Dharmendra

Internet-of-Things Hacking

Discussion & Conclusion Chapter 5

# 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 exits 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.