A Raise of Security Concern in IoT Devices: Measuring IoT Security Through Penetration Testing Framework

Abdul Ghafar Jaafar[1], Saiful Adli Ismail[2], Abdul Habir[3], Khairul Akram Zainol Ariffin[4], Othman Mohd Yusop[5]
Faculty of Artificial Intelligence, Universiti Teknologi Malaysia (UTM), 54100, Kuala Lumpur, Malaysia[1, 2, 3, 5]
Center for Cyber Security-Faculty of Technology & Information Science, Universiti Kebangsaan, Malaysia[4]

Abstract—Despite the widespread adoption of IoT devices across different industries to enhance human activities, there is a pressing need to address the vulnerabilities associated with these devices, as they can potentially give rise to a plethora of cyber threats. Cyberattacks targeting IoT devices are predominantly attributed to inadequate patching and security updates. Furthermore, the current atmosphere pertaining to IoT penetration tests primarily focuses on specific devices and sectors while leaving certain fields behind, such as household devices. This study delves into recent penetration testing on IoT devices. Further, it discusses and critically analyzes the significance and issues in conducting IoT penetration tests. The findings of this study reveal a substantial demand for automated IoT penetration testing to serve diverse industries because conducting such testing has the capacity to diminish the consequences of cyber-attacks across numerous industries that utilize IoT devices for various purposes. This study is intended to be a ready reference for the research community to construct effective and innovative solutions in IoT penetration testing, which covers various fields.

Keywords—IoT Security; IoT penetration testing; security assessment; automated penetration testing; penetration testing framework

I. Introduction

The Internet of Things (IoT) has emerged as a transformative paradigm, connecting billions of devices to facilitate seamless communication and automation across different domains. However, the widespread adoption of IoT technologies has also introduced significant security challenges. As a result, rigorous research efforts are being undertaken to protect IoT ecosystems from malicious threats. Approximately 50 billion IoT devices are anticipated by 2030 [1]. This expansion results from changes implemented by the government and various industries, including transportation, education, and finance [2]. Nevertheless, inconsistent monitoring of the security level of these devices has rendered them vulnerable and exploitable. The rapid growth of unprotected IoT devices connected to the global network [3] has led to malware attacks, security breaches, and personal data [4]. Insufficient user understanding regarding the security of IoT devices is also a contributing factor to these attacks. In this vein, malicious actors can exploit IoT devices and expose them to malicious attacks [5], such as command injection, distributed denial of service (DDoS) attacks, eavesdropping, and man-in-the-middle attacks (MITM) [6]. Consequently, organizations suffer from financial loss, reputational damage, and loss of trust due to online system disruptions following these attacks.

From the perspective of technology providers, such as Fortinet [7], cybercriminals utilize IoT Botnets to conduct DDoS attacks to target multiple devices simultaneously. According to [8], cyber intruders primarily target smart home appliances in the form of a Botnet to attack critical digital infrastructures that have inadequate security measures. Akhilesh, Bills [8] also highlighted that IoT devices represent primary targets for various malware. For example, the Mirai Botnet instigated a massive DDOS attack in 2016, the largest one documented up to that point [8, 9]. The attack exploited over 300,000 infected IoT devices, disrupting several significant websites and digital services, including GitHub, PayPal, Amazon, the BBC, PlayStation Network, and Spotify [8]. There have been a number of studies [8, 10, 11] stating that the Botnet malware source code was released on Hack Forums and GitHub post-attack, where anyone could create a copy of Mirai or incorporate its components into their malicious software.

The presence of IoT devices, particularly household appliances, leads to complexity in handling cyber-attacks. The effectiveness of cyber-attacks against IoT devices is significantly remarkable compared to attacks on databases and web applications. The leading cause of this issue is the increasing number of vulnerabilities in these devices, coupled with customers' inadequate understanding of the significance of updating their devices with patches. Thus, conducting penetration testing represents a viable solution to address this issue.

Household appliances, for example, lead to complexity in handling cyber-attacks. The effectiveness of cyber-attacks against IoT devices is significantly remarkable compared to attacks on databases and web applications. The leading cause of this issue is the increasing number of vulnerabilities in these devices, coupled with customers' inadequate understanding of the significance of updating their devices with patches. These vulnerabilities are often exacerbated by the limited computational resources and simplistic designs of many IoT devices, which make implementing robust security measures challenging. Due to this, penetration testing is greatly emphasized to proactively identify and mitigate security flaws before malicious actors can exploit them. Penetration testing involves simulating cyber-attacks on systems to evaluate their security and uncover vulnerabilities. Conversely, the current state of the penetration testing industry has shortcomings in addressing specific fields such as IoT devices, which are classified as smart homes, agriculture, transportation, and healthcare. These sectors are characterized by unique security challenges, including diverse device ecosystems, varied communication protocols, and the critical nature of their operations.

Security is one of the crucial aspects when it comes to IoT devices design and development since once the devices have been compromised by cyber-attack all sensors will be affected [12]. Hence, necessitate a specialized approach to penetration testing. Traditional penetration testing methods, well-suited for conventional IT infrastructure, may not fully address the nuanced vulnerabilities inherent in IoT ecosystems. For instance, smart home devices like thermostats and security cameras often operate in interconnected networks, where a single compromised device can jeopardize the entire system. Aside from that, IoT devices monitor environmental conditions in agriculture and automate farming processes, making their security crucial for food safety and production efficiency. On the other hand, transportation systems increasingly rely on IoT for vehicle-to-vehicle communication and traffic management, where security breaches can have severe implications for public safety. Healthcare is another critical domain where IoT devices, such as remote monitoring systems and smart medical equipment, play a pivotal role. The security of these devices is vital, as any compromise can directly impact patient health and safety. The complexity and sensitivity of healthcare IoT devices necessitate rigorous and continuous security testing to ensure their reliability and integrity.

To effectively address these challenges, the penetration testing industry must evolve to incorporate automated testing solutions tailored to the specific needs of IoT environments. Automated penetration testing can provide consistent and comprehensive assessments, enabling end users and organizations to monitor and fortify their IoT devices continuously against emerging threats. Automated penetration testing can become more efficient, reducing the time and resources required to identify vulnerabilities and implement necessary security measures. One significant advantage of automated penetration testing is its ability to continuously perform security assessments without expert intervention, which helps in the initial detection of vulnerabilities, allowing end users and organizations to take proactive measures in handling security issues before they can be exploited. Automated tools can be programmed to run regular scans and tests, ensuring that newly discovered vulnerabilities are promptly identified and mitigated. This approach is vital in the dynamic landscape of IoT as it is used by various sectors where cyber threats are continuously evolving.

The review of IoT security has been carried out by a number of academics, including Kaur, Dadkhah [13], who reviewed the complexities underpinning security dataset evolution and future directions in IoT, emphasizing IoT datasets, machine learning algorithms, and architecture. Meanwhile, Mocrii, Chen [14] reviewed IoT-based intelligent home devices that only entail IoT system architecture, software, communications, data privacy, and security. Although Yaacoub, Noura [15] reviewed IoT device exploitation vulnerabilities, the study only emphasized specific devices: drones, smart devices, and hardware (including smartphones and tablet vulnerabilities). Radoglou Grammatikis, Sarigiannidis [16] comprehensively analyzed IoT challenges, threats, and solutions but only focused on possible threats and the associated countermeasures.

Malhotra, Singh [17] reviewed the IoT evolution, associated issues, and security challenges similarly. The authors provided a healthcare case study on IoT architecture, security, and privacy issues. Furthermore, Abed and Anupam [18] performed a similar review of security challenges in an IoT network with past works by Radoglou Grammatikis, Sarigiannidis [16], [17]. Regardless, this study emphasized current attacks on IoT technology, communication protocols prevalent in IoT systems, and the role of artificial intelligence (AI) in IoT security. Azrour, Mabrouki [19] similarly reviewed critical IoT issues, emphasizing authentication. Meanwhile, Zhu, Yang [20] review of IoT device testing developments prioritized real-time testing and self-healing, big-data analysis in IoT testing, and the development of IoT test tools for further research.

Despite the wealth of recent review papers pertaining to IoT security, there is a lack of IoT security review from the perspective of penetration testing. Recent penetration testing methodologies need to be critically analyzed, and the challenges related to their extension to IoT devices should be discussed. Hence, this study aims to review recent penetration testing conducted on IoT devices. Additionally, it discusses and critically analyzes the importance and challenges associated with performing penetration tests on IoT devices and the contribution of this study as follows:

1) Reveals the significant gap in IoT penetration testing methodologies and emphasizes the need for automated penetration testing that can cater to end-user and expert users to accommodate IoT environments' unique characteristics and vulnerabilities.

2) Systematically identifies and categorizes common vulnerabilities in IoT devices and outlines specific attack vectors associated with IoT attacks.

3) Evaluate existing IoT penetration testing methodologies and discuss their effectiveness and limitations.

The remainder of the paper is structured as follows. Section II delves into the implementation of the IoT across different sectors, while Section III reviews the IoT infrastructure. The security challenges associated with IoT are explored in Section IV, and the importance of penetration testing is elucidated in Section V. Section VI explains security testing, followed by an elaboration on the penetration testing framework in Section VII. Section VIII encompasses a discussion and analysis of the findings, leading to the ultimate conclusion presented in Section IX.

II. Implementation Across Various Sectors

The IoT technology connects devices and sensors to the Internet, offering numerous benefits across various sectors due to their real-time ability to collect, transmit, and analyze data. Industries that can gain advantages from IoT are various but are not restricted to homes, farming, transportation, and healthcare.

This section delves into the main sectors that highly utilize IoT devices, which can increase efficiency and productivity to enhance safety and quality of life.

