Date of publication JUN-30, 2023, date of current version NOV-23, 2022.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.22.2.3084

A Study on Internet of Things Devices Vulnerabilities using Shodan

RAJASEKAR V.R[1], RAJKUMAR S[2]

[1]School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India, rajasekarv.r2017@vitstudent.ac.in
[2]School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India, rajkumars@vit.ac.in

Corresponding author: Rajasekar V.R, Rajkumar S (e-mail: rajasekarv.r2017@vitstudent.ac.in, rajkumars@vit.ac.in)

ABSTRACT IoT has attracted a diverse range of applications due to its adaptability, flexibility, and scalability. However, the most significant barriers to IoT adoption are security, privacy, interoperability, and a lack of standards. Due to the persistent online connectivity and lack of security measures, adversaries can quickly attack IoT systems for various adversarial operations, financial gain, and access to sensitive data. We conducted a massive vulnerability scan on IoT devices using Shodan, the IoT search engine. The discovered vulnerabilities are analyzed using the Octave Allegro risk assessment method to determine the risk level (Critical, High, Moderate, Low, None), and the results are classified based on the vulnerabilities. The research findings are intriguing, shocking, and alarming, revealing the bitter reality that IoT devices are rapidly increasing while simultaneously eroding users' privacy on a never-before-seen scale. Our search discovered 13,558 webcams with outdated components, 11,090 devices disclosing NAT-PMP information, and 16,356 connected devices responding to remote telnet access. Around 2,456 IoT devices were found with the Heartbleed vulnerability, 674 with the Ticketbleed vulnerability, and 9,241 with expired SSL certificates. Nearly 18,638 IoT consumer devices are configured with insecure default settings; 11,481 devices with default SNMP agent community names; 4,987 devices running on non-standard ports; and 4,425 Cisco devices are configured with generic or default passwords.

KEYWORDS Internet of Things; Vulnerability assessment; Risk Analysis; Shodan; Octave Allegro; CVE.

I. INTRODUCTION

KEVIN Ashton coined the term "Internet of Things" in 1990 [1] to refer to RFID-tagged items that are electronically identifiable, trackable, and capable of Internet interaction. The Massachusetts Institute of Technology (MIT) presented an IoT vision in 2001 [2], and the International Telecommunication Union (ITU) formally established the IoT in 2005 [3]. The European Research Cluster on the Internet of Things (IERC) defines the IoT as "a dynamic global network infrastructure with self-configuring capabilities based on standards and communication protocols, in which physical and virtual things have identities, physical attributes, virtual personalities, and communicate intelligently" [4]. The IoT, a novel paradigm, rapidly absorbed modern wireless telecommunications and profoundly influenced numerous facets of human life, including smart assistants, smart vehicles, smart homes, smart environments, smart retail, smart agriculture, smart cities, smart transportation, smart healthcare, smart industry, and smart wearables. Researchers' forecasts vary significantly, with a low estimate of 20 billion and a high estimate of 125 billion connected devices by the end of 2030. According to the US's National Intelligence Council (NIC) [5], Internet nodes will be embedded in everyday objects such as food packaging, furniture, and paper documents by 2025. IHS Markit [6] predicted that there would be about 125 billion connected devices by the end of 2030, and Gartner [7] of the US predicted that there would be about 20.4 billion connected devices by the end of 2020, too. The global IoT market will be approximately US $193.60 billion in 2020 and reach the US $657.31 billion by 2025 [8]. According to Fortune business insights [9], the global IoT market was valued at US $190.0 billion in 2018 and is expected to grow to the US $1,102.6 billion by 2026. According to a McKinsey Global Institute report, the economic impact of IoT applications could range between US $3.9 and 11.1 trillion annually in 2025 [10]. Due to the proliferation of Internet-connected devices and IoT infrastructure over the last few years, the frequency and size of DDoS attacks via IoT botnets have increased significantly [11, 12]. Due to the low level of human interaction with IoT devices, severe security and privacy issues arise, such as device tracking and data collection [13, 14].

Due to resource constraints such as limited battery life, processing, and storage capabilities, the online use of traditional Internet protocols, reduced packet size, and device efficiency in terms of quality and security are challenging

[15]. Given the societal impact of IoT device vulnerabilities, this study aims to determine the most vulnerable category of IoT devices, the most frequently exploited vulnerability in IoT devices, and the associated risk level. The remainder of this paper is organized as follows: Section 2 discusses the preliminary study, which includes IoT components vulnerability model, attacks on IoT devices, and the Shodan search engine; Section 3 discusses related works in the domain of IoT device vulnerability assessment; Section 4 discusses the research methodology used in this work; Section 5 discusses the Octave Allegro risk assessment methodology; Section 6 discusses the results and observations of our study, and Section 7 concludes the paper with recommendations.

II. PRELIMINARY STUDY

A. IoT COMPONENTS VULNERABILITY MODEL

As depicted in Figure 1, a typical IoT System comprises seven interconnected components to form a complete system. Every component has its functionality and contribution, and at the same time, every component has its vulnerability. This section describes the functionality of every component of an IoT system and the associated vulnerabilities.

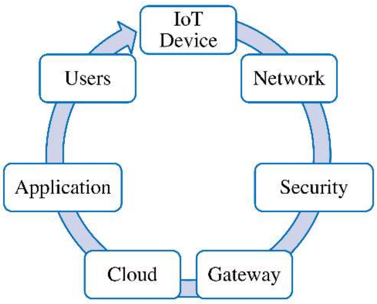

Figure 1. IoT Components

a. IoT devices

IoT devices comprise the layer of sensors, actuators, and smart objects that measure environmental data and physical characteristics. Common IoT device vulnerabilities and threats are outlined in Table 1.

b. Network

The network component transfers data collected by IoT devices to the gateway via the Internet, mobile communication networks, satellite networks, and wireless sensor networks. The most prevalent network vulnerabilities and threats are described in Table 1.

c. Security

Security comprises all elements that guarantee data transfer security, prevent illegal access, and regulate access. Common security weaknesses and attacks are outlined in Table 1.

d. Gateway

An IoT gateway is a physical or virtual platform that acts as an intermediate between IoT devices and the Cloud to ensure controlled data flow and security, order transfer, data preprocessing, energy savings, and latency reduction. In IoT environments, the devices and gateway are susceptible to the threat vectors indicated in Table 1.

e. The Cloud

A cloud is a data storage, in-depth analysis, and management resource. The Cloud is where much sensor data is turned into useful information. The Cloud can be equipped with analytics software, visualization tools, artificial intelligence (AI), and machine learning for in-depth data analysis and processing. Common Cloud-related vulnerabilities and attacks are listed in Table 1.

f. Application

An application is the user interface for IoT technology. Users may monitor analytics and statistics, manage devices, and operate the system. Common application vulnerabilities and exploits are outlined in Table 1.

g. Users

Users, who utilize the IoT system for their reasons and comfort, are a crucial component. Table 1 lists common vulnerabilities and threats connected to users.

