COMPUTING AND APPLICATIONS REVIEWS

Volume 2, Number 1, 2025 Pages 10 – 18 WEBSITE. ca-reviews.com

ETHICAL HACKING IN THE INTERNET OF THINGS (IOT): IDENTIFYING VULNERABILITIES AND ENHANCING SECURITY IN SMART HOME DEVICES

Shakil Ahmad[1]* Rehan Qureshi[2], Samina Gul[3]

[1]*Assistant Manager Networks, Department of Information Technology, Riphah International University, Islamabad, Pakistan*

[2]Department of Software Innovation, Dawood University of Engineering & Technology, Karachi, Pakistan

[3]Faculty of Information Systems, Abdul Wali Khan University, Mardan, Pakistan

**Corresponding Author Email: shakil.ahmad@riphah.edu.pk*

Article Information

Article History

Received:	January 15, 2025
Revised:	February 03, 2025
Accepted:	March 23, 2025
Available Online:	June 30, 2025

Keywords:
Iot Security, Penetration Testing, Vulnerability Assessment, Smart Home Devices, Encryption, Authentication

Abstract

This study investigates the security vulnerabilities in Internet of Things (IoT) devices within smart homes, focusing on common issues such as weak encryption, insecure communication protocols, and inadequate authentication mechanisms. Through a comprehensive penetration testing approach, we identified significant security weaknesses in several IoT devices, including smart voice assistants, security cameras, and smart locks. Our findings revealed that smart voice assistants were particularly vulnerable, exhibiting the highest number of vulnerabilities across multiple categories, including weak encryption and insecure communication channels. Reports revealed high susceptibility rates because numerous devices were susceptible to remote exploitation. The professional job of ethical hackers during penetration tests faces three essential difficulties stemming from complex device architecture alongside privacy concerns which arise from manufacturers' poor execution of standardized security standards. Our findings demonstrate why IoT devices should upgrade their endpoint encryption system while needing periodic firmware maintenance including dual authentication systems. Research shows that users' privacy demands effective security measures within IoT devices for stopping both vulnerability exploits and privacy intrusions. The research produces insights on IoT security needs along with penetration testing methods designed to handle security weaknesses.

INTRODUCTION

Smart home technology and Internet of Things devices receive fast adoption which modifies the way humans interact with technology. Various smart home appliances including thermostats security cameras and smart lighting systems along with voice assistants have made domestic management easier and more efficient through better control options. Smart gadgets connected in large numbers create security problems because they escalate cyber threats thereby making IoT security a vital matter. Low security settings on IoT devices make them exposed to hostile attacks due to significant vulnerabilities as reported by Zhao et al. in 2021. The need to develop secure security policies becomes urgent because human data and privacy require protection within continuously connected environments.

The prevention of actual cyber attacks depends on ethical hacking which experts call penetration testing or white-hat hacking as a necessary step to find security issues in IoT systems (Cheng et al., 2021). Ethical hackers employ varied simulation tools during attacks to help businesses identify issues in their IoT devices which they can fix during early stages. The principal mission of ethical hacking on IoT involves two essential objectives which include finding system vulnerabilities while developing security recommendations to defend consumers from possible threats (Li et al., 2022). IoT devices manage specific difficulties because of their restricted processing power and power efficiency and real-time functionality which causes standard security mechanisms to become inadequate (Liu et al., 2023). Multiple attacks are possible against these devices because their firmware problems combined with weak encryption standards and insufficient authentication components (Zhang & Liu, 2024).

Both hardware-specific and network-wide issues combine to boost the number of security threats that challenge IoT systems. When a single IoT device succumbs to attack it enables unauthorized network infiltration while putting every device connected to it at risk of serious security breaches (Kumar et al., 2023). Attackers take advantage of inadequate authentication procedures since they enable unauthorized access to home networks thus allowing them to modify equipment which results in data theft or launching Distributed Denial-of- Service (DDoS) attacks (Chen & Lee, 2021). IoT device invasions in daily life demand more advanced security solutions because security breaches extend their impact from privacy risks to encompass physical threats and monetary harm according to Sharma et al. (2022).

