

SECURITY ANALYSIS OF INTERNET OF THINGS (IOT) DEVICES IN SMART HOMES

NAME :- PARTH TABLAWALA

ID :- 2515744

PROGRAM :- MSC CYBERSECURITY & DIGITAL FORENSICS

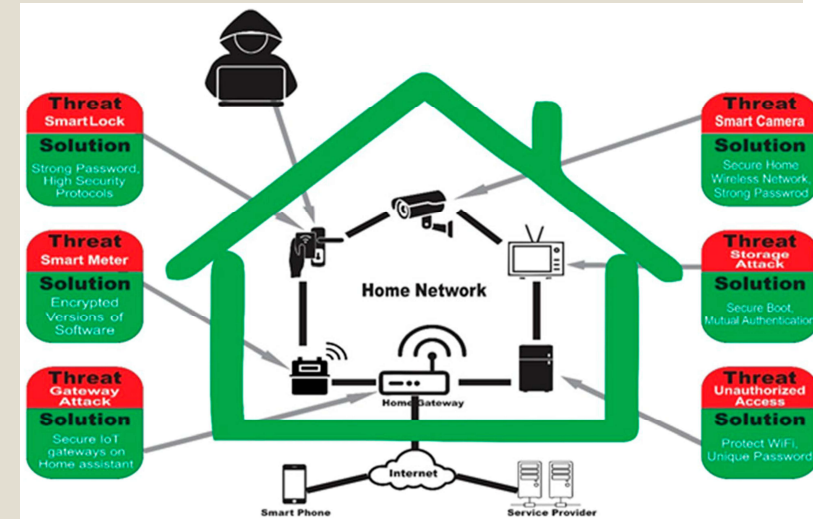
SUBMISSION TO :- DR. SURESH SHANMUGASUNADARAM

Introduction

- The fast evolution of the Internet of Things (IoT) has changed the modern digital environment significantly as it allows connected devices to communicate and collect and exchange data via the internet. The smart home ecosystem is one of the most evident applications of the IoT technology in which various devices, including smart cameras, thermostats, lighting systems, voice assistants, and security sensors, are connected to automatize all processes in a house and make it convenient and efficient. Smart home technologies come in handy with many advantages such as ability to monitor remotely and sustainable use of power, improved comfort and better quality of living to its users. Nevertheless, more and more connected devices have also brought about severe cybersecurity and privacy issues. Most IoT products are built with little security features that can be easily attacked by cyberattacks, intruders and data theft.

Research Context / Background

- The high-speed growth of the Internet of Things (IoT) has revolutionized the digital ecosystems of today by making devices that are connected to automatically gather, share, and process data using internet-connected networks (Magara and Zhou, 2024).
- Technologies used in smart homes have undergone huge levels of introduction globally owing to the availability of internet, low expenses of such devices, and the fact that consumers are ever demanding automated living conditions. With these systems, users can remotely operate and watch over the devices in their homes via mobile apps or cloud services to a great extent to improve the level of convenience, comfort, and living standards (Rock, Tajudeen and Chung, 2024).
- Although these devices have these benefits, the rising number of connected devices in a smart home has increased the scope of the Digital attack, and home networks are now susceptible to cybersecurity risks (Lata and Kumar, 2022).
- Smart home environment based on IoT represent a typical heterogeneous network where the devices of various manufacturers can work with different communication protocols. This complexity makes it highly challenging to handle security and poses interoperability problems, which, in turn, can result in security gaps that can be exploited by attackers in the connected ecosystem (Netinant et al., 2024).



Contd...

- A number of papers have reported that several IoT devices are implemented with weak authentication measures, non-encrypted communication paths and insecure firmware update protocols (Mufidah and Nuha, 2024).
- Moreover, Smart home devices usually store and transmit user sensitive data such as personal habits, surveillance and location-based activities. In case of their attack, attackers can gain access to sensitive household information, hence it poses serious privacy and cybersecurity risks (Magara and Zhou, 2024).
- It is noted that users will also have insufficient technical awareness, which may cause insecure IoT settings, default settings, and weak passwords and out-of-date software that pose an additional threat to the system (Philip, Luu and Carte, 2023).



