods designed to maintained the embedding computing technologies with lessening price, emergence of smart hardware system into the smart internet of things system which predicted and maintained the security solution. Since information & communication technology which conventional the courtesy in current years. The internet of things system security needs review & planning. Machine learning and artificial intelligence technology system control & organize the working of internet of things system. The two machine learning approach identified supervised and unsupervised approach to

identify the vulnerability attack in the system. Since machine learning methods able to identify the vulnerable attack in the system.

Decision tree and naïve bays algorithm works efficiently to identify any suspicious activity in the system. Hence machine leaning approach identified the vulnerable attack approach to mitigate the solution and minimize the security solutions.

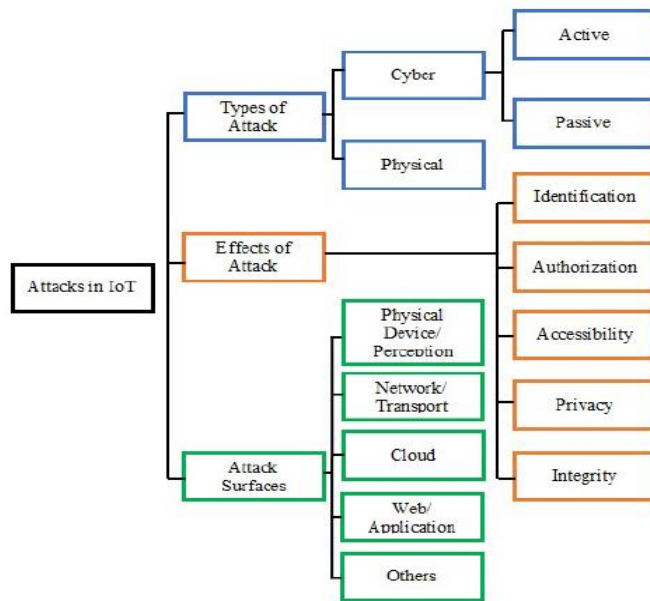


Figure 1 : list of IOT security attack

Machine learning approach for webshell detection in internet of things devices

(D. and Damaševičius, R., 2022) internet of things system is massive number of technology based on sensor technology interconnected with smart WIFI system. Intelligence smart solution identify the vulnerability attack which classify the smart home solution living standard based on cyberattack solution. Data moderating, data leakage stops form fake safety bout keys. Machine learning methods identified the security and individual solutions composed of various challenges & security solutions. The machine learning methods identified the random forest tree, decision tree, naïve bays classifier composed on various detection methods. The extensive machine learning approach discuss the webshell detection in lightweight and heavyweight computer system.

Machine learning method internet of things designed

(Korotaev, V.V., 2019.) Machine learning emergence technologies which clutched the courtesy and industrial control system, various industrial control systems expected to achieve the near future in which to maintain the pervasive computing. Since machine learning methods organized the way to manage in healthcare system IOT system composed of various identified solution. Cryptographic hash functions which deploys the one-way hash functions, ECC founded one-time key with consequence of operating system which has not careful. Operating system which is not allowed to prevent the methods to organized the applications of internet of things system.

Lightweight Cryptography of Internet of Things System

(Prema, K.V. 2021) the combinations of IOT system enable intelligence infrastructure system mutual and various self-organized devices. The internet of things system intelligence solution to exchange sensitive data, including human interconnected of network devices. This research analyzed the data integrity of internet of things applications in major security solution concerned, denial of service attack, forgery and chosen cipher text attacks. Machine learning methods support data integrity approach which concerned to review the insights applications.

Big data Privacy Preserving in Multi-Access Edge Computing

(X. and Sun, Y., 2018) multi-edge computing devices which become more essential to complete the various internet of things devices. Multi-access edge computing system enables them heterogeneous internet of things system. Hacker attacker centralized the communication devices in order to manage the hacker attack. The major privacy concerns issues to organized & managed the hacker attack, internet of things system enable them to view the advanced functional system to organized the security measurements.

Testing the Security ESP32 Internet of things devices

(Chamornmarn, T., 2019) physical model of internet of things system includes various communication protocols pattern model, measurements of internet security solution has been proposed and implemented on internet things system. The experimental model attempt to measures the security protocols and transmit data. Various security attack has been identified in order to identify the network access, network traffic interception management. The ESP32 server which attacks the internet of things system and managing the internet of things system security. Various security protocols has been designed & identified proposed on security measurements to achieve numerous security planning. The wireless sensor network basic knowledge designed & planned according to the security measurement policy. The probability of network analysis tool has been designed according to the network security protocols. Network traffic interception analysis designed & planned according to the network security policies, hence Kali Linux operating system designed for ethical hacking and penetration testing which is based on complete security solution. It minimize the hacking attack permanently by deploying the security solution which minimize the hacking system.

Intrusion detection system enhance network security using RaspberryPI Honeypot in Kali Linux

(Jeremiah, J., 2019) cyber security has been changed the security management system in order to minimize the security planning the measurements cybersecurity planning has been designed to minimize the security solution. Data integrity protection access the information gain in which the various connected devices identified and managed according to the network security protocols. Data integration & smart IOT devices security has been measured & designed on the basis of cyber space. Security is one the major concerned protocols measurement in which the data access & privacy managed based on security measurement.

Kali Linux Honeypot Cybersecurity

Honeypot is network attached system setup as decoy, designed to appear as high value asset like a server and its objective to detect deflect the steady hacking attempts that might have otherwise led to unauthorized access to information system. They are most often used by large

enterprises and companies involved cybersecurity research. Usually the honeypot operation consist of a computer application and IOT data to simulate the behavior of real system. The objective to deploy Kali Linux Honeypot is to secure the Internet of things system for instances but it's completely isolated and closely monitored.

The exact placement of honeypot varies depending on its sophistication the aims to attract and its proximity on sensitive resources inside the corporate network. It might be placed in the network demilitarized zone or DMZ to still be part of the network or outside the external firewall to detect attempts to enter in the internal network its matter to placement of honeypots

Kali Linux Binwalk Firmware Security

Kali Linux Binwalk extract the internet of thing IOT smart devices firmware in order to manage the smart devices security, firmware is security analytics tools in order to maintain and managed the security solution network.

Security verification in IOT devices Firmware

(Kuo, S.Y., 2018) the IOT embedded devices manage the IP WIFI CAM and drone attack since the internet of thing applications widely used by various resources and connected network. Since the hacker identified and attempts on network security analysis, since the major discovery of intrusion detection system which gain the security access on hidden embedded devices. Firmware discovery analyzed on exploiting password activity including OWASP and UL-2900 the Kali Linux shell script dependency algorithm identified with common development of suspicious shell script activity. Since the real world embedded devices needs internal data theft security, IOT firmware file secure and extracted by Binwalk library in order to secure the hardware functions. The effectiveness of reverse firmware binary is 96% on predicting the efficiency of open source tools. The results indicate that the given solution has been measured and identified based on the security protocols, hence the entrance problematic on two internet of thing devices revived the validation. Ethical hacking method on Kali Linux which leaks the IOT firmware password on common vulnerabilities attack.

SVM based intrusion detection identification of GRID device Firmware

(Shi, Z., 2019,) identifying the binary program which are set of instruction in order to quality the reverse analysis of firmware. Firmware is usually used to leaks the IOT hardware instruction description header in order to implements the cyber security rules based on Kali Linux operating system. SVM based intrusion detection system which recognized the common feature selection methods trained by support vector machine. The machine learning classifier trained and tested based on the dataset attributes value of firmware file which is extracted by Binwalk to identify the security mechanism. Since the result has been presented proposed on SVM binwalk on dataset 98% accuracy to achieve the better accuracy outcome.

Large-Scale firmware function security based on Simhash

The development of internet of things devices which has more than more physical attention SDK(software development kit) libraries based on software binary files proposed to view the resultant value of simhash function identify the security protocol methods proposed on strong identification method. The security information extracted and used by various research analysis to keep in view of internet of thing security analysis. Modern internet of thing devices secured through the binwalk firmware analysis based on penetration testing tool method. The firmware security features functionality identified and measured through the basic security and internal file

management system of Kali Linux system. The implementation of simhash functions based on firmware data analysis keep in view to maintain the security analysis hence large security detection & prevention which has scale the security detection.

Research Aim & Objective

Research aim to identify the security pattern of internet of thing system and research objective achieved through these following strategies:

1. Objective to design the binwalk firmware security analysis based on Kali Linux operating system ethical hacking method.
2. Development of machine learning algorithm to identify vulnerable data of internet of thing devices (IOT) system, improve the accuracy score.
3. Review the technical literature on Internet of thing smart home devices and planned the research gap.

Research Considerations

Research has been designed & maintained through the following chapters to complete the research thesis as follows:

Chapter 1 based on introduction, chapter composed of technical literature review finding and methods are based on machine learning and Kali Linux system.

Chapter 2 Literature Review

Technical literature review which review the internet of thing system hacking vulnerabilities and needs to address the solution through practical programming method which identify the hacking issues and challenges. Technical literature which deliver the comprehensive solution to solves various complexity.

Related Work

(Stanislav, M. and Beardsley, T., 2015) hacking IOT the case studies based on baby monitor exposures and vulnerabilities, internet of thing system which used to secure and protect the environment. This research presented the feature of baby monitor IOT system intensively personal use care for IOT. Infants and toddler baby needs extra care for security purposes, IOT system connected with other family member to indicate any dispute. Components using by IOT system composed of chipsets, firmware and software includes to deal with system. The device founded on video baby monitory system the safety and security purposes which discover the findings to meet the environment. Common vulnerabilities happened in this system hence local communication is not encrypted, and remote communication is not encrypted, nearest attacker might attack to change the device system. (Ding, A.Y., De Jesus, G.L. and Janssen, M., 2019,) ethical hacking technique permitted for boosting the internet of thing devices to organize the vulnerabilities, internet of thing system uses to monitor the home and industrial control system. This research investigate qualitative analysis to review the literature to probe the bug bounty program including responsible disclosure to manage the security processes penetration testing to boost the test with overall managed the internet security. (Robberts, C. and Toft, J., 2019) finding vulnerabilities in IOT devices hence various internet of thing devices needs security to secure the internal environment, (Park, J. and Tyagi, A., 2017) using power signs to hack internet of thing devices the power channel provides the framework for instruction level, hence the consumer electronics which digitally inherit the security problems of digital world in the process. Since the internet of thing devices to classify the devices in outdated security which is not permitted to do the validation outcome. Preliminary analysis has taken to investigate the vulnerability issues in the IOT devices. (Saha, T., Aaraj, N., Ajjarapu, N. and Jha, N.K., 2021.) Smart hacking approaches to investigate the risk probe, internet of thing IOT system wide range of application, which includes healthcare, wearable, nuclear power plants, autonomous vehicle, smart cities and smart home. Since the IOT devices are not secure hacker might be prevented to capture the internet of thing system, innovative method identify to detect the incident response which are exploited the internal data, intelligent response represent the systematic view of regular expression which conducting by machine learning method to generate the attack and security vulnerabilities. Hence the machine learning method deploy to detect the vulnerability attack in IOT system which has using the accuracy score of 97%, IOT system internal security needs improved security mechanism which prediction based on machine learning method, but still needs to refined the algorithm since the defense device needs the cost to measure the security parameter in depth of security measurement hence cyber physical system using sensor

to feed data in computing elements. Internet of thing devices to constrained the resource to facilitate them in advance.

Blockchain Strengthen the Internet of thing

(Kshetri, N., 2017) blockchain might be able to control the IOT system security the key findings of this research investigate the blockchain-IOT security method which measures the eco-IOT system. This work highlight the blockchain based solution in many aspects hence centralized cloud server, the cross management system address the special issues and challenges which identify the security method in the IOT system. Blockchain system proposed on supply chain business in resource for tracking the security breaches.

Penetration testing tool for internet of thing System

(Visoottiviseth, V., Akarasiriwong, P., Chaiyasart, S. and Chotivatunyu, S., 2017) internet of thing system is rapidly growing system in every field of life with implementations to handle the sensitive information, the hardware and software development of IOT system needs security system to improve the efficiency of the system, IOT system easily captured and target by hacker in which various probability occur to damage the overall system of communication, since penetration testing system IOT called PENTOS in order to prevent the security measurement, penetration testing automatically backup the system of target IOT wireless devices including WIFI and Bluetooth. The system allows user to implements the penetration testing methods in order to identify the IOT hacking attack in real time, such as password attack, web attack, wireless attack in which various privileges algorithm identified, this research suggest penetration testing solution which investigate all real time threats and needs to deploy the secure environment to avoid hacker.

IOT Forensic digital investigation framework for IOT System

(Sathwara, S., Dutta, N. and Pricop, E., 2018) security matters and intimidations attack to classify the auspicious tests hence the needs of forensic methods which investigate IOT related crime. Since IOT investigation various security challenges in forensic investigation, since it contains varieties of information which identify the private and public network domain, IOT system support forensic investigation to probe the crime in real time, hence the integration of large number of information pool, the addition of great quantity of IOT forensic attention to deploy in depth to discover the IOT security methods. This research develop forensic ecosystem which helps to determine the information, the objective to find the crime in real time by the help of forensic IOT eco system.

Security and privacy challenges in internet of things

(Lee, J.H. and Kim, H., 2017.) This research discover security and privacy matter which includes IEEE consumer electronics magazine, since security and privacy is concerned with every domain of network, since artificial intelligence algorithm used in variety of form to secure the network , machine learning and deep learning programming extensively used to protect the IOT system. Security as service various IOT devices contains limited security approach. Various IOT system

patching devices seems to be the big problem, the new security parameters which protect the overall internet of thing system from the hacker. Most of the home appliance devices connected with WI-FI internet system or ZigBee such as television, washing machine, Air conditioner, refrigerators and dryer to protecting these devices which are connected in real time remote user which is very challenging part. Beside this blockchain system introduce to secure the cryptocurrency such as bitcoin. Blockchain is novel system, since security in connected car by transformation of information which needs improvement, carpool system easily captured and hacked by hacker to destroy the communication in between the user and car cab.

Building ethical hacking site for learning and student engagement

(Lehrfeld, M. and Guest, P., 2016) this research discovers the ethical hacking simulation which aids to investigate the understanding of penetration testing tool, hence ethical hacking is way to organize and manage the testing methodology which capture the real time network traffic predict and detect the threats in the given system since ethical hacking is platform to store the network platform.

Ethical hacking the need for cybersecurity

(Patil, S., Jangra, A., Bhale, M., Raina, A. and Kulkarni, P., 2017) hacking is expert field which classify the working and knowledge management in the system under the ethical hacking to probe the attack in real situation, ethical hacking is method to provides the security in the system, since the unauthorized hacker captured the system, hackers identify the probe to investigate the system in which various formation has been carried out to take idea about the problem. This research suggest solution to implement ethical hacking technique to secure the internet of thing system from hacking attack.