A. Smart Home

IoT devices, including smart TVs, speakers, and streaming devices, are seamlessly integrated into a connected home entertainment system. This integration facilitates the streaming of content and control over playback and allows for the customization of various settings. Such functionalities can be accessed conveniently through voice commands or dedicated smartphone applications, enhancing the overall entertainment experience for individuals. IoT devices in homes allow creators of IoT technology to collect information and monitor electricity usage. This enables them to analyze power consumption and develop IoT devices that are more efficient in terms of energy usage. The implementation of this method is also noted by Hassija, Chamola [21], who mentioned that IoT monitoring systems are implemented to track energy and water consumption, and users are being advised to conserve costs and resources.

B. Smart Agriculture

IoT devices, such as drones, satellites, and ground-based sensors, have facilitated the remote monitoring of agricultural fields for farmers. These devices offer a range of valuable data, including high-resolution imagery, thermal mapping, and information on crop growth, water stress, and pest infestations. Through remote monitoring, farmers can promptly identify issues, take timely measures, and make informed decisions based on the data to optimize productivity. A survey by Hassija, Chamola [21] outlines that IoT devices in agriculture can help increase crop yields and reduce financial losses by allowing farmers to monitor and control temperature and humidity levels in grain and vegetable production, thus reducing the risk of fungal and microbial contamination. Khan, Su'ud [22] highlighted the transformation from conventional farming to smart pharming, including pest control, yield optimization, drought response, and land suitability. Even though the implementation of IoT in agriculture provides benefits, the device can be compromised, which can lead to incorrect data in measuring water levels for crops. This problem is also noted by [21].

C. Smart Transportation

IoT sensors are embedded in roads, traffic lights, and infrastructure to gather data associated with traffic flow, congestion, and road conditions. This information is then analyzed to optimize traffic flow, reduce congestion, and improve safety. The intelligent traffic management system is an example that can dynamically adjust traffic signals, reroute vehicles, and provide real-time updates to drivers through mobile apps or in-vehicle systems through IoT devices. Khan, Su'ud [22] elaborate that transportation systems like Intelligent Transportation Systems (ITS) have catalyzed navigation, route optimization, minimal power consumption, vehicle emissions, and the detection of traffic conditions based on streetlights and innovative parking systems [23]. Concerning car parking, intelligent parking reservation systems, for example, can significantly reduce the time spent searching for a parking space and increase the number of spaces available in parking lots through visual devices, infrared sensors, and magnetic fields [24]. IoT devices can also be hand-held devices that receive information on the road surface from implanted sensors to prevent accidents. In this regard, vehicles can exchange information regarding road conditions with other counterparts through a social network, possibly preventing road accidents.

D. Smart Healthcare

The IoT potentially benefits healthcare providers and patients. For example, large-scale patient data can be collected and analyzed. This information serves to identify potential health risks and develop individualized treatment plans for patients. The IoT devices can remotely monitor patients' vital signs and enable healthcare providers to track patients' health status from any location for reduced and enhanced hospital readmissions and patient outcomes, respectively. Moreover, smart healthcare that remotely monitors patients with IoT devices is cost-effective. Healthcare providers can mitigate the need for expensive hospital stays and emergency room visits. Additionally, IoT devices automate healthcare processes (medication management) and reduce healthcare providers' workload. As Khan, Su'ud [22] explained, IoT, wearable devices, mobile applications, and their associated features could coordinate people from different departments to respond actively to the medical ecosystem. In other words, the information and communication system is inextricably linked to the healthcare system [25].

III. Architecture

There are multiple tiers at which IoT can function, and this is determined by the functionality of the device, which is designed by the developer. However, there are varying interpretations about the idea of IoT tiers. One method categorizes an IoT architecture into three layers following their properties [26-29]. At the same time, other counterparts divide the architecture into finer-grained layers (four-layer architectures [30, 31] or the seven-layer IoT World Forum Reference Model [32]). Schiller, Aidoo [33] noted that IoT devices contain three layers: sensing, network, and application. Fig. 1 illustrates the IoT layers.

A. Application Layer

The application layer in IoT architecture is established through software applications and services that operate on top of the network and sensing layers. This level provides clients and programs with sophisticated features and services. Essentially, devices and applications are the two categories comprising the application layer. Applications are directly executed on IoT devices and provide data collection, processing, and control capabilities. Meanwhile, applications operate on cloud-based platforms or servers and provide data storage, analysis, and visualization services. The top layer constitutes the location for applications and middleware. This layer, which generally interacts with users through an application and specific services [26-29], can also imply cloud computing, integrations to other applications, and resolution or web services based on the circumstance.

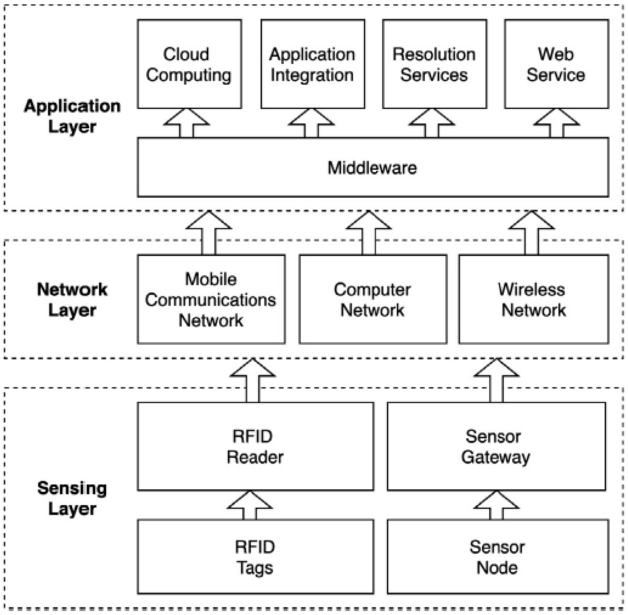

Fig. 1. The IoT architecture [33].

B. Network Layer

The network layer in IoT is accountable for overseeing the communication among devices that are linked within the IoT ecosystem. It performs functions such as managing the addressing, directing, and transmitting of data packets throughout the network. The IoT network layer frequently functions in situations with limited resources, emphasizing low-power and low-bandwidth communication. Schiller, Aidoo [33] explain that the network or communication layer communicates between the machines and services. This middle layer, which contains protocols used by mobile communication networks, computer networks, or wireless networks (constrained application protocol, CoAp, or ZigBee), requires data transmission between IoT devices and other network devices or servers [26-29, 34]. The network layer also includes MQTT, CoAP, and HTTP protocols to determine data formatting and transmission over the network. These protocols facilitate interoperability between multiple IoT devices and efficient and reliable data exchange.

C. Sensing (Perception) Layer

The sensing layer in IoT architecture comprises physical devices and sensors responsible for collecting data from the physical environment. This data is subsequently transmitted to the network layer. The primary function of these devices and sensors is to detect and measure various environmental parameters, such as temperature, pressure, and acceleration, as well as capture visual and auditory information through thermometers, barometers, accelerometers, cameras, and microphones, respectively. This layer is commonly known as the "edge" of the IoT network, given the occurrence of data generation and processing. Wearable health monitoring devices are sometimes integrated with appliances, vehicles, or infrastructure and worn by the user in others. Following Schiller, Aidoo [33], this layer contains devices (sensors, RFID readers, or tags) and a gateway. Sensors and actuators are frequently integrated with the environment [26-29].

IV. SECURITY CHALLENGES

One of the prominent security concerns in the field of IoT is frequently associated with design limitations stemming from limited resources. A prime example of this is the issue of storage constraints, which can render devices unable to store and execute software updates and patches on a regular basis, ultimately resulting in the emergence of vulnerabilities. The IoT device has limited resources [6] to store security updates, resulting in various cyberattacks, such as DDoS, eavesdropping, and MITM. Also, weak authentication mechanisms are increasingly recognized as a significant concern because they are vulnerable to malware and ransomware attacks, inadequate encryption protocols, and the risk of unauthorized access to sensitive data. As a result, it poses significant threats to the IoT landscape. For example, the WannaCry ransomware attack 2017 compromised many personal devices, computers, and medical equipment [35]. This situation exemplifies the significance of protecting IoT against five threats to all IoT systems [36]. IoT devices contain significant hardware vulnerability due to IoT products favoring functionality over security, thus rendering them vulnerable to various security threats. The absence of security consciousness among end-users further exacerbates the challenge, as they remain oblivious to the significance of security updates. Consequently, they become increasingly susceptible to social engineering and phishing attacks.

In addition to resource constraints, a substantial number of IoT devices are equipped with default usernames and passwords, which users frequently neglect to change. As a result, this grants cyber intruders the opportunity to exploit the vulnerability by employing default login credentials in order to gain unauthorized access and assume control over the devices. Owing to the specificity and complexity of IoT devices [37], existing tools are unable to detect command injection vulnerability, which poses a more significant challenge in safeguarding IoT devices against cyber threats.

A. OSI layer Versus IoT Layer

The IoT layer is a simplified layer derived from the OSI layer to accommodate the specific requirements of IoT devices, which necessitate different protocols and methods of data transmission. Consequently, cyber-attacks that target the OSI layers can also be executed at the IoT layer. The IoT layer is particularly vulnerable compared to the OSI layers due to the limited availability of patches and the lack of awareness and knowledge required to perform updates. As previously mentioned, IoT devices are utilized across various sectors, making their maintenance considerably more challenging than devices that operate based on the OSI layer, which is typically managed by competent administrators with knowledge of security updates. Table I illustrates the cyber-attacks associated with IoT devices.