Research Problem

- This has drawn considerable cybersecurity threats due to the fast development of smart home systems that have IoT, owing to the fact that most of the connected interfaces do not have advanced security control measures. Cyber attackers will find it easy to target these types of environments because they are highly vulnerable to attacks by people intending to gain unauthorized access to the household networks and the sensitive information of the users (Lata and Kumar, 2022).
- Smart home networks are normally made up of a large number of heterogeneous appliances that are linked together via one network infrastructure. In the event of an attack on one vulnerable device, the attackers would use it as a means of access into the other devices to move laterally throughout the network, breaking the entire system.
- Reason being, a number of studies have found that most IoT devices have poor default passwords, lack of sufficient encryption and a cumbersome provision of updates. The problems leave long term holes in them that are not fixed yet, making smart home networks more susceptible to cyber threats (Mufidah and Nuha, 2024).
- Poor user awareness about the concept of the IoT security is another issue that can be a challenge. Numerous web based owners do not implement the right authentication controls, or update the firmware regularly, thus exposing any systems linked to it without knowing (Nemec Zlatolas, Feher and Hnelbl, 2022).
- This gap must be filled in order to come up with practical solutions, which can improve the practice of sharing data in a secure manner and that guards against new cyber threats the smart home ecosystems is vulnerable to.

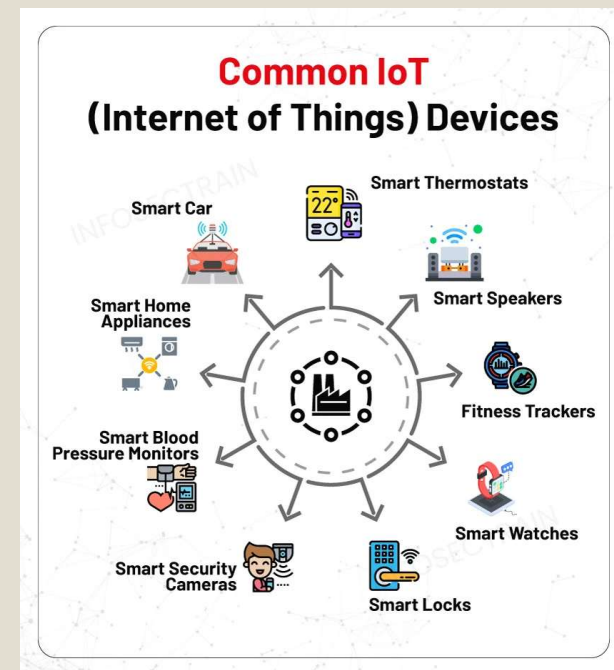
Research Aim and Objectives

In this research, the security risks of IoT devices in smart home environments and mitigation at the network level will be analysed, using a qualitative, secondary-data-based research design, using Cisco simulation software. The research Objectives are

- To pursue this purpose, the study will seek the following objectives:
- To examine the current state of the situation, introduce IoT in smart households and establish the most severe security risks of interconnected domestic appliances.
- To analyse available scholarly and industry sources of common smart home IoT vulnerabilities, threats, and attack vectors.
- To comment on the weaknesses of the current security measures utilised in smart home systems of the Internet of Things, in particular, authentication, communication protocols, and network architecture.
- To develop a simulated smart home IoT network in Cisco Packet Tracer (or in any other Cisco-supported network simulation tool) to represent possible security vulnerabilities and countermeasures.
- To experiment with possible network-level security measures that can involve segmentation, access control, firewall policies and secure communication design in the simulated environment.

