# ISF: Security Analysis and Assessment of Smart Home IoT-based Firmware

AKASHDEEP BHARDWAJ

University of Petroleum and Energy Studies, Dehradun, India; bhrdwh@yahoo.com

KESHAV KAUSHIK

University of Petroleum and Energy Studies, Dehradun, India; officialkeshavkaushik@gmail.com

DR. MOHAMMED ALSHEHRI*

Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Majmaah, 11952, Saudi Arabia

Corresponding Author Email: ma.alshehri@mu.edu.sa, moham_alshe@aol.com

DR. AHMED ABO-BAKR MOHAMED

Department of Computer Science, College of Computer and Information Sciences, Majmaah University, Majmaah 11952, Saudi Arabia

Department of Information Technology, Faculty of Computer and Information, Assiut University, Assiut 71515, Egypt

Email ID: amohamed@mu.edu.sa

DR. ISMAIL KESHTA

Computer Science and Information Systems Department, College of Applied Sciences, AlMaarefa University, Riyadh, Saudi Arabia

Email: imohamed@mcst.edu.sa

The applications and services offered by the Internet of Things (IoT) have grown significantly during the past few years. Device makers and corporate suppliers have taken notice of this, which has led to a sudden inflow of new-age firms. Confidential data and information are involved as IoT device use rises. IoT device security has emerged as a major issue and is becoming more and more significant. Appropriate security measures are needed to prevent dangers and hazards associated with the adoption of smart technology in smart cities and houses that run IoT devices, according to security evaluations. In order to safeguard the smart home environment, our research focuses on IoT device firmware. The security methodology presented in this research may be used to analyze and investigate IoT firmware, revealing sensitive data and hardcoded user IDs and passwords that can be used in future attacks and breach of IoT devices. The authors put out an idea for how real-time datasets produced by IoT search engines may be analyzed using keywords according to different device kinds, locations, and manufacturers. The results showed that it took device owners 11–13 months to upgrade the firmware. Only HP and Cisco routinely provided firmware updates to protect IoT devices among IoT device makers.

**Keywords:** Internet of Things, Cybersecurity, Firmware, Entropy, Hardcoded, Attack Vector, Hypothesis

## 1 INTRODUCTION

The digital world today has a home system and smart devices are integrated and connected over the Internet. Smart homes, industries, retail stores, smart cities, offices, healthcare, transportation, and manufacturing units aid end-users in performing routine tasks to improve their quality of life and work to create unique digital experiences with these connected devices, or IoT [1], which generate raw data, process, and transmit the information, integrating with other devices. Manufacturing equipment, gas turbines, and electric utility transformers are among the high-value physical assets that are becoming increasingly digitally linked. Smart, linked assets provide fuel for enterprises


1550-4859/2023/1-ART1 $15.00
http://dx.doi.org/10.1145/3578363

focused on resource efficiency and cost reduction. These assets offer continuous, real-time data on their present operational state, potentially upending the traditional operations and maintenance approach. Those that do not keep up will find it difficult to adapt to real-time changes and disruptions in their working environments. Consumer and domestic home appliances, along with industrial devices such as sensors for monitoring humidity, temperature, movement, and toxic levels in the house or industrial plants, are examples of IoT devices. Some new-age use cases for IoT adoption domains are:

- **Healthcare**: remote patient monitoring [2] of blood pressure or glucose or asset tracking using radio frequency and medicine dispensing smart cabinets and, supply chain management sensors and smart pill bottles [3].
- **Smart Home**: Fully connected home environments provide smart homeowners with unmatched and unique comfort and control. Tunable lights, automatic music, sensing gas and water leaks, turning off the power, water geysers [4] make the home energy efficient and eliminate unnecessary home consumption wastage.
- **Manufacturing**: Industry 4.0 and new-age IoT devices have opened up smarter ways of working [5]. Real-time remote monitoring of worker health and equipment, automation of warehouse tasks, and digitalization of paperwork provide greater control over the inventory.
- **Transportation**: from vehicle maintenance, improving safety and operational awareness to reducing traffic and providing smart freight stows, [6] IoT devices integrate with HVAC, cars, forklifts, and trucks to substantially improve human travel.
- **Telecom**: connectivity, data storage, and management services with data analytics help improve speeds, bandwidth, power efficiency, revenues, and delivery services [7].