B. OWAPS Security

The rapid expansion of IoT has led to increased efficiency and convenience. Notwithstanding, the prevalence of interconnected devices results in novel and intricate security concerns. Protecting IoT devices and sensitive data has become crucial at personal, organizational, and social levels. The Open Web Application Security Project (OWASP), a leading authority on IoT-specific security threats, specifies ten security vulnerabilities: (1) weak, guessable, or hard-coded passwords, (2) insecure network services, (3) insecure ecosystem interfaces, (4) lack of secure update mechanism, (5) use of insecure or outdated components, (6) insufficient privacy protection, (7) insecure data transfer and storage, (8) lack of device management, (9) insecure default settings, and (10) lack of physical hardening. These security flaws result from IoT devices' three-layered (sensing or physical, network, and application) design. Each layer reflects specific vulnerabilities following a narrow focus on security. From a scholarly perspective [29, 43, 44], every IoT layer denotes security flaws. These susceptibilities have caused industrial concern and increased the necessity to implement penetration against IoT devices. Fig. 2 illustrates specific security flaws against each layer of IoT devices.

TABLE I. ATTACK IN IOT DEVICES

No.	IoT Attack	Details
1.	Malicious Code Injection	A malicious code injection is launched by injecting malicious code into the sensor with a USB stick to control user data[38].
2.	Malicious Node Injection	The attacker exploits the IoT system by adding a malicious node to the network, which allows them to steal data between legitimate nodes [38, 39].
3.	Sleep Deprivation Attack	The attacker can disrupt the sensor’s sleep cycle to extend its battery life, drain its power, and cause it to shut down [38, 40].
4.	Physical Damage	Attackers can harm IoT components, including sensors and tags. For example, shoplifters in shopping malls can remove, damage, or replace tags with malicious intentions [38, 41].
5.	RFID Spoofing	Intruders can manipulate RFID tags by imitating legitimate ones through RFID spoofing [38, 42].
6.	MITM Attack	An attacker with access to two nodes could control and remotely modify the communication between the nodes [38].
7.	RFID Unauthorized Access	The attacker can control and modify the tags following their requirements, as they are publicly available [38].

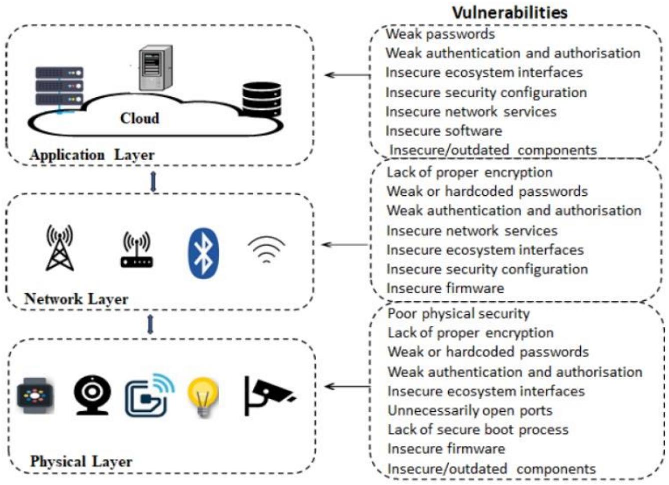
Vulnerabilities
Cloud
Application Layer
Weak passwords
Weak authentication and authorisation
Insecure ecosystem interfaces
Insecure security configuration
Insecure network services
Insecure software
Insecure/outdated components
Network Layer
Lack of proper encryption
Weak or hardcoded passwords
Weak authentication and authorisation
Insecure network services
Insecure ecosystem interfaces
Insecure security configuration
Insecure firmware
Physical Layer
Poor physical security
Lack of proper encryption
Weak or hardcoded passwords
Weak authentication and authorisation
Insecure ecosystem interfaces
Unnecessarily open ports
Lack of secure boot process
Insecure firmware
Insecure/outdated components

Fig. 2. The IoT layers with security flaws [44].

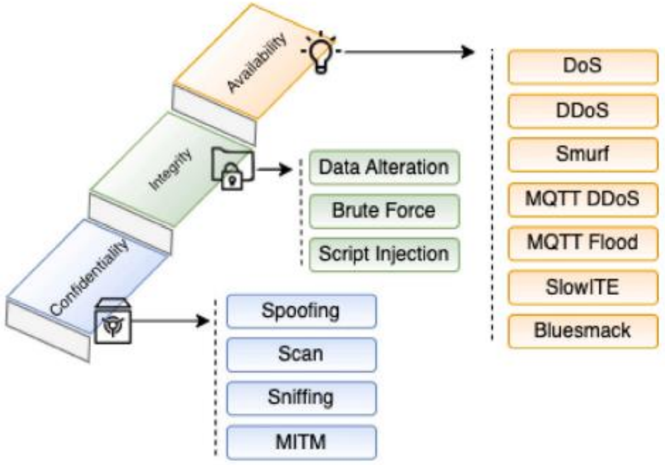

Fig. 3. Threat on IoT devices based on security principles [45].

Threats to IoT devices pose a significant risk to the principles of confidentiality, integrity, and availability, which are crucial for the security of these systems. Confidentiality is compromised when eavesdropping and data breaches occur due to weak encryption protocols and insecure communication channels. As a result, sensitive information becomes exposed to unauthorized access. Integrity is threatened by tampering and injection attacks, where malicious actors alter or inject false data into IoT systems, thereby corrupting data and affecting the reliability and accuracy of decision-making processes. Availability is at risk from denial-of-service (DoS) attacks and other forms of disruption, which can incapacitate IoT devices and services, leading to significant operational downtime and loss of service. These vulnerabilities underscore the necessity for robust security mechanisms, including strong encryption, secure authentication, and resilient network architectures, to safeguard IoT ecosystems against these multifaceted cyber threats. The IoT medical gateway, for example, introduces potential security risks because attackers can exploit this gateway to manipulate information before it reaches the healthcare provider, and they can execute DoS/DDoS or MITM attacks, resulting in the alteration or unavailability of critical patient data Neto, Dadkhah [45]. Fig. 3 indicates the threat to IoT devices based on the security principle.

C. Commercial Hardware Vulnerability

Commercial hardware vulnerabilities arise due to several factors. These include a lack of knowledge regarding update procedures, particularly devices associated with home appliances, limited hardware resources such as storage capacity, and inadequate authentication mechanisms. As a result, it can lead to exploitation and the compromise of sensitive data. Malhotra, Singh [17] describes that vulnerability as the flaws in a system that could be exploited to execute malicious actions. Scholars [46-49] acknowledged that the exploitation of vulnerabilities has become widely known as a result of the availability of public hacking databases, such as the Google Hacking Database and MITRE ATT&CK. These databases enable hackers to enhance their creativity by gaining insight into existing tricks and techniques, thereby facilitating the development of novel methods to exploit vulnerabilities in IoT devices. Most IoT devices nowadays are visible to the

Internet, and the existence of the online database, as mentioned above, aids hackers in effortlessly exploiting publicly accessible IoT devices through online IoT search engines. Besides that, other researchers [17, 50] added that hackers could manipulate IoT vulnerabilities to compromise legitimate user services' security, privacy, and availability.

Vulnerability is commonly revealed through research and submitted to software system providers. The product owner is accountable for publicly announcing security concerns by issuing a security advisory report within 90 days [51]. At this stage, all parties must collaborate to ensure that security loopholes are promptly published so that users can take necessary measures. Threat actors discover the vulnerability before the researchers can launch advanced attacks. Zero-day vulnerabilities result from this factor, as security flaws are yet to be officially reported or available in the vulnerability database. In Zhao, Ji [49], developers struggle to holistically address zero-day vulnerabilities or prevent bugs despite meticulous programming and code auditing. Hence, periodical security assessments should be rapidly and fully automated. Cyber intruders can use all the information on various vulnerabilities identified by trusted resources to launch attacks. Alternatively, technology producers could use the information to generate patches that effectively secure their products. Table I presents vulnerability in IoT devices, which was published by [52, 53] and seconded by Janiszewski, Felkner [54]. Commercial IoT hardware vulnerabilities are indicated in Table II.

TABLE II. COMMERCIAL IOT DEVICE VULNERABILITIES

No	Device and CVE	Severity	Description
1.	Device : Smart TV CVE-2019-6005	Critical	Smart TV Box fails to restrict access permissions
2.	Device : Smart TV CVE-2019-11890	High	Sony Bravia Smart TV vulnerability related to input validation on devices
3.	Device : Smart TV CVE-2015-5729	Critical	Plural Samsung Smart TV and Xpress of Soft Access Point vulnerabilities that capture essential information on functions
4.	Device : Camera CVE-2022-39858	High	SAMSUNG mobile devices reflect path traversal vulnerability
5.	Device : Camera CVE-2021-3615	Medium	Lenovo Smart Camera Code injection vulnerability
6.	Device : Burglar Alarm CVE-2019-9659	Critical	Plural Chuango vulnerability related to input validation in products
7.	Smart Homes Devices CVE-2018-9162	Critical	Contec Smart Home vulnerabilities related to lack of authentication for critical functions
8.	Smart Home Application CVE-2020-14114	High	Vulnerability can be caused by illegal calls that attackers can exploit to leak sensitive information.
9.	SmartCare Application CVE-2021-26638	High	Exposed to authentication bypass and information exposure
10.	Rubetek Smart Home CVE-2020-9550	High	Permit attackers to remotely sniff and spoof beacon requests

D. Industrial Concern

A diverse range of industries has adopted IoT due to its simplicity and cost-effectiveness. However, industry players have expressed a pressing concern regarding the presence of the vulnerability, which has the potential to be exploited and thereby lead to substantial disruptions in supply chain operations, production lines, and overall business activities. The attack can significantly impact organizations, leading to downtime, delays, and financial losses. Fortinet [7] stated that cybercriminals use IoT Botnets to conduct DDoS attacks and simultaneously target multiple devices. The Mirai Botnet was responsible for shutting down various primary services and websites in 2016. Specifically, Mirai exploited vulnerabilities in unprotected devices with a publicly accessible Botnet code. Mirai Bonet occurred due to various reasons. Leyden [55] reported that only 27.1% of suppliers offer a vulnerability disclosure policy. The statistics indicate slow progress that hampers security researchers from reporting security bugs in IoT devices. According to Kaspersky [56], 64% of enterprises globally employ IoT solutions. Nevertheless, 43% of these organizations fail to offer comprehensive protection due to the absence of compatibility between security solutions and specific IoT devices and systems. Almost half of the businesses are concerned that cybersecurity products would hinder IoT performance (46%). Inadequate staffing or specific IoT security expertise similarly deter businesses from implementing cybersecurity tools (35%). Barracuda [57] highlighted the possibility of new hazards, such as actual physical destruction through IoT.

