

Introduction

The hazards and vulnerabilities associated with IoT devices, illustrated through experiments how hackers can break into IoT networks by looking for open ports, breaking passwords, scanning networks, and executing deauthentication attacks. The goal of my effort was to increase public awareness of the need to protect personal IoT devices from potential harm.



Project Goals

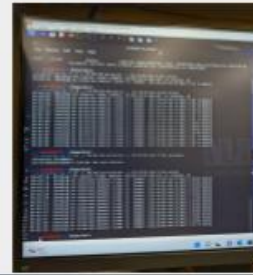
Examine and identify potential risks that an Internet of Things device can encounter; illustrate how an attacker might approach and target a network. This was done with the intention of demonstrating how hackers work and how to create defences against specific attacks before data is lost or stolen.

Goals

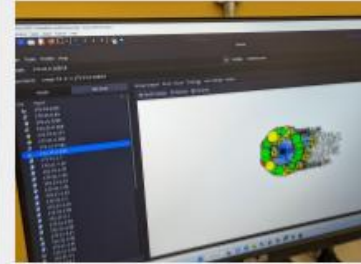
Explain the significance of IoT security and the ease with which devices may be secured with hardware-based security and malware scanners. Identify and assess the most prevalent IoT security issues, including weak authentication, insecure networks, obsolete firmware, and vulnerabilities. To successfully communicate the hazards associated with IoT devices, present real-world attack scenarios that involve testing in a controlled setting and simulating assaults such as DDoS and data breaches.

Method

The study applied a thorough mixed-methods approach to demonstrate practical dangers and vulnerabilities related to Internet of Things (IoT) devices. Qualitative methods were used, such as firsthand observations of IoT device usage and security measures in diverse situations, as well as a thorough literature analysis to acquire current information and insights from prior studies. Quantitative techniques comprising practical experiments were carried out on a variety of IoT devices in a controlled laboratory setting to supplement the qualitative study. The purpose of these studies was to examine the security resilience of the devices and replicate real-world attack scenarios. Specifically, password cracking efforts to obtain unauthorised access, port discovery to find possible entry points, deauthentication attacks to interfere with wireless connections, and network scanning to find active devices and open ports were employed. Through the integration of both qualitative and quantitative methodologies, the study offered a comprehensive comprehension of IoT security issues, supported by actual data from real-world tests. The results made clear how urgent it is to fix IoT device vulnerabilities and how better security measures are required to fend off such attacks.



Conclusion



To raise awareness about the potential vulnerabilities and risks associated with IoT devices, and provide recommendations for improving personal IoT security. Through practical experiments, it demonstrated how attackers can compromise IoT networks and devices, emphasizing the importance of proper security measures and staying informed about emerging threats.