IoT technology and security differ from information technology systems and security. While IoT devices play a huge role in businesses and human lives, the lack of IoT security has focused on the new-age threats and risks that arise during and after IoT implementation. Several emerging factors make IoT security critical today. IoT cyberattacks include device OS and application vulnerabilities [8], misconfigurations [9], unknown exposure, malware attacks [10], and data privacy theft [10] [11]. The primary reason for the emergence of the IoT attacks is complex and dynamic environments, like remote workplaces, 5G connectivity, and lack of security foresight by vendors. Although IoT devices may appear to be specialized to be threatening, they are network-connected [12] general-purpose computers that may be hijacked by attackers, causing issues beyond IoT security.

Attacks on IoT infrastructure [13] [14] cause damage not just in terms of data breaches and inconsistent operations, but also in terms of physical injury to the facilities or, worse, to the humans who operate or rely on them. IoT security failures can lead to data breaches, privacy leaks, or worse, loss of life. Organizational reputation and image can be impacted or worse, people's trust in the government's ability to secure their data [15]. Due to the realities of IoT manufacturing, device costs are kept low, making security an afterthought. Furthermore, most of these gadgets are aimed at cost-conscious clients with little expertise in choosing and installing secure infrastructure. People who are not the majority owner or controller of a gadget often withstand the worst of the device's vulnerability. The Mirai botnet, for example, spreads by exploiting hardcoded passwords hidden in chipset firmware. The software known as Mirai attacks everyday electronics like intelligent devices as well as static routing & transforms them into undead networks of remote-controlled drones. Malicious hackers employ Mirai botnets to launch huge dispersed disruption of services (DDoS) assaults against software applications. Most owners were unaware that they needed to update their passwords or were unsure how to do so. Botnet attacks harmed hundreds of billions of home devices targeting device manufacturers who did not provide any patches or control over the impacted devices. Design, production, deployment, administration, and decommissioning timelines are frequently estimated in decades. Due to the composition, context, and surroundings, response time may be prolonged. For example, linked machinery at a power plant is frequently anticipated to last more than 20 years without needing to be replaced. Attacks on a Ukrainian energy supplier, on the other hand, resulted in disruptions within seconds after the enemies launched an attack on the industrial control structure. IoT device security includes application, network, and physical aspects that influence the

services, processes, and controls implemented to safeguard the IoT ecosystem. Most IoT devices in industrial plants were not designed for secure service delivery such as energy grids or building automation systems. IoT security threats exploit vulnerabilities that can be categorized into four levels. Communication network attacks are the initial step in compromising IoT device data and controller commands. Data transported among IoT devices and servers are subject to various attacks, as the IoT device is subject to lifecycle attacks as it moves from user to maintenance, application software attacks, and physical attacks that directly target the device's firmware and chips.

The novel contribution and highlights of this research are to address the following research gaps:

- Objective 1: Background study and Literature review focusing on IoT firmware and propose a security framework for securing smart home environments.
- Objective 2: proposed methodology/contribution with novelty perspectives by conducting firmware analysis, investigations using open-source tools to reveal hardcoded user IDs, passwords, and sensitive information for planning further attacks to compromise the devices.
- Objective 3: Experimental results with clear stating of parameters and Performance comparison
- Objective 4: Create hypotheses for the analysis of a live dataset from IoT search engines using keywords according to manufacturer, region, and device information.

This paper is organized as follow: The second section presents research studies in a similar domain and identifies research gaps, motivating the authors to plan this research. Section three presents the proposed research methodology to exploit weak device firmware and evaluates the home environment devices for detecting sensitive information and vulnerabilities. Section four presents the experimental outcomes and results from scanning and analyzing the device firmware in the first stage. Finally, the conclusion is presented as the summary of this research.

