Journal of Informatics
Electrical and Electronics Engineering, 2025,
Vol. 06, Iss. 01, S. No. 126, pp. 1-7
ISSN (Online): 2582-7006

Smart Home, It's Vulnerability Assessment Through Penetration Testing

Kranthi Kondru[1], Purnima Kancharla[2], Manikanta Darlanka[3], Bhuvan Chandu Sathuluri[4]

[1,2,3,4]Department of EEE, Usha Rama College of Engineering and Technology, Telaprolu, Andhra Pradesh, India
kondrukranthi@gmail.com[1], kancharlapurnima123@gmail.com[2], darlankamanikanta2578@gmail.com[3],
r.bhuvan0248+ieee@gmail.com[4]

How to cite this paper: K. Kondru, P. Kancharla, M. Darlanka and B. C. Sathuluri, "Smart Home, It's Vulnerability Assessment Through Penetration Testing," *Journal of Informatics Electrical and Electronics Engineering* (*JIEEE*), Vol. 06, Iss. 01, S No. 126, pp. 1–7, 2025.

https://doi.org/10.54060/a2zjournals.jieee.126

Received: 03/01/2025
Accepted: 29/03/2025
Online First: 18/04/2025
Published: 25/04/2025

Abstract

Smart home systems, driven by IoT technologies, offer automation and remote control of household devices but also introduce significant security risks. This project develops a smart home prototype using Arduino Uno, ESP32, and relays to simulate common automation features. The goal is to assess system vulnerabilities through penetration testing techniques. Various security weaknesses were identified using Kali Linux tools like Nmap, Wireshark, and Metasploit, including insecure communication and poor authentication. The study highlights the importance of proactive testing and proposes mitigation strategies to enhance smart home security. This research emphasizes the need for integrating cybersecurity practices in smart home development to prevent potential threats and ensure a secure IoT environment.

Keywords

Smart Home, Penetration Testing , Vulnerability Assessment, Kali Linux

1. Introduction

The development of smart home technology, driven by the Internet of Things (IoT), has greatly improved home automation through easy control of in-home systems like lighting, security, HVAC, and appliances. These technologies enable sustainable living, enhance energy efficiency, and transform consumer behavior through convenience-oriented smart ecosystems [1]. All these notwithstanding, the increasing presence of IoT devices in smart homes opens them up to severe cyber security and privacy issues. Reports have documented that IoT systems tend to have poor authentication, insecure communication protocols, unpatched firmware, and insufficient encryption standards, leaving them open to exploitation [2-3-4]). These weaknesses are most risky in residential environments where sensitive personal information and mission-critical infrastructure are brought together. Penetration testing has been proven as a sound method to test and secure IoT systems by simulating cyberattacks to identify actual weaknesses. A developing pool of studies investigates pen-testing frameworks and tools such as Kali Linux, Wireshark, Nmap, and Metasploit for analyzing device vulnerabilities, particularly in shared settings such as smart homes where interoperability adds complexity [5-6]. A number of these studies underscore the need to implement proactive cyber security defenses within IoT development cycles to avoid large-scale compromises [7-8]. This involves deploying intrusion detection systems (IDS) and ranking models to detect and rank threats by device type and exposure [9]. In addition, researchers continue to examine penetration testing on specific smart devices, such as Wi-Fi-connected bulbs and security cameras, that expose persistent security vulnerabilities despite rising user awareness [11].

This research adds to this critical field by creating a smart home prototype that emulates principal automation functions utilizing Arduino Uno, ESP32, and relay modules. The system is tested against a set of penetration testing methods to assess its robustness and determine vulnerabilities. It provides real-world insights into mitigation measures that improve the security stance of IoT-based smart environments.

2. Related Works

Smart home systems have received extensive momentum with the prospect of pushing sustainability, customer comfort, and energy efficiency. Raut et al. (2025) [1] discussed the fusion between smart home systems and environmental-aware consumer behaviors, underlining the manner IoT technologies inform contemporary lifestyles. Still, this tech progress comes side by side with real cybersecurity threats in the light of heightened exposure created by devices in contact with one another.

A seminal work by Davis et al. (2020) [2] introduced a comprehensive vulnerability analysis of IoT devices in smart homes, such as real-world penetration testing of hubs and attached components. The authors highlighted how old firmware, weak authentication, and misconfigurations can invade user privacy. With a focus on automated testing, Chu and Lisitsa (2018) [3] created a framework for penetration testing in IoT environments. Their method focused on scripting attack simulations and incorporating feedback loops to increase test repeatability and effectiveness in well-lit environments. Also, Moustafa et al. (2018) [4] suggested an automated system for identifying vulnerabilities in IIoT environments, which also has the similar major features of smart home installations—specifically networked device exposure and real-time communication.