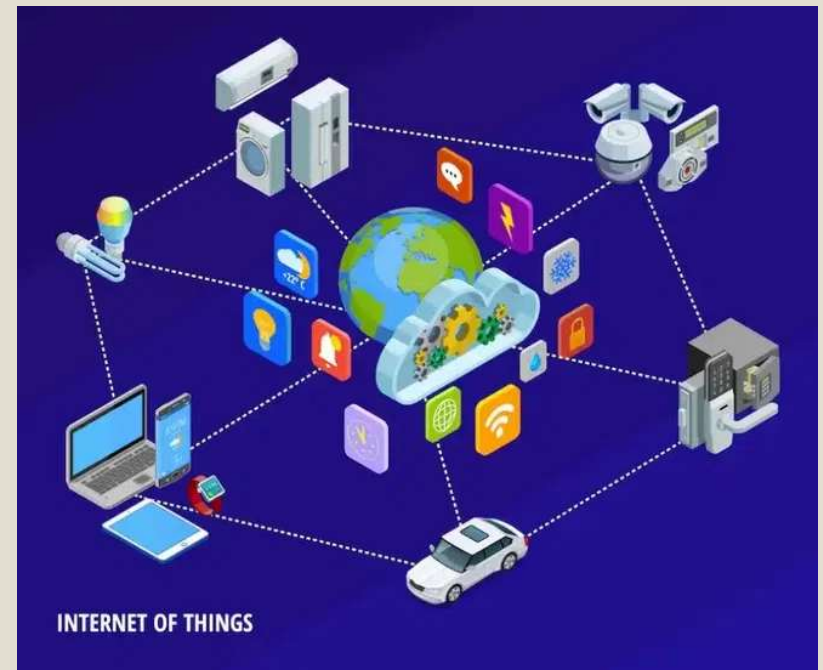
Literature Review and Research Gap

- The recent literature shows that the internet of things smart home technologies have developed at a very high pace and are characterized by the capabilities to automatize home functions using their devices that are connected to each other like smart cameras, locks, sensors, and appliances. These systems are convenient, energy saving, and can be monitored at a distance, which improves the quality of life of users significantly (Rock, Tajudeen and Chung, 2024).
- The study suggests that smart home IoT systems architecture is complex and heterogeneous by nature and contains an abundance of devices that use a variety of wireless protocols, cloud computing, and mobile applications to communicate. Such interconnected design enlarges the attack surface, and it forms more vulnerability points (Magara and Zhou, 2024).
- Some reports have also determined susceptible vulnerabilities in the IoT devices such as weak authentication, default passwords, insecure firmware updates and low encryption protocols. The latter weaknesses are done frequently due to the fact that manufacturers are worried about both cost and quick deployment of products rather than solid security design (Lata and Kumar, 2022).



Contd...

- Research has also been reported on some of the attack vectors against the smart home environment such as man-in-middle attacks, eavesdropping, denial-of-service attacks, and the recruitment of malware-based botnets. These risks have the ability to undermine user privacy and the integrity of operations of smart homes devices (Sayeduzzaman et al., 2024).
- The security models that have been suggested in the literature include the segmentation of the network, good authentication scheme, encryption-based communication system, and intrusion detection systems. These strategies are used to minimize the threat of unauthorized access and contain the propagation of cyberattacks in the IoT networks (Mufidah and Nuha, 2024).
- Majority of these developments have been undertaken based on a theoretical approach or at the device level how to mitigate the vulnerabilities but without demonstrating how the architecture can be used in mitigating these threats in practice in the smart home environment.
- The gap that is critical in the research is the elaboration of the available, simulation-based models that would depict the manner in which the secure network design and architecture can execute the security of smart home IoT and the ability to share data securely.



Research Methodology

- The qualitative research design employed in the study is the analysis of a secondary data. It is an appropriate methodology, as the study is intended to establish the knowledge of the weaknesses of the IoT and approximate the potential remedies rather than give statistical measures through quantitative data collection.
- The Design science Research strategy of the research involves a combination of theoretical discussion and development of a practical artifact. This research project aims to explore security weakness and preventive action in a simulated smart omen IoT network setting, which is the artifact of the research.
- Peer-reviewed literature sources that will be utilized as secondary sources of data include peer-reviewed academic journals, conference papers, cybersecurity reports, and technical documentation. These resources are credible and give information on IoT vulnerabilities, attack patterns and security systems suitable to the smart home setting.

Contd...

- A way of doing it will be created with the help of simulation and using Cisco Packet Tracer software a realistic smart home network will be modelled with connected IoT devices, routers, and user devices. Such environment will facilitate examination of possible security vulnerabilities under a controlled environment.
- There will be two types of network design developed in the simulation. Model 1 will be a standard consumer smart home network where all devices are on the same network and there are no isolation and access controls.
- The second model will also bring with it better security architecture comprising of network segmentation, firewall policies and access control settings that are meant to minimize attack surfaces and to curb any lateral movement within the network.