## 2 LITERATURE SURVEY

IoT has evolved into a pervasive computing service platform that offers a new paradigm for the creation of diverse and distributed systems. However, it needs to embrace a cloud-based structure to solve resource restrictions owing to a lack of appropriate computing systems devoted to the storing and processing of large amounts of IoT data. As a result, several difficult security and trust issues have developed in the cloud-based IoT setting. The goal of this study is to investigate and analyze IoT device firmware from a security perspective.

The problem of evaluating IoT and the lack of safety standards that best fulfil the security criteria expose the defense capabilities of IoT-based smart environments. To close the gap, [16] looked at current security assessment and evaluation frameworks, including many NIST special releases on security approaches that emphasize their key areas of concentration, to see which ones may potentially fulfil some of the security concerns of smart environments. IoT suppliers, particularly start-ups, are working on a wide range of intriguing IoT devices and Smart Apps, also known as smart applications. While this appears to be good for IoT innovation, a few of these companies produce IoT devices and smart apps with security issues. [17] Aids IoT producers, the authors provided a security structure based on IoT hardware platforms. The framework comprised components for eliciting security requirements, security best practices suggestions for safe production, and, most importantly, a component that offers lightweight encryption primitives for both hardware and software implementations. In this study, the components of the proposed framework were discussed, created, and implemented in detail. Depending on user inputs and real-world circumstances, the writers provided security requirements and recommendations.

One of the main concerns is the variety of IoT implementation; this heterogeneity creates substantial barriers, particularly in terms of data security. IoT device security testing and analysis is a complex task since it demands a range of security testing processes, including hardware & software security testing methodologies. [18] Proposed a fresh IoT-focused cybersecurity testbed architecture. The security testbed is built to run traditional and sophisticated security tests on a wide range of IoT devices with various software/hardware combinations.

Advanced analytical approaches based on machine learning are utilized in the testbed to monitor the full functioning of the IoT device under test. The architectural architecture of the proposed security testbed is discussed, as well as a comprehensive account of the testbed's execution. Several different IoT testing situations are utilized to demonstrate how the testbed works with various IoT devices. The findings of the testbed show that it can detect vulnerabilities and hacked IoT devices.

[19] recommended an Internet-wide penetration test as the first step in ensuring the confidentiality of data, security, and availability, and also Internet-security protocol compliance. [20] proposed a security infrastructure for the energy IoT Cloud that may be used in the power IoT Cloud. Furthermore, a safety mechanism is designed that can function successfully in such a setting. Studies for this application used a smart meter as an instance, which is an important piece of power system equipment, to generate attack context situations that occur often. The pathways of attacks that exploit the vulnerability of a smart meter system were then checked using inference rules created for each attack step. Consequently, it was verified that by using inference rules, high-level attack detection results may be achieved.

[21] presented a taxonomic study of IoT security from the perspectives of perception, transportation, and application. The authors emphasized the most important topics to guide future research. [22] For the security and reputation of cloud services, authors proposed a new paradigm for trust assessment. In order to facilitate the assessment of cloud services and ensure the security of cloud-based IoT settings, this paradigm blends security- and reputation-based trust assessment approaches. The security-based trust evaluation approach uses cloud-specific security metrics to assess the security of a cloud service [23]. Additionally, reputation-based trust management technology assesses a cloud service's reputation using feedback evaluations on its quality. The proposed assessment methodology outperforms earlier trust evaluation approaches in experiments using synthetic security measure datasets and real-world online service datasets to evaluate the trustworthiness of cloud services.

Severe cyberattacks against the devices of Industrial IoT networks have been reported in recent years. Consequently, attackers can exploit the interconnections between the vulnerabilities to get access to the network's core. Because of the vulnerabilities in its devices, [24] addressed the security challenges in the IIoT network. The authors presented a graphical model to demonstrate the vulnerability relations in the IIoT network since graphs are efficient at capturing relationships between elements. This aids in the formulation of network security challenges as graph-theoretic problems. The suggested model serves as a security framework for network risk evaluation. A set of risk mitigation measures was also offered to improve the network's overall security. Detection and elimination of attack paths with high risk and short hop-length are among the techniques. The authors also presented a strategy for identifying hot spots, or significantly linked vulnerabilities.