Ethical Hacking for Boosting IOT Vulnerability management

(Ding, A.Y., De Jesus, G.L. and Janssen, M., 2019) growing number of internet incident happened on daily, since internet of thing system damage by outsider hacker which needs data to spoils them and damage the overall system. Ethical hacking is the method to organize such hacking and prevents them to capture the sensitivity vulnerability attack in the system. It was noted that the IOT system hacking techniques which needs extra training for the persons which implements security parameter within the IOT system. Kali Linux Operating system which organized these such parameters to implements IOT security, hacking technique wide range of Parrot operating system and Kali Linux provides the such security tools to avoid vulnerability attack in the network.

Enabling Trust and Security TIP for IOT IEEE

(Hudson, F.D., Laplante, P.A. and Amaba, B., 2018) enabling privacy, security, trust, identity, safety which is critical for the people and critical to manage the hyperactive world. IEEE takes the lead to deploy the IOT security techniques in order to minimized the vulnerability attack in the system, since IEEE, national science foundation and internet2 sponsors works together to presents IEEE trust security workshop in 2018, since the presentations of these discussion enable them to provides solution on the following areas such as end to end encryption, security access

control, identity management architectural framework including policy standard which uses the standard security parameter.

Consumer IOT Security Vulnerabilities Case Studies and Solution

(Alladi, T., Chamola, V., Sikdar, B. and Choo, K.K.R., 2020.) since IOT devices is increasing and becomes general in the people community so there is needs to understands the security parameter of these such systems which has describes the commons the security functions which needs to protect them this research presents the IOT security management and suggest some explanation and designs the parameters of security implementations to avoid the vulnerability attack. This research design the future security planning.

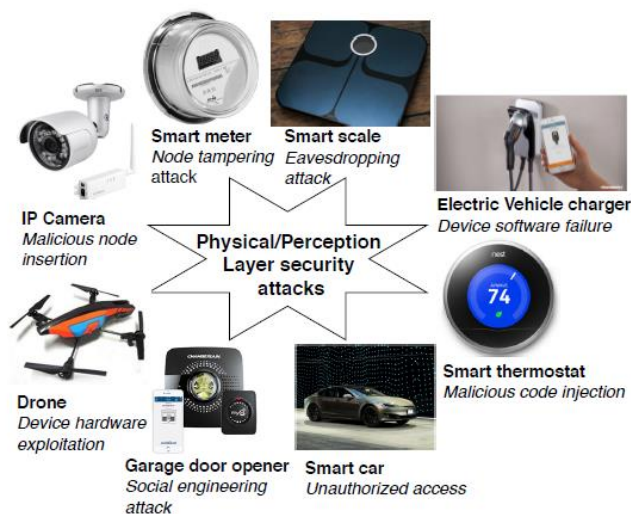


Figure 2: eight common physical attack on the physical IOT security layer

Since potential attack on the physical layer electric vehicle charge on charger point which might be vulnerable for the electric vehicle, exploiting the buffer overflow in the IOT system which communications between the android application app and Bluetooth executable devices, denial of service attack could be carried out to manage the file system of the overall system, device charger might be disrupted at any time in primitive control of the system.

Eavesdropping attack

Data is coming from the IOT system which has sniffed and overlapped in the system such as man in the middle attack which capturing the critical network information Fitbit aria is explained in this article, hence wireless access points enable them the user to capturing the sensitive information over the network which needs necessary to protect them from the vulnerable attack the Kali Linux and virtual machine assigns them to design the security mechanism, author implementing DHCP server to scan the IP addresses and forwarding IP tables over the interface, the traditional network scanning tools is not enough to manage the security such as Wireshark system which scans the real time computer network protocols and IP addresses of the both host and destination addresses which is not in common for practice.

Social Engineering Attack

Social engineering attacks is playing trap card to capture the email id and system passwords of the user and might be able to use them to organize the security parameter.

Consumer IOT devices which is not designing the security parameter this research presents the case studies based finding to prevent them and identify them the common hacking attack which are common in practice, the smart cities and smart homes system critically installed the network infrastructure and summarized the common network attack which needs them to identify them the IOT security attack thus the common interface of the system which plans the testing and patching method and cross sector collaborations which exists in emerging technology.

Healthcare IOT Benefits, Vulnerabilities and Solutions

(Nausheen, F. and Begum, S.H., 2018) the existing IOT system provides various benefits to wearable healthcare system and mobile application development to ensures the patient and medical data, since the interactions of medical devices which has safe and secure, the management of security and privacy to manage and organize the system parameter patch hence ensures the patient, the medical data manage through the IOT system, there is needs to create awareness in the IOT system which enable them to identify the system process, since the potential risk of security measurement always challenging to organize the internal security, the control communications which are implantable to manage the IOT system, this research suggest access control schemes using the box encryption to achieve the desired requirements of the IOT system.

Checksum code

Straight forward temper proofing technique which organize the guards and works together to protect the network hence code fragments called guards which helps to executes potential security measurement, guard allows to ease the access and organize the security parameter control program. Check sum code perform the integrity action control program which review the tempering method.

API Information Extraction

API information obtained the code and instruction to extract the information which is extracted by the application file, the DEX file contains the code file which stores the code, since API extracted information like package information to return the extracted value information composed on API framework which stores information. Since the API extraction method composed of package name, class, API name and API description which using the parameters of naïve bays machine learning classification model.

Survey on Security and Privacy Issues in Edge computing assisted in IOT

(Alwarafy, A., Al-Thelaya, K.A., Abdallah, M., Schneider, J. and Hamdi, M., 2020) internet of thing composed of ground-breaking model which provides massive application to control and manage real life problem of humans. Various smart devices are deployed with various functionalities including massive communications system network, the massive growth of IOT system which are

leading to communication network data and offloading method which are sensitive, since edge computing is common computing technique to organize the system to bring data processing and manage the overall system. Since it has noted that the quality of service which needs network protocol and security parameter to manage organize the system, since the system are composed of unique features.

Classification security and privacy attack

1. Malicious hardware software injection

Attacked used malicious hardware application to communicate between the EC nodes which inject the malicious user input in EC server, hence exploits the communication process which enables them the EC server to exploit. Hardware injection which replaces the hardware path to actual location which inject the hardware circuits.

2. Jamming Attack

It allows hackers to flood the network which counterfeit the messages and creating the communications parameters and storage resources the render authorized user access unable to infrastructure based on EC assisted IOT network.

3. Distributed Denial of Service Attack

DDOS attack which is common attack based on sleep deprivation and battery draining which has most famous types of DDOS attack. Since the EC nodes does not communicate the overall process of the system which operate the authorized access control model, though the most shared attack of distributed denial of service is jamming the network signal prior sending and receiving packets are jamming.

4. Physical Attacks of Tempering

This attack happens when the EC nodes/device capture the cryptographic data and might be able to temper the network from the software operations.

5. Eavesdropping or Sniffing

Confrontational which listens the private conversations based on user name and password its sniffs the packets and control the access control parameter to measures the network this method identify the network shared passwords.

6. NON Network Side Channel Attack

Hacker modifies the network route and even the nodes does not route the data the instances of recent nodes are being captured and optimized by the hacker and change the route node address.

7. Routing Information attack

Since its old fashioned attack hacker modify their locations which does not able to being captured by any agent and resources, since this attack prevents the node to change the routing information location hence the malicious EC node which might be black hole which drain the network packets by selecting the data. Worm holes which address the packets and also identify the network neighbor's id.

8. Forgery Attack

Attacker inject the new data packets and fraud lent interface which might be damage the receiving system interface since the capturing and modifying data which has common practices of the hacker hence hacker adding the malicious data packets on the captured network and replaced them the exchange packets on layer 2 network.

9. Unauthorized Control Access

Neighboring EC nodes which are communicates between them and share common data attack can access unsecure EC node which also controls the connected node in the network.

10. Integrity Attack Machine Learning

Machine learning model deployed by the organization administrator to detect and capture the hacking attacks on the IOT system, might be attacker change the training process and builds the machine learning models and manipulate and misleading the content without changing the training process.

11. Replay and freshness Attack

Hackers captures the record data traffic in particular period of time the historical data might be change the real time data of the network.

12. Unnecessary logging attack

The log files might be able to change the locations and might be able to damage the EC locations the developed infrastructures system and applications errors are attempt to successful deployed the overall security measurements.

Intrusion detection system

Intrusion detection system classified the network which are control the network so far in the development of IOT system needs intrusion detection to classify the hacking attack in the real situation. So there is needs to separate the detection policy which are filter and scan then connects to the IOT system.

Cryptography Method

Strong and efficient encryption are composed of utilizing the network communication process which are against the common network attack. Since the encryption and decryption method enhance the network security methods.

Securing Fog Computing of Internet of thing Applications Challenges and Solutions

(Ni, J., Zhang, K., Lin, X. and Shen, X., 2017) since internet of thing is connected worlds of billions of thing which collect connect in the real time on the other hand IOT support the featured access control list which organize latency control in the system so there is needs to implements IOT security over the fog computing resources since the geographic control list of fog computing which has mange the resources including smart traffic management and home energy management system hence fog computing system integrated and connected in real time with the internet of thing system so its easily control and managed through the third party system which needs extended security parameters. So always concerns with privacy and security measurement which are deeply concerned on network edge computing system. Since the

architecture of fog computing which connected on critical fog node hence cyber-attack easily prevented within the system hence the potential challenges of fog computing needs review on the measurement of critical security management issues in the real time.

Security in Internet of thing challenges and solution and Future direction

(Kumar, S.A., Vealey, T. and Srivastava, H., 2016) internet of thing system enable various critical features to executes live in the modern world, hospital, cities, grids, organization and buildings hence security and privacy are major concerns in adaptation of internet of thing system. This research review and evaluate the security attack in preventions of security measurement.

Secure Protocols for IOT

IPV6 is identified as possible solution in the smart object communication since internet engineering task force joint venture of IPSO alliance to promote the internet of thing protocols which are based on standard interoperation ability to classify the smart object network. Since the IPV6 protocol stack which are intended deployment to plans the security protocols of IOT system comparison to IPV4 which are most commonly used protocol but easily captured and spoils them hacker without no such meaning. Since the IOT system protocol methods are best predictable method to identify them the central protocols method.

Layers of IOT System

1. Application layer, which composed of various applications and services which are IOT provider in common includes smart home, smart industrial control system, including smart healthcare and smart transport.
2. Perception Layer, this layer composed of sensory technology including temperature sensor, vibration sensor, pressure sensor, RFID sensor which allows devices to connect themselves.
3. Network layer: this layer composed of network communication software based on physical components including topologies, server, network node, objectives of this layer to transmit data within all network using IP table.
4. Physical Layer: composed of basic hardware of IOT system and smart appliances and power supply which acts as backbone in the network to control smart object.

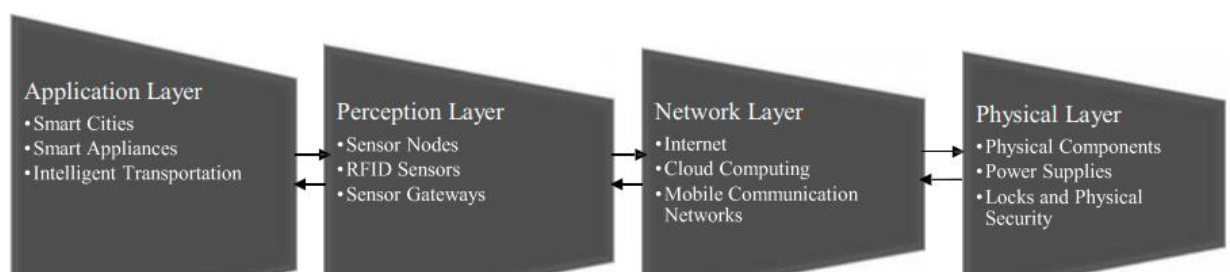


Figure 3: IOT Layard Approach

Security Methods to Protect IOT

(Kumar, S.A., Vealey, T. and Srivastava, H., 2016) game theory method adapted to secure IOT system which involves simulation strategy which prevent detect and avoid attack. Another solution composed of PKI-Like Protocol which involves encrypting the routes and nodes source and destinations based encryption and decryption method hence data are sent through the off-spring nodes. Another solution are suggested this research based on RFID radio frequency identification which allows device to communicate with another device like human. Next solution cyber sensor are sensor which detect real time data and deployed preference based privacy models.

Since intelligence transport system used security method known as risk analysis which are composed by certificate authorities to monitor and organize the network nodes. Suggest middle ware security methods used to secure the communication.

Another solution suggested this research composed of access control authentication which fixes the loopholes in the IOT device which secure the system and integrity. The request authentication request device composed by registration authority, since keep in touch smart object technology which access near field communication using the radio frequency identification which facilitate tele monitoring process.

Self-managed cells composed of policy and discovery method which allows easy management and measurement.

Machine learning based IDPS enhancement with complementary features for IOT home Networks

(Illy, P., Kaddoum, G., Kaur, K. and Garg, S., 2022) the internet of things network system security and vulnerability attack happened so needs to secure the smart home, smart industry and smart healthcare system. This research contribution are based on intrusion detection and prevention system which are machine learning based approach which improves the detection accuracy, since this research focused on smart home system to quantify the features which brought out to view the security measurements since intrusion prevention system qualify to control and manage the denial of service attack. The software defined network based method deployed the architecture based on IDPS network.

SDN based predictive alarm manager for security attack detection at IOT Gateways

(Thorat, P., Dubey, N.K., Khetan, K. and Challa, R., 2021) major threats in IOT system growing malicious traffic injection attack where IOT system is being hacked and prevented, the real time network solution addressed composed of software defined networking based predictive alarm manager solution to control the IOT system in real time. The solution is implemented at the gateways of the IOT system hence the experimental result has been conducting to detect the malicious software application about 96% precision recall score.

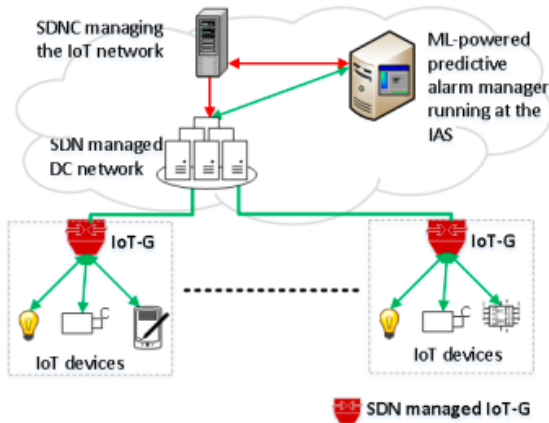


Figure 4: SDN based predictive alarm manager

Machine learning model classify the intrusion which are based on the decision value the three metrics alarms system reducing the network parameter to achieve the certain the goals. Since alarms manager sends and receive the network protocols. This research using the predictive alarms system based on machine learning modeling which classify the incoming traffic from the IOT gateway hence identifies the using the ensembles models about 95% accuracy including precision recall around 99% accuracy. The software defined network block the flooding flows of information.