Table 1. IoT Components vulnerabilities

Component	Vulnerability	Description
Devices	Node capture	An unauthorized user seizes and completely controls a node.
	Fake node	Attacker creates a fictitious node, inserts and prevents the sending data.
	Cloning of things	Introducing fake objects based on the physical features of the authentic node.
	Malicious substitutions	Installing a product of inferior quality which is vulnerable will be a honeypot.
	Tracking Objects	Extracts of information from obtained data, thereby collecting user behavior patterns.
Network	Eavesdropping	An adversary intercepts, changes, or deletes data exchanged between two devices.
	Man in the Middle Attack	An attacker intercepts and relays communications between two parties that believe they are communicating directly.
	Meet-in-the-middle	Cryptographic space-time tradeoff attack against encryption techniques.
	Identity theft	Using someone else's identity to gain unauthorized access to system resources.
	Denial of Service attack	An attack is intended to render a system or network inaccessible to its intended users.
	Bluesnarfing	Theft of information from a Bluetooth-connected wireless device.
	Bluejacking	Sending unwanted Bluetooth messages to Bluetooth-capable devices.
	Replay Attacks	Valid data transmission is repeated or delayed deliberately or fraudulently.
	Routing Attacks	Spoofing, modifying or replaying routing information.
Security	Access Management	User access to the IoT network; authentication difficulties are severe.
	Data Breaches	Data can be accessed since stored in an insecure or unencrypted format.
	Malicious software	Utilization of flawed, unpatched, and updated software.
Gateway	Spoofing	Impersonating another person can be used for many attacks.
	Denial-of-Service	To render a machine or network unreachable to its intended users.
	Tampering	Manipulate memory/computing and gather further knowledge via interaction.
	Data theft	The illicit transfer of personal, confidential, or financial information.
	Privilege Escalation	Occurs when an application acquires access to rights it should not have.
Cloud	Cloud Misconfiguration	Misconfiguration can open the door for data exfiltration and unwanted access.
	Unsecure community	Lacks secure connectivity, access restrictions, and integrity of data.

	Misapplication of Cloud	Results in brute-force attacks, trojans, SQL injections, botnets, and phishing.
Application	Password Vulnerability	Use of default passwords, which are easily guessed and readily available.
	Lack of updates	Excluding the update process for operational reasons.
	Unprotected IoS	Applications with inherent vulnerabilities owing to poor coding and design.
	Insecure or obsolete app components	Utilization of insecure and untested frameworks and libraries from a third party.
	Unprotected data storage	Secure data transfer, such as TLS/SSL, is lacking in IoT applications and protocols.
Users	Lack of Updates	Inability to update, firmware validation, secure delivery & anti-rollback.
	Lack of device management	Asset management, update management, secure decommissioning, system monitoring, and response capabilities.
	Weak passwords	Credentials that are quickly brute forced, publicly available, or unchangeable.
	Insufficient privacy	Personal information stored on the device is utilized insecurely and inappropriately.

B. ATTACKS ON IoT DEVICES

The primary reasons for attacks on interconnected things and devices are an insecure web interface, misconfiguration, insufficient authentication, ignoring security patches, vulnerable software, expensive security controls [16], insecure network services, and device availability [17]. Existing IoT security mechanisms are primarily concerned with data protection and access control, adequately not addressing real-world issues such as tracking, profiling, leakage, accountability, responsibility, and privacy [14,18]. In 2011, University of Washington researchers attacked a car's Bluetooth system, allowing the driver to make hands-free phone calls [19]. In 2013, over 1.2 billion Internet-connected devices were tracked, with an average of 300 million new scan probes added each month [20]. In 2015, attackers took down Sony Pictures' gaming consoles, televisions, and smartphones [21]. In the same year, Internet-connected embedded devices such as CCTV cameras were hacked and used to launch a DDoS attack against the IoT infrastructure [22]. Hackers took complete control of a Jeep SUV [23] in the Jeep Hack (2015) by exploiting a firmware vulnerability in the IoT-connected CAN bus and controlling the air conditioning, radio, and windshield wipers, as well as deactivating the ignition system. The well-known IoT botnet attack, the "Mirai attack (2016)" [24], took control of significant websites via a massive DDOS attack utilizing hundreds of thousands of compromised IoT devices such as home routers, air-quality monitors, and personal surveillance cameras. The attack infected over 600,000 vulnerable IoT devices. In 2017, hackers breached a fish tank at a North American casino, attacked the network, gathered sensitive data, and transferred it to Finland [25]. In 2017, the security flaw known as "Devil's Ivy" granted attackers complete remote access to the IoT devices of twenty-four large companies, including Bosch, Canon, Cisco, D-Link, Fortinet, Hitachi, Honeywell, Huawei, Mitsubishi, Netgear, Panasonic, Sharp, Siemens, Sony, and Toshiba [26-28].

C. SHODAN SEARCH ENGINE

In 2009, programmer John Matherly created "Shodan.io," a search engine for the IoT [29], a popular tool for unauthorized surveillance [29], which focuses on locating and exploiting IoT device vulnerabilities. Shodan can see an infinite number of accessories; it aggregates over 3.7 billion public IPv4 addresses and hundreds of millions of IPv6 addresses to discover vulnerabilities [30]. Shodan [29] enables the search for IoT devices by specifying their type, location, and various other parameters, returning graphical results that include the IP address, location, open ports, and credentials of the IoT devices. Shodan's internet-wide port scanner probes devices' ports, captures the resulting banners, indexes the corresponding public IP address, and stores the results in an interim database for future lookups. Shodan [31] has been a dependable tool for IoT researchers and security professionals to determine the type of devices on the Internet. Shodan's database aids device discovery by providing necessary information [32], enabling users to discover devices connected to the Web via various channels, including administration flags [33-36]. Shodan monitors Web servers, HTTP (80), FTP (21), SSH (22), Telnet (23), SNMP (161), and Taste (5060) administrations. Shodan's results are excessively numerous, potentially irrelevant (i.e., obsolete, non-specific, and incomplete), challenging to comprehend, and require efficient interpretation.

