

Internet-of-Things Hacking

Thesis Introduction Chapter 1



July 26, 2022

Dharmendar

Table of Contents

[Chapter # 1: Internet of things hacking 3](#_Toc109737315)

[Smart Home Security 3](#_Toc109737316)

[Machine Learning based solution for Security of internet of things (IOT) 3](#_Toc109737317)

[Machine learning approach for webshell detection in internet of things devices 4](#_Toc109737318)

[Machine learning method internet of things designed 4](#_Toc109737319)

[Lightweight Cryptography of Internet of Things System 4](#_Toc109737320)

[Big data Privacy Preserving in Multi-Access Edge Computing 5](#_Toc109737321)

[Testing the Security ESP32 Internet of things devices 5](#_Toc109737322)

[Intrusion detection system enhance network security using RasberryPI Honeypot in Kali Linux 5](#_Toc109737323)

[Kali Linux Honeypot Cybersecurity 5](#_Toc109737324)

[Kali Linux Binwalk Firmware Security 6](#_Toc109737325)

[Security verification in IOT devices Firmware 6](#_Toc109737326)

[SVM based intrusion detection identification of GRID device Firmware 6](#_Toc109737327)

[Large-Scale firmware function security based on SImhash 6](#_Toc109737328)

[Research Aim & Objective 6](#_Toc109737329)

[Research Considerations 7](#_Toc109737330)

# Chapter # 1: 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

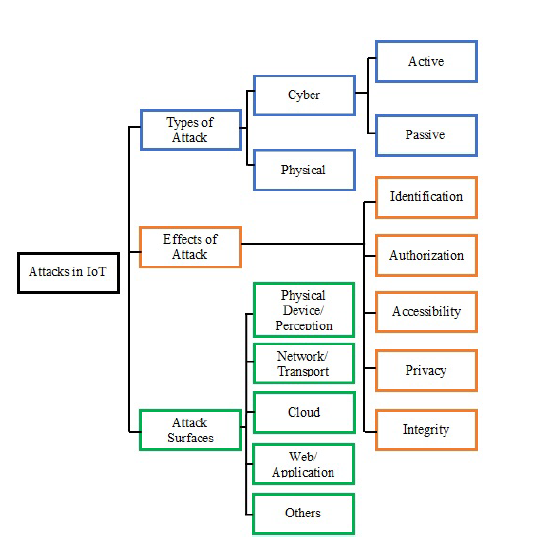
(Manhas, J. and Kotwal, S., 2021) smart home solutions related with each other to manage the smart electric system in organized manner. Smart home solution based on sensor technology and alarm which detects house changes condition from smoke development the opening, closing of doors and windows. If the 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: 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 RasberryPI 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.