V. THE NEED FOR PENETRATION TESTING

Due to poor security structures, IoT devices require comprehensive security assessment. Failure to comply with this requirement may lead to severe consequences, including data loss and leakage. Moreover, the utilization of wireless connectivity as a means of communication further increases the attack frequency. This assumption is consistent with the finding from [5], where the research points out that the majority of IoT devices utilize wireless communication, which can potentially lead to an increase in the occurrence of cyber-attacks. The concern about IoT security was also highlighted by Akhilesh, Bills [8], who stated that default communication can lead to vulnerability. Despite multiple updates, most devices rely on the insecure HTTP protocol rather than the secure channel. Consequently, this vulnerability enables attackers to intercept and decode an HTTP packet, thereby gaining unauthorized access to private data stored on the device [58]. According to [59], protocols like SSH and Telnet are the most popular remote access protocols for IoT devices. The devices are susceptible to cyberattacks that allow unauthorized access through open ports or services, such as FTP, Telnet, or SSH [60].

IoT devices are vulnerable to extensive cyber-attacks, primarily due to inadequate security design and a lack of timely software updates and patches, especially in the domains of smart homes, agriculture, transport, and healthcare. This phenomenon arises due to a deficiency in knowing how to carry out updates, as most IoT devices are utilized by end-users with limited knowledge of device security. Security breaches like stealing sensitive information and personal data are possible cyber-attacks due to malware attacks against IoT devices following the design loophole of IoT devices [4]. Alonazi, HamdiI [6] claimed that command injection can infiltrate IoT devices. Likewise, [6] IoT devices are vulnerable to DDoS attacks, eavesdropping, and MITM. Alshammari and Alserhani [61] highlighted the potentiality of IoT devices in impacting ransomware attacks, as IoT applications and devices perform critical activities. Alshammari and Alserhani [61] denoted password cracking as another attack that can be launched to gain passwords of IoT operating systems, services, and web applications installed on the testbed or in the production environment. Notably, IoT device owners often fail to apply security patches for device stability and to prevent cyberattacks following poor technical knowledge. Most IoT devices, currently designed for home use and owned by multiple users, motivate cyber intruders to attack these devices. Alonazi, HamdiI [6] describe that smart home service industries and medical devices are more vulnerable to cyberattacks, given technology producers' inability to consider security constraints during device development.

Depending on the application of the IoT device, certain industries, such as healthcare and agriculture, may require a complex IoT infrastructure to facilitate information exchange between different locations, which can become challenging to manage. In addition, inadequate security infrastructure and a lack of timely software updates and patches further hinder the prevention of cyber-attacks. The study in [62] also describes that controlling and managing these devices has become complicated, while [63] stated that such issues lead to the requirement for enhancing IoT security. Alashhab, Zahid [64] noted that IoT devices must be secure to prevent their illegal activation. The structure of the IoT security must be lightweight to ensure the devices can perform well, owing to resource constraints. According to [28], low-security support in IoT can undermine user confidence and lead to technology failure; meanwhile, An and Cho [65] exemplified instability as an IoT issue. The use of IoT devices in various sectors further increases the need for penetration testing. Furthermore, identifying and characterizing security prerequisites, potential cyberattacks, and their implications on the system can significantly develop and select an optimal protection system [66]. Consequently, penetration testing proves pivotal in mitigating the impact and possible occurrence of attacks in the IoT context.

VI. Security Testing

Cybercriminals predominantly focus on IoT devices because they have the capability to gather, analyze, and transmit confidential data, and various sectors utilize it. The consequences of successful intrusions into IoT systems can have significant negative implications for an individual's privacy, critical infrastructure, and public safety. Consequently, IoT security testing is crucial in identifying and addressing vulnerabilities, weaknesses, and misconfigurations. This section explains the procedures that can be employed for IoT security testing.

A. IoT Penetration Testing

Security analysts use IoT penetration testing to detect and exploit flaws to safeguard IoT devices. The IoT device security can be "pen tested" in the real word. Meanwhile, "penetration testing" involves assessing the whole IoT system instead of just a single device or software.

B. Threat Modeling

Threat modeling assists users in detecting potential vulnerabilities in their IoT devices. For example, a camera can spy on occupants of a private residence in a specific range. The images could be viewed by physically breaking into the camera or hacking its system.

C. Firmware Analysis

One of the most crucial concepts to grasp is that firmware is software, not unlike other computer programs or applications. Firmware is only used by embedded electronic devices (smartphones, routers, or health trackers), which function as specialized minicomputers. The device components must be extracted and subjected to a battery of tests for firmware analysis and the detection of vulnerabilities, such as backdoors and buffer overflows.

VII. Penetration Testing Framework

The existing approach to penetration testing in IoT devices involves systematic evaluation. This process identifies and exploits weaknesses in the device's firmware, software, and network connectivity. Given the need for IoT devices to be periodically analyzed, IoT-oriented security analysis technologies must be developed to guarantee device security and dependability [37]. Penetration testing or ethical hacking is inextricably linked to IoT device security. The recent growth of IoT device interconnections has rendered them more susceptible to cyberattacks. Penetration testing on an IoT device can identify potential security flaws, strengthen security measures, and prevent unauthorized access to sensitive information. Notably, IoT architecture, communication protocols, and security mechanisms must be holistically understood for thorough and effective penetration testing following the complexity of IoT ecosystems. Seasoned IoT security experts should thoroughly conduct penetration testing to detect unauthorized access. The insights gained from a successful penetration test can help organizations better understand and mitigate their IoT device security risks, protect sensitive data, and prevent costly security breaches. Various standards and methodologies have been extensively used with different capabilities, and a detailed explanation can be located in the manuscript [67].

A limited number of studies have been conducted on IoT penetration testing; however, those who selected the topic focused on specific penetration tests, such as smart home devices and cameras [68] or an intelligent home voice assistant [69]. Another empirical work illustrated the system's vulnerability to cyberattacks. Inexpensive hardware (an ordinary laptop and a USB dongle costing under 20 USD) was used to test the device with the standard penetration testing software. Vulnerabilities in the voice assistant enabled penetration testers to sniff data across a network attached to the voice assistant, read messages, and even control devices.

Bella, Biondi [70] performed a penetration test against an IP camera and adopted a six-step penetration testing methodology, known as penetration test IoT (PETIoT): (1) experiment setup, (2) information gathering, (3) traffic analysis (4) vulnerability assessment, (5) exploitation and (6) fixing. Based on the study, three zero-day vulnerabilities were practically discovered and exploited on camera under the CVSS standard: one with high severity and the other with medium severity. The first vulnerability, improper neutralization of inbound packets, permits complete DoS. Second, the insufficient entropy in encrypted notifications permits a violation of motion detection. Third, clear text transmission of video streams permits violation by unauthorized parties.

Suren, Heiding [51] proposed using practical and agile threat research for IoT (PatrIoT) to address the drawbacks in conducting penetration testing with four key elements of methodology: (1) planning, (2) threat modeling, (3) exploitation, and (4) reporting. The authors selected IoT device categories as smart homes and successfully discovered vulnerabilities. Each stage contains specific sub-activities. For example, the planning stage constitutes scoping, information-gathering, and enumeration, while the threat modeling stage encompasses attack surface decomposition, vulnerability analysis, and risk scoring. The exploitation stage contains known vulnerabilities, as well as exploit development and post-exploitation. The final reporting stage involves the activity of reporting templates, vulnerability disclosure, and CVE.

Heiding, Süren [71], who previously introduced PatrIoT, used the same methodology to investigate the security level of connected home devices using 22 devices in five categories: intelligent door locks, smart cameras, smart car adapters or garages, smart appliances, intelligent car accessories, and various smart home devices. A total of 17 vulnerabilities were successfully detected and published as new CVEs. Specific CVEs received a high severity ranking (9.8/10) from NVD. According to this study, devices that are currently on the market and used worldwide are vulnerable to attacks that could be detrimental to users.

Faeroy, Yamin [72], who examined vulnerabilities in IoT devices, such as autonomous monitoring and tracking systems, developed an autonomous agent whose decision-making process paralleled the execution plan model (EP Model). The seven-step PTES comprising (1) pre-engagement interactions, (2) intelligence gathering, (3) threat modeling, (4) vulnerability analysis, (5) exploitation, (6) post-exploitation, and (7) reporting was used in this study. The agent decision models were monitored with a formal temporal logic of action (TLA+) language. Resultantly, penetration testing could be automated with the EP model. The agents rendered the target device inoperable and successfully forged a connection with the client.

Akhilesh, Bills [8] recommended an automated penetration testing framework with PTES to identify the most common vulnerabilities in smart home-based IoT devices. The study evaluated the security of five smart home-based IoT devices (TP-link smart plug, TP-link smart bulb, TP-link smart camera, Google Home mini, and LIFX smart bulb) to identify the most common vulnerabilities in those devices. Following the research outcomes, both the TP-Link smart bulb and smart camera scored the highest in insecurity, while Google Home Mini scored the lowest (highly secure).

Rak, Salzillo [73] suggested an expert security assessment (ESSecA) system for security professionals and penetration testers to evaluate the safety of IoT gadgets and networks. The testing methodology contains four stages: (1) system modeling, (2) threat modeling, (3) planning, and (4) penetration testing. ESSecA can almost automatically generate comprehensive penetration testing or attack plans by integrating current security analysis methods [69, 74-76]. The proposed system structure led to penetration testing plans based on the level of risk involved and structured following the threats posed by an attack.