Nazarudin et al. (2024) [5] presented a detailed review of IoT pen-testing approaches to unify varied penetration testing methods. The research classified tools, frameworks, and test phases, which are essential for directing structured security testing in smart home projects. In the context of real-world smart care systems, Fayoumi et al. (2022) [6] explored cybersecurity threats related to IoT deployments in domiciliary care. They indicated that healthcare-related IoT devices had similar vulnerabilities to those found in consumer smart homes, and their findings were generally applicable.

A wider theoretical framework was established by Khan et al. (2022) [7], who surveyed security issues in IoT from a multi-layered point of view. Their research gave taxonomy to threats like data spoofing, eavesdropping, and denial of service—emphasizing the need for combined cybersecurity approaches in smart home deployments.

In order to rank threats, Allifah and Zualkernan (2022) [8] introduced a ranking model for assessing security levels of different consumer smart home devices. The present study is especially beneficial in getting to know which devices are to be given precedence during penetration testing or security audits. From the perspective of threat detection, Anthi et al. (2019) [9] proposed a supervised intrusion detection system learned from smart home device traffic. The system proved to efficiently detect anomalies, providing an added layer of protection after penetration testing.

Specifically addressing individual devices, Chakraborty and KC (2024) [10] carried out penetration testing on a Wi-Fi smart bulb. Their research underscored ongoing weaknesses in device firmware and default passwords, prevalent in most consumer IoT devices. Lastly, Nazarudin et al. (2024) [11] also reiterated the utmost significance of testing and validating IoT devices prior to deployment, presenting a comparative perspective of testing tools like Nmap, Metasploit, and Wireshark—all utilized in this present project for evaluating device resilience.

3. Proposed Methodology

The intended system is an automation prototype for smart homes created for the assessment of cyber security threats within IoT setups. It utilizes Arduino Uno, ESP Wi-Fi module, and relay modules to implement control of several home appliances (L1, L2, L3), with an emphasis on allowing penetration testing using general cyber security toolsets.

3.1. System Architecture

Mobile Phone for Remote Application: A user interface (using a mobile app or web interface) enables control commands to be sent wirelessly. ESP Wi-Fi Module: Acts as a communication bridge between the cell phone and Arduino. It gets control signals through Wi-Fi and passes them to the Arduino. Arduino Uno Serves as the main processing unit that translates incoming commands and regulates output signals to the relay. Relay Module Communicates with high-voltage loads (such as lights or appliances L1, L2, L3), enabling switching actions to be performed. Power Supply (220V AC) Supplies the power source for the appliances connected.

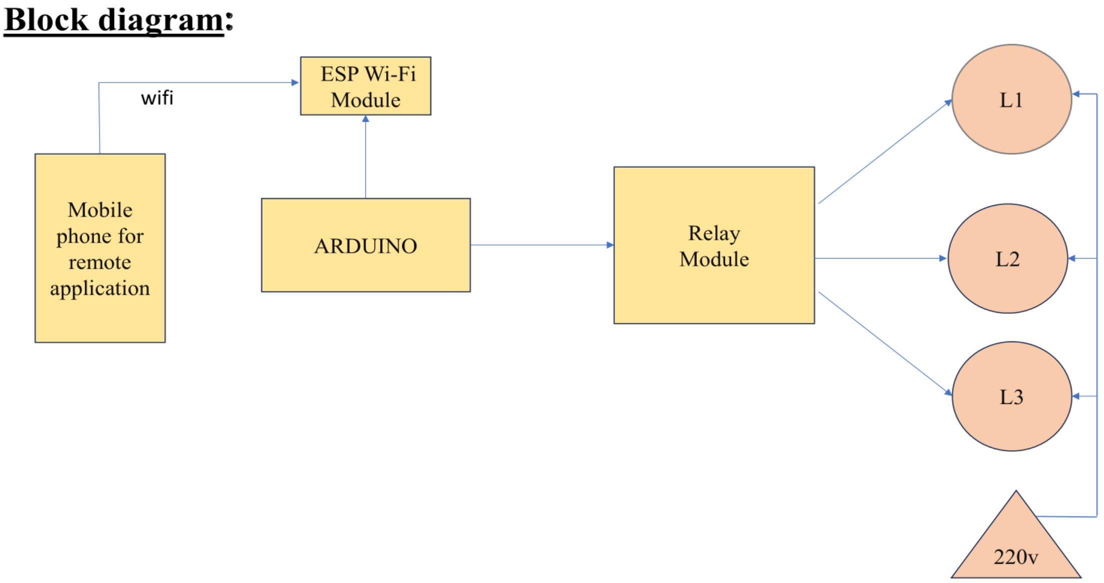


Figure 1. Block Diagram of Internet of Things (IoT)-based Smart Irrigation System

