Internet-of-Things Hacking

Dharmendra

CHAPTER 2 DISSERTATION

Contents

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 Since the internet of thing devices to classify the devices in outdated security which is not permitted to do the validation outcome.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.

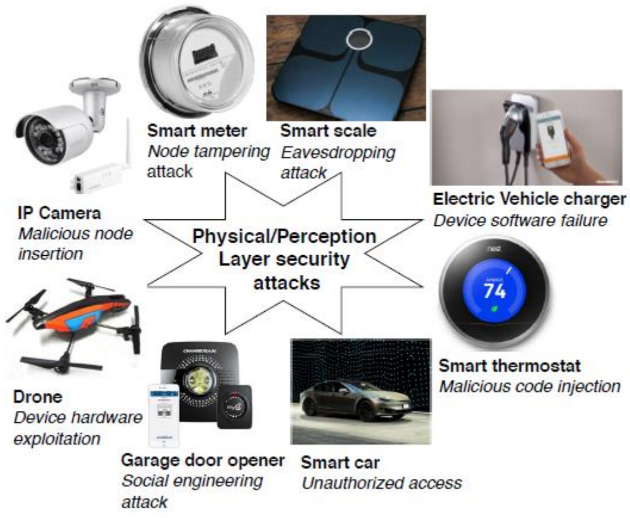

Figure 1: eight common physical attack on the physical IOT security layer

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.

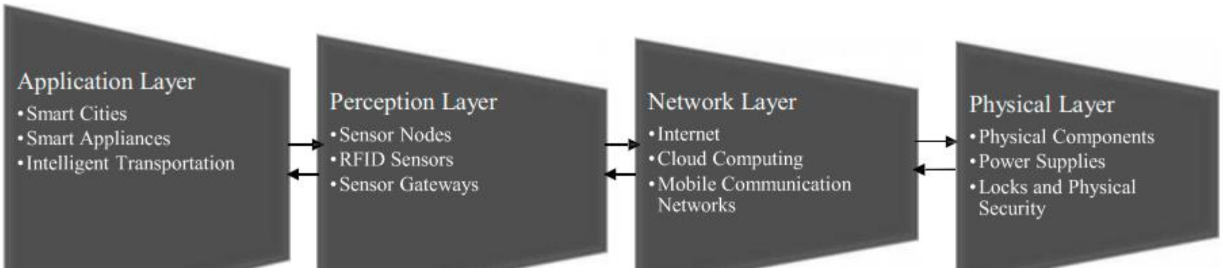

Figure 2: IOT Layard Approach

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.

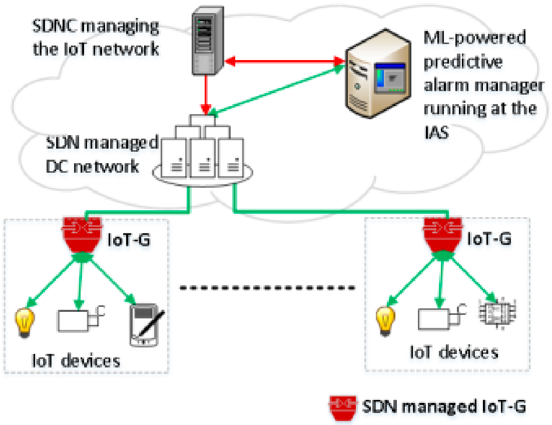
SDNC managing the IoT network
ML-powered predictive alarm manager running at the IAS
SDN managed DC network
IoT-G
IoT-G
IoT devices
IoT devices
SDN managed IoT-G

Figure 3: 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.

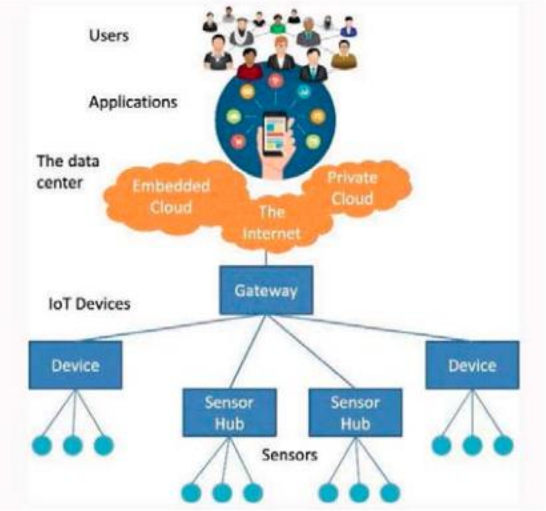

Figure 4: Adaptive model

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.

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: TIPPSS 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.