Yadav, Paul [77] proposed an automatic, adaptable, and thorough end-to-end penetration testing framework called IoT-PEN. The proposed framework constitutes (1) installation, (2) information gathering, (3) extraction, and (4) vulnerabilities reported and target-graph generation. The framework capability has been assessed through IoT devices, including smart bulbs, bridges, gateways, servers, and mobile applications. This modular and adaptable framework has a plug-and-play design for penetration testing and considers the diversity of IoT devices. The IoT-PEN depends on a server-client architecture, where a resource-containing system functions as the server. All IoT nodes act as the clients. A specialized script scans a network of devices and identifies possible vulnerabilities. The user can select the necessary modules and automatically generate a novel framework.

Abdalla and Varol [68] evaluated IP camera security by (1) defining the area, (2) implementing the process, and (3) reporting and presenting the outcome. Despite the inability to note the specific penetration methodology, this study effectively disclosed the following security flaws in the IP camera: (1) default credentials, (2) information transferred without encryption, (3) lack of encryption, and (4) weak methods in protecting sensitive data.

Given the review that had been carried out, this study came to the review conclusion that the majority of current studies have utilized manual penetration testing. In contrast, three earlier studies advocated an automation technique, while one study chose a semi-automation approach (see Table IV for more information). Regardless of manual or automated penetration testing, there is a strong need for penetration testing to be conducted by end users, such as smart home users and farmers. Given the variances in user knowledge, users should be equipped with a simple and effective penetration methodology. IoT devices can operate in a safe and secure environment with security assessment like penetration testing. In addition, the automated mode of execution makes it convenient for a wide range of users, regardless of their background, to evaluate the level of security device.

Aside from that, in the majority of the earlier research, the penetration testing process was broken down into four stages. On the other hand, because of the requirement of automated IoT penetration tests that must be carried out at the end-user level, certain steps must be avoided because they are irrelevant. In this vein, automated penetration tests must critically measure the security level of IoT devices without security experts' interactions. This study also found that vulnerability scanning, exploitation, and reporting are the only stages that allow end-users to conduct self-penetration tests across sectors in an automated manner. Suren, Heiding [51], the IoT penetration testing report denotes specific attributes, such as a dedicated section for hardware and radio components containing high-quality images and video demonstrations. Nevertheless, these materials only apply to organizational-level penetration testing, deemed inappropriate for end-user environments. Table III summarizes the IoT penetration testing methodology, followed by Table IV, which shows the details of the prior work on IoT.

TABLE III. SUMMARY OF PENETRATION TEST

No.	Authors	Penetration Test Methodology	Penetration Test Stage
1.	Bella, Biondi [70]	Penetration Test Internet of Things (PETIoT)	(1) Experiment setup (2) Information gathering (3) Traffic analysis (4) Vulnerability assessment (5) Exploitation (6) Fixing
2.	Suren, Heiding [51]	Practical And Agile Threat Research for Iot (PatrIoT)	(1) Planning (2) Threat modeling (3) Exploitation (4) Reporting
3.	Heiding, Süren [71]		
4.	Faeroy, Yamin [72]	Penetration Testing Execution Standard (PTES)	(1) Pre-engagement interactions (2) Intelligence gathering (3) Threat modeling (4) Vulnerability analysis (5) Exploitation (6) Post-exploitation (7) Reporting
5.	Akhilesh, Bills [8]		
6.	Rak, Salzillo [73]	Expert System for Security Assessment (ESSecA)	(1) System modeling (2) Threat modeling (3) Planning (4) Penetration testing
7.	Yadav, Paul [77]	End-to-End Penetration Testing framework (IoT-PEN)	(1) Installation (2) Information gathering (3) Extraction (4) Vulnerabilities reported and target-graph generation.
8.	Abdalla and Varol [68]	Nil	(1) Defining the area (2) Implementation of the process (3) Outcome reporting and presentation

TABLE IV. DETAILS OF PRIOR WORK IN IOT PENETRATION TESTING

No.	Authors	Device Categories	Penetration Method	Vulnerability Database	IoT Devices	Vulnerabilities
1.	Bella, Biondi [70]	Smart Home Device	Manual Penetration Testing	Common Vulnerability Scoring System (CVSS) Common Weakness Enumeration (CWE)	IP Camera (TP-Link TAPO C200)	1. Improper neutralization of inbound packets allows complete DoS. 2. Insufficient entropy in encrypted notifications allows a breach of motion detection. 3. Clear text transmission of video stream allows breach by unintended actors.
2.	Heiding, Süren [71]	Smart Home Device & Transport	Manual Penetration Testing	National Vulnerability Database (NVD)	Smart Door Locks, Smart Cameras, Smart Appliances, Smart Car Adapters/Garages, Intelligent Car Accessories	1. Smart Door Locks: CVE-2019-12942 and CVE-2019-12943. 2. Smart Cameras: (1) Communication interception (medium), (2), Broken authentication, (3) Privilege escalation (medium), (4) Communication interception (medium) (5) Code injection (critical), (6) security misconfiguration/design flaw, (7) DoS (critical), (8) CSRF, Communication interception (critical), (9) Tampering with the firmware (medium), Tampering with the firmware (critical). 4. Smart Car Adapters: (1) Communication interception (medium). 5. (2) Brute force [CVE-2019-12941], (3) Code injection (critical), (4) Broken authentication [CVE-2019-12797]. 6. Smart Garage: XSS (critical) [CVE-2020-12282], Session hijacking (critical), Unrestricted file upload [CVE-2020-12837, CVE-2020-12843], Clickjacking [CVE-2020-13119], Broken authentication,

No.	Authors	Device Categories	Penetration Method	Vulnerability Database	IoT Devices	Vulnerabilities
						Communication interception (medium), Security misconfigurations, Privilege escalation (critical) [CVE-2020-12838, CVE-2020-12839, CVE-2020-12842], CSRF [CVE-2020-12280, CVE-2020-12281, CVE-2020-12840, CVE-2020-12841].
3.	Faeroy, Yamin [72]	Transportation	Automated Penetration Testing	Nil (not mentioned)	Autonomous Monitoring Tracking Systems A200 AIS Class A	1. Vulnerable to Evil Twin attack (ESSID is visible to anyone).
4.	Suren, Heiding [51]	Smart Home	Manual Penetration Testing	Common Vulnerabilities and Exposures (CVE)	AI robot Ryze tello drone Samsung smart fridge Xiaomi Mi home security camera Yale L3 smart door lock Yanzi air quality sensor Xiaomi Mi home security camera	1. Sensitive data exposure 2. Lack of transport encryption 3. Command injection. 4. Authentication bypass 5. Insecure SSL/TLS issues 6. Insecure authorization 7. Backdoor firmware 8. Insure data storage
5.	Akhilesh, Bills [8]	Smart Home Device	Automated Penetration Testing	Common Vulnerability Scoring System (CVSS) CVSS score	TP-Link Smart Plug, TP-Link Smart Bulb, TP-Link Smart Camera, Google Home Mini, And The LIFX Smart Bulb	1. TP-Link Smart Plug: A potentially insecure network service vulnerability. 2. TP-Link Smart Bulb: Lack of transport encryption and insecure firmware vulnerability 3. P-Link Smart Camera: Lack of transport encryption and insecure firmware vulnerability 4. Google Home Mini: No vulnerabilities were detected. 5. The LIFX Smart Bulb: No vulnerabilities were detected
6.	Rak, Salzillo [73]	Smart Home Device	Semi-Automated Penetration Testing	MITRE database ATT&CK	Smart Sockets, Power Production/Consumption Measurements, Control Of Charging Stations, Room Temperature and Humidity, Outdoor Temperature	Devices vulnerable to the following attacks: 1. Packets sniffing 2. Identity spoofing 3. Brute force 4. Data stealing 5. Privilege escalation. 6. Snarfing 7. CONNECT flood. 8. PUBLISH flood. 9. DoS impersonation
7.	Yadav, Paul [77]	Smart Home Device & Network Device	Automated Penetration Testing	National Vulnerability Database (NVD)	smart bulbs, bridges, gateways, servers, and mobile applications	1. CVE-2012-5696 allows remote attackers to obtain the plaintext database password via a direct request. 2. CVE-2017-14797 lack of transport encryption in the public API in Philips Hue Bridge BSB002 SW 1707040932 allows remote attackers to read API keys. 3. CVE-2018-18394 (User-sensitive data stored). 4. CVE-2018-18392 (Privilege escalation in IoT gateways). 5. CVE-2015-2883: Weaved cloud web service, as demonstrated by the name parameter to device Settings.php or share Device.php. 6. CVE-2019-4047: Allow an authenticated user to access the execution log files as a guest user. 7. CVE-2014-0220 Allow remote authenticated users to obtain sensitive configuration information via the API.
8.	Abdalla and Varol [68],	Smart Home Device	Manual Penetration Testing	Nil (not mentioned)	IP Camera (Intelligent Onvif YY HD)	1. Default credentials. 2. Information transferred without encryption. 3. Lack of encryption 4. Sensitive data is protected by weak methods

VIII. Discussion and Analysis

This section discusses and critically analyses the gaps in securing IoT devices, which future works can address. The critical analysis is presented in eight sections as follows:

A. *Incompetent User*

The majority of the IoT devices that fall under the category of smart homes are susceptible to vulnerabilities. This pattern indicates that smart home devices are the prime target due to critical vulnerabilities. Such weak points can expose digital assets to cyberattacks, such as DDoS and malware. Security assessments must be regularly performed against these devices to prevent cyber intruders from manipulating user devices. Nevertheless, recent research [8, 70-73, 77-79] has not offered a solution for normal users to conduct penetration testing. Given the multitude of incomprehensible steps and software to normal users, this approach requires security experts. Even though automated penetration testing, as suggested by previous studies shown in Table IV, is capable of conducting security assessments automatically, it is primarily designed for penetration testers or IT experts. This leaves end users who utilize IoT devices in industries such as transportation, healthcare, and agriculture vulnerable to cyber threats if proper assessments are not conducted. Aside from that, IoT devices consist of multiple layers, as illustrated in Fig. 1, and each layer is vulnerable to cyber threats due to various factors, as indicated in Fig. 2. Given this context, the utilization of automated penetration testing, which end-users can perform, becomes crucial. This allows them to implement necessary security measures, such as applying security updates, in order to prevent and mitigate the impact of cyber threats.