Blockchain-aided edge framework for cybersecurity for internet of thing

(Hazra, A., Alkhayyat, A. and Adhikari, M., 2022) blockchain technology is promising technology which suggest solution to cybersecurity hence the variety of reinforcement, healthcare, smart home, smart transport system ability to control and scale the information management system. Edge computing system designed to allow cloud services, hence edge computing combines works with blockchain technology enable them to transparent the information the protection of blockchain technology works together in the blockchain technology to organize the internet of thing system communication.

Deep Intrusion detection system in Lambda architecture based on edge cloud computing for IOT

(Alghamdi, R. and Bellaiche, M., 2021) IOT device enable in massive amount of data to analyze the vulnerability in the network which causes to stop communication between the smart user and smart IOT system. Since the heterogeneous IOT device prevented by cyber-attack, in real situation. Intrusion detection system identify the problem and scales the solution based on real time investigation, since the intrusion detection system composed of lambda architecture to implements in IOT security to address the challenges. Since the system decrease the training phase in positive direction to meet the solution and minimize the hacking attack over the system. The system is able to detection any vulnerability in the network and prevent them and block them with ID based.

Internet of thing security requirements issues related to sensor

(Alqarni, H., Alnahari, W. and Quasim, M.T., 2021) security is critical concern in the network management hence smart home IOT system connected with each other using the smart WIFI system, since the design and limitation of ad hoc wireless sensor network communicate between them on particular terms since limited memory and weak processing which are identify the cause of communication model.

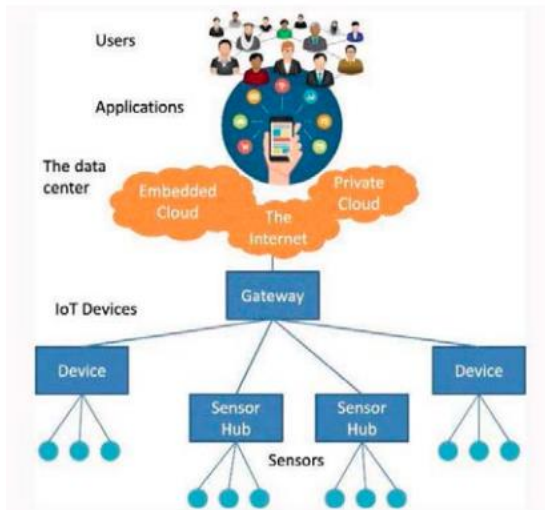


Figure 5: Adaptive model

The development of IOT system using the smart sensor system which transmit data using the physical layer. Security and privacy model generated by the system to manage the requirements on fundamental aspects points of view.

DEEP LSTM approach for intrusion detection in IOT device for smart home

(Zaghloul, Z.S. and Li, C., 2021) since IOT device able to identify the communication pattern which enable them to transmit data on the smart user. This research investigated that about 70% IOT devices easily hacked due to poor security system in the IOT, so the protocol methods of IOT system is old fashioned which needs advance security measurement, such as IPV6 is new parameter of security which does not easily hacked. The efficient methods of security identified the security measurement parameter which are needed to safeguards the system from hacking attack. So there is needs to implements the security to secure the smart home system, this research suggest deep learning method detect anomaly in the network and predict the smart home attack in the system. Since the cyber-attack and security attack which are occurred to identify the security measurement which are proposed on long term memory architecture which achieve the highest accuracy of exiting deep learning model.

Secure User authentication for rapid smart home IOT Management

(Luo, H., Wang, C., Luo, H., Zhang, F., Lin, F. and Xu, G., 2021.) this research suggest security solution to manage the smart home IOT system which are proposed on gateway based 2 factor

security authentication model hence secure the user authentication framework which are dedicated on gateways based solution on layer 2 security methods. Since the universal factor of security methods identify the mechanism of security tools and technique in the management of IOT system. Since the commercial IOT server are based on Alibaba cloud, GSF2 protest to enhance the security mechanism against the malicious attack including high factor.

IOT Security for Smart Home Issues and Solutions

(Antzoulis, I., Chowdhury, M.M. and Latiff, S., 2022) the internet of thing system is increasing popular system to manage the smart home system and regulate the electronic devices the smart home technology enables the user to act securely and manage their energy resources such as television, door bells, vacuum cleaner and kitchen appliances this research suggest automated firmware technology solution including blockchain, machine learning, intrusion detection and prevention control system which protect the IOT devices.

Hyperledger Fabric framework with 5G network blockchain based security IOT Smart home

(Ali, R.F., Muneer, A., Dominic, P.D.D. and Taib, S.M., 2021) IOT devices are internet connected devices which only changes of single point of failure the phishing attack, network protocol attack this research trying to eliminate the data security and hacking attack discovery, the features of blockchain technology fabricate the IOT data which are smart IOT based solution to monitor and organize the overall security methods of internet of thing system. IOT based smart home solution needs security protocol management to secure the system from outside access.

IOT enables smart Energy Grid

(Abir, S.A.A., Anwar, A., Choi, J. and Kayes, A.S.M., 2021) the conventional power system of IOT system which enable them to identify the security methods in the system including domain knowledge. This research reviews the IOT enabled smart grid system including sensing communications computing technology which meets the requirements. This research suggest solution as follow:

1. Blockchain technology
2. Machine Learning
3. Artificial intelligence programing
4. Ethical hacking (Kali Linux)

Conclusion of Literature Review

This research investigate the comprehensive overview of the IOT based hacking and solution, various issues and challenges exists to secure the communication between the smart android device to IOT system, this research going to develop solution based on smart home IOT system security solution. Since IOT system is not completely measures with proposed security method the research gap has been identified in the development of smart home IOT system so this research project going to fulfill the research gap in IOT system. The technical literature review address various security issues and challenges in the IPV4 layer so the solution is suggested

through literature by using the IPV6 protocol method, but the issues to secure the WIFI network, man in the middle attack, internet attack and many more attacks might be happened due to poor planning of security mechanism. This research presents the complete security solution of smart home IOT system which complete the research gap in 2022 research methods.

Research Methods:

- The research methods are based on intrusion detection machine learning system by using the IOT dataset.
- Ethical Hacking methods using Kali Linux and Parrot Operating system to secure IOT system.

Research Gap

The research gap has been identified in the technical literature review findings, this research combines all the research to fulfill the research gap by investigating and development of Machine learning molding and ethical hacking method in real time situation to secure the home IOT system.

Chapter 3: Methodology

Introduction

Research methodology of internet of thing system which are part of smart home solution, botnet is network IOT device which has infected by malware, hacker can playing botnet attack card to capture the IOT data easily by sending malware attack to the IOT system. Since botnet would be used to perform distributed denial of service attack, the hacking attack which steal data, send spam, which would allow the hacker and attacker to access the connected device hence typically the router is infected by malware and creates interrupt in the communication between the IOT network and mobile phone.

Research Philosophy

Hacking was used in 1955, which major purpose to identify the technical term and knowledge which gives power to the hacker. Since the first internet hacker certainly identify media and produced first denial of service attack in 1989, the biggest hack in the history happened in 2013, 3 billion yahoo accounts hacked by hacker which was known as yahoo epic data breach. Since yahoo did not admit the problem due to its neglected the popularity. In May 2019 first American financial corporation real estate and mortgage insurer business which was exposed 900 customer file openly in the media.

Hence the internet of thing was coined in 1999 by the computer scientist Kevin Ashton. Since first IOT device was invented in 1993 namely toaster, which was on and off over the internet, the entire process for bread making which warms the bread on particular time period, beside this the IOT devices popularity increase in 2008 year.

ECHO IV first home automation device created by Westinghouse engineer in 1966. Which was the first true home automation device to control temperature and appliances.

Shortcomings in the Literature

Several machine learning methods has been implemented in the past to scan and predict malware and hacking attack in the IOT system, some research generates diverse dataset, which are implements basic machine learning programing composed on decision tree method and Ada Boost.

Various research studies deploy security encryption method but left with no finding to meet the security requirement of IOT.

Some research studies deploy advance machine learning algorithm composed of dataset of IOT to identify malware and hacker in the network.

Research Strategy

1. IOT Penetration testing (Kali Linux)
2. Machine learning method experiencing through the IOT dataset.
3. Encryption method

The research method concerned about denial of service attack of smart home IOT system which has evidently been driven by huge number of compromised internet connected devices. All of the internet connected devices are behind the router network system which easily hacked and captured by hacker.

IOT DOS and DDOS Dataset

Internet of thing IOT device various vulnerability network attack occurred to violate the security of the system, the most frequent using of internet of thing devices which are captured through the internet network. The denial of service attack and distributed denial of service attack are reported in the IOT network, since the most frequency security system using the firewall method intrusion detection system which are unable to detect the complexity of DOS and DDOS attack.

Dataset Features

Data contains the following values which contains in csv file.

pkSeqID	stime	flgs	flgs_number	proto	proto_number	saddr	sport	daddr	dport	
pkts	bytes	state	state_number	ltime	seq	dur	mean	stddev	sum	min
max	spkts	dpkts	sbytes	dbytes	rate	srate	drate	TnBPSrcIP	TnBPDstIP	
TnP_PSrcIP	TnP_PDstIP	TnP_PerProto	TnP_Per_Dport	AR_P_Protocol_P_SrcIP						
AR_P_Protocol_P_DstIP	N_IN_Conn_P_DstIP	N_IN_Conn_P_SrcIP	AR_P_Protocol_P_Sport							
AR_P_Protocol_P_Dport	Pkts_P_State_P_Protocol_P_DestIP									
Pkts_P_State_P_Protocol_P_SrcIP	attack	category	subcategory							

Python Libraries for preprocessing

Dataset to detect anomalies in the IOT network and this dataset contains seven different attack scenear4io such as brute force Heartbleed Botnet Dos and DDOS attack web attacks and infiltration of the network from inside , we have used various kinds of libraries in this regard such as the SKLEARN is also known as scikit-learn which has huge and very useful machine learning library which features various algorithms like support vector machine, random forest, k nearest neighbors classification regression, k-means hence it also support python numerical and scientific libraries such as numpy and scipy hence numpy libraries support large multi-dimensional arrays and metrics are used in this project.

Machine Learning Programming

(Guizani, M., 2020) Label encoder which is part of SKLEARN which is used to convert the label into numeric form so as to convert them into machine readable form hence another part is sklearn is known as standard scalar which is standardize the features of the data such that its distribution will have a mean value 0 and standard deviation 1. Which has useful function in the data which has negative values.

Logistic Regression Model

(Ghoneim, A. and Alrashoud, M., 2020) Logistic regression modeling which is also known to be part of machine learning python sklearn library which has used to predict the probability of a categorical dependent variable or binary variable that contains one or zero.

Random Forest Classifier

(Otoum, Y. and Nayak, A., 2020,) Random forest is supervised machine learning algorithm that is widely used in classification and regression for problems which estimated the which builds the number of decision tree classifier on various samples from the dataset and used averaging to predict to improve the predictive accuracy.

SVC (Support Vector Classifier)

(Alrajeh, N.A. and Alsolami, F., 2020) Support vector classification is another interesting machine learning algorithm which classify based on support vector classification method, and solved regression problem which detect classification regression and outlier detection. Since the implementation of four different kernel parameter that is linear, polynomial, RBF and Sigmoid and hence the RBF kernel type is used by default and if the kernel type to be used by algorithm is not mentioned.

Decision Tree

(Du, X. and Guizani, M., 2020) Decision tree which is supervised machine learning programming which uses multiple algorithm to split data into two or more nodes according to certain parameter in which we used the parameter criteria based on entropy whose function is to be measure the quality of the split.

Gaussian Naïve Bays Algorithm

(Moh, M. and Raju, R., 2018,) It is used for conditional probability purpose that is to estimate the mean and standard deviation from theta, and in this programming the use of matplotlib library for visualization purposes which will used during the execution part to visualized the confusion matrix and heatmap.

Result

(Moh, M. and Raju, R., 2018) Dataset will generate performance metrics which will show the accuracy, precision, recall score. Since the classification model is defined as percentage of correct predictions for the test data, these values are represented in the confusion matrix which gives the accuracy ratio and precision is defined as a rate of correctly classified positives or true positives and its gives us the precision ratio. Hence recall is the metric that quantifies how many of the actual positives were found or recalled it is also very important metric as undetective positive might have serious consequences in some areas for example a model that does not recall the cases of DDOS attacks means that malicious network traffic will go on unnoticed increase the potential harm of the system and its users.

Ethical Hacking Kali Linux Hacking tools to Secure IOT

1. Wireshark

(Abdalla, P.A. and Varol, C., 2020) Network scanning tool which scans the internet of thing smart home connected devices in real time. Wireshark tool which enable them to identify them to communicate with external router which captures packets and debug network. The beauty of Wireshark tool is export pcap file in system hence PCAP data attacker attempt to identify them the sniffing protocol attack, this method identify the packet attack and protocol attack in the system.

2. Binwalk

(Sheng, Q. and Huang, X., 2016,) In Kali Linux Bin Walk is firmware extraction tool its support ethical hacker to identify the IOT device firmware, Binwalk firmware support smart home internet of thing devices which enable them to identify the contents of file system which extracted the data, Binwalk managing the libmagic library which compatible with python, which extracts the vulnerability in the IOT network.

3. Firmwalker

(Haddad, R.J., 2019,) Firmwalker is based on bash script which scans the files and extracted the information form the IOT firmware and see the vulnerability in the network. The tool extracted the data into the text file since the tools works amazingly to highlight the potential issues.

4. OWASP ZAP (Zed Attack Proxy)

Web based interface which support ethical hackers to identify any vulnerability in the internet network in the real situation. ZED attack allows hackers to perform proxy ethical hacking attack in the system. The fuzzy security system attack the web interface and find potential susceptibility

5. Metasploit

(Moravec, J., 2018) In Kali Linux Operating system to predict the hacking attack in the real time which allows ethical hacker to make penetration testing segments and test the attack in IOT app. Metasploit tool allows them to perform attack on IOT apps. Metasploit app which perform certain attack on them to identify them the target attack. The vulnerability black hat attack hacker's exploits.