Integration of cloud and IoT is seen as a key enabler for a wide range of applications. However, some organizations are hesitant to use such technology, while others simply overlook security concerns when integrating Cloud and IoT into their operations. [25] established an end-to-end security evaluation methodology based on a software-defined network (SDN) to evaluate the security levels for Cloud IoT offerings to tackle this challenge, taking into account the value of corporate data in Cloud IoT. The authors designed a three-layer framework by merging SDN and Cloud IoT [26], which comprises unique indicators to define its security features, simplify network management, and focus on the analysis of data flow through Cloud IoT. Then, interviews with industry and academic experts were conducted to determine the significance of these elements for overall security.

Authors [27] developed a system for integrating gradient and form cues into a deep learning network, and it is resilient in terms of detecting faces with severe occlusion. Smart objects that are connected and communicate with one another in an unprotected environment require a secure communication ecosystem on multiple levels. Unlike traditional networks, IoT technology has its own set of features, including a variety of resource limits and diverse network protocol needs. To launch a DDoS attack, the attacker takes advantage of several security vulnerabilities in an IoT system [28]. The rise in DDoS attacks has highlighted the need to address the consequences for the IoT industry. [29] suggested an IoT-based security architecture for the IoT network. Based

on the counter values of several network characteristics, the authors created a counter-based DDoS attempt detection tool. Through SDN, the algorithm displayed high performance with better outcomes. Additionally, the proposed framework efficiently detects the attack in a short period while using minimal CPU and memory resources.

After establishing [30] the weights of attributes, security assessments of alternatives are done using security criteria. The results of the proposed security assessment method indicate that among the alternatives, the most reliable and secure option is selected. This was a unique approach to IoT security evaluation, and the proposed approaches had never been utilized previously for IoT security assessment and decision making in healthcare systems [31].

[32] pointed out that QoS and security are interrelated and non-negligible issues, and that studying both of these elements together is necessary to relieve heterogeneity (or vice versa). The authors highlighted substantial and plausible instances to urge researchers to examine QoS and security together to relieve heterogeneity at the SDN-IoT control layer. The researchers provided a paradigm for converting m diverse controllers into n homogenous controller groups. The reaction time of the SDN controller was an important observation and analysis in this study. The authors exhibited the mathematical model and a proof of concept in a virtual SDN environment to verify the suggested technique. The suggested architecture was shown to greatly reduce heterogeneity, preserve QoS, and improve security. Individuals working in network security were able to deal with heterogeneity, QoS, and security in more effective and promising ways as a result of this basic study.

[33] focuses on improving safety in autonomous devices by modifying the contending window's duration to send actual information to smart sensors at the appropriate moment. In the event of overcrowding, a concept has been put forth to shorten travel times and offer high capacity with low latency. [34] Utilizing S-boxes, numerous conventional encryption methods have been developed. A crucial part of several clusters of encryption protocols is the S-box. It operates with UNICODE text, including UTS-16, and encrypts information with high levels of security. Python was used to evaluate it for UNicODE text. [35] The construction of intelligent microgrids is made simpler by using the fuzzy expert architecture. Electricity administration is made possible by using input parameters such irradiance, electricity efficiency, temperature, as well as the energy of unpredictable and manageable demands. The specialist agency's conclusions are addressed to clarify how to manage the generation and usage of modular energy.