III. RELATED WORKS

This research is based on the literature review in three key areas: IoT devices, vulnerabilities, and vulnerability assessment. Allen-Bradley discovered four honeypots in 2014 while tracking ICS devices for the US Military exposed to Shodan [29]. Later that year, Bodenheim et al. [35] investigated Shodan's SCADA capabilities and concluded that Shodan poses a threat to Internet-connected things. Markowsky et al. [36] demonstrated in 2015 that the Internet of Things (IoT) is naturally reachable via Shodan, and Patton et al. [37] investigated several emerging IoT vulnerabilities in mid-2017. In 2018, Samtani et al. used Shodan to scan and identify over half a million devices, of which tens of thousands had critical flaws. OCTAVE [38] is a mechanism for discovering and assessing vulnerabilities to information security. In 1999, the Software Engineering Institute (SEI) at Carnegie Mellon University published the conceptual framework that formed the foundation of the original OCTAVE technique. Since its initial release in September 1999, the OCTAVE approach has undergone numerous revisions and modifications [38]. OCTAVE Allegro [39, 40] is a version of the OCTAVE approach, which is a comprehensive evaluation of an organization's operational risk environment that yields improved results without requiring extensive risk assessment experience. In [41], the authors utilized the OCTAVE allegro methodology to identify risks in the fleet management system (FMS), identified and ranked the risks to be mitigated, presented mitigation recommendations, and demonstrated the solution's effectiveness. In [42], the authors utilized the OCTAVE allegro approach to evaluate the information system risk at the ed-tech organization to determine the risk mitigation priorities. In [43], the authors established a risk assessment model for universities based on OCTAVE allegro, assessed and evaluated the risk in Higher education Institutes, measured the risk severity, estimated the risk acceptance threshold, and enhanced risk management decision-making. The above facts, vulnerabilities in IoT devices, the significance of the Shodan search engine, and the effectiveness of the OCTAVE Allegro risk assessment methodology urged us to combine all three aspects and execute a massive vulnerability scan on connected IoT devices.

IV. RESEARCH METHODOLOGY

Indeed, the steadily increasing number of connected things and the plethora of potential vulnerabilities afflicting the devices compel the researcher community to regularly conduct large-scale IoT vulnerability assessments. To address this gap, we pose the following research questions:

1. *Which categories of IoT devices are most vulnerable?*
2. *What are the most frequently exploited vulnerabilities in IoT devices?*
3. *What is the risk level associated with the vulnerabilities?*

The methodology adopted to address the research questions consists of three key steps:

1. *Footprinting/identification of IoT devices*
2. *Risk identification*
3. *OCTAVE Allegro based risk assessment*

The IoT device footprinting phase is depicted in Figure 2, in which the Shodan search engine is used to locate IoT devices using various keywords.

IoT Devices Search
Shodan.io
IoT Devices footprinting

Figure 2. IoT device footprinting

After identifying the devices, we manually examined each device for available risks. Our search was concentrated on eight distinct areas, including outdated components, the use of an insecure protocol, the execution of an insecure protocol, the execution of insecure network services, software vulnerability in the devices, insecure default settings in the devices, services running on non-standard ports, the device running with default credentials, and the devices with default operating system credentials. After identifying the impact area and the risks associated with each area, we used the OCTAVE ALLEGRO risk assessment methodology to assess the identified risk. The phases and steps of OCTAVE ALLEGRO are depicted in Figure 3, and the approach is detailed in Section V.

V. OCTAVE ALLEGRO RISK ASSESSMENT

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a technique for identifying and assessing information security issues [40]. The purpose of OCTAVE is to assist the organization in developing qualitative risk evaluation criteria that describe the company's operational risk tolerance, identifying the assets that are crucial to the organization's mission, identifying vulnerabilities and threats to those assets, and determining and evaluating the potential consequences for the organization if the threat is materialized [40]. OCTAVE Allegro is a variation of the OCTAVE approach, a complete assessment of the organization operational risk environment that produces improved outcomes without requiring substantial expertise in risk assessment [40].

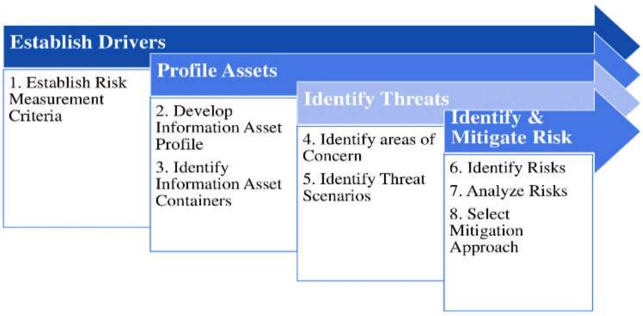
Establish Drivers
1. Establish Risk Measurement Criteria
Profile Assets
2. Develop Information Asset Profile
3. Identify Information Asset Containers
Identify Threats
4. Identify areas of Concern
5. Identify Threat Scenarios
Identify & Mitigate Risk
6. Identify Risks
7. Analyze Risks
8. Select Mitigation Approach

Figure 3. OCTAVE Allegro Phases and Steps

OCTAVE Allegro focuses on information assets in the context of how they are utilized, where they are kept, delivered, and processed, and how they are impacted by risk, vulnerability, and disruption. Four essential OCTAVE Allegro processes are: 1. Establish Drivers 2. Profile assets 3. Identify Threats 4. Identify and mitigate risk. As demonstrated in Figure 5, OCTAVE Allegro has eight distinct steps over its four levels.

A. ESTABLISHING DRIVERS

Step 1: Establishing Risk Measurement Criteria

The principal objective of this step is to identify the most significant impact areas. We identified eight impact areas based on the top IoT vulnerabilities identified by OWASP. We ranked each impact area according to its frequency of appearance in Shodan searches. Column 1 (impact area) in Table 2 depicts the impact area identified for this work.

B. PROFILE ASSETS

Step 2: Developing Information Asset Profile

We developed four categories of profiles, communication, configuration, hardware, and software because these are the four essential components of an IoT network. Column 2 (assets profile) in Table 2 depicts the asset profiles identified for this work.