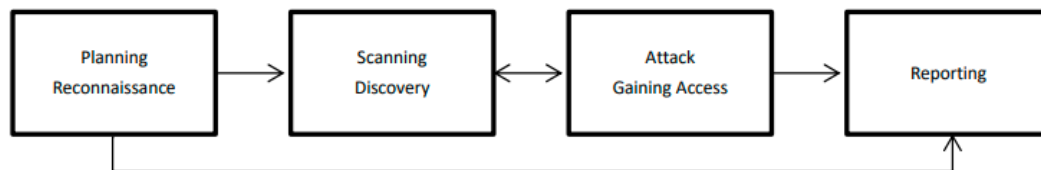


Figure 6: the four stages of penetration testing

Ethical Hacking on IOT Device Penetration Testing

(Lakshmi, H. and MJ, P.K., 2022) Cyber-attacks are becoming more popular due to capturing the sensitive information in the Internet of thing based system. Since internet of thing system easily captured and hacked through the external router of the smart home network. Kali Linux penetration testing is wide range of ethical hacking security solution tool which enable the ethical hacker to protect the internet of thing system by deploying them towards the method of various security tools. The objective of this research to validate and evaluate the internet thing devices security by deploying the ethical hacking system.

Mitigating Security Risk and Threats

(Toutsop, O., Das, S. and Kornegay, K., 2021) Lessening threats security attack involves by reviewing them to identify the critical function of the system the internet of thing system dividing them into different component by simplifying them the complex system. Since the potential threats composed of identify them the mitigation schemes of the internet thing network. Acquiring firmware for IOT devices according to penetration testing cook book which defined the four relevant approaches as follows:

1. Obtain firmware from vendor website
2. Mirror or proxy network traffic when updating the device
3. Googling/ Researching
4. Decompiling associated mobile applications

Kali Linux is Debian driven Linux distribution which helps in cyber security investigation by doing penetration testing, it support to identify the man in the middle attack in the internet of thing network. TCPDUMP tool which has piped the network protocol and sniff the packets in the network. Beside this Ettercap is the kali Linux tool which support active and passive examination protocol including encrypted exchange communication between the networks. Another tool Macchanger which implements in Linux which aids in network to capture the fake network and fake hardware device by detecting the fake MAC address, it's possible through the possible network.

Analysis

The investigation of this research proposed on machine learning and second method proposed on ethical hacking Kali Linux method, since machine learning method is not completely secure the smart home internet of thing devices beside this Kali Linux system is purely designed for cyber security analysis. Its enable them to identify the network traffic rules and it detect all hacking attack based on router and real time internet network. Cyber security solution are composed of development of security protocol method to secure the smart home system through ethical hacking platform. Various ethical hacking tools and technique are available in Kali Linux and parrot operating system which enable the smart security solution which deeply concerned to secure the smart home devices from the hacking attack and any suspicious activity attack in real situation. Parrot is another turn of security solution which combines works on Kali Linux.

Ethical Concern

This research does not harm any human being during the research finding, its follow the all rules and regulations of research ethics, the deeply concerned to avoid plagiarism during the research finding. Ethical hacking platform using the Kali Linux which is free operating system distribution which enables them to capture them network vulnerability attack and hacking attack during the discovery of hacking attack. Machine learning programing only enable to capture the dataset related issues during the network scanning tools. The development with python programing which might be able to identify the dataset malicious activity during the internet of thing vulnerability attack. It identify them to capture the machine learning accuracy score with precision and recall.

Chapter 4: Result & Analysis

Python Machine learning programming

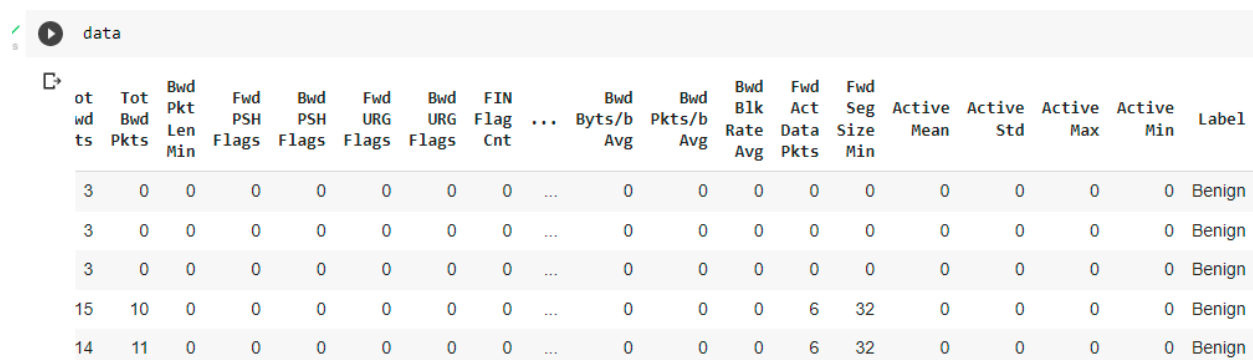
Using support vector machine classifier, Decision tree and Naïve bays modeling to predict the Internet of thing malware and hacking activity by using through the dataset.

Dataset information

Dataset is based on different values in which to make predictions of internet thing attack.

Label columns is presenting the attack name and type.

Dataset head:



The screenshot shows a Jupyter Notebook cell with the variable 'data' selected. Below the cell, the first five rows of the dataset are displayed in a table format. The columns include various network traffic metrics and a 'Label' column.

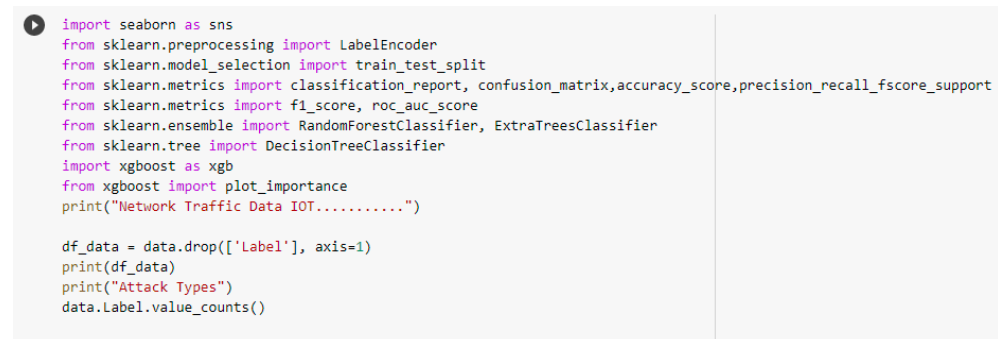
ot wd ts	Tot Bwd Pkts	Bwd Pkt Len Min	Fwd PSH Flags	Bwd PSH Flags	Fwd URG Flags	Bwd URG Flags	FIN Flag Cnt	...	Bwd Byts/b Avg	Bwd Pkts/b Avg	Bwd Blk Rate Avg	Fwd Act Data Pkts	Fwd Seg Size Min	Active Mean	Active Std	Active Max	Active Min	Label
3	0	0	0	0	0	0	0	...	0	0	0	0	0	0	0	0	0	Benign
3	0	0	0	0	0	0	0	...	0	0	0	0	0	0	0	0	0	Benign
3	0	0	0	0	0	0	0	...	0	0	0	0	0	0	0	0	0	Benign
15	10	0	0	0	0	0	0	...	0	0	0	6	32	0	0	0	0	Benign
14	11	0	0	0	0	0	0	...	0	0	0	6	32	0	0	0	0	Benign

Figure 7: data output

Network Traffic IOT dataset

Internet of thing devices data captured from Wireshark software by scanning the real time network PCAP network file, PCAP is data file created during scanning the network, the files contains the data & information which add to controlling the network traffic and defining the network. The PCAP extension file of Wireshark tool which enable them to identify the network data, identify the real time network data based on protocol. Hence the network used to analyze the network data by the cyber security analyst.

Python libraries



```
import seaborn as sns
from sklearn.preprocessing import LabelEncoder
from sklearn.model_selection import train_test_split
from sklearn.metrics import classification_report, confusion_matrix, accuracy_score, precision_recall_fscore_support
from sklearn.metrics import f1_score, roc_auc_score
from sklearn.ensemble import RandomForestClassifier, ExtraTreesClassifier
from sklearn.tree import DecisionTreeClassifier
import xgboost as xgb
from xgboost import plot_importance
print("Network Traffic Data IOT.....")

df_data = data.drop(['Label'], axis=1)
print(df_data)
print("Attack Types")
data.Label.value_counts()
```

Figure 8: python libraries

The following network data library has been added to capture the real time network data of IOT system.

Seaborn:

Seaborn is known as python statistical library to graph by using the matplotlib functions hence seaborn is data visualization library which integrated on pandas data structure since visualize the data in the terms of x and y variable by separating the data and understand them in more meaningful way.

LabelEncoder:

Label Encoder library is common python library to handling the categorical variable hence this method in which each label is assigned unique value which based on integer value based on alphabetical order.

SKLEARN train test split:

In machine learning model evaluation and validation process there is needs to split the dataset into two phase train and test by using the x and y variable system. The train test and split library is python data science library scikit-learn, which splits data into subset & minimize the potential for bias on the basis of data evaluations and validation process.

Classification Report confusion matrix:

Classification report in python machine learning measures the quality of predictions from the classification programming method hence predictions are based on true positive and false positive and true negative and false negative outcome, which predicts the performance metrics of training and testing data and produce classification report.

Precision Recall and Accuracy score:

The meaningful method to identify the dataset score based on the measurement validation. The outcomes are presented to identify the F1 score and precision recall score. The better score of Naïve bays SVM and decision tree is 90% score.

RandomForestClassifier:

In python programming the random forest classifier library which the random forest estimate the fits a number of decision tree classifier on various sub samples of the dataset and uses the averaging to improve the predictive accuracy and control over fitting.

Network traffic IOT DATA

Network Traffic Data IOT.....												
	Dst	Port	Protocol	Tot	Fwd	Pkts	Tot	Bwd	Pkts	Bwd	Pkt Len Min \	
0		0	0			3			0		0	
1		0	0			3			0		0	
2		0	0			3			0		0	
3		22	6			15			10		0	
4		22	6			14			11		0	
...	
8642		80	6			2			0		0	
8643		80	6			5			6		0	
8644		80	6			3			0		0	
8645		80	17			1			1		131	
8646		80	0			3			0		0	
	Fwd	PSH	Flags	Bwd	PSH	Flags	Fwd	URG	Flags	Bwd	URG	Flags \
0			0			0			0			0
1			0			0			0			0
2			0			0			0			0
3			0			0			0			0
4			0			0			0			0
...

Figure 9: network traffic data outcome

Wireshark PCAP FILE Network

PCAP file is part of real time network analysis file which are composed of real time network analysis file, hence the TCPDUMP file which are program to identify the real time network monitoring analysis. The PCAP icon file in which to view all packets information of IOT device in real time.

TPC/UDP packet information by scanning through the Wireshark tool.

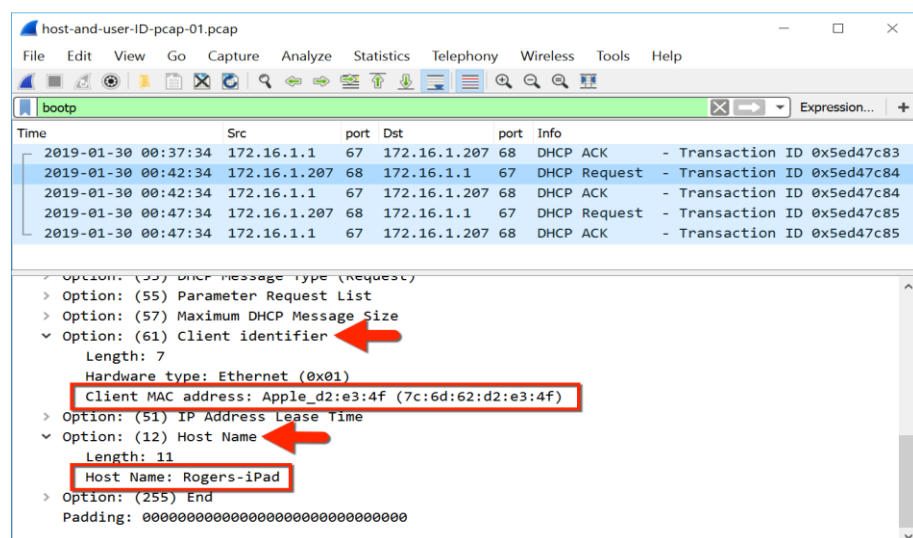


Figure 10 Wireshark file

Data Preprocessing in Python Notebook

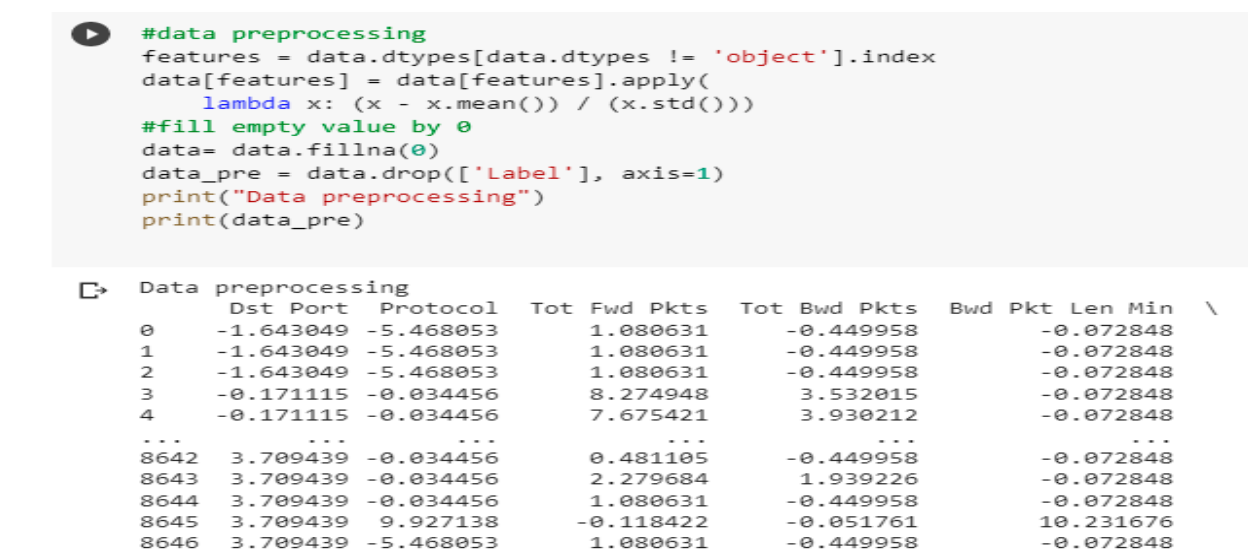


Figure 11 python data preprocessing

Data preprocessing in python in order to achieve the data cleaning and dataset optimization process to remove the data redundancy through data preprocessing steps

Dataset to be cleaned and optimized by determining the dataset labels in which the IOT attack occurred.