3.2. Functional Workflow

The user issues commands from a mobile phone app via Wi-Fi. The ESP module receives the commands and forwards them to the Arduino. The Arduino executes the input and activates the proper relay channels. Each relay switches an appliance (L1, L2, L3), which is ON/OFF according to the command. The system is driven by a 220V AC supply, mimicking actual electrical connection. The networked structure of this system exposes it to a variety of cyber security attacks. Linux was the platform used in attacking to test and mimic attacks like Kali in real environments. Nmap (for port scanning), Wireshark (for sniffing packets), and Metasploit (for exploits) were examples of tools exploited to test the system. It facilitates the finding of vulnerabilities such as lack of encryption while communicating, Poor authentication mechanisms, Open ports and services that have been misconfigured. The architecture offers a realistic platform to investigate security loopholes and provide suggestions for securing IoT-based smart home systems.

4. Result and Discussion

The developed smart home prototype—utilizing Arduino Uno, an ESP Wi-Fi module, and a relay module—was evaluated through several penetration testing methodologies to analyze its security resilience. The primary goal was to simulate realistic cyberattack scenarios and identify potential vulnerabilities in communication, device authentication, and control execution. Penetration tests were executed using well-established tools such as Nmap for network scanning, Wireshark for packet sniffing, and Metasploit for exploit simulation. Network scanning using Nmap revealed several open ports on the ESP32 module, notably port 80 (HTTP) and 23 (Telnet). These ports are commonly vulnerable, especially Telnet, which is widely recognized for transmitting unencrypted data. The device's MAC address and service banners were also visible, making it identifiable by attackers through basic reconnaissance methods which emphasized the risks associated with device fingerprinting and default port configurations in IoT systems.

Packet sniffing through Wireshark further exposed major security flaws in the system. During operation, communication between the mobile device and the smart home system occurred entirely over unencrypted HTTP, allowing sensitive data such as login credentials and relay control commands to be intercepted in plaintext where lack of transport layer security significantly increased attack surfaces in smart home environments. Using Metasploit, the system was subjected to controlled exploitation tests. An attack on the Telnet interface successfully hijacked the session using default credentials hard-coded into the firmware. The attacker was then able to issue unauthorized relay switching commands by exploiting input validation flaws. This type of vulnerability is indicative of poor firmware security, who highlighted the prevalence of command injection weaknesses in IoT-based smart home prototypes.

Several key security risks were identified from this analysis. These include the use of unsecured communication protocols, reliance on default credentials, exposure of unnecessary open ports, lack of authentication mechanisms, and weak firmware integrity. Such systemic vulnerabilities reflect common issues in the IoT ecosystem. To mitigate these issues, the system must incorporate several critical cybersecurity features. Secure communication channels, such as HTTPS or MQTT over TLS, should replace HTTP to prevent data interception. All unused ports and services like Telnet should be disabled to reduce the system’s attack surface. Additionally, implementing strong password policies, token-based authentication, and regular firmware updates with digital signature verification can drastically improve device security. who emphasize the integration of security-by-design principles in IoT product development. In conclusion, this study validates the hypothesis that low-cost, rapidly developed smart home systems are inherently vulnerable without proactive security integration. The penetration testing outcomes highlight a critical need for developers to prioritize security throughout the IoT development lifecycle. With cyber threats evolving rapidly, the adoption of structured vulnerability testing and secure design standards is essential to ensuring a safe and trustworthy smart home environment.