Step 3: Identifying Information Assets Containers

Identification of the information asset container is divided into two, namely technical and non-technical, with an external and an internal side for each. Column 3 (assets containers) in Table 2 depicts the asset containers identified for this work.

Table 2. Establishing drivers and profile assets

Impact Area	Assets Profile	Assets Container
Insecure Network Services	Communication	Technical
Services running in non-standard ports	Communication	Technical
Insecure Default Settings	Configuration	Non-Technical
Device default credentials	Configuration	Non-Technical
Outdated Components	Hardware	Technical
Insecure Protocol	Software	Technical
Software Vulnerability	Software	Technical
Operating System Credentials	Software	Non-Technical

C. IDENTIFYING THREATS

Step 4: Identifying Areas of Concern

Identify areas of concern by reviewing each container to see and determine potential areas and continue by documenting each identified area of concern. Areas of concern are extended to get threat scenarios and then document them to see if they affect security requirements. Table 3 shows the identified areas of concern for each impact area.

Table 3. Impact area and area of concern

Impact Area	Area of Concern
A. Insecure Network Services	Unauthorized remote access and data leakage.
B. Services running in non-standard ports	Operating a well-known service from a non-standard port Remaining anonymous False sense of security
C. Insecure Default Settings	Vulnerabilities in the system's default settings Vulnerable generic protocols
D. Device default credentials	Usage of weak default passwords Prohibits users from changing the default password Users prefer not to change passwords
E. Outdated Components	Devices that cannot update securely Lack of firmware validation Transmit data in an unencrypted format Lack of anti-rollback procedures Security update warnings
F. Insecure Protocol	Usage of protocols without security features Usage of protocols which are outdated
G. Software Vulnerability	Flaw in software Flaws due to software design or coding
H. Operating System Credentials	The use of insecure default passwords Disallows users to modify the default password Users would rather not update their passwords

Step 5: Identifying Threat Scenarios

When identifying a threat scenario, the threat characteristics, actors, means, goals, outcomes, and security requirements of the area of concern having been identified in step 4, are described. Instead of providing the threat scenario for all the areas of concern, we provided the threat scenario for only one area of concern in Table 4.

Table 4. Threat Scenario - Example

Impact Area	Area of Concern
Insecure Network Services	Unauthorized remote access and data leakage.
Actor	External User
Means	Through the external connection (Internet)
Goal	Unauthorized access to the device, data, and network.
Outcomes	Data Leakage, loss of confidentiality, availability, and integrity
Security Requirements	System which blocks the unauthorized users

D. IDENTIFYING AND MITIGATING RISK

Step 6: Identifying Risks

In this step, the risks associated with each impact area are identified. Each area has been assigned a priority value and grouped into four impact categories: critical, high, moderate, and low. An impact value is assigned to each category within the range of 1 to 4. Table 5 displays identified risks for each impact area, along with their assigned priority ratings and corresponding impacts. The Risk score (rs) is computed using the equation (1).

$$risk\_score = (priority\_value * impact\_value) \quad (1)$$

Table 5. Identifying Risk and Risk Score

IA	PV	Risks	Impact Value				RS
			C	H	M	L	
A	1	MiniUPnPd Version 1.0	4				4
		MiniUPnPd Version 1.2	4				4
		MiniUPnPd Version 1.4		3			3
		MiniUPnPd Version 1.6			2		2
		MiniUPnPd Version >1.6				1	1
B	2	Malicious port mapping (E)	4				8
		NAT-PMP Information (D)		3			6
C	3	Unencrypted Service	4				12
		Bluekeep	4				12
		SMB Version 1		3			9
D	4	Heartbleed	4				16
		Ticketbleed	4				16
		Expired SSL Certificates		3			12
E	5	SNMP Agent default community names		3			15
		SNMP Agent default community (Public)			2		10
F	6	MQTT			2		12
		CoAP			2		12
		AMQP			2		12
		XMPP			2		12
G	7	Router (OpenWRT)				1	7
		CISCO last-modified			2		14
		CISCO VPN Concentrator		3			21
		Router (Netgear)			2		14
H	8	CentOS		3			24
		RedHat		3			24
		Windows	4				32
		Fedora		3			24
		Ubuntu		3			24

IA: Impact Area, PV: Priority Value, C: Critical, H: High, M: Medium, L: Low, RS: Risk Score

Step 7: Analyzing Risk

a. Outdated Components

Outdated IoT components include devices that cannot update securely, lack firmware validation, transmit data in an unencrypted format, lack anti-rollback procedures, and security update warnings. The use of third-party hardware or software carries dangers and endangers the overall system's security. Vulnerabilities in outdated components can be used to launch an attack and interrupt the device regular operation. This study considers the outdated versions of MiniUPnP [44] used in various connected consumer devices.

b. Insecure Network Services

Network services running on the device can jeopardize the system security and integrity. When an IoT device is connected to the Internet, it opens the door to unauthorized remote access and data leakage. By exploiting flaws in the network communication model, attackers can successfully compromise the security of an IoT endpoint. In this work, we examine the NAT-PMP mapping protocol [45] because it is primarily used to establish automatic NAT and port forwarding between consumer IoT devices. Insecure configuration and failure to enforce NAT-PMP restrictions create a high level of vulnerability, allowing an external attacker to gather additional information about the network.

c. Software Vulnerabilities

A software vulnerability is a flaw in software that enables an attacker to take control of the affected system. These flaws can occur due to the software design or a coding error. A software vulnerability can be used to steal or manipulate sensitive data, connect a system to a botnet, install a backdoor, or plant other types of malware. Additionally, once an attacker has gained access to one network host, he or she can use that host to gain access to other hosts on the same network. In this work, we searched for devices with Heartbleed [46], Ticketbleed [47], and expired SSL certificates in OpenSSL and TLS/SSL.

d. Insecure Default Settings

Vulnerabilities in the system's default settings expose it to various security risks, resulting from hardcoded passwords, inability to keep up with security updates, or outdated components. We considered SNMP a vulnerable generic protocol used by default in conventional IoT consumer devices to share community names and network-related information.

e. Services Running on Non-Standard Ports

Operating a well-known service from a non-standard port is an excellent approach to remain anonymous, which is often referred to as the concept of security by obscurity, and it is widely regarded as an ineffective and obsolete approach. The effect of remaining hidden may mislead the server/device operator into a false sense of security. We examined the IoT data protocols MQTT (1833), CoAP (5683), AMQP (5672), and XMPP (5222) that operate over non-standard ports in this study.

f. Device & OS Default Credential

Cyber-attacks are more likely to occur on IoT devices with weak default passwords. Manufacturers of IoT devices must pay close attention to password settings when launching the device [24]. Either the device prohibits users from changing the default password, or the users prefer not to change it even if they can. Additionally, successful attempts to gain unauthorized access to one device expose other devices in the system to risk as IoT devices frequently share default passwords.