Project Planning and Resources

- The research project will follow a satisfactory schedule that will include several tasks, including literature review, research design, simulation generation, data analysis, and preparation of final report. One step will be followed by another in order to have a systematic completion of every stage.
- The first step will be a comprehensive analysis of the scholarly literature connected with the topic of IoT security, smart home architecture, cybersecurity threats, the network defence mechanisms. This action will offer a theoretical foundation of the research.
- The second step will also be aimed at creating the simulated smart home network environment in Cisco Packet Tracer. The simulation will entail prevalent IoT devices which will comprise smart cameras, thermostats, lights and home gateways.

Contd...

- The third one will be bringing the security settings within the simulation environment which will include network segmentation, firewall settings and access control controls which are supposed to enhance the security.
- The fourth stage will examine the behaviour between the insecure and the secure network architecture to help in determining the vulnerabilities that may be present and it would also determine how well the adopted security measures perform.
- Some of the resources that will be used to support the research will be Cisco Packet Tracer simulation software, academic databases, and other cybersecurity research publications which will provide the research with theoretical and technical backgrounds.

Project Impact and Limitations

- One may assume that the suggested research will contribute to the current body of literature in the sphere of the IoT cybersecurity by providing an insight into the weaknesses in smart home environments and discovering the most effective security solutions in networks.
- The study has the potential to influence the creation of better understanding of the importance of secure network design in the implementation of smart home devices and connected technologies in both homeowners and consumers of the technologies.
- In technical terms, the study can prove that the network segmentation and access control policies and the better design of the architecture can greatly decrease the attack surface on the IoT ecosystems.
- Cybersecurity may also be taught on the basis of the research that could prove how such simulators as Cisco Packet Tracer could be used to explore smart home security without visiting gadgets or an intrusive attack.

Contd...

- The research can assist in mentoring the learners, scholars and system architects to have the concept of effective means of operation to achieve secured environment in IoT and enable safe information transfer between networking counterparts.
- There are also some limitations of the research. It is a simulated analysis and hence may not be sufficient enough to reflect the richness of the physical world smart home and the physical network traffic environment.
- The research is primarily founded on the secondary sources of information and this may not help in establishing the findings on actual experiments or information collection in real life among real users.

References

- Magara, T. and Zhou, Y., 2024. Internet of things (IoT) of smart homes: privacy and security. *Journal of Electrical and Computer Engineering*, 2024(1), p.7716956.
- Lata, M. and Kumar, V., 2022. IoT network security in smart homes. *Cybersecurity in smart homes: architectures, solutions and technologies*, pp.155-176.
- Netinant, P., Utsanok, T., Rukhiran, M. and Klongdee, S., 2024. Development and assessment of internet of things-driven smart home security and automation with voice commands. *IoT*, 5(1), pp.79-99.
- Sayeduzzaman, M., Hasan, T., Nasser, A.A. and Negi, A., 2024. An internet of things-integrated home automation with smart security system. *Automated Secure Computing for Next-Generation Systems*, pp.243-273.
- Nemec Zlatolas, L., Feher, N. and Hölbl, M., 2022. Security perception of IoT devices in smart homes. *Journal of Cybersecurity and Privacy*, 2(1), pp.65-73.
- Philip, S.J., Luu, T.J. and Carte, T., 2023. There's No place like home: Understanding users' intentions toward securing internet-of-things (IoT) smart home networks. *Computers in Human Behavior*, 139, p.107551.
- Rock, L.Y., Tajudeen, F.P. and Chung, Y.W., 2024. Usage and impact of the internet-of-things-based smart home technology: a quality-of-life perspective. *Universal access in the information society*, 23(1), pp.345-364.
- Mufidah, N.F. and Nuha, H.H., 2024. Performance and security analysis of lightweight hash functions in IoT. *Jurnal Informatika: Jurnal Pengembangan IT*, 9(3), pp.264-270.

Thank
you