Dataset Head

```
data.head(3)
```

	Dst Port	Protocol	Tot Fwd Pkts	Tot Bwd Pkts	Bwd Pkt Len Min	Fwd PSH Flags	Bwd PSH Flags	Fwd URG Flags	Bwd URG Flags	FIN Flag Cnt	...	Bwd Byts/b Avg	Bwd Pkts/b Avg	Bwd Blk Rate Avg	Fwd Act Data Pkts	Fwd Seg Size Min	Active Mean	Active Std	Active Max	Act
0	-1.643049	-5.468053	1.080631	-0.449958	-0.072848	-0.069019	0.0	0.0	0.0	0.0	...	0.0	0.0	0.0	-0.118055	-6.291794	0.0	0.0	0.0	
1	-1.643049	-5.468053	1.080631	-0.449958	-0.072848	-0.069019	0.0	0.0	0.0	0.0	...	0.0	0.0	0.0	-0.118055	-6.291794	0.0	0.0	0.0	
2	-1.643049	-5.468053	1.080631	-0.449958	-0.072848	-0.069019	0.0	0.0	0.0	0.0	...	0.0	0.0	0.0	-0.118055	-6.291794	0.0	0.0	0.0	

3 rows x 31 columns

Figure 12 data head

Checking Missing values in dataset

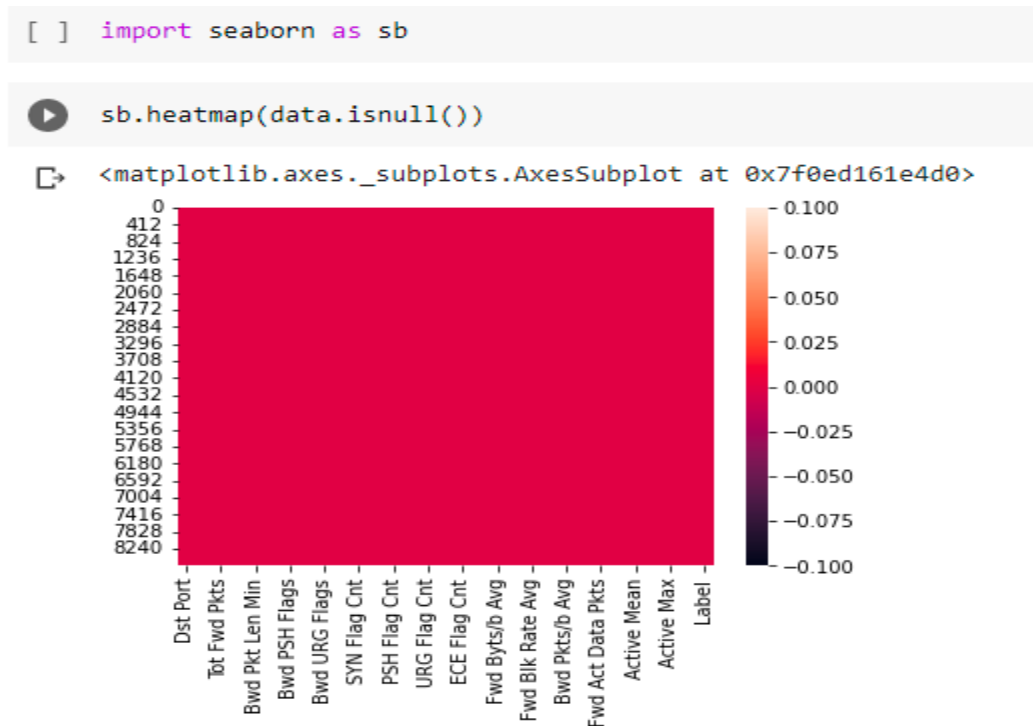


Figure 13 data heatmap

Predicting any missing value in the dataset to determine the values of the dataset, since the data cleaning is the organized process in which the various processing has been optimized. Dataset organized and managed through the python preprocessing library.

Dataset information

```
[ ] data.info()

<class 'pandas.core.frame.DataFrame'>
RangeIndex: 8647 entries, 0 to 8646
Data columns (total 31 columns):
 #   Column                                  Non-Null Count  Dtype  
---  -
 0   Dst Port                               8647 non-null   float64
 1   Protocol                               8647 non-null   float64
 2   Tot Fwd Pkts                           8647 non-null   float64
 3   Tot Bwd Pkts                           8647 non-null   float64
 4   Bwd Pkt Len Min                        8647 non-null   float64
 5   Fwd PSH Flags                          8647 non-null   float64
 6   Bwd PSH Flags                          8647 non-null   float64
 7   Fwd URG Flags                          8647 non-null   float64
 8   Bwd URG Flags                          8647 non-null   float64
 9   FIN Flag Cnt                           8647 non-null   float64
10  SYN Flag Cnt                           8647 non-null   float64
11  RST Flag Cnt                           8647 non-null   float64
12  PSH Flag Cnt                           8647 non-null   float64
13  ACK Flag Cnt                           8647 non-null   float64
14  URG Flag Cnt                           8647 non-null   float64
15  CWE Flag Count                          8647 non-null   float64
16  ECE Flag Cnt                           8647 non-null   float64
17  Down/Up Ratio                          8647 non-null   float64
18  Fwd Byts/b Avg                         8647 non-null   float64
19  Fwd Pkts/b Avg                         8647 non-null   float64
20  Fwd Blk Rate Avg                       8647 non-null   float64
21  Bwd Byts/b Avg                         8647 non-null   float64
22  Bwd Pkts/b Avg                         8647 non-null   float64
```

Figure 14: data information

Decision tree classifier

```
[ ] DT = DecisionTreeClassifier()

[ ] data
```

	Dst Port	Protocol	Tot Fwd Pkts	Tot Bwd Pkts	Bwd Pkt Len Min	Fwd PSH Flags	Bwd PSH Flags	Fwd URG Flags	Bwd URG Flags	FIN Flag Cnt	...	Bwd Byts/b Avg	Bwd Pkts/b Avg	Bwd Blk Rate Avg	Fwd Act Data Pkts	Fwd Seg Size Min	Active Mean	Active Std	Ac
0	-1.643049	-5.468053	1.080631	-0.449958	-0.072848	-0.069019	0.0	0.0	0.0	0.0	...	0.0	0.0	0.0	-0.118055	-6.291794	0.0	0.0	
1	-1.643049	-5.468053	1.080631	-0.449958	-0.072848	-0.069019	0.0	0.0	0.0	0.0	...	0.0	0.0	0.0	-0.118055	-6.291794	0.0	0.0	
2	-1.643049	-5.468053	1.080631	-0.449958	-0.072848	-0.069019	0.0	0.0	0.0	0.0	...	0.0	0.0	0.0	-0.118055	-6.291794	0.0	0.0	

Figure 15: Decision tree classifier

Feature Selection

```
[ ] X= data[['Dst Port','Protocol','Tot Fwd Pkts','Active Mean','Active Std','Active Max','Active Min']]
    y=data[['Label']]

[ ] X_train, X_test, y_train, y_test = train_test_split(X, y, random_state=10, test_size=0.2)
```

Figure 16: feature selection training & testing

Separating the dataset feature turns into the variable into x and y to determine the variable outcome.

Decision tree classifier to Detect IOT attack libraries

```
#Decision Tree Classifier to DETECT IOT Attack
import pandas as pd
from sklearn.svm import SVC
from sklearn.model_selection import GridSearchCV
from sklearn.metrics import classification_report, confusion_matrix
from sklearn.model_selection import train_test_split
import time
import numpy as np
import seaborn as sns
import matplotlib.pyplot as plt
from sklearn.tree import DecisionTreeClassifier
```

Figure 17: decision tree classifier library

This section taken from (GitHub 2022.)

```
[ ] start = time.time()
    print('program starting')
    print()

    DT.fit(X_train, y_train)
    print()

    print('prediction:')
    y_pred = DT.predict(X_test)
    print(y_pred)
    print()

    print('Score')
    score= DT.score(X_test, y_test)
    print(score)

    end = time.time()
    print('program has ended')
    print()

    print('time cost:')
    print(end - start, 'seconds')
```

Figure 18 : prediction analysis

Outcome

program starting

```
prediction:
['Benign' 'Benign' 'FTP-BruteForce' ... 'FTP-BruteForce' 'FTP-BruteForce'
 'FTP-BruteForce']
```

```
Score
1.0
program has ended
```

```
time cost:
0.03423905372619629 seconds
```

Figure 19: outcome of prediction decision tree

Decision Tree Classification report

```
print("Classification Report")
print(classification_report(y_test,y_pred))
```

Classification Report

	precision	recall	f1-score	support
Benign	1.00	1.00	1.00	111
FTP-BruteForce	1.00	1.00	1.00	1619
accuracy			1.00	1730
macro avg	1.00	1.00	1.00	1730
weighted avg	1.00	1.00	1.00	1730

Figure 20: classification report decision tree

Naïve Bays Model to DETECT IOT Attack

```
#Naive Bays model

from sklearn.svm import SVC
from sklearn.model_selection import GridSearchCV
from sklearn.metrics import classification_report, confusion_matrix
from sklearn.model_selection import train_test_split
import time
import numpy as np
```

Figure 21: Naïve Bays modeling

Print data columns

```
for col in data.columns:  
    print(col)
```

```
Dst Port  
Protocol  
Tot Fwd Pkts  
Tot Bwd Pkts  
Bwd Pkt Len Min  
Fwd PSH Flags  
Bwd PSH Flags  
Fwd URG Flags  
Bwd URG Flags  
FIN Flag Cnt  
SYN Flag Cnt  
RST Flag Cnt  
PSH Flag Cnt  
ACK Flag Cnt  
URG Flag Cnt  
CWE Flag Count  
ECE Flag Cnt  
Down/Up Ratio  
Fwd Byts/b Avg  
Fwd Pkts/b Avg
```

Figure 22 print data columns

```
print(data.columns.tolist())
```

```
['Dst Port', 'Protocol', 'Tot Fwd Pkts', 'Tot Bwd Pkts', 'Bwd Pkt Len Min', 'Fwd PSH Flags', 'Bwd PSH Flags', 'Fwd URG Flags', 'Bwd URG Flags', 'FIN Flag Cnt', 'SYN Flag Cnt', 'RST Flag Cnt', 'PSH Flag Cnt', 'ACK Flag Cnt', 'URG Flag Cnt', 'CWE Flag Count', 'ECE Flag Cnt', 'Down/Up Ratio', 'Fwd Byts/b Avg', 'Fwd Pkts/b Avg']
```

Naïve Bays Modeling

```
from sklearn.preprocessing import MinMaxScaler  
scaler = MinMaxScaler()  
scaler.fit(X)  
normalized_x = scaler.transform(X)  
normalized_x
```

```
array([[0.        , 0.        , 0.01851852, ..., 0.        , 0.        ,  
        0.        ],  
       [0.        , 0.        , 0.01851852, ..., 0.        , 0.        ,  
        0.        ],  
       [0.        , 0.        , 0.01851852, ..., 0.        , 0.        ,  
        0.        ],  
       ...,  
       [0.18058691, 0.35294118, 0.01851852, ..., 0.        , 0.        ,  
        0.        ],  
       [0.18058691, 1.        , 0.        , ..., 0.        , 0.        ,  
        0.        ],  
       [0.18058691, 0.        , 0.01851852, ..., 0.        , 0.        ,  
        0.        ]])
```

Figure 23 data transformation naïve bays

Training and testing the dataset

```
[ ] from sklearn.naive_bayes import GaussianNB

X_train, X_test, y_train, y_test = train_test_split(normalized_x, y, random_state=100, test_size=0.2)

[ ] clf = GaussianNB()
    clf.fit(X_train, y_train)
```

GaussianNB()

Figure 24 training testing naïve bays model

```
start = time.time()
print('program starting')
print()

clf = GaussianNB().fit(X_train, y_train)
print()
print(clf.score(X_test, y_test))
print()

y_pred = clf.fit(X_train, y_train).predict(X_test)
print(y_pred)
print()

end = time.time()
print('Program has been ended ')
print()
print('Time COST')
print(end - start, 'seconds')
```

Figure 25: printing the model

```
program starting

1.0

['FTP-BruteForce' 'FTP-BruteForce' 'FTP-BruteForce' ... 'FTP-BruteForce'
 'FTP-BruteForce' 'FTP-BruteForce']

Program has been ended

Time COST
0.04795718193054199 seconds
```

Figure 26: printing the model validate the result

Naïve Bays Classification report

```
print("Classification Report :")
print(classification_report(y_test, y_pred))
```

Classification Report :	precision	recall	f1-score	support
Benign	1.00	1.00	1.00	129
FTP-BruteForce	1.00	1.00	1.00	1601
accuracy			1.00	1730
macro avg	1.00	1.00	1.00	1730
weighted avg	1.00	1.00	1.00	1730

Figure 27 naïve bays classification report

Support Vector Machine modeling

```
#SVM Support Vector Classifier
import pandas as pd
from sklearn.svm import SVC
from sklearn.model_selection import GridSearchCV
from sklearn.metrics import classification_report, confusion_matrix
from sklearn.model_selection import train_test_split
import time
import numpy as np

[ ] SVM_classifier = SVC()
X_train, X_test, y_train, y_test = train_test_split(X, y, random_state = 10, test_size = 0.2)

[ ] start = time.time()
print('Program has working to start')
print()

SVM_classifier = SVC(C=1.0, cache_size=1500, verbose=True).fit(X_train, y_train)
print()
print(SVM_classifier.score(X_test, y_test))
print()

y_pred = SVM_classifier.predict(X_test)
print(y_pred)
print()
```

Figure 28 support vector machine libraries

```
Program has working to start

[LibSVM]
1.0

['Benign' 'Benign' 'FTP-BruteForce' ... 'FTP-BruteForce' 'FTP-BruteForce'
 'FTP-BruteForce']

Program has ended

time cost
0.07349491119384766 seconds
```

Figure 29 model printing

SVM Classification Report

```
print("Classification Report")
print(classification_report(y_test, y_pred))
```

	precision	recall	f1-score	support
Benign	1.00	1.00	1.00	111
FTP-BruteForce	1.00	1.00	1.00	1619
accuracy			1.00	1730
macro avg	1.00	1.00	1.00	1730
weighted avg	1.00	1.00	1.00	1730

Figure 30 SVM report classification

Kali Linux IOT Ethical Hacking Analysis:

What's an IOT device anyhow? Hence the term given to non-standard device connected to the internet usually the embedded operating system (Firmware) which interface them since the embedded sensor in the IOT device which can send, collect and exchange data

1. Security Camera
2. Smart Home Devices such as outlets, light, switches, electronic devices
3. Raspberry PI
4. Connected appliances such as washers, dryers, ovens, etc.
5. Wireless router
6. Wearable : apple watch, Pedometers, heart monitors
7. Autonomous ag equipment and cars

Firmware

Code running on hardware which is critical to hardware operations. Provides the necessary actions on how the device is supported to work, it makes the IOT device work and what the manufacturer intended to do it.