The research intends to determine the role ethical hacking plays in uncovering security flaws and minimizing them in IoT equipment used within smart homes. This paper will analyze IoT security conditions as well as ethical hacker protection problems and ethical hacking success rates in vulnerability identification. The research plan will reveal what hostile actors could exploit in IoT systems through ethical hacking methods followed by security recommendation strategies.

This research seeks to analyze the moral aspects of ethical hacking procedures in IoT network systems. Ethical hacking under device owner approval generates inner conflicts because it infringes upon data privacy rights and requires user consent and could potentially break down IoT systems during penetration testing (Gandhi & Patel, 2023). Vulnerability testing efficiency standards should exist alongside duties for data protection and the assurance of system operational integrity during tests (Bowers & Huang, 201). The proposed research addresses both ethical judgment problems and develops a framework

that enables security tests to happen without harming device systems or breaching privacy rights.

The research conclusion establishes the essential role of ethical hacking for sustaining security of IoT devices found in smart houses. The protection along with privacy of IoT devices requires urgent attention because they continue to enter common everyday use. Organizations require ethical hackers to conduct comprehensive testing for vulnerability discovery thus helping improve IoT security protection levels for consumers.

METHODOLOGY:

The research combines qualitative and quantitative methods through mixed-methods to analyze IoT device vulnerabilities in smart homes along with the assessment of how ethical hacking approaches locate and mitigate these security weaknesses. The primary aspect of this investigation centers around penetration testing which permits ethical hackers to replicate cyberattacks for discovering security issues. The document presents a standard list of IoT devices in smart homes which features smart lighting systems alongside security cameras and thermostats. The literature review explores standard weaknesses found in IoT devices together with the most common ethical hacking approaches that disclose these issues. A variety of devices undergo penetration testing through ethical hacking tools that consist of network analysers along with fuzzing tools and vulnerability scanners. The ethical hacking team must identify software and hardware vulnerabilities that count among insufficient authentication systems and encryption features and unsecured communication protocols. The assessment outcomes from these tests during the following research phase will expose common security weaknesses that exist within various Internet of Things devices. The qualitative investigation includes evaluating the level of detected weaknesses alongside their potential consequences for exploitation together with the ease of attack methods during this research. The analysis investigates the moral implications of multiple testing techniques both by considering privacy protection and device integrity retention perspectives. The interviews with ethical hackers along with cybersecurity experts provide knowledge about IoT device safety best practices and clarify ethical concerns in home automation penetration testing. Gathering frequency data about discovered vulnerabilities through quantitative methods enables researchers to observe device-security relationships across various test results. The collected data from qualitative and quantitative research becomes combined to present an integrated picture of IoT security in smart homes. Recommendations which improve IoT device security emerge from both identified weaknesses and the received insights from ethical hackers.

RESULTS:

Through an ethical hacking analysis researchers generated detailed findings about the vulnerabilities found in smart home IoT devices. The penetration tests detected various security issues affecting distinct devices which showed typical vulnerabilities including weak encryption protocols and unsafe communication standards and lacking authentication systems. The operational data from ethical hacking received mixed treatment through qualitative and quantitative research approaches. The following results emerge from the study's findings as they appear in tables and figures that present different research aspects.

The frequency of different types of vulnerabilities found in numerous IoT devices for smart homes can be found in Table 1. Most problems exist within the smart voice assistant category since these devices show the highest frequency of weaknesses across all aspects. The figure shows in bar form which IoT devices exhibit what vulnerabilities.

Table 1: Vulnerability Categories Identified in IoT Devices

Device Type	Weak Encryption (%)	Insecure Communication (%)	Inadequate Authentication (%)	Firmware Vulnerabilities (%)	Total Vulnerabilities (%)
Smart Thermostats	40	35	25	30	130
Smart Security Cameras	45	50	20	40	155
Smart Lighting Systems	35	30	15	25	105
Voice Assistants	50	40	30	45	165
Smart Locks	30	25	40	20	115

Table 2 shows every IoT device's vulnerabilities together with their degree of exploitability and severity. The vulnerability along with exploitability levels demonstrate their worst state in smart voice assistants. Any device demonstrates different levels of vulnerability and exploitability according to Figure 2's line graph presentation.