Although the penetration testing conducted by IT expert they are struggling to perform penetration testing on multiple IoT devices manually. Faeroy, Yamin [72] explained that penetration testing IoT devices do not significantly vary from penetration testing larger computer systems. Meanwhile, Suren, Heiding [51] observed that conventional penetration testing has been well-documented over the years as opposed to the IoT ecosystem. Following recent studies [72], automated penetration testing for IoT devices has become complex due to their multiple applications and heterogeneity. Regardless of prior studies' views, this paper suggests that implementing automated penetration testing can effectively target inexperienced users, including end users and junior system administrators. This approach can expedite the identification of cyber threats at the initial stage.

B. Automated Penetration Test

The emergence of AI has catalyzed automated penetration testing. Automated penetration testing streamlines and complements traditional manual testing, as it can be implemented with various methods and tools. Likewise, Faeroy, Yamin [72] conceded to the possible interactions between automated penetration testing tools and other security processes, such as vulnerability management, incident response, and compliance management. Detecting and exploiting security flaws could be significantly improved by integrating machine learning. Regardless, Suren, Heiding [51] argued that automated tools, such as vulnerability scanning, may fail to detect security flaws. Manual assessment is necessary and could inspire vulnerability scholars. Bella, Biondi [70] similarly rejected the proposed solution and noted that the automated scanners were incapable of detecting vulnerabilities due to the absence of relevant signatures in the vulnerability database. Three scholars [8, 72, 77] recently introduced automated penetration tests. Nevertheless, the methodologies were unconvincing, as the study may derive imprecise outcomes during the vulnerability assessment. Given that the proposed method may erroneously detect false positives and negatives during the assessment process, evaluating the result with a confusion matrix is vital to assess the effectiveness of automated penetration testing. Automated penetration test requires result verification to affirm that security flaws exist. Result verification is necessary for automated penetration testing to verify the emergence of security flaws. Lacking this feature will impact the assessment result. Hence, automated penetration testing should utilize dual evaluations that are automatically conducted using distinct evaluation techniques, and it is crucial to have these functionalities in order to allow end-users to carry out these assessments autonomously with results that can be trusted.

C. Open-Source Software

The utilization of open-source software in the context of penetration testing may result in fault result classification, even when employing a database vulnerability with high levels of accuracy. This particular platform permits code modifications to align with the user's requirements. However, due to a lack of functional testing after code modification, false results may happen. For instance, false positives and negatives occur owing to inaccurate classification with a high-accuracy vulnerability database. Suren, Heiding [51] concurred that download exploitation tools from the public database require alteration for successful execution. This research found out that, although this issue is well known, it has not received significant attention. Due to this atmosphere, automated penetration testing with double assessment is the only means of ensuring the accuracy of the result. Double assessment involves running parallel tests using different methodologies or tools to cross-verify the findings. This redundancy helps identify discrepancies and validate the results, reducing the likelihood of false positives and negatives. While open-source software offers significant advantages in terms of flexibility and cost-effectiveness for penetration testing, it also presents challenges related to result accuracy. Addressing these challenges requires a combination of rigorous testing and the usage of multiple assessment tools to guarantee that the result is correct.

D. Vulnerability Assessment and Penetration Test

IoT devices require robust security assessment due to the existence of various vulnerabilities. As indicated in Table II, end users use most IoT devices daily. Furthermore, IoT devices are adopted by home users and various industries such as transportation, agriculture, and healthcare, which increase the need for security assessment. As indicated in Fig. 1, the IoT device has three layers, making it vulnerable to different cyberattacks. Thus, to fix this issue, vulnerability assessment and penetration testing are the first critical steps in identifying and mitigating these vulnerabilities, allowing for the development of robust defense mechanisms tailored to each layer's specific threats.

Vulnerability assessment identifies the weak point of a device, while penetration testing legally launches the attack to internalize the impact distance if cybercriminals exploit the devices. Both processes prove vital; however, they can probably generate incorrect output following false positives and negatives. Suren, Heiding [51] indicated the third stage of penetration testing as exploitation, which determines whether a system is genuinely vulnerable and identifies what an attacker could achieve through manipulation. Bella, Biondi [70] asserted that vulnerability assessment and penetration testing sessions ensure the effective implementation of security measures. In line with recent studies [72], a penetration tester may exploit the identified vulnerabilities or elevate its privileges within the system to reveal additional vulnerabilities as proof of concept. Both vulnerability assessment and penetration testing are crucial components of IoT penetration testing, as they help protect the device from cyber threats and ensure appropriate security measures are applied to the devices, such as patches; it is essential to utilize a high-accuracy vulnerability database to ensure accurate results and eliminate false positives.

Following the current study [8, 51, 70, 71, 73, 77], most of them used the vulnerability database during vulnerability scanning, while others [68, 72] were silent. This study emphasized that a non-standard vulnerability database could generate false positive and negative results, which impacts the vulnerability assessment output. Consequently, confusion and panic may be introduced among IoT players, and the potential reduction of user trust in embracing IoT devices may occur. Both vulnerability and penetration testing are vital to be conducted in the form of an autonomous approach while considering the vast number of IoT devices adopted by organizations and catering to end-user incompetency in performing technical aspects.

E. Penetration Testing Challenge for IoT Devices

Security professionals are required for penetration testing. During the course of this review, it was discovered that there are constraints in terms of offering an efficient and user-friendly penetration testing procedure. Although automated penetration testing has been introduced by several studies [8, 72, 77], this approach reflects a specific downside. For example, Akhilesh, Bills [8] could only detect five vulnerabilities: (1) insecure web interface, (2) remote access vulnerability, (3) improper authentication, (4) insecure network services, (4) lack of transport encryption, and (5) insecure firmware or software. The automated penetration test proposed by Yadav, Paul [77] proved better than that of Akhilesh, Bills [8] due to integration with the vulnerability database, which presented more vulnerabilities. Regardless, the authors only evaluate his proposed work on specific IoT devices. Faeroy, Yamin [72] used a highly intricate PTES methodology that confounded end-users. Rak, Salzillo [73] presented a semi-automated penetration testing that only contains a threat model and attack plan, while other processes still require manual execution. Notably, IoT penetration testing requires a different approach following manual execution, which security experts can only manage.

Although a self-pen testing application could be provided with IoT devices to measure their security level, this approach requires additional resources. Alonazi, HamdiI [6] acknowledged the resource constraints of IoT devices. Due to insufficient resources, Anitha and Arockiam [80] added that IoT devices are more susceptible to security weaknesses and cyber intruders' manipulations. Furthermore, including sophisticated security features in IoT devices would significantly increase development costs. Most IoT producers partially ignore the security landscape in IoT devices, with emphasis on the device functionality. As most service providers do not consider security constraints at the outset, Bhavadharini, Karthik [81] claimed that smart home services and medical devices are more vulnerable to cyberattacks.

F. Resource Limitation

IoT devices are susceptible to cyberattacks due to resource constraints. Such insufficiency can lead to two outcomes. First, the devices can be overloaded by DDoS attacks, thus rendering IoT applications and services unavailable following the absence of resources to surf genuine client requests. Second, storage limitations prevent the devices from having built-in protection software, which exposes them as prime targets for attack. Othman, KOY45 [82] denoted memory and power consumption as the two common limitations of electronic devices that render security tools ineffective. Pawar and Kalbande [83] addressed similar concerns about data security and privacy in IoT devices within the healthcare sector, specifically when transferring medical data. Current IoT devices, such as Zima Board, exemplify an IoT gadget that can be programmed to operate in multiple sectors, such as the banking sector's automatic teller machine (ATM). The highest model of this device is equipped with a processor speed between 1.1-2.2GHz, 8 GB of memory, and storage limited to 16 GB [84]. Another product competitor is Nvidia, with a maximum processor speed of 2GHz and a memory and storage size of 64GB [85]. As delineated by several studies [6, 80, 82], existing IoT devices strongly indicate resource constraints. Notwithstanding, the security of IoT devices must take precedence over resource expansion to prevent cyberattacks.

G. After Sales Service and End of Support

The product owner is responsible for providing after-sales services, such as periodic security updates to protect IoT devices from Botnets. As highlighted in various studies on smart agriculture [22], smart transportation [22-24, 86], smart home [22, 87], and intelligent healthcare [22], the use of IoT devices in various sectors increases the need for high device security. Notably, IoT devices can become outdated and susceptible to multiple attack types. Software vendors do not provide updates for obsolete devices, which exposes these gadgets to cyberattacks. Furthermore, financial loss, company direction adjustments, and ownership changeovers can affect IoT device support. In addition, the limited duration of support from IoT device manufacturers, namely for providing operating system or firmware updates, is also a significant factor leading to the spread of vulnerable IoT devices in the market. In this context, IoT industry players face challenges, as extending the support period can increase operational costs. Furthermore, addressing emerging cyber threats may necessitate large-scale updates to be pushed to user devices, which could present issues due to limited IoT resources.

Nevertheless, another significant aspect that requires attention is that most users of IoT devices tend to use them for extended periods, even in the absence of available updates. This challenge poses a significant issue since this is the root cause of vulnerability. Furthermore, personal IoT devices can be used for more extended periods as long as they remain practical. These challenges need to be taken into serious consideration in order to mitigate the vulnerabilities of IoT devices to various types of attacks. An IoT device contains application and network layers [33], which can be exploited without timely security updates.