## 3 PROPOSED RESEARCH METHODOLOGY

The authors designed and implemented an IoT home environment with a Smart IoT-based Wireless router and IP Camera focusing on Firmware security aspects of the devices, and not on design and other Cybersecurity aspects in the first stage of research. To maximize signal power as well as range, an intelligent router constantly modifies its path in response to environmental changes. a Linksys network gateway that enables mobile software integration. In IoT devices, wireless connections are made via the data link layer. The reason for focusing on Firmware analysis is all IoT devices execute firmware code at the heart of the device with components like Kernel, Filesystem, Bootloader, and other resources performing the device functions. The firmware is a part of a computer software that is stored in a non-volatile component of the gadget as well as enabling it to carry out the tasks for whom it was designed. It is made up of a number of parts, including the kernels, driver, storage, and recourses. The main controller of these activities is the kernel. It is aware of the underlying hardware that are easily accessible as well as which programs require them. The timeframe for every program to utilize those assets is then allocated. The kernel must be carefully protected within the operating system because it is essential to a user's functioning. Every program requires a boot loader, which is an essential software component. The boot loader is the primary software component to install as well as execute when a computational machine is turned on for the first time. It offers a user interface via which they can install an operational system and software. The management of user information is a file program's primary goal. Data storage, retrieval, and upgrading fall under this category. A sequence of characters that are gathered as well as maintained in a manner that is effective for the device is what certain storage devices

receive as information for preservation. Bootloader initializes device hardware components and allocates resources to enable the device to function at device startup. Every program requires a boot loader, which is an essential component of technology. It is the initial software component to load as well as execute every time a computational machine is turned on for the first time. It offers a user experience via which they can install an operational software and devices. The kernel is the middleware between the device hardware, starting all device processes and services. The filesystem has individual files and stores data for the IoT device, including web and network services. Yet this is one of the most neglected attack vectors by the device manufacturers and device owners. Mirai Botnet [36] is a famous use case in IoT Security that impacted IoT devices by using default credentials in Firmware. Possible vulnerability areas of firmware research are sensitive URLs, encrypted hardcoded credentials, Keys and algorithms, access logs, local access routes, and environment details. Hard-coded identities frequently produce a sizable security gap that enables an adversary to get beyond the security settings that the program operator has set up. It could be challenging for the network manager to find this gap. In the second stage of research, the authors analyzed the dataset of the firmware installed on various IoT devices accessible over the Internet and evaluated the heterogeneity of the devices with hypotheses.

This research analyzed the possible vulnerabilities that can be exploited due to weak device firmware and evaluated the home environment devices to detect vulnerabilities. This research uses Kali Linux [37] as the primary vulnerability scan and attack system to perform firmware analysis. An open-source, Debian-based Linux system called Kali Linux is designed for numerous data measures like digital evidence, refactoring, as well as vulnerability scanning. A study of the firmware provides further information regarding the integrated platform and its contents. It benefits, Determine the programming flaws in the integrated platform. Boost the durability and assault resilience of the business. The researchers followed the five-step process as presented in Figure 1 to perform Firmware analysis and attacks as the first step of this research. The first step involved the authors extracting Gaining accessibility to IoT device software and employing kinds of attacks to release the device firmware memory, through URAT connectivity or JTAG. The authors also downloaded the firmware BIN files directly from various vendor portals. In the next step, the author set up tools like Binwalk to scan the firmware files. A BIN file, commonly referred as a binary file, is a filesystem that houses data from a CD or DVD, such as photographs as well as movies. Due to the increased utilization of digital material above CDs and DVDs in latest days, this type has become less common, but it is still helpful if they want to retrieve old material that has been stored on the system. The operable as well as shareable file for the hardware is typically converted to a binary (. bin) or message code (. hex). The precise information that is transferred to the integrated memory is contained in this source format. The next section presents the steps followed to analyze each firmware. Step three set up and tested the firmware files using more scan and attack tools. Devices connected over a network, Host-based scanning, wireless barcode readers, software scanners, relational scanners, imagers that are dependent on hosts, and more. Step four documented the findings, and these were reported to vendors as part of the information disclosure.