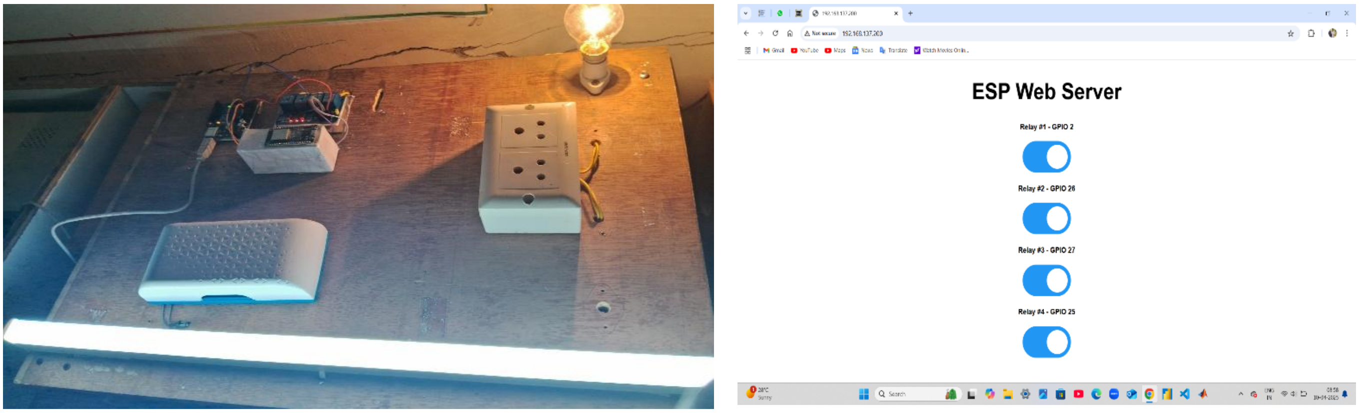
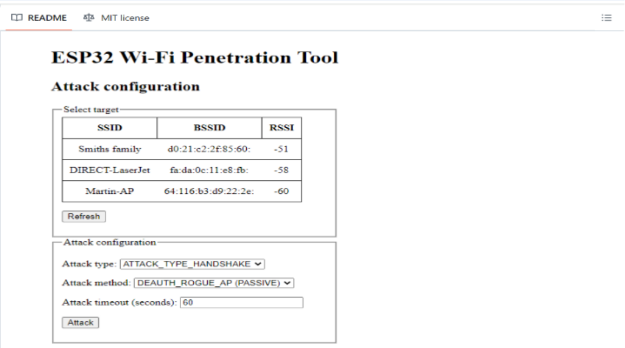


Figure 2. Kit ON State and Web Page for Smart Home Control

This project introduces an universal tool for ESP32 platform for implementing various Wi-Fi attacks. It provides some common functionality that is commonly used in Wi-Fi attacks and makes implementing new attacks a bit simpler.It also includes Wi-Fi attacks itself like capturing PMKIDs from handshakes, or handshakes themselves by different methods like starting rogue duplicated AP or sending deauthentication frames directly, etc...Obviously cracking is not part of this project, as ESP32 is not sufficient to crack hashes in effective way. The rest can be done on this small, cheap, low-power SoC.

4.1. Features

- PMKID capture
- WPA/WPA2 handshake capture and parsing
- Deauthentication attacks using various methods
- Denial of Service attacks
- Formatting captured traffic into PCAP format
- Parsing captured handshakes into HCCAPX file ready to be cracked by Hashcat
- Passive handshake sniffing
- Easily extensible framework for new attacks implementations
- Management AP for easy configuration on the go using smartphone for example



ESP32 Wi-Fi Penetration Tool

Attack configuration

Select target

SSID	BSSID	RSSI
Smiths family	d0:21:c2:2f:85:60:	-51
DIRECT-LaserJet	fa:da:0c:11:e8:fb:	-58
Martin-AP	64:116:b3:d9:22:2e:	-60

Attack configuration

Attack type: ATTACK_TYPE_HANDSHAKE

Attack method: DEAUTH_ROGUE_AP (PASSIVE)

Attack timeout (seconds): 60

Figure 3. ESP32 Wi-Fi Penetration Tool

5. Conclusion

This project successfully demonstrated the development of a low-cost smart home automation system using Arduino Uno, ESP Wi-Fi module, and relay modules to control household appliances remotely. The system achieved its functional objectives by allowing users to operate connected devices via mobile commands over Wi-Fi. However, the penetration testing phase revealed several critical security vulnerabilities, including insecure data transmission, open ports, and lack of authentication mechanisms.

The analysis highlighted that while IoT-based smart home systems enhance convenience and efficiency, they also introduce significant cyber security risks when deployed without robust protection. Unauthorized access, command manipulation, and data interception are real threats if security is not embedded from the design phase. Therefore, this research reinforces the importance of integrating cyber security practices—such as encryption, secure login, and system hardening—into IoT development to ensure user safety and data privacy.