VI. RESULTS AND DISCUSSION

The findings of this work are fascinating, shocking, and alarming, revealing the bitter reality that the number of IoT devices is rapidly increasing while simultaneously eroding users' privacy on a never-before-seen scale. Out of 210,125 scanned devices, 28,409 (13.52%) are vulnerable, with 3,623 (12.75%) devices at a critical risk level, 13,131 (46.22%) devices at a high-risk level, 8,964 (31.56%) devices at a medium-risk level, and 2,691 (9.47%) devices at a low-risk level. We will further classify our findings based on the vulnerabilities (risks) listed out in Table 2.

A. OUTDATED COMPONENTS

The most frequently exploited critical vulnerability in IoT consumer devices is outdated versions of MiniUPnP [44], which can be used in various ways, including launching DoS attacks. This vulnerability allows malware, trojans, or worms to bypass the router's firewall and infect connected devices. Our search discovered 13,558 webcams, the typical consumer IoT device; the results are analyzed and tabulated in Table 6 based on the MiniUPnPd version [44]. Out of 13,558 scanned webcams, 33.5% (4,542) of webcams continue to use MiniUPnPd 1.0 (*risk_score 4*), 36.5% (4,949) of webcams use MiniUPnPd 1.2 (*risk_score 4*), 11% (1,491) of webcams use MiniUPnPd 1.4 (*risk_score 3*), 11.5% (1,559) of webcams use MiniUPnPd 11.6 (*risk_score 2*), and 7.5% (1,017) are with MiniUPnPd > 1.6 (*risk_score 1*). The study shows that many webcams connected to the Internet are equipped with vulnerable, insecure, and out-of-date components.

Table 6. Outdated Components Analysis

Vulnerability Type	Vulnerability	# of devices	Percentile	Risk Level	RS
Use of outdated components	MiniUPnPd Version 1.0	4,542	33.5%	C	4
	MiniUPnPd Version 1.2	4,949	36.5%	H	4
Device Type Webcams	MiniUPnPd Version 1.4	1,491	11%	H	3
	MiniUPnPd Version 1.6	1,559	11.5%	M	2
	MiniUPnPd Version >1.6	1,017	7.5%	L	1

B. INSECURE PROTOCOL

The NAT-PMP mapping protocol (NAT-PMP) [45] is primarily used to establish automatic NAT and port forwarding among consumer IoT devices. Unsecured configuration and failure to enforce NAT-PMP restrictions result in a high level of vulnerability, allowing an external attacker to gain additional information about the network. The typical limits not configured in the NAT-PMP block mapping requests are sent to or received on the NAT gateway's external IP address or external network interface. Table 7 summarizes the number of webcams that responded to our external NAT-PMP probes for malicious port mapping manipulation and device disclosure. Almost 61.5% (8,338) of the 13,558 scanned internet-connected webcams responded to eternal NAT-PMP port mapping manipulation inquiries, and 81.8% (11,090) of the 13,558 devices disclosed information about the NAT-PMP.

Table 7. Insecure Protocol Analysis

Vulnerability Type	Vulnerability	# of devices	Percentile	Risk Level	RS
Use of insecure protocol	Malicious port mapping (External)	8,338	61.5%	C	8
Device Type Webcams	NAT-PMP Information disclosure	11,090	81.8%	H	6

C. INSECURE NETWORK SERVICES

Our search was widened to include IoT devices that support industry-standard network protocols such as Telnet [48], FTP [49], RDP [50], and SMB [51]. Telnet and FTP are well-known for their unencrypted data transmission vulnerabilities, making them vulnerable to attacks such as brute force, bounce, and MITM attacks, resulting in the attacker's login credentials being outflowed. The RDP contains numerous vulnerabilities, the most recent is the BlueKeep vulnerability (2019). These flaws enable attackers to connect to RDP services to steal or modify data, install malware, or perform other malicious acts. Due to a critical vulnerability in the server message block (SMB) service, US-CERT [52] recommends blocking all SMB versions. Regrettably, many versions of Windows and other operating systems come with SMB enabled by default. Our search revealed 20,885 IoT devices configured to use insecure network services such as Telnet, FTP, Remote Desktop Protocol (Bluekeep), and SMB version 1 (Wannacry ransomware) [51]. Table 8 details the number of devices in each category and their associated risk levels. Approximately 78.31% (16,356) of the 20,885 scanned devices support telnet, 20.28% (4,236) support FTP, 0.75% (156) support RDP, and 0.65% (137) support SMB version 1.

Table 8. Insecure Network Services Analysis

Network Service	Vulner-ability	TCP port listening	# of devices	Percent.	Risk Level	RS
Telnet	Unencrypted Service	23/2323	16,356	78.31%	C	12
FTP	Unencrypted Service	21	4,236	20.28%	C	12
RDP	BlueKeep	3389	156	0.75%	C	12
SMB	SMB Version 1	139/445	137	0.65%	H	9

D. SOFTWARE VULNERABILITIES

Our search for devices with specific vulnerabilities, such as Heartbleed [46], Ticketbleed [47], and expired SSL certificates, was classified as software vulnerabilities in OpenSSL and TLS/SSL. Such exposures result in disclosing client information, passwords, and the server's private key. Heartbleed is a vulnerability in the widely used OpenSSL cryptographic software library that allows for data theft protected by SSL/TLS encryption. The Ticketbleed vulnerability in F5's BIG-IP appliances' TLS/SSL stack enables a remote attacker to extract up to 31 bytes of uninitialized memory at a time, which may contain sensitive data or key material from other connections. We found that about 2,456 IoT devices have the Heartbleed vulnerability, 674 have the Ticketbleed vulnerability, and almost 9,241 have expired SSL certificates, as shown in Table 9.