Bootloader

The bootloader the piece of code and software that runs before any operating system loaded into the memory. Bootloader usually contains several ways to boot the operating system kernel and also contains commands for debugging and modifying the kernel environment.

The common bootloader:

1. U-BOOT
2. RedBOOT
3. BareBox
4. BusyBox

Why examines the Firmware

The control on firmware which control the IOT devices, since various vulnerability hacking attacked occurred in internet of thing device, it allows the device to work and configured the common mistakes in the programming , IOT device which easily entry point of hacker which attack the entire network and swivel from.

Features in firmware

Firmware contains hardcoded based on:

1. Credentials
2. Keys
3. Network values

Encryption not used for sensitive information and updates are not encrypted and update are not verified before upload and install.

Security issues in IOT devices

1. Weak Guessable and hardcoded password
2. Insecure network service
3. Insecure ecosystem interfaces
4. Lack of secure update mechanism
5. Use of insecure obsolete machineries
6. Insufficient privacy protection
7. Insecure data transfer and storage
8. Lack of device management
9. Insecure default settings
10. Lack of corporeal inurement

Static and Dynamic Analysis

The static analysis looks on firmware while using the IOT operation.

- Analyze the file system and inspect bootloader
- Looks for hardcoded item
- Use tools firmadyne, Binwalk, Firmwalker etc.
- Dynamic operation looking the process of operation, involuntary static analysis which not exactly often confused them.
- Need to have device which needs to access them
- The virtualize operation on internet of thing device using the penetration testing process in Kali Linux such as NMAP, Metasploit.

Static Analysis

The static analysis are based on Firmware, which extract the Binwalk file system and uncompressed the file system and component if required. The firmware looking the binaries which presents on the firmware and analyze them according to them and identify vulnerability. Hence the common binaries such as busybox, corresponding to exploit on the given version. Since analyze binaries based on disassembly on IDA.

Dynamic Analysis

The firmware running on the system which extract the physical device, virtualize device, QEMU. Since the penetration testing tools in Kali Linux

1. NMAP
2. Metasploit
3. TCPDUMP NETCAT
4. Wireshark

Binwalk

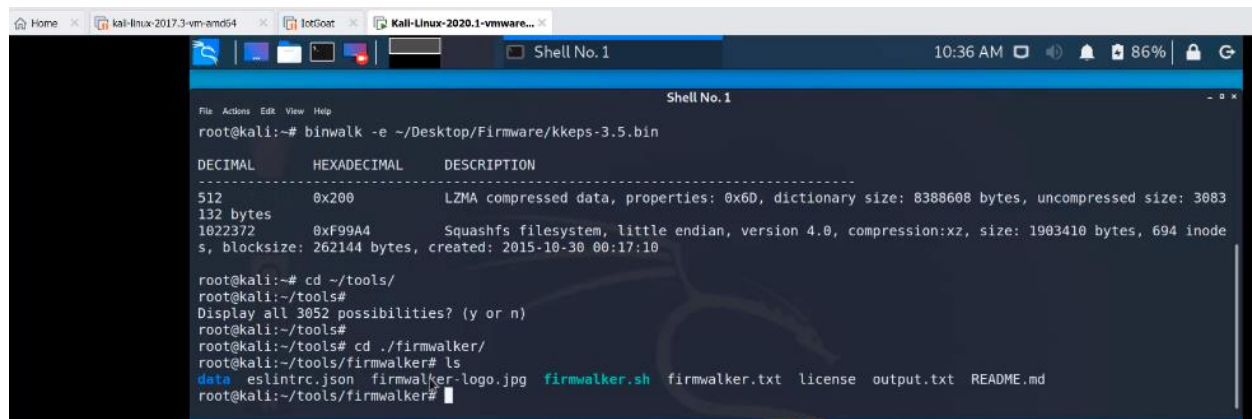
(Zhao, W. and Shi, Z., 2019) Binwalk is tool for searching a firmware image embedded files and executable code, hence Binwalk professional tool also available on cloud based.

Binwalk Entropy Calculation

Internet of thing is hardware based eco system connected with wireless internet network in real time backend the mobile and smart devices also connected on all smart home internet of thing devices. Since firmware updates are always delivered based on compressed file. In order to determine the encryption firmware file which are composed of entropy compressed file. To process the analysis composed of decompressed and encrypted form.

Firmware analysis in Kali Linux

Smart IOT device firmware download from Google GitHub



```
root@kali:~# binwalk -e ~/Desktop/Firmware/kkeps-3.5.bin

DECIMAL      HEXADECEMAL  DESCRIPTION
-----
512          0x200       LZMA compressed data, properties: 0x60, dictionary size: 8388608 bytes, uncompressed size: 3083
132 bytes
1022372      0xF99A4     Squashfs filesystem, little endian, version 4.0, compression:xz, size: 1903410 bytes, 694 inode
s, blocksize: 262144 bytes, created: 2015-10-30 00:17:10

root@kali:~# cd ~/tools/
root@kali:~/tools#
Display all 3052 possibilities? (y or n)
root@kali:~/tools#
root@kali:~/tools# cd ./firmwalker/
root@kali:~/tools/firmwalker# ls
data  eslintrc.json  firmwalker-logo.jpg  firmwalker.sh  firmwalker.txt  license  output.txt  README.md
root@kali:~/tools/firmwalker#
```

Figure 31: Firmware Kali Linux analysis

To executes firmwalker.sh file in order to optimize the performance of IOT device hardware.

Extracted the KKEP bin file in Kali Linux operating system.