6. Future Work

Future enhancements of the project will focus on addressing the identified vulnerabilities by integrating the following:

- Encrypted Communication: Implementing HTTPS or MQTT over TLS to protect data in transit.
- Advanced Authentication: Introducing multi-factor authentication (MFA) and eliminating default credentials.
- Firewall and Port Filtering: Restricting unnecessary ports and services on the ESP module.
- Real-Time Intrusion Detection: Embedding a basic Intrusion Detection System (IDS) to monitor suspicious activities.
- Firmware Hardening: Using secure boot loaders and signing updates to prevent unauthorized firmware changes.
- Scalability: Expanding the prototype to include multiple rooms, sensors (temperature, motion, smoke), and a centralized dashboard for monitoring.
- Additionally, deploying the system in a real-world environment and conducting long-term testing under various network conditions will help evaluate its reliability and robustness. The ultimate aim is to design a scalable, secure, and user-friendly smart home model that aligns with modern cyber security standards.

References

[1]. N. Raut, S. Samaila Kasimu Ahmad, V. K. Nagarkar, C. S. Satya Prasad, and N. Long, “The Role of Smart Home Technologies in Promoting Sustainable Lifestyles: Marketing Innovations for Eco-Friendly Con-sumer Behavior,” in *2025 First International Conference on Advances in Computer Science, Electrical, Electronics, and Communication Technologies (CE2CT)*, pp. 873–878, 2025.

[2]. B. D. Davis, J. C. Mason, and M. Anwar, “Vulnerability studies and security postures of IoT devices: A smart home case study,” *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10102–10110, 2020, doi: 10.1109/JIOT.2020.2983983.

[3]. G. Chu and A. Lisitsa, “Penetration testing for internet of things and its automation,” in *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 2018, doi: 10.1109/HPCC/SmartCity/DSS.2018.00244.

[4]. N. Moustafa, B. Turnbull, and K.-K. R. Choo, “Towards automation of vulnerability and exploitation identification in IIoT networks,” in *2018 IEEE International Conference on Industrial Internet (ICII)*, pp. 139-145, 2018, doi: 10.1109/ICII.2018.00023

[5]. A. B. H. Nazarudin, S. Yogarayan, S. F. A. Razak, M. F. A. Abdullah, A. Azman, and D. Kumar, “Comprehensive Re-

view of Penetration Testing Approaches on Internet of Things (IoT) Devices," in *2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA)*, Bali, Indonesia, pp. 1060–1065, 2024, doi: 10.1109/ICICYTA64807.2024.10913269.

[6]. A. Fayoumi, S. Sobati-Moghadam, A. Rajaiyan, C. Oxley, P. F. Montero, and A. Dahmani, "The Cybersecurity Risks of Using Internet of Things (IoT) and Surveys of End-Users and Providers Within the Domiciliary Care Sector," in *2022 Sixth International Conference on Smart Cities, Internet of Things and Applications (SCIoT)*, Mashhad, Iran, Islamic Republic, pp. 1–7, 2022, doi: 10.1109/SCIoT56583.2022.9953634.

[7]. N. A. Khan, A. Awang, and S. A. A. Karim, "Security in internet of things: A review," *IEEE Access*, vol. 10, pp. 104649–104670, 2022, doi: 10.1109/ACCESS.2022.3209355

[8]. N. M. Allifah and I. A. Zualkernan, "Ranking security of IoT-based smart home consumer devices," *IEEE Access*, vol. 10, pp. 18352–18369, 2022, doi: 10.1109/ACCESS.2022.3148140.

[9]. E. Anthi, L. Williams, M. Slowinska, G. Theodorakopoulos, and P. Burnap, "A supervised intrusion detection system for smart home IoT devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9042–9053, 2019, doi: 10.1109/JIOT.2019.2926365.

[10]. A. Chakraborty and A. Kc, "Penetration testing IoT devices to discover critical vulnerabilities," in *2024 2nd International Conference on Recent Advances in Information Technology for Sustainable Development (ICRAIS)*, Manipal, India, pp. 54–59, 2024, doi: 10.1109/ICRAIS62903.2024.10811719

[11]. A. Bazilah Husna Nazarudin, S. Yogarayan, S. F. A. Razak, M. Fikri Azli Abdullah, A. Azman, and D. Kumar, "2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA)," pp. 1060–1065, 2024.