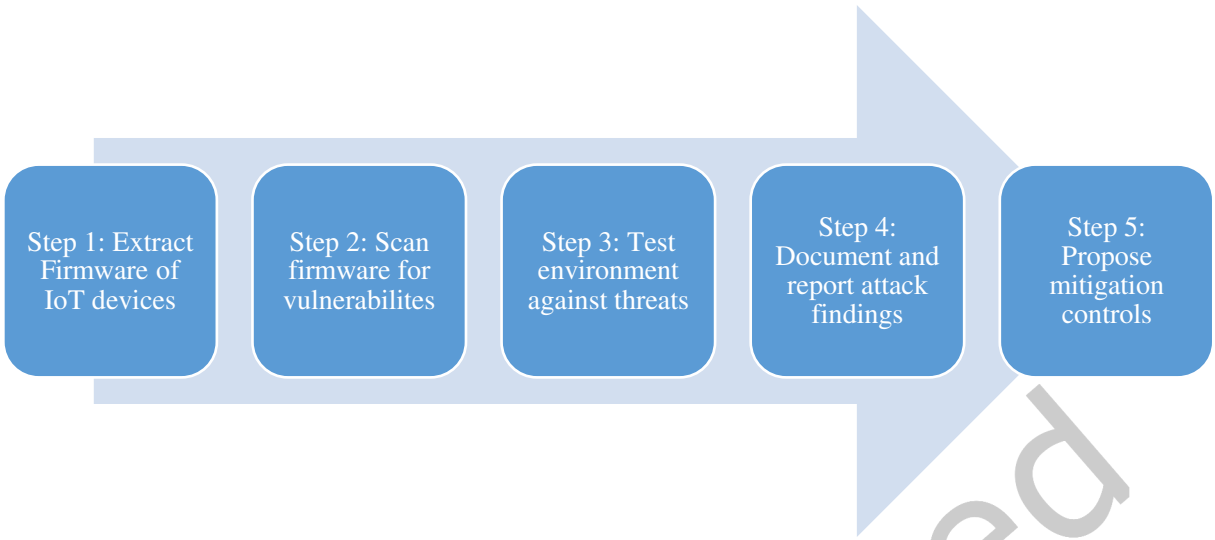


Figure 1: Proposed Research Methodology Process

In the first stage of research, the home environment implementation is performed which includes smart devices commonly found in home environments: TP-Link Wireless router [38] for sharing Internet access with a home device and Keekoon IP Camera [39] for surveillance and remote monitoring as illustrated in Figure 2. The features are ideal case, progressed anti-malware, RE-mode, range, ports for internet connectivity, complete coverage video conferencing and 4K broadcasting, and so on.

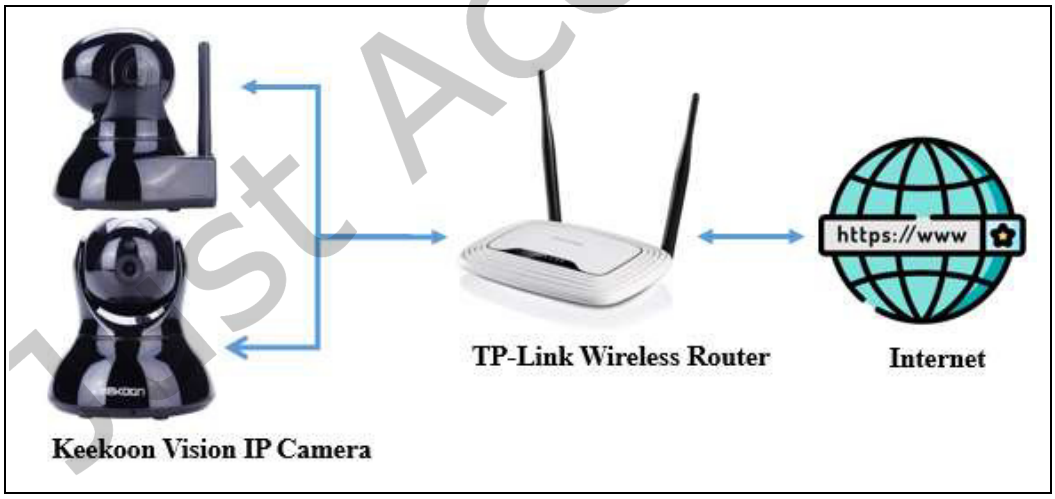


Figure 2: Smart Home IoT Device Setup

The authors configured the TP-Link IoT router with the advanced dashboard portal as illustrated in Figure 3 to view and configure the wireless access point and perform management, which includes firewall rules that provided an extra layer of security against new-age adversaries attempting to breach the home network. Serious hazards can result from improperly maintaining firewall rules and modifications, including obstructing legal data, falling offline, or even being attacked. Among the most crucial firewall administration tasks is keeping the firewall rules up to date, but several firms still have trouble with it. Among all IoT devices, routers are likely the most commonly utilized. The intelligent devices as well as other equipment can access to the web and exchange the