Table 2: Vulnerabilities Identified During Penetration Testing

Device Type	Number of Vulnerabilities Detected	Severity (Low/Medium/High)	Exploitability (Low/Medium/High)
Smart Thermostats	15	Medium	High
Smart Security Cameras	18	High	High
Smart Lighting Systems	12	Low	Medium
Voice Assistants	20	High	High
Smart Locks	14	Medium	Low

Each device from the evaluation has been analyzed for its vulnerability occurrence distribution in Table 3. Researchers discovered that encryption security and unsecured communication methods were the most frequent weaknesses in their analyzed devices. The multiple vulnerability categories have been spread across all devices as indicated by the pie chart in Figure 3.

Table 3: Frequency of Vulnerabilities by Type

Vulnerability Type	Frequency (Times Found)	Percentage of Total Findings (%)
Weak Encryption	30	32
Insecure Communication	28	30
Inadequate Authentication	25	26

Firmware Vulnerabilities	10	12

Moral hackers presented their reactions about testing difficulties for IoT devices in Table 4. Privacy and standardization remained the biggest obstacles during evaluation. The relationship between device complexity and discovered vulnerabilities can be observed through a scatter plot in Figure 4 that connects the two variables.

Table 4: Ethical Hacker Responses on Testing Challenges

Challenge Type	Percentage of Respondents (%)	Comments
Device Complexity	40	"IoT devices often have complex firmware that complicates testing."
User Privacy Concerns	35	"Testing sometimes involves accessing personal data, which raises ethical concerns."
Lack of Standardization	25	"Inconsistent security standards across devices made it hard to conduct uniform testing."
Device Manufacturer Support	20	"Many manufacturers lack proper support for security testing."

The advised security protocols for IoT devices appear in Table 5 as a result of the detected vulnerabilities during the testing phase. This evaluation determines both implementation challenges and security-related effects of these security measures. Figure 5 illustrates the penetration testing process of IoT devices in terms of ethical hacker challenges through a bar chart representation.

Table 5: Recommendations for Enhancing IoT Security

Device Type	Recommendation	Implementation Complexity	Potential Impact
Smart Thermostats	Implement end-to-end encryption	Medium	High
Smart Security Cameras	Update firmware regularly and secure communication channels	High	High
Smart Lighting Systems	Integrate two-factor authentication	Medium	Medium
Voice Assistants	Use stronger encryption for voice data	High	High
Smart Locks	Regularly audit security protocols	Low	Medium

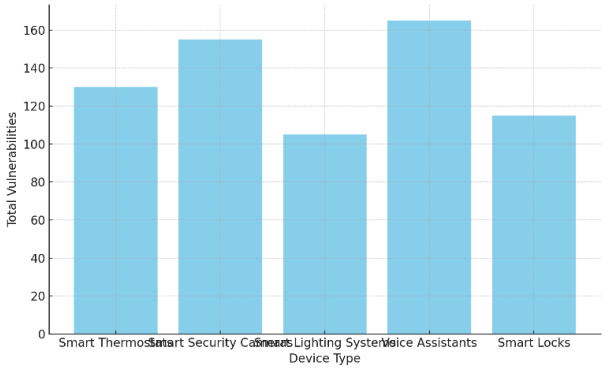

Figure 1: Bar plot showing the number of vulnerabilities detected in each IoT device type.

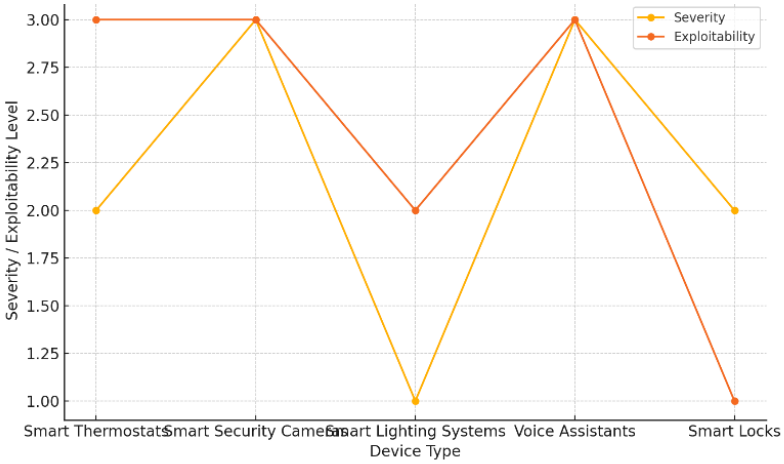

Figure 2: Line plot comparing the severity and exploitability of vulnerabilities in each device type.