Table 9. Software Vulnerability Analysis

Vulnerability	# of devices	Risk Level	RS
Heartbleed	2,456	C	16
Ticketbleed	674	C	16
Expired SSL Certificates	9,241	H	12

E. INSECURE DEFAULT SETTINGS

The SNMP is a vulnerable generic protocol used in conventional IoT consumer devices to share self-information, such as default community names and network-related information. By correctly guessing the community names ('public' to read and 'private' to write), attackers can gain additional information about a device, such as its operating system, version, etc., and this allows the attacker to utilize the vulnerabilities to exploit and cause harm to the device and network. We concentrated on two standard consumer IoT devices: smart TVs and printers and analyzed SNMP agent default community names (Public and Privates). The number of devices discovered with the mentioned vulnerabilities is shown in Table 10. Our search discovered 18,638 IoT consumer devices with insecure default settings, which included 61.6% (11,481) with SNMP agent default community names (private) and 38.4% (7,157) with SNMP agent default community names (public).

Table 10. Insecure Default Settings Vulnerability Analysis

Vulnerability	Devices	# of devices	Risk Level	RS
SNMP Agent Default Community Names (Private)	Smart TV and Printers	11,481	H	15
SNMP Agent Default Community Name (Public)	Smart TV and Printers	7,157	M	10

F. SERVICES RUNNING ON NON-STANDARD PORTS

Running services on a non-standard port is a novel method of concealment, referred to as "security by obscurity," and is widely regarded as an ineffective and deprecated technique. Running the services might give the owner of the server/device a false sense of security. Our search for IoT data protocols (MQTT, CoAP, AMQP, and XMPP) that operate on non-standard ports included the terms "product: MQTT-port: 1833", "product: CoAP-port: 5683", "product: AMQP-port: 5672", and "product: XMPP-port: 5222". Our search identified 4,987 devices that were running services on non-standard ports, with 56.86% (2267) using the MQTT protocol, 31.25% (1246) using the CoAP protocol, 8.55% (341) using the AMQP protocol, and 3.33% (133) using the XMPP protocol; the risk level associated with each protocol is analyzed and tabulated in Table 11.

Table 11. Services running in non-standard ports.

IoT Data Protocols	Port Number	# of devices	Percentile	Risk Level	RS
MQTT	1833	2267	56.86%	M	12
CoAP	5683	1246	31.25%	M	12
AMQP	5672	341	8.55%	M	12
XMPP	5222	133	3.33%	M	12

G. DEVICE DEFAULT CREDENTIAL

The search for default credentials on internet-connected devices revealed an unpleasant truth: the IT community's information security awareness is still lacking. As shown in Table 12, our search identified nearly 4,914 vendor-based networking devices (CISCO, Netgear, and OpenWRT) that used default credentials, anonymous access, or generic credentials. The presence of around 4,425 Cisco devices identified as "Cisco, last modified" or "200 Cisco Last-Modified" indicates that Cisco devices do not require initial authentication; these conditions may indicate the use of generic or default passwords. 38 Cisco devices were discovered with Cisco VPN 3000 series concentrator vulnerabilities that allow remote attackers to generate a denial-of-service attack by flooding the SSL or telnet services with invalid login requests. Our search found almost 291 Netgear routers and 169 OpenWRT routers set up with default credentials.

Table 12. Device default Credentials

Vulnerability	# of devices	Percentile	Risk Level	RS
Cisco Last-Modified	4425	90.05%	M	14
CISCO VPN Concentrator	38	0.77%	H	21
Router (Netgear)	291	5.92%	M	14
Router (OpenWRT)	160	3.26%	L	7

H. OS DEFAULT CREDENTIAL

The Mirai botnet attack [24] highlighted the dangers of default passwords and how they add significant complexity to IoT systems. Our search uncovered 16,936 operating systems that included vendor-supplied passwords. An attacker can remotely access the device by utilizing a vendor-supplied default password, exposing sensitive business information. Table 13 shows the percentages of various devices with vendor-supplied passwords embedded in their operating systems. CentOS is the most popular operating system, accounting for 93.53% (15,840), with Ubuntu accounting for 3.87% (656), Fedora accounting for 2.03% (343), Windows accounting for 0.44% (75), and RedHat accounting for 0.13% (22).

Table 13. Operating System Credential Issues

Operating System	# of devices	Percentile	Risk Level	RS
CentOS	15840	93.53	H	24
RedHat	22	0.13	H	24
Windows	75	0.44	C	32
Fedora	343	2.03	H	24
Ubuntu	656	3.87	H	24

Step 8: Select Mitigation Approach

In this step, a suitable mitigation strategy must be chosen or proposed for each risk based on its risk score and its impact. This work's primary purpose is to reveal the number of internet-connected devices with various vulnerabilities and their impact. As this work focused on internet-connected devices used globally by various entities, adopting a specific risk mitigation strategy would not address the issue. In the following section, however, we provide recommendations for IoT stakeholders to defend their networks based on the findings of this study.

VII. CONCLUSIONS AND RECOMMENDATIONS

This study conducted a large-scale vulnerability scan to identify common security issues and vulnerabilities in connected IoT devices. The identified vulnerabilities are analyzed to determine the risk level. We discovered 13,558 webcams with outdated components such as MiniUPnPd, around 8,338 webcams connected to the Internet responded to persistent NAT-PMP port mapping manipulation queries, while 11,090 devices disclosed information about the NAT-PMP. Remote telnet access is supported on 16,356 scanned devices, FTP is supported on 4,236 devices, RDP is supported on 156 devices, and SMB version 1 is supported on 137 devices. Further, 2,456 IoT devices were discovered with Heartbleed vulnerable, 674 with Ticketbleed vulnerable, and 9,241 with expired SSL certificates. Additionally, our search identified 18,638 IoT consumer devices with insecure default settings and 11,481 with default SNMP agent community names. 4,987 devices use non-standard ports to run services (2,267-MQTT, 1,246-CoAP, 341-AMQP, 133-XMPP). Around 4,425 Cisco devices are configured with default passwords, 38 Cisco devices are vulnerable to the Cisco VPN 3000 series concentrators vulnerability, 291 Netgear routers, and 169 OpenWRT routers are configured with default credentials, totaling 15,840 devices with default passwords. The research findings are fascinating, shocking, and alarming, revealing the bitter reality that the number of IoT devices is rapidly growing while eroding users' privacy on an unprecedented scale.

As a result of this study, the following recommendations are made for IoT stakeholders.

R1: Use an approved naming convention for IoT devices.