Now extracted the squashed root file in the system

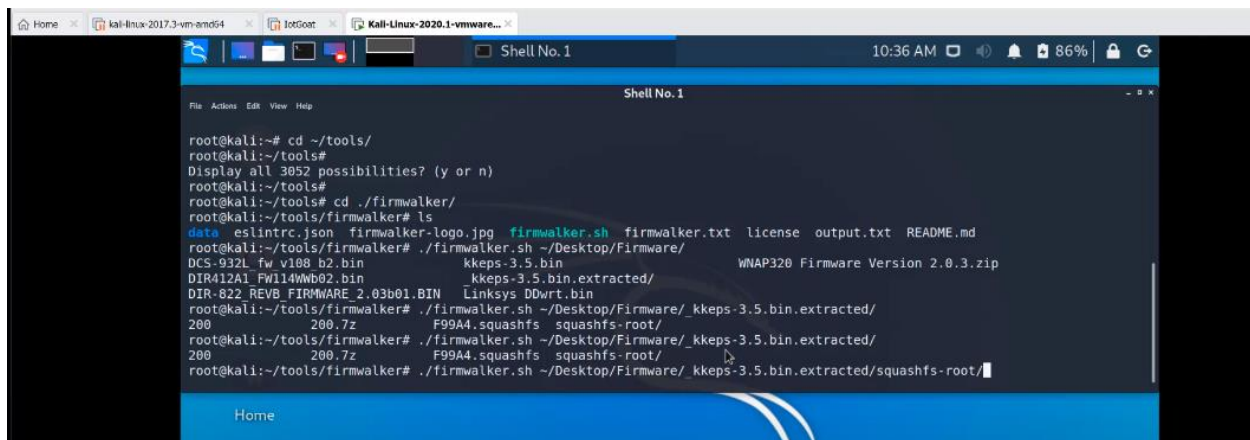


Figure 32: Firmware Kali Linux analysis security checking IOT hardware

Squashed root file searching the email address in IOT system

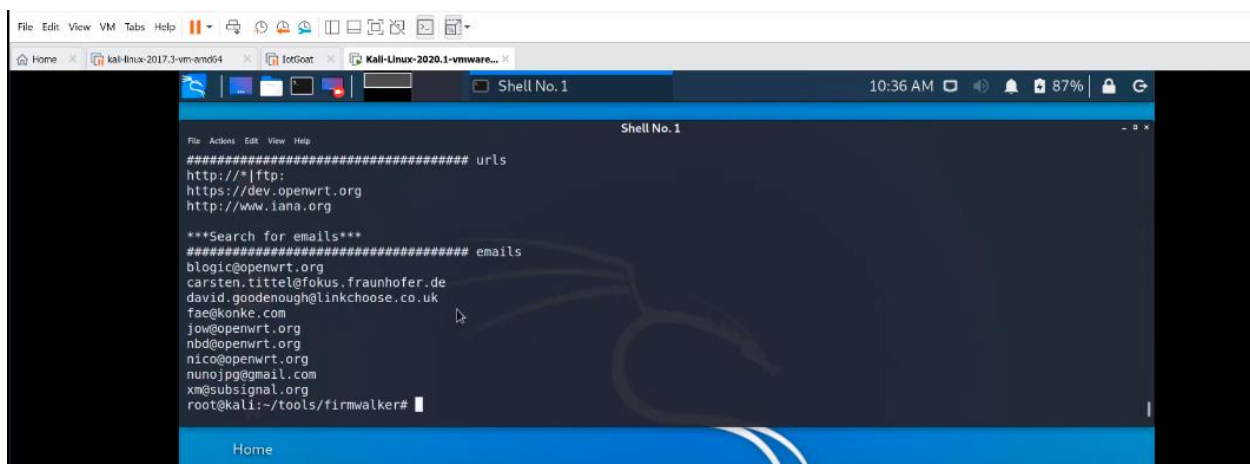


Figure 33: Firmware Kali Linux analysis security checking IOT hardware

Searching for URL

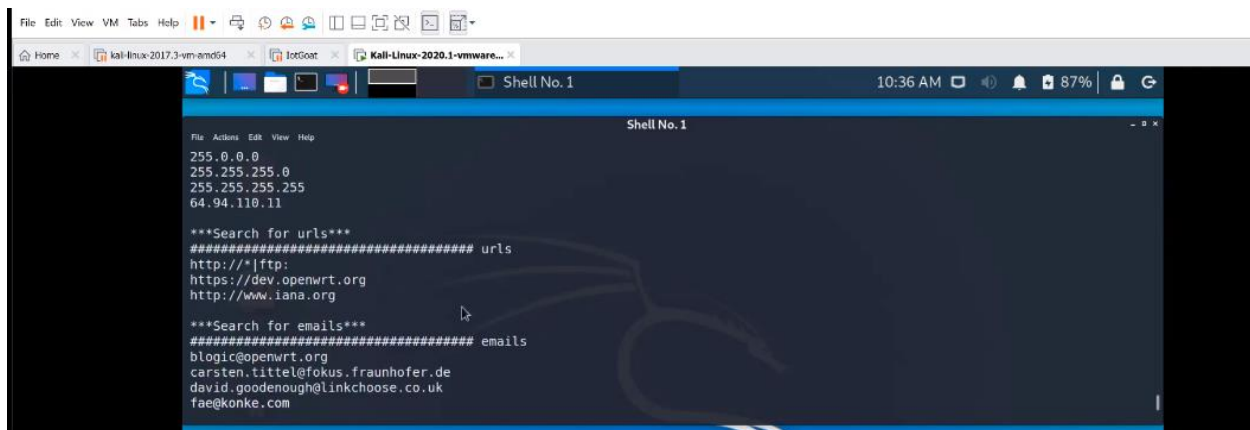


Figure 33: searching URL

Searching for Encoded IP Address

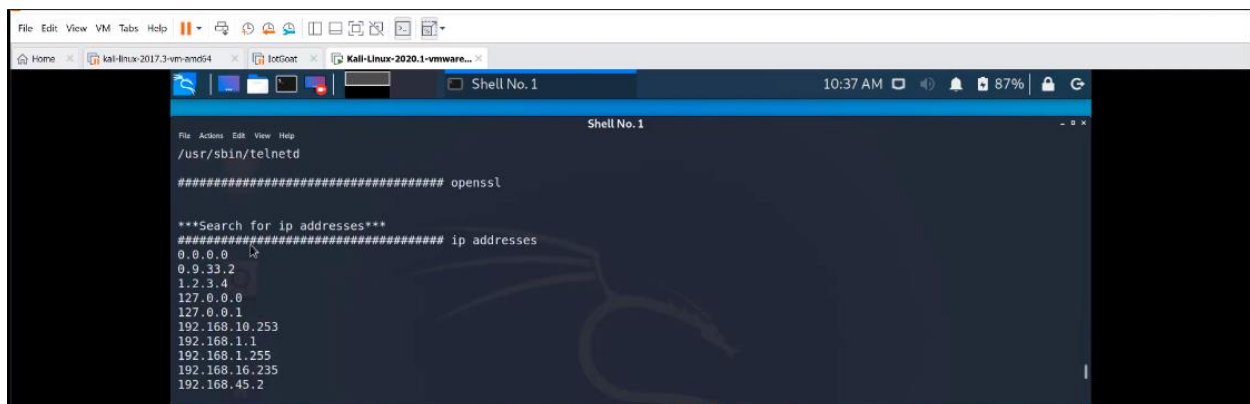


Figure 34: searching encoded IP address

Searching for OPEN SSL

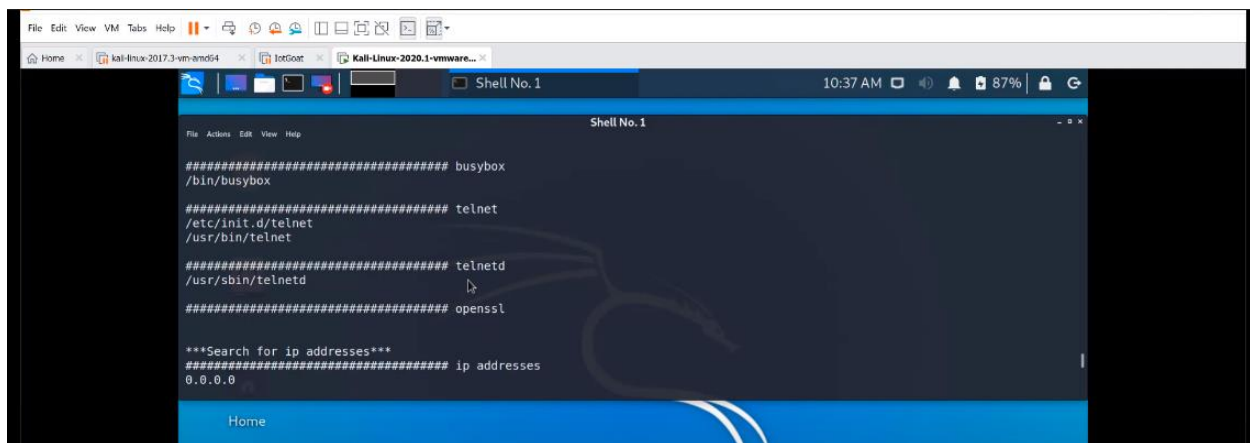


Figure 35: searching open SSL

Searching for telnet with private key

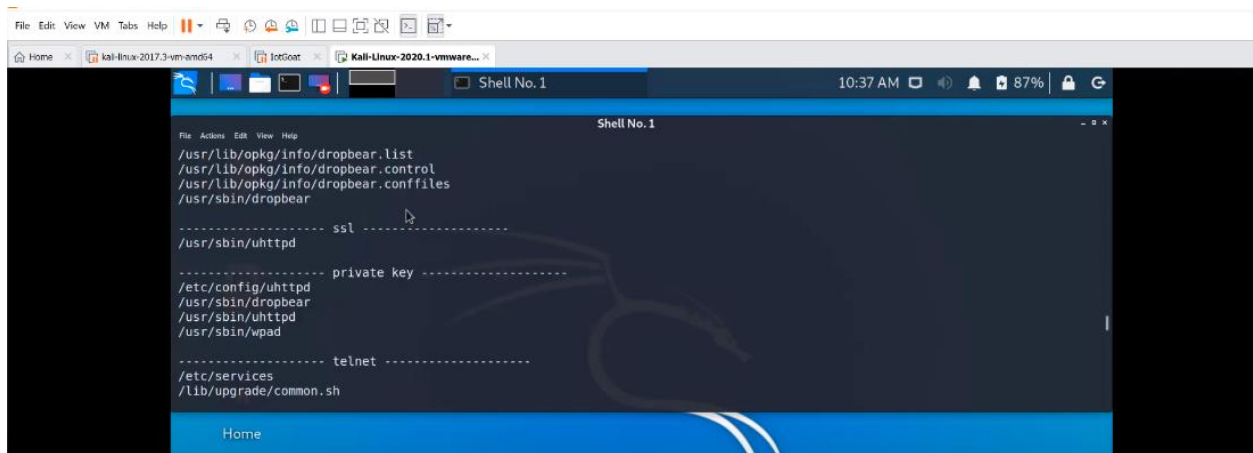


Figure 36: searching malicious user

So Binwalk is used to extract the file system of firmware IOT hardware device to execute the internal firmware data.

Firmadyne

Firmadyne is automated and scalable system for performing emulation and dynamic analysis of Linux based firmware embedded system.

It makes use of Binwalk and QEMU

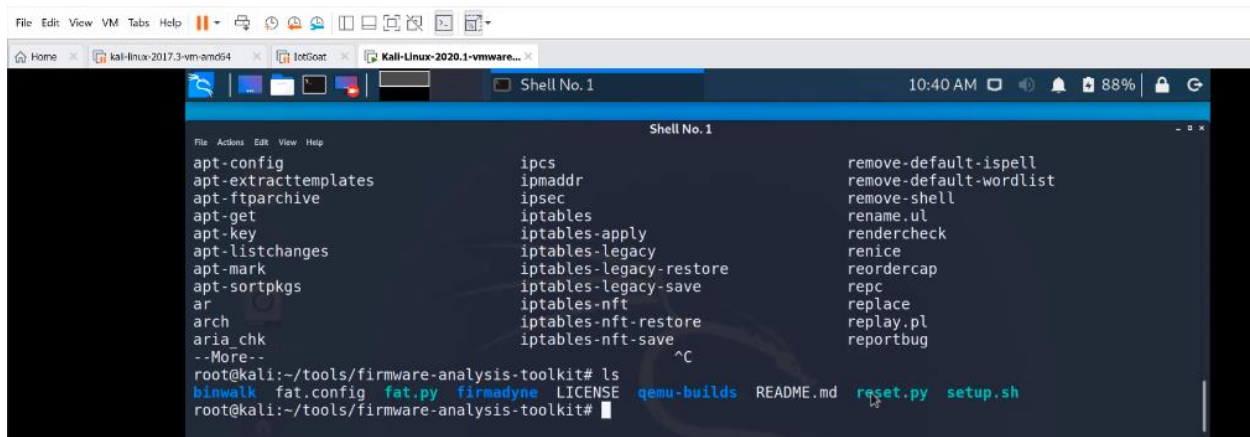
It includes the extracted file from kernel file system and stores in the database system.

1. 3 basic automatic analysis has been performed using the Firmadyne system. It used to access the web pages and this script iterate through the each file within the file system of firmware and image that appear to be served by a webserver and aggregates the results based whether they appear to required authentication.
2. SNMP information dumps contents of public and private SNMP V2c without credit, hence the vulnerability check this script test based on tests for the presence of 60 known vulnerability exploit from Metasploit.

Firmware Analysis Toolkit

(Doshi, R., Apthorpe, N. and Feamster, N., 2018) Simply the script to automate Firmadyne which is the tool used for firmware emulation. Hence the firmware filename as an argument to the script hence the script display the IP address which are assigned to the created network interfaces. The firmware boots up PING the IP which was shown in the browser.

Firmware analysis toolkit directory



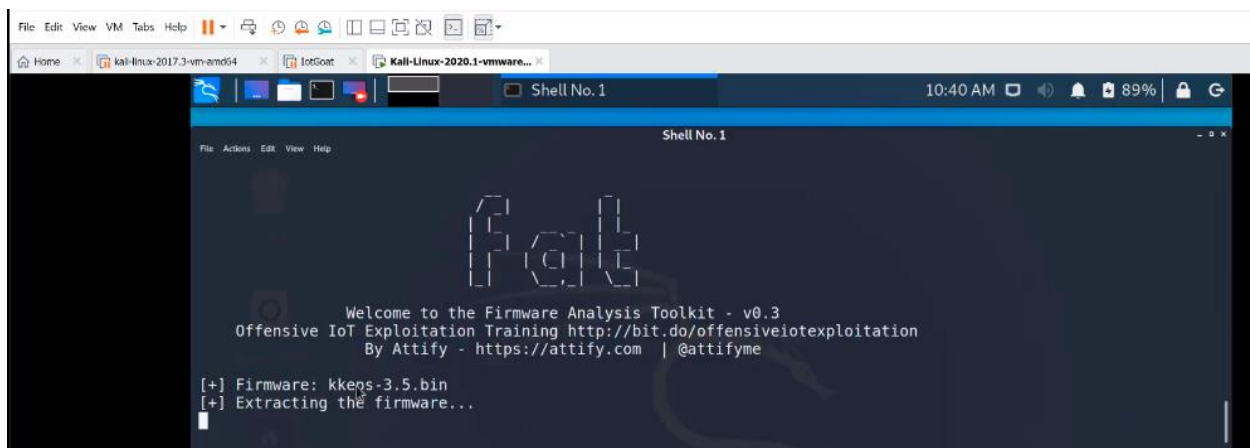
```
File Edit View VM Tabs Help 10:40 AM 88%
kali-linux-2017.3-vm-amd64 Kali-Linux-2020.1-vmware...
Shell No. 1
File Actions Edit View Help
apt-config ipcs remove-default-ispell
apt-extracttemplates ipmaddr remove-default-wordlist
apt-ftparchive ipsec remove-shell
apt-get iptables rename.ul
apt-key iptables-apply rendercheck
apt-listchanges iptables-legacy renice
apt-mark iptables-legacy-restore reordercap
apt-sortpkgs iptables-legacy-save repc
ar iptables-nft replace
arch iptables-nft-restore replay.pl
aria_chk iptables-nft-save reportbug
--More--
root@kali:~/tools/firmware-analysis-toolkit# ls
binwalk fat.config fat.py firmadyne LICENSE qemu-builds README.md reset.py setup.sh
root@kali:~/tools/firmware-analysis-toolkit#
```

Figure 37 firmware directory toolkit

Reset.py this file should be run analyzing the firmware.

Fat is firmware toolkit analysis toolkit, offensive IOT Exploitation training the offensive threads.

it includes the Firmware: KKEP-3.5.bin and the extracted firmware file.



```
File Edit View VM Tabs Help 10:40 AM 89%
kali-linux-2017.3-vm-amd64 Kali-Linux-2020.1-vmware...
Shell No. 1
File Actions Edit View Help
Welcome to the Firmware Analysis Toolkit - v0.3
Offensive IoT Exploitation Training http://bit.do/offensiveiotexploitation
By Attify - https://attify.com | @attifyme

[+] Firmware: kkeps-3.5.bin
[+] Extracting the firmware...
```

Figure 38: defensive security FAT IOT analysis

IOT device Firmware file has been extracted

Now test the file in browser:

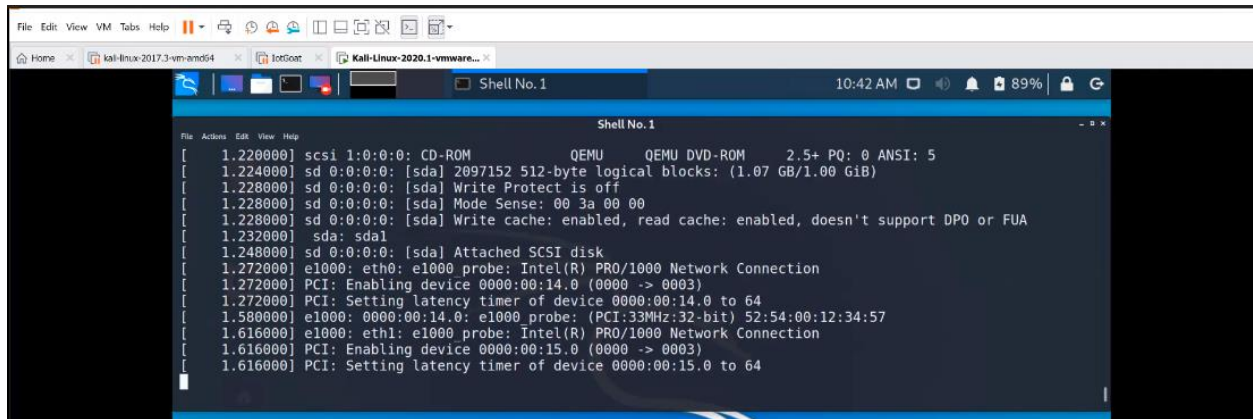


Figure 39: security execution

The IP address: 192.168.10.256 extracted from IOT device and executes in web browser.

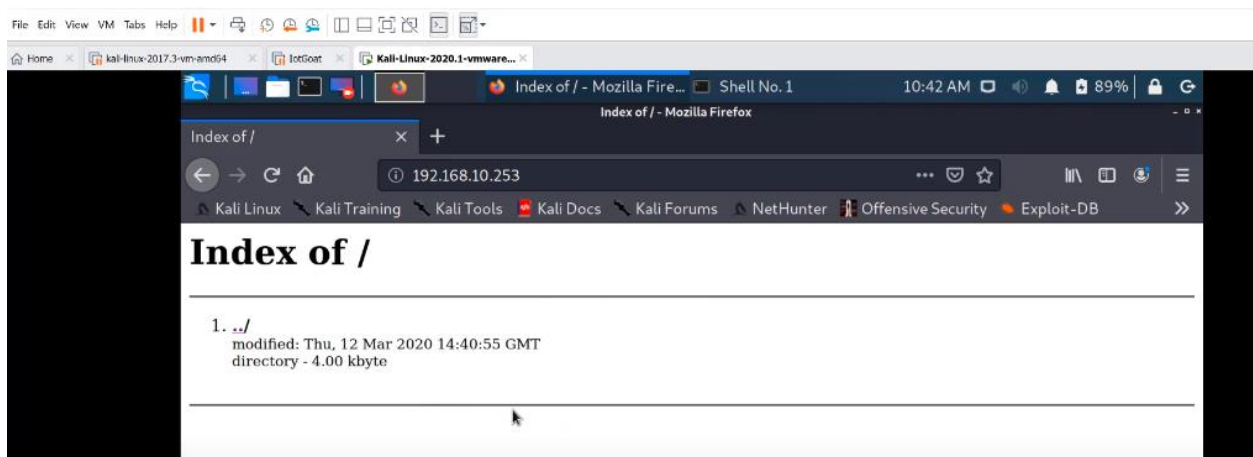


Figure 40: check web URL hacker user

Machine Learning VS Ethical Hacking for IOT Security

(Strecker, S., Haaften, W.V. and Dave, R., 2021) It has been determined and analyzed that the ethical hacking Kali Linux method is very good, machine learning modeling is not good to secure because its only work to analyze the PCAP Wireshark data to view the infected network data packets by experience through the machine learning modeling.

Ethical Hacking by using the Kali Linux operating system which enable the smart home user to determine the real time ethical process in which the various security tools has been attached to secure the IOT device through the firmware analysis.

So it is strongly recommended by various researcher that Kali Linux security is the only way to secure smart home IOT devices.

Critical Analysis Ethical Hacking to Secure IOT devices

(Mukundini, K. and Karthi, R., 2020) Kali Linux operating system freely available for everyone, which organized the smart internet of thing security system. Various IP address based security in which encryption method adapted to hide the device and secure the device. Security method of Kali Linux is an organized method to predict the infected IOT system.

So it was noted that the internet of thing system secure through the Kali Linux operating system, the security method is very easily to deploy in real time, such as

1. Secure the Internal router through Kali Linux tool
2. Secure the internet WIFI through Kali Linux tool
3. Hide the Internet of thing device through Kali Linux tool security
4. Hide the location and IP address of smart IOT device through Kali Linux system

(Alzahrani, T. and Karimian, N., 2021) So it has been observed carefully and predicted that the machine learning method does not support in fully cooperation to secure the internet of thing devices from hacking attack and malware attack. Kali Linux is the best way to organized security in more appropriate manner.

Chapter # 5: Discussion & Conclusion

Machine learning methods continuous trying to deploy improved version of advanced machine learning methods in order to minimize the internet of thing hacking attack. Smart home internet of thing system is designed to control the electronic home appliance in which internet WIFI is connected with smart device and mobile phone. The major discovery of internet of things application is to negotiation energy & resource management. Internet of thing devices is facing various security issues research gap, in order to maintain the hardware & software functionality. Machine learning methods is unable to secure the smart home solution because the real time monitoring needs improvement advanced machine learning methods needs to improve the security parameters. Security implementation development is always taking consideration in which the desired outcome might be retrieved and planned. Kali Linux and parrot operating system particularly designed for maintaining the ethical hacking system to prevent from cyber-attack. Penetration testing is advanced and organized method to manage the internet of thing security mechanism. Somehow the router and external internet firewall is not secured due to various issues and challenges, the internet of thing system attacked by various security protocols to capture the internet of thing system internal data. Internet of things system always facing security issues & challenges which needs to review them, cyberattack occurred by closely related to the implementation of security system solutions. The development of advanced penetration testing system which are needs to review them in order to maintain the security precautions.