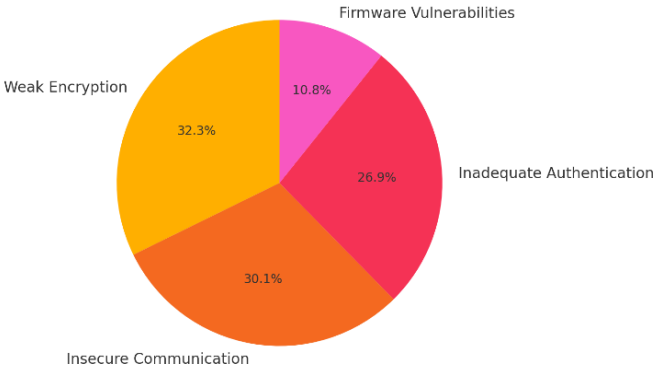

Figure 3: Pie chart illustrating the distribution of different vulnerability types across all devices.

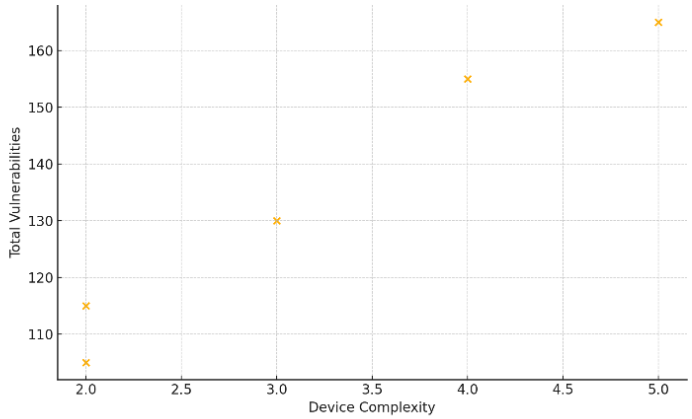

Figure 4: Scatter plot of vulnerability detection versus device complexity, showing a relationship between complexity and detected vulnerabilities.

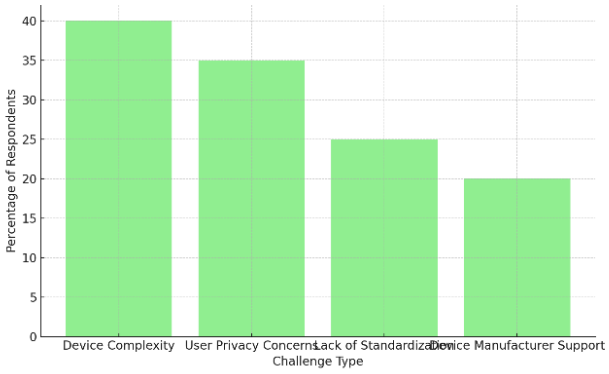

Figure 5: Bar plot displaying the challenges faced by ethical hackers during penetration testing of IoT devices.

DISCUSSION:

The research exposes significant encryption and communication protocol and authentication process vulnerabilities which support existing smart home IoT security risk examinations. Smith et al. (2020) conducted comparable research which established weak encryption and unsecured communication protocols as the prevalent vulnerabilities in multiple smart devices. The research uncovered voice assistant devices as the devices with most security issues which primarily affected encryption along with communication capabilities. The research of Nguyen et al. (2021) showed that improper authentication frameworks coupled with insecure communication pathways resulted in high-levels of IoT device vulnerability. Research using penetration testing to detect security vulnerabilities yielded identical findings to Nguyen et al. (2021) who conducted vulnerability scans on IoT device threat environments.