R2: Any IoT-enabled device boot process must be protected against the execution of malicious programs with appropriate scanning.

R3: Keep sensors and appliances under regular surveillance to prevent tampering and reconfiguration.

R4: Precautions should be taken to prevent the injection of malicious code into devices.

R5: Utilize two-factor authentication whenever possible and have access exclusively to the IT systems they are authorized to use for their assigned job.

R6: The architecture and endpoints of IoT networks must be frequently examined to guarantee security.

R7: All control commands and data should pass via a gateway to prevent direct access from outside the network.

R8: Monitor and check physical security of the devices regularly.

R9: Turn off the IoT devices that are not in use.

R10: All the devices must be equipped with a cryptographic key to execute any command.

R11: Allow only the encryption-capable devices to be connected to the network.

R12: Use network segmentation to protect IoT devices from your IT network core infrastructure.

R13: A comprehensive IoT security strategy must be created by documenting all relevant aspects.

R14: Whenever a new security breach is discovered, all IoT devices belonging to a particular vendor must apply security fixes.

R15: Configure automated updates to reduce the attack window between patch releases. Ensure that device lifecycle details are recorded and acted upon.

R16: Provide an ongoing training program on the security features and methods for existing users.

References

[1] "That IoT - RFID JOURNAL", [Online]. Available at: https://www.rfidjournal.com/

[2] "Auto-ID Labs", [Online]. Available at: https://www.autoidlabs.org/

[3] "ITU-T", [Online]. Available at: http://www.itu.int/internetofthings/

[4] "IERC-ERC on the IoT", [Online]. Available at: http://www.internet-of-things-research.eu/about_iot.htm

[5] "Gartner", [Online]. Available at: https://www.gartner.com/

[6] "Disruptive Civil Technologies", [Online]. Available at: http://globaltrends.thedialogue.org/

[7] "Connected IoT devices", [Online]. Available at: https://www.eenewseurope.com/

[8] "IoT Market growth trends", [Online]. Available at: https://www.mordorintelligence.com/

[9] "Internet of Things Market Size, Growth - IoT Industry Report 2026", [Online]. Available at: https://www.fortunebusinessinsights.com/industry-reports/

[10] "Unlocking the potential of the IoT - McKinsey", [Online]. Available at: https://www.mckinsey.com/

[11] P. Schaumont, "Security in the IoT: A challenge of scale," in Proceedings of the Design, Automation, and Test in Europe, 2017, pp. 674–679. https://doi.org/10.23919/DATE.2017.7927075.

[12] "Insight into the global threat landscape", [Online]. Available at: https://events.theregister.co.uk/paper/

[13] J. Sathish Kumar, and Dhiren R. Patel, "A survey on internet of things: Security and privacy issues," *International Journal of Computer Applications*, vol. 90, no. 11, pp. 20-26, 2014. https://doi.org/10.5120/15764-4454.

[14] M. Abomhara and G. M. Køien, "Security and privacy in the Internet of Things: Current status and open issues," *Proceedings of the International Conference on Privacy and Security in Mobile Systems (PRISMS)*, 2014, pp. 1-8. https://doi.org/10.1109/PRISMS.2014.6970594.

[15] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K, Wehrle, "Security challenges in the IP-based Internet of Things", WPC, vol. 61, issue 3, pp. 527-542, 2011. https://doi.org/10.1007/s11277-011-0385-5.

[16] H. Ning, H. Liu, and L. T. Yang, "Cyberentity security in the internet of things," *Computer (Long. Beach. Calif).*, vol. 46, no. 4, pp. 46–53, 2013. https://doi.org/10.1109/MC.2013.74.

[17] E. Bertino and N. Islam, "Botnets and Internet of Things Security," *Computer (Long. Beach. Calif).*, vol. 50, no. 2, pp. 76–79, 2017. https://doi.org/10.1109/MC.2017.62.

[18] M. A. Razzaq, S. H. Gill, M. A. Qureshi, and S. Ullah, "Security issues in the Internet of Things (IoT): A comprehensive study," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, pp. 383-388, 2017. https://doi.org/10.14569/IJACSA.2017.080650.

[19] "Remote Exploitation of an Unaltered Passenger Vehicle - Privacy PC," [Online]. Available at: https://privacy-pc.com/articles/

[20] "Tour the World's Webcams With the Search Engine for the Internet of Things | WIRED," [Online]. Available at: https://www.wired.com/2013/07/shodan-search-engine/

[21] "Sony Pictures Hack Could Also Impact Sony's PS4, Phone, and TV Business," https://www.forbes.com/

[22] "PCWorld - News, tips, and reviews from the experts on PCs, Windows, and more," [Online]. Available at: https://www.pcworld.com/article/3089346/security/

[23] R. Hofstede, A. Pras, A. Sperotto and G. D. Rodosek, "Flow-based compromise detection: Lessons learned," *IEEE Security & Privacy*, vol. 16, no. 1, pp. 82-89, 2018. https://doi.org/10.1109/MSP.2018.1331021.

[24] "The Mirai botnet explained: How IoT devices almost brought down the internet | CSO Online," [Online]. Available at: https://www.csoonline.com/article/

[25] "Hackers once stole casino database through lobby fish tank thermometer - Business Insider," [Online]. Available at: https://www.businessinsider.com/

[26] "Devil's Ivy' Vulnerability Could Afflict Millions of Internet-Connected Cameras and Card Readers – WIRED," [Online]. Available at: https://www.wired.com/

[27] "Masscan - Penetration Testing Tools," [Online]. Available at: https://tools.kali.org/

[28] "Nmap Network Scanning - the official Nmap Project Guide to Network Discovery and Security Scanning," [Online]. Available at: https://nmap.org/book/

[29] R. C. Bodenheim, *Impact of the Shodan Computer Search Engine on Internet-facing Industrial Control System Devices*, Air Force Institute of Technology Wright-Patterson AFB OH Graduate School of Engineering and Management, Master Thesis, 2014. https://doi.org/10.1016/j.ijcip.2014.03.001.

[30] L. Eeckhout, "The Internet of Things Revolution," *IEEE Micro*, vol. 36, no. 6, pp. 4-4, 2016. https://doi.org/10.1109/MM.2016.93.

[31] J. Matherly, *The Complete Guide to Shodan: Collect. Analyze. Visualize. Make Internet Intelligence Work For You*, Kindle, ASIN: B01CDIU880, 2016.