Critical Discussion

Investigating the robustness of IOT security cameras against cyberattack

(Trabelsi, Z., 2022) the experimental results present which are based on machine learning vs Kali Linux testing, since internet of things devices able to collect data enable the user to manage and secure their security credentials. Since internet of things devices facing various vulnerability security attack which are evaluate the robustness and resilience of specific kinds of internet of things system. This research objectives to achieve the security measurements of internet of things smart home solution which needs more depth review on technical research finding, research gap identified which needs more technical considerations, the technical literature finding which are designed to develop the advance machine learning strategies & techniques. Cyberattack identified by protocol assessment testing such as Wireshark network analysis, various cyber security solution are designed by scanning the real time computer network such as real time network scanning focused on protocol pattern to identify the pattern in the communication.

Wireshark VS CSV

Wireshark file composed of network scanning file, Wireshark tool enable them to capture & identify the network security pattern such as TCP and UDP parameter form source address to destinations. Wireshark file is extracted during the real time network scanning of internet of thing system. Wireshark file benefits is to analyze them through development of machine learning algorithm to scan the vulnerability attack in the PCAP file. Beside this comma separated value file (CSV) file contains spreadsheet contents in order to maintain the various security system. CSV file enable them to identify the IOT data but this file is created after analysis of PCAP file, so major finding is to analyze the PCAP Wireshark data file in which the various security issues has been challenged. Security measurements & tools has maintained through the sufficient information of CSV file but the issues still exists that the CSV file is not updated & maintained on regular basis. PCAP Wireshark file enable them to develop the network security solutions in real time.

Machine learning VS Kali Linux

Internet of thing data generated during the internet scanning methods since the features of smart home device end point which are creating data composed on destination server via the internet link. IOT internet of thing based system is infected with cyberattack and mitigate through machine learning algorithm but the advanced approach deploy to maintain the security it should be based on Kali Linux solution. Since the machine learning methods used to identify the security prevention protocols based on data discovery. Objective of machine learning models which builds the advanced security mechanism should be sensor technology scan during the security control measurement. Internet of things environment in order to build the machine learning modeling in which to minimize the network security attack. Since machine learning modeling enable them to identify the dataset which improve the security mechanism protocols but needs to review them.

Kali Linux security system is excellent platform to achieve the penetration testing and ethical hacking system. Ethical hacking is platform to identify the network security, various network attack identify though the development of internet of thing based system. Ethical hacking is organized way to manage the entire security of system of cyberattack, since the cyberattack minimized and controlled by penetration testing system.

Anomaly detection method prevented on machine learning modeling experiencing through the dataset, hence the advanced & improved machine learning modeling system might be able to detect any vulnerability attack.

Kali Linux Security Solution

Ethical hacking security solution designed to minimize the actual hacking attack, this training course has been designed to maintain the cybersecurity of smart internet of thing system. Since ethical hacking system application is applicable to design and carrying the ethical hacking discovery. Since ethical hacking security solution is the major discover to minimize the cyber-attack. Hacker can creates algorithm & motivate the malicious activity file to maintain and understand the malicious activity. Various malicious and hacking activity developed composed of security solution tool, Wireshark is amazing tool to scans the real time network security, since Wireshark tools enable them to identify the security solutions.

Penetration testing in IOT System

The internet of things objects offers new devices & services to maintain the IOT network. New and advanced penetration testing tool enable them to capture the needed complement method. Testing IOT security composed of IP camera which these applications are expansion rapidly since security & privacy of internet of thing system merged with major problem. Recent studies identified that maintaining the major problem of network security.

Since security & privacy maintained & updated through penetration testing system, various security implementation of internet of thing devices which emerged the connected devices. Internet of thing system security implementation perfectly works on scanning the network and establish security breaches on them.

The motivation of IP camera undertake more effective security solution to maintain the security through Kali Linux based solution. This research concluded on Kali Linux solution.

References

- Stanislav, M. and Beardsley, T., 2015. Hacking iot: A case study on baby monitor exposures and vulnerabilities. *Rapid7 Report*.
- Ding, A.Y., De Jesus, G.L. and Janssen, M., 2019, September. Ethical hacking for boosting IoT vulnerability management: A first look into bug bounty programs and responsible disclosure. In *Proceedings of the Eighth International Conference on Telecommunications and Remote Sensing* (pp. 49-55).
- Robberts, C. and Toft, J., 2019. Finding vulnerabilities in iot devices: Ethical hacking of electronic locks.
- Park, J. and Tyagi, A., 2017. Using Power Clues to Hack IoT Devices: The power side channel provides for instruction-level disassembly. *IEEE Consumer Electronics Magazine*, 6(3), pp.92-102.
- Saha, T., Aaraj, N., Ajjarapu, N. and Jha, N.K., 2021. SHARKS: Smart Hacking Approaches for Risk Scanning in Internet-of-Things and cyber-physical systems based on machine learning. *IEEE Transactions on Emerging Topics in Computing*.
- Kshetri, N., 2017. Can blockchain strengthen the internet of things?. *IT professional*, 19(4), pp.68-72.
- Visoottiviseth, V., Akarasiriwong, P., Chaiyasart, S. and Chotivatunyu, S., 2017, November. PENTOS: Penetration testing tool for Internet of Thing devices. In *TENCON 2017-2017 IEEE Region 10 Conference* (pp. 2279-2284). IEEE.
- Sathwara, S., Dutta, N. and Pricop, E., 2018, June. IoT Forensic A digital investigation framework for IoT systems. In *2018 10th international conference on electronics, computers and artificial intelligence (ECAI)* (pp. 1-4). IEEE.
- Lee, J.H. and Kim, H., 2017. Security and privacy challenges in the internet of things [security and privacy matters]. *IEEE Consumer Electronics Magazine*, 6(3), pp.134-136.
- Lehrfeld, M. and Guest, P., 2016, March. Building an ethical hacking site for learning and student engagement. In *SoutheastCon 2016* (pp. 1-6). IEEE.
- Patil, S., Jangra, A., Bhale, M., Raina, A. and Kulkarni, P., 2017, September. Ethical hacking: The need for cyber security. In *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)* (pp. 1602-1606). IEEE.
- Ding, A.Y., De Jesus, G.L. and Janssen, M., 2019, September. Ethical hacking for boosting IoT vulnerability management: A first look into bug bounty programs and responsible disclosure. In *Proceedings of the Eighth International Conference on Telecommunications and Remote Sensing* (pp. 49-55).
- Hudson, F.D., Laplante, P.A. and Amaba, B., 2018. Enabling trust and security: TIPSS for IoT. *IT Professional*, 20(2), pp.15-18.
- Alladi, T., Chamola, V., Sikdar, B. and Choo, K.K.R., 2020. Consumer IoT: Security vulnerability case studies and solutions. *IEEE Consumer Electronics Magazine*, 9(2), pp.17-25.
- Nausheen, F. and Begum, S.H., 2018, January. Healthcare IoT: benefits, vulnerabilities and solutions. In *2018 2nd International Conference on Inventive Systems and Control (ICISC)* (pp. 517-522). IEEE.
- Alwarafy, A., Al-Thelaya, K.A., Abdallah, M., Schneider, J. and Hamdi, M., 2020. A survey on security and privacy issues in edge-computing-assisted internet of things. *IEEE Internet of Things Journal*, 8(6), pp.4004-4022.

- Ni, J., Zhang, K., Lin, X. and Shen, X., 2017. Securing fog computing for internet of things applications: Challenges and solutions. *IEEE Communications Surveys & Tutorials*, 20(1), pp.601-628.
- Kumar, S.A., Vealey, T. and Srivastava, H., 2016, January. Security in internet of things: Challenges, solutions and future directions. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 5772-5781). IEEE.
- Illy, P., Kaddoum, G., Kaur, K. and Garg, S., 2022. ML-based IDPS enhancement with complementary features for home IoT networks. *IEEE Transactions on Network and Service Management*.
- Thorat, P., Dubey, N.K., Khetan, K. and Challa, R., 2021, January. SDN-based predictive alarm manager for security attacks detection at the IoT gateways. In *2021 IEEE 18th annual consumer communications & networking conference (CCNC)* (pp. 1-2). IEEE.
- Hazra, A., Alkhayyat, A. and Adhikari, M., 2022. Blockchain-aided Integrated Edge Framework of Cybersecurity for Internet of Things. *IEEE Consumer Electronics Magazine*.
- Alghamdi, R. and Bellaiche, M., 2021, May. A deep intrusion detection system in lambda architecture based on edge cloud computing for IoT. In *2021 4th International Conference on Artificial Intelligence and Big Data (ICAIBD)* (pp. 561-566). IEEE.
- Alqarni, H., Alnahari, W. and Quasim, M.T., 2021, March. Internet of things (IoT) security requirements: Issues related to sensors. In *2021 National Computing Colleges Conference (NCCC)* (pp. 1-6). IEEE.
- Azumah, S.W., Elsayed, N., Adewopo, V., Zaghloul, Z.S. and Li, C., 2021, June. A deep lstm based approach for intrusion detection iot devices network in smart home. In *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)* (pp. 836-841). IEEE.
- Luo, H., Wang, C., Luo, H., Zhang, F., Lin, F. and Xu, G., 2021. G2F: A secure user authentication for rapid smart home IoT management. *IEEE Internet of Things Journal*, 8(13), pp.10884-10895.
- Antzoulis, I., Chowdhury, M.M. and Latiff, S., 2022, May. IoT Security for Smart Home: Issues and Solutions. In *2022 IEEE International Conference on Electro Information Technology (eIT)* (pp. 1-7). IEEE.
- Ali, R.F., Muneer, A., Dominic, P.D.D. and Taib, S.M., 2021, December. Hyperledger Fabric Framework with 5G Network for Blockchain-based Security of IoT Smart Home Applications. In *2021 International Conference on Decision Aid Sciences and Application (DASA)* (pp. 1109-1114). IEEE.
- Abir, S.A.A., Anwar, A., Choi, J. and Kayes, A.S.M., 2021. Iot-enabled smart energy grid: Applications and challenges. *IEEE access*, 9, pp.50961-50981.
- Manhas, J. and Kotwal, S., 2021. Implementation of intrusion detection system for internet of things using machine learning techniques. In *Multimedia Security* (pp. 217-237). Springer, Singapore.
- Tahsien, S.M., Karimipour, H. and Spachos, P., 2020. Machine learning based solutions for security of Internet of Things (IoT): A survey. *Journal of Network and Computer Applications*, 161, p.102630.
- Zeadally, S. and Tsikerdakis, M., 2020. Securing Internet of Things (IoT) with machine learning. *International Journal of Communication Systems*, 33(1), p.e4169.
- Yong, B., Wei, W., Li, K.C., Shen, J., Zhou, Q., Wozniak, M., Połap, D. and Damaševičius, R., 2022. Ensemble machine learning approaches for webshell detection in Internet of things environments. *Transactions on Emerging Telecommunications Technologies*, 33(6), p.e4085.

Din, I.U., Guizani, M., Rodrigues, J.J., Hassan, S. and Korotaev, V.V., 2019. Machine learning in the Internet of Things: Designed techniques for smart cities. *Future Generation Computer Systems*, 100, pp.826-843.

Khalifa, M., Algarni, F., Khan, M.A., Ullah, A. and Aloufi, K., 2021. A lightweight cryptography (LWC) framework to secure memory heap in Internet of Things. *Alexandria Engineering Journal*, 60(1), pp.1489-1497.

Rao, V., Prema, K.V. 2021 a review on lightweight cryptography for Internet-of-Things based applications. *J Ambient Intell Human Comput* **12**, 8835–8857 (2021).

Du, M., Wang, K., Chen, Y., Wang, X. and Sun, Y., 2018. Big data privacy preserving in multi-access edge computing for heterogeneous Internet of Things. *IEEE Communications Magazine*, 56(8), pp.62-67.

Visoottiviseth, V., Kotarasu, C., Cheunprapanusorn, N. and Chamornmarn, T., 2019, November. A Mobile Application for Security Assessment Towards the Internet of Thing Devices. In *2019 IEEE 6th Asian Conference on Defence Technology (ACDT)* (pp. 1-7). IEEE.

Barybin, O., Zaitseva, E. and Brazhnyi, V., 2019, October. Testing the security ESP32 internet of things devices. In *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)* (pp. 143-146). IEEE.

Jeremiah, J., 2019, September. Intrusion detection system to enhance network security using raspberry pi honeypot in kali linux. In *2019 International Conference on Cybersecurity (ICoCSec)* (pp. 91-95). IEEE.

Tien, C.W., Tsai, T.T., Chen, Y. and Kuo, S.Y., 2018, October. UFO-Hidden Backdoor Discovery and Security Verification in IoT Device Firmware. In *2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)* (pp. 18-23). IEEE.

Ma, Y., Han, L., Ying, H., Yang, S., Zhao, W. and Shi, Z., 2019, May. SVM-based instruction set identification for grid device firmware. In *2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)* (pp. 214-218). IEEE.

Trabelsi, Z., 2022, March. Investigating the Robustness of IoT Security Cameras against Cyber Attacks. In *2022 5th Conference on Cloud and Internet of Things (CIoT)* (pp. 17-23). IEEE.

Kiran, K.S., Devisetty, R.K., Kalyan, N.P., Mukundini, K. and Karthi, R., 2020. Building a intrusion detection system for IoT environment using machine learning techniques. *Procedia Computer Science*, 171, pp.2372-2379.

Sahu, K., Kshirsagar, R., Vasudeva, S., Alzahrani, T. and Karimian, N., 2021, January. Leveraging Timing Side-Channel Information and Machine Learning for IoT Security. In *2021 IEEE International Conference on Consumer Electronics (ICCE)* (pp. 1-6). IEEE.

Strecker, S., Haaften, W.V. and Dave, R., 2021. An analysis of IoT cyber security driven by machine learning. In *Proceedings of International Conference on Communication and Computational Technologies* (pp. 725-753). Springer, Singapore.

Doshi, R., Apthorpe, N. and Feamster, N., 2018, May. Machine learning ddos detection for consumer internet of things devices. In *2018 IEEE Security and Privacy Workshops (SPW)* (pp. 29-35). IEEE.

Ma, Y., Han, L., Ying, H., Yang, S., Zhao, W. and Shi, Z., 2019, May. SVM-based instruction set identification for grid device firmware. In *2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)* (pp. 214-218). IEEE.