information they produce because they transfer IP signals to and from a wireless router or between and to IoT networks. For setting up the IP Camera to monitor the home environment,

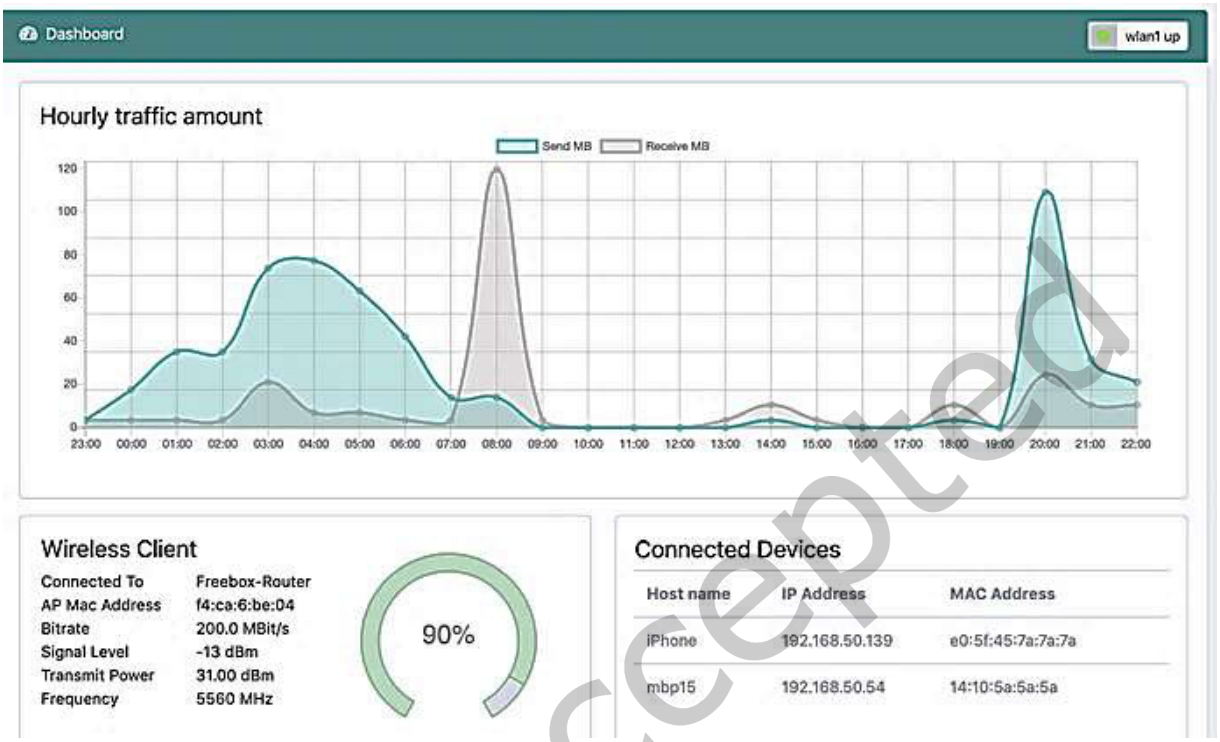


Figure 3: TP-Link Internet-Sharing IoT Wireless Router Dashboard

As previously indicated, panning resembles turning our heads from left to right then backward again. A topic can be followed as it moves across the screen by using panning. Additionally, it can be utilized to draw the audience 's awareness to fresh information. To tilt is to raise and lower the body. Simulating smart home IoT devices, the authors configured the Keekoon Vision IP