[32] C. Mohan, "ARIES/KVL: A key-value locking method for concurrency control of multi-action transactions operating on B-tree indexes," *Proceedings of the 16th International Conference on Very Large Data Bases, VLDB'90*, 1990, pp. 392-405. https://doi.org/10.1007/978-981-10-0448-3_28.

[33] P. Kumar and V. S. Rathore, "Improvising and optimizing resource utilization in big data processing," *Advances in Intelligent Systems and Computing*, vol. 436, pp. 345–353, 2016.

[34] S. Rawat, P. Kumar, and G. Jain, "Implementation of the principle of jamming for hulk gripper remotely controlled by Raspberry Pi," *Advances in Intelligent Systems and Computing*, vol. 436, pp. 199–208, 2016. https://doi.org/10.1007/978-981-10-0448-3_16.

[35] R. Bodenheim, J. Butts, S. Dunlap, and B. Mullins, "Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices," *Int. J. Crit. Infrastruct. Prot.*, vol. 7, no. 2, pp. 114–123, 2014. https://doi.org/10.1016/j.ijcip.2014.03.001.

[36] L. Markowsky and G. Markowsky, "Scanning for vulnerable devices in the Internet of Things," Proceedings of the 8th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS'2015, vol. 1, 2015, pp. 463–467. https://doi.org/10.1109/IDAACS.2015.7340779.

[37] "SCADA 2017 The Future of SCADA Security: Jonathan Pollet red tiger security," [Online]. Available at: http://docplayer.net/

[38] R. A. Caralli, J. F. Stevens, L. R. Young, W. R. Wilson, *The OCTAVE Allegro Guidebook, v1.0. Cert Program*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213. May 2007, [Online]. Available at: http://www.cert.org/octave/allegro.html

[39] R. A. Caralli, J. F. Stevens, L. R. Young, W. R. Wilson, *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. CMU/SEI-2007-TR-012, CERT Program*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213. May 2007, https://doi.org/10.21236/ADA470450.

[40] C. Alberts, S. Behrens, R. Pethia, & W. Wilson, *Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM) Framework, Version 1 (CMU/SEI-99-TR-017, ADA367718)*, Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999. https://doi.org/10.21236/ADA367718.

[41] S. Alfarisi, & N. Surantha, "Risk assessment in fleet management system using OCTAVE allegro," *Bulletin of Electrical Engineering and Informatics*, no. 11, pp. 530-540, 2022. https://doi.org/10.11591/eei.v11i1.3241.

[42] I. B. Wiguna, J. S. Suroso, S, Anugerah, "Information system risk management with OCTAVE alegro at Ed-Tech company," *Journal of Theoretical and Applied Information Technology*, vol. 100, no. 20, pp. 6258-6271, 2022.

[43] V. Gerardo, & A. Fajar, "Academic IS risk management using OCTAVE allegro in educational institution," *Journal of Information Systems and Informatics*, vol. 4, issue 3, pp. 687-708, 2022. https://doi.org/10.51519/journalisi.v4i3.319.

[44] M. Yu, J. Zhuge, M. Cao, Z. Shi, and L. Jiang, "A survey of security vulnerability analysis, discovery, detection, and mitigation on IoT devices," *Future Internet*, vol. 12, no. 2, p. 27, 2020. https://doi.org/10.3390/fi12020027.

[45] "NAT-PMP Vulnerability", [Online]. Available at https://resources.infosecinstitute.com/

[46] Z. Durumeric, F. Li, J. Kasten, J. Amann, J. Beekman, M. Payer, N. Weaver, D. Adrian, V. Paxson, M. Bailey, and J. A. Halderman, "The matter of heartbleed," *Proceedings of the Conference on Internet Measurement*, 2014, pp. 475-488. https://doi.org/10.1145/2663716.2663755.

[47] H. Al-Alami, A. Hadi, and H. Al-Bahadili, "Vulnerability scanning of IoT devices in Jordan using Shodan," *Proceedings of the 2nd IEEE International Conference on the Applications of Information Technology in Developing Renewable Energy Processes & Systems (IT-DREPS)*, 2017, pp. 1-6. https://doi.org/10.1109/IT-DREPS.2017.8277814.

[48] J. Klein, and K. R. Walcott, "Exploiting Telnet security flaws in the Internet of Things," *Future of Information and Communication Conference*, Springer, Cham, 2019, pp. 713-727. https://doi.org/10.1007/978-3-030-12385-7_51.

[49] L. Xia, C. S. Feng, Y. Ding, and W. Can, "Design of secure FTP system," *Proceedings of the International Conference on Communications, Circuits, and Systems*, 2010, pp. 270–273. https://doi.org/10.1109/ICCCAS.2010.5582002.

[50] "Microsoft: Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability - Endpoint Vulnerability – FortiGuard," [Online]. Available at: https://fortiguard.com/

[51] "A Vulnerability in Microsoft Windows SMB Server Could Allow for Remote Code Execution (CVE-2020-0796)," [Online]. Available at: https://www.cisecurity.org/

[52] "Microsoft Server Message Block RCE Vulnerability – CISA," [Online]. Available at: https://www.us-cert.gov/ncas/

*Mr. **RAJASEKAR V.R** is pursuing his Ph.D. from the School of Computer Science and Engineering, Vellore Institute of Technology, India, in the Internet of Things Security. His areas of expertise are computer networking, computer security, the Internet of Things, and Cyber Security. He is proficient in conveying conceptual knowledge, developing learning materials, and extensive participation in co-curricular and professional development activities.*

*Dr. **RAJKUMAR S** is currently working as Associate Professor in the School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India. He received B.E. in Computer Science and Engineering from Anna University, Chennai, India (2008) M.E. in Computer Science and Engineering from Anna University, Chennai, India (2010). He has completed a Ph.D. at Vellore Institute of Technology, Vellore, India (2017). His research interest includes computer vision, visual perception, object detection, medical image processing, infrared image processing, biometrics, information hiding, and network security. He has published more than 60 research papers in international conferences and journals. He is also a reviewer for many reputed journals like Computers & Electrical Engineering, Computers in Biology and Medicine, Infrared Physics and Technology, Journal of Medical Imaging and Health Informatics, International Journal of Advanced Computer Research, International Journal of Advanced Technology and Engineering Exploration, International Journal of Intelligent Systems Technologies and Applications, IET Computer Vision. He is a member of IAENG, a life member of CSI, and a senior member of IEEE.*

•••