H. Countermeasure

Individuals and organizations should be equipped with countermeasures against IoT cyber threats. The IoT devices must be used cautiously to mitigate detrimental effects and fostering a security-conscious culture among users is crucial. Educating users on best practices for IoT device security, such as regularly updating firmware, changing default credentials, and recognizing phishing attempts, can substantially reduce the risk of cyber incidents. Due to IoT technology continues to evolve and integrate into critical infrastructure, the development and deployment of adaptive and resilient security measures become increasingly important to safeguard against emerging threats and ensure the reliability and safety of interconnected systems. The two-factor authentication is a preventive measure apart from advising users to create strong and secure passwords to prevent their devices from being illegally accessed by cybercriminals. Nevertheless, two-factor authentication may inconvenience some people, who deem it complicated and troublesome. In line with Malkawi, Obaid [66], IoT enables the automation of multiple systems and services, including healthcare, homes, traffic lights, and electricity grids. Operating system and firmware updates could be another alternative to prevent IoT devices from becoming a victim of cyberattacks. On the contrary, the update should be minor due to storage and processing constraints. Suresh and Priyadarsini [88] explained that limited storage restricts data processing in IoT devices.

I. Encryption

IoT devices require encryption to secure the traffic and its data. However, some IoT producers neglect robust encryption due to resource limitations such as processing power and memory constraints, leaving devices vulnerable to cyber-attacks and data breaches. This oversight can lead to significant security risks, compromising individual device integrity and the broader network to which these devices are connected. As IoT technology proliferates across various sectors, efficient, low-overhead encryption solutions become increasingly critical to protect sensitive data in resource-constrained environments. The solution provided by Mozaffari-Kermani and Reyhani-Masoleh [89] could address these issues by using a low-cost S-box for the Advanced Encryption Standard (AES). The authors suggest using logic gate implementation on a regular basis in composite fields rather than traditional lookup tables, which can significantly reduce the power consumption and the physical area required on hardware chips, particularly for AES applications that necessitate fast and low-complexity operations. However, using a cryptography algorithm in IoT devices leads to an attack since hackers can mount active side-channel analysis attacks through fault injections [90]. IoT devices have been used in various sectors, and the use of IoT devices in critical sectors such as healthcare further increases the need for robust security.

The IoT resource constraint leads to implementing security measures being deferred, scaled back, or entirely unfeasible, compromising device integrity and network security and heightening the risk of breaches and cyber-attacks. Choo, Kermani [91] stated that the hardware and software security systems, which require storing data, are critical and can be challenging to address due to their unique constraints.

IX. Conclusion

This study delves into the recent phenomenon of penetration testing on IoT devices. Furthermore, it undertakes a comprehensive discussion and critical analysis of the significance and challenges of conducting penetration tests on IoT devices. This study found that there is a significant need to find a way to conduct penetration testing across various fields without user intervention. The multidimensionality and applicability of IoT deployment across various industries amplify the necessity for an automated approach in conducting security assessments of the devices. The ultimate goal is to enable end-users to execute these assessments independently or to have devices equipped with features that allow users to perform the tests themselves. This would provide a significant advantage in safeguarding IoT devices against becoming primary targets of cyber threats. Penetration services require hiring professionals and are expensive. Although cloud penetration testing is indeed a viable option, it may not be suitable for end-users with limited technical proficiency. This is particularly true for individuals who are unable to carry out pre-configuration and connectivity checks to ensure that their device can be properly connected to and scanned by a cloud penetration tester. This study discovers that there is a need for a new penetration testing approach that can deal with IoT security assessment for a diverse range of end-users, regardless of their educational background and technical proficiency level. The consequences of having weak security infrastructure can be harmful. Therefore, it is essential to address the current limitations appropriately.

Acknowledgment

This work was supported/funded by the Ministry of Higher Education under Fundamental Research Grant Scheme (FRGS/1/2021/ICT07/UTM/02/2).

References

[1] Papatsimouli, M., et al. Internet of things (IOT) awareness in Greece. in SHS Web of Conferences. 2022. EDP Sciences.

[2] Patton, M., et al. Uninvited connections: a study of vulnerable devices on the internet of things (IoT). in 2014 IEEE joint intelligence and security informatics conference. 2014. IEEE.

[3] Colakovic, A. and M. Hadzialic, Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. Computer networks, 2018. 144: p. 17-39.

[4] Alharbi, A., M.A. Hamid, and H. Lahza, Predicting Malicious Software in IoT Environment Based on Machine Learning and Data Mining Techniques. International Journal of Advanced Computer Science and Applications, 2022. 13(8).

[5] Asassfeh, M., N. Obeid, and W. Almobaideen, Anonymous authentication protocols for iot based-healthcare systems: a survey. International Journal of Communication Networks and Information Security, 2020. 12(3): p. 302-315.

[6] Alonazi, W.A., et al., SDN Architecture for Smart Homes Security with Machine Learning and Deep Learning. International Journal of Advanced Computer Science and Applications, 2022. 13(10).

[7] Fortinet. What Makes an IoT Device Vulnerable. 2023 [cited 2023 18 April]; Available from: https://www.fortinet.com/resources/cyberglossary/iot-device-vulnerabilities.

[8] Akhilesh, R., et al., Automated Penetration Testing Framework for Smart-Home-Based IoT Devices. Future Internet, 2022. 14(10): p. 276.

[9] Antonakakis, M., et al. Understanding the mirai botnet. in 26th {USENIX} security symposium ({USENIX} Security 17). 2017.

[10] Bing, K., et al. Design of an Internet of Things-based smart home system. in 2011 2nd International Conference on Intelligent Control and Information Processing. 2011. IEEE.

[11] Ghaffarianhoseini, A., et al., The essence of smart homes: Application of intelligent technologies towards smarter urban future, in Artificial intelligence: Concepts, methodologies, tools, and applications. 2017, IGI Global. p. 79-121.

[12] Gugueoth, V., et al., A review of IoT security and privacy using decentralized blockchain techniques. Computer Science Review, 2023. 50: p. 100585.

[13] Kaur, B., et al., Internet of Things (IoT) security dataset evolution: Challenges and future directions. Internet of Things, 2023. 22: p. 100780.

[14] Mocrii, D., Y. Chen, and P. Musilek, IoT-based smart homes: A review of system architecture, software, communications, privacy and security. Internet of Things, 2018. 1-2: p. 81-98.

[15] Yaacoub, J.-P., et al., Security analysis of drones systems: Attacks, limitations, and recommendations. Internet of Things, 2020. 11: p. 100218.

[16] Radoglou Grammatikis, P.I., P.G. Sarigiannidis, and I.D. Moscholios, Securing the Internet of Things: Challenges, threats and solutions. Internet of Things, 2019. 5: p. 41-70.

[17] Malhotra, P., et al., Internet of things: Evolution, concerns and security challenges. Sensors, 2021. 21(5): p. 1809.

[18] Abed, A.K. and A. Anupam, Review of security issues in Internet of Things and artificial intelligence - driven solutions. Security and Privacy, 2022: p. e285.

[19] Azrour, M., et al., Internet of things security: challenges and key issues. Security and Communication Networks, 2021. 2021: p. 1-11.

[20] Zhu, S., et al., Survey of testing methods and testbed development concerning Internet of Things. Wireless Personal Communications, 2022: p. 1-30.

[21] Hassija, V., et al., A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access, 2019. 7: p. 82721-82743.

[22] Khan, Y., et al., Architectural Threats to Security and Privacy: A Challenge for Internet of Things (IoT) Applications. Electronics, 2022. 12(1): p. 88.

[23] Al-Dweik, A., et al. IoT-based multifunctional scalable real-time enhanced road side unit for intelligent transportation systems. in 2017 IEEE 30th Canadian conference on electrical and computer engineering (CCECE). 2017. IEEE.

[24] Messaoud, S., et al., Machine learning modelling-powered IoT systems for smart applications, in IoT-based Intelligent Modelling for Environmental and Ecological Engineering: IoT Next Generation EcoAgro Systems. 2021, Springer. p. 185-212.

[25] Zhang, X. and Y. Wang, Research on intelligent medical big data system based on Hadoop and blockchain. EURASIP Journal on Wireless Communications and Networking, 2021. 2021(1): p. 1-21.

[26] Gou, Q., et al. Construction and strategies in IoT security system. in 2013 IEEE international conference on green computing and communications and IEEE internet of things and IEEE cyber, physical and social computing. 2013. IEEE.

[27] Li, S., Security Architecture in the Internet. Securing the Internet of Things, 2017: p. 27.

[28] Sethi, P. and S.R. Sarangi, Internet of things: architectures, protocols, and applications. Journal of Electrical and Computer Engineering, 2017. 2017.

[29] Hassan, W.H., Current research on Internet of Things (IoT) security: A survey. Computer networks, 2019. 148: p. 283-294.

[30] Bujari, A., et al., Standards, security and business models: key challenges for the IoT scenario. Mobile Networks and Applications, 2018. 23: p. 147-154.

[31] Zhang, J., et al. The current research of IoT security. in 2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC). 2019. IEEE.

[32] Stallings, W., The internet of things: network and security architecture. Internet Protoc. J, 2015. 18(4): p. 2-24.

[33] Schiller, E., et al., Landscape of IoT security. Computer Science Review, 2022. 44: p. 100467.

[34] Stiller, B., et al., An overview of network communication technologies for IoT. Handbook of Internet-of-Things, 2020. 12.

[35] Ghafur, S., et al., A retrospective impact analysis of the WannaCry cyberattack on the NHS. NPJ digital medicine, 2019. 2(1): p. 98.

[36] Rajendran, G., et al. Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures. in 2019 International Carnahan Conference on Security Technology (ICCST). 2019. IEEE.

[37] Chen, H., et al., IoTCID: A Dynamic Detection Technology for Command Injection Vulnerabilities in IoT Devices. International Journal of Advanced Computer Science and Applications, 2022. 13(10).