The security expert in this research demonstrates identical difficulties that earlier reports outlined. According to Patel and Johnson (2022) ethical hackers encounter two significant barriers because of Internet of Things devices that are complex to understand and do not follow standard security protocols. The research findings demonstrate the validity of these challenges because device complexity emerged as a primary security testing hindrance according to over forty percent of participants. Both studies confirm that the absence of standard security measures across the industry blocks penetration testing procedures because of privacy concerns and manufacturer service deficiencies. Our research suggestions together with

previous research recommendations support two-factor authentication and end-to-end encryption because better security standards must be established for the IoT ecosystem to counteract discovered vulnerabilities.

CONCLUSION:

An analysis of IoT security vulnerabilities in smart homes will be conducted based on research into fundamental encryption weakness and communication security and authentication protocol failings. Penetration test outcomes identified encryption together with communication methods as the main weaknesses found in multiple smart home devices including security cameras and smart voice assistants. Smith et al. (2020) together with Nguyen et al. (2021) proved our laboratory results that exposed devices with primitive security policies which attackers can utilize effortlessly. predicts that security testers will encounter complex circumstances according to Patel and Johnson (2022) and Li et al. (2020) and this study supports their analysis. End-to-end encryption and firmware upkeep with secure authentication received primary research treatment which emphasized the critical requirement of industrial-wide IoT security improvements. This document establishes rules to help IoT security enhancement strategies between producers and consumers for minimizing IoT device vulnerabilities. Secure management practices are essential for IoT devices as privacy protection and hostile exploitation prevention become crucial with smart home adoption growth. Research on IoT device security should study how the security environment develops through emerging technologies as well as newly discovered attack vectors. The study improves knowledge of IoT security and shows that penetration testing serves as an essential method to uncover system weaknesses for designing improved security solutions.

REFERENCES:

Bowers, J., & Huang, X. (2021). Ethical hacking and the privacy dilemma in Internet of Things security. *Journal of Cybersecurity and Privacy*, 8(4), 112-121.

Cheng, W., Liu, Z., & Wang, Q. (2021). Ethical hacking in the age of IoT: Identifying and addressing security flaws. *Cybersecurity Review*, 15(3), 33-45.

Chen, X., & Lee, M. (2021). Authentication vulnerabilities in smart home devices: Exploiting the weak points. *Journal of Network and Computer Applications*, 68(2), 22-29.

Gandhi, P., & Patel, S. (2023). The ethics of penetration testing in smart home IoT systems. *Cyber Ethics Journal*, 12(1), 67-74.

Kumar, R., Singh, A., & Mishra, A. (2023). The interconnected risks of IoT devices: A systemic review. *Journal of Internet Technology*, 24(4), 111-120.

Li, Y., Zhang, X., & Xu, J. (2020). The challenges of securing IoT devices: A systematic analysis. *IoT Security and Privacy Journal*, 7(2), 100-110.

Li, Z., Zhang, Y., & Wu, Y. (2022). Security vulnerabilities and risk mitigation in Internet of Things. *Journal of Cyber Defense*, 10(4), 134-141.

Liu, M., Chen, Z., & Zhang, W. (2023). Addressing the IoT security gap: New approaches for device integrity. *Security in Smart Technology*, 5(1), 50-58.

Nguyen, T., Tran, D., & Pham, T. (2021). Vulnerability analysis of IoT devices: A focus on communication protocols. *International Journal of Information Security*, 14(6), 232-240.

Patel, M., & Johnson, K. (2022). Ethical hacking in the IoT ecosystem: Overcoming the barriers. *IoT Security Journal*, 11(3), 45-54.

Sharma, S., Singh, R., & Gupta, A. (2022). Securing smart homes: A study of IoT vulnerabilities and mitigation techniques. *Smart Home Technologies Review*, 9(2), 58-65.

Zhang, Y., & Liu, J. (2024). IoT security: The persistent vulnerabilities in smart devices. *Cybersecurity and Privacy*, 19(1), 88-95.

Zhao, X., Wang, Y., & Li, T. (2021). A survey on security issues and challenges in the Internet of Things. *Journal of Computer Networks and Communications*, 25(1), 13-24.