[38] Karale, A., The challenges of IoT addressing security, ethics, privacy, and laws. Internet of Things, 2021. 15: p. 100420.

[39] Ahemd, M.M., M.A. Shah, and A. Wahid. IoT security: A layered approach for attacks & defenses. in 2017 international conference on Communication Technologies (ComTech). 2017. IEEE.

[40] Alam, M., M.M. Tehranipoor, and U. Guin, TSensors vision, infrastructure and security challenges in trillion sensor era: Current trends and future directions. Journal of Hardware and Systems Security, 2017. 1: p. 311-327.

[41] Kim, J., C. Yang, and J. Jeon. A research on issues related to RFID security and privacy. in Integration and Innovation Orient to E-Society Volume 2: Seventh IFIP International Conference on e-Business, e-Services, and e-Society (13E2007), October 10–12, Wuhan, China. 2007. Springer.

[42] Peris-Lopez, P., et al. RFID systems: A survey on security threats and proposed solutions. in Personal Wireless Communications: IFIP TC6 11th International Conference, PWC 2006, Albacete, Spain, September 20-22, 2006. Proceedings 11. 2006. Springer.

[43] Tewari, A. and B.B. Gupta, Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Future generation computer systems, 2020. 108: p. 909-920.

[44] Baho, S.A. and J. Abawajy, Analysis of Consumer IoT Device Vulnerability Quantification Frameworks. Electronics, 2023. 12(5): p. 1176.

[45] Neto, E.C.P., et al., A review of Machine Learning (ML)-based IoT security in healthcare: A dataset perspective. Computer Communications, 2023.

[46] Costin, A., A. Zarras, and A. Francillon. Automated dynamic firmware analysis at scale: a case study on embedded web interfaces. in Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. 2016.

[47] Sharma, V., et al., A framework for mitigating zero-day attacks in IoT. arXiv preprint arXiv:1804.05549, 2018.

[48] Costin, A., et al. A large-scale analysis of the security of embedded firmwares. in 23rd {USENIX} Security Symposium ({USENIX} Security 14). 2014.

[49] Zhao, B., et al., A large-scale empirical study on the vulnerability of deployed iot devices. IEEE Transactions on Dependable and Secure Computing, 2022. 19(3): p. 1826-1840.

[50] Deogirikar, J. and A. Vidhate. Security attacks in IoT: A survey. in 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). 2017. IEEE.

[51] Suren, E., et al., PatrIoT: practical and agile threat research for IoT. International Journal of Information Security, 2023. 22(1): p. 213-233.

[52] VARIoT. VARIoT IoT vulnerabilities database. 2023 [cited 2023 28 May 2023].

[53] (NVD), N.V.D. National Vulnerability Database. 2023 [cited 2023 28 May 2023]; Available from: https://nvd.nist.gov/vuln/search.

[54] Janiszewski, M., et al., Automatic actionable information processing and trust management towards safer internet of things. Sensors, 2021. 21(13): p. 4359.

[55] Leyden, J. IoT Vendors Faulted For Slow Progress In Setting Up Vulnerability Disclosure Programs. 2023 [cited 2023 18 April]; Available from: https://portswigger.net/daily-swig/iot-vendors-faulted-for-slow-progress-in-setting-up-vulnerability-disclosure-programs.

[56] Kaspersky. 43% of businesses don't protect their full IoT suite. 2023 [cited 2023 18 April]; Available from: https://www.kaspersky.com/about/press-releases/2022_43-of-businesses-dont-protect-their-full-iot-suite.

[57] Barracuda. Why IoT is important. 2022 [cited 2023 18 April]; Available from: https://www.barracuda.com/support/glossary/iot-security.

[58] Smith, C. Lack of Transport Encryption–OWASP. 15 April 2023]; Available from: https://wiki.owasp.org/index.php/Top_10_2014-I4_Lack_of_Transport_Encryption.

[59] Costa, L., J.P. Barros, and M. Tavares. Vulnerabilities in IoT devices for smart home environment. in Proceedings of the 5th International Conference on Information Systems Security e Privacy, ICISSP 2019. 2019. SciTePress.

[60] Smith, C. Top 10 2014-I3 Insecure Network Services–OWASP. 15 April 2023]; Available from: https://wiki.owasp.org/index.php/Top_10_2014-I3_Insecure_Network_Services.

[61] Alshammari, T.M. and F.M. Alserhani, Scalable and Robust Intrusion Detection System to Secure the IoT Environments using Software Defined Networks (SDN) Enabled Architecture. International Journal of Computer Networks and Applications (IJCNA), 2022. 9(6).

[62] Lu, Y. and L. Da Xu, Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 2018. 6(2): p. 2103-2115.

[63] Sarker, I.H., et al., Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. Mobile Networks and Applications, 2022: p. 1-17.

[64] Alashhab, A.A., et al., Low-rate DDoS attack Detection using Deep Learning for SDN-enabled IoT Networks. International Journal of Advanced Computer Science and Applications, 2022. 13(11).

[65] An, G.H. and T.H. Cho, Improving Sinkhole Attack Detection Rate through Knowledge-Based Specification Rule for a Sinkhole Attack Intrusion Detection Technique of IoT. International Journal of Computer Networks and Applications (IJCNA), 2022. 9(2).

[66] Malkawi, O., N. Obaid, and W. Almobaideen, Toward an Ontological Cyberattack Framework to Secure Smart Cities with Machine Learning Support. International Journal of Advanced Computer Science and Applications, 2022. 13(11).

[67] Keshri, A. Top 5 Penetration Testing Methodologies and Standards. 2023 [cited 2023 13 May 2023]; Available from: https://www.getastra.com/blog/security-audit/penetration-testing-methodology/.

[68] Abdalla, P.A. and C. Varol. Testing IoT security: The case study of an ip camera. in 2020 8th International Symposium on Digital Forensics and Security (ISDFS). 2020. IEEE.

[69] Rak, M., G. Salzillo, and C. Romeo. Systematic IoT Penetration Testing: Alexa Case Study. in ITASEC. 2020.

[70] Bella, G., et al., PETIoT: PEnetration Testing the Internet of Things. Internet of Things, 2023. 22: p. 100707.

[71] Heiding, F., et al., Penetration testing of connected households. Computers & Security, 2023. 126: p. 103067.

[72] Faeroy, F.L., et al., Automatic Verification and Execution of Cyber Attack on IoT Devices. Sensors, 2023. 23(2): p. 733.

[73] Rak, M., G. Salzillo, and D. Granata, ESSecA: An automated expert system for threat modelling and penetration testing for IoT ecosystems. Computers and Electrical Engineering, 2022. 99: p. 107721.

[74] Casola, V., et al. Towards automated penetration testing for cloud applications. in 2018 IEEE 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE). 2018. IEEE.

[75] Ficco, M., et al. Threat modeling of edge-based IoT applications. in Quality of Information and Communications Technology: 14th International Conference, QUATIC 2021, Algarve, Portugal, September 8–11, 2021, Proceedings 14. 2021. Springer.

[76] Granata, D., et al. Security in IoT Pairing & Authentication protocols, a Threat Model, a Case Study Analysis. in ITASEC. 2021.

[77] Yadav, G., et al. Iot-pen: A penetration testing framework for iot. in 2020 International Conference on Information Networking (ICOIN). 2020. IEEE.

[78] Valente, J., M.A. Wynn, and A.A. Cardenas, Stealing, spying, and abusing: Consequences of attacks on internet of things devices. IEEE Security & Privacy, 2019. 17(5): p. 10-21.

[79] Williams, R., et al. Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach. in 2017 IEEE International Conference on Intelligence and Security Informatics (ISI). 2017. IEEE.

[80] Anitha, A.A. and L. Arockiam, A review on intrusion detection systems to secure IoT networks. International Journal of Computer Networks and Applications, 2022. 9(1): p. 38-50.

[81] Bhavadharini, R.M., et al., Wireless networking performance in IoT using adaptive contention window. Wireless Communications and Mobile Computing, 2018. 2018.

[82] Othman, T.S., K.R. KOY45, and S.M. Abdullah, Intrusion Detection Systems for IoT Attack Detection and Identification Using Intelligent Techniques. International Journal of Computer Networks and Applications (IJCNA), 2023. 5: p. 6.

[83] Pawar, R.S. and D.R. Kalbande, Privacy-Preserving Mechanism to Secure IoT-Enabled Smart Healthcare System in the Wireless Body Area Network. International Journal of Computer Networks and Applications (IJCNA), 2022. 9(6): p. 746-760.

[84] Zimaboard. ZimaBoard - Single Board Server for Creators. 2023 [cited 2023 4 May 2023].

[85] Nvidia. Jetson Modules. 2023 [cited 2023 4 May 2023]; Available from: https://developer.nvidia.com/embedded/jetson-modules.

[86] Jain, B., et al., A cross layer protocol for traffic management in Social Internet of Vehicles. Future Generation computer systems, 2018. 82: p. 707-714.

[87] Khedekar, D.C., et al., Home automation−a fast - expanding market. Thunderbird International Business Review, 2017. 59(1): p. 79-91.

[88] Suresh, S.A. and R.J. Priyadarsini, Design of Maintaining Data Security on IoT Data Transferred Through IoT Gateway System to Cloud Storage. International Journal of Computer Networks and Applications (IJCNA), 2022.

[89] Mozaffari-Kermani, M. and A. Reyhani-Masoleh. A low-cost S-box for the Advanced Encryption Standard using normal basis. in 2009 IEEE International Conference on Electro/Information Technology. 2009.

[90] Mozaffari-Kermani, M. and R. Azarderakhsh. Reliable hash trees for post-quantum stateless cryptographic hash-based signatures. in 2015 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS). 2015. IEEE.

[91] Choo, K.-K.R., et al., Emerging embedded and cyber physical system security challesnges and innovations. IEEE Transactions on Dependable and Secure Computing, 2017. 14(3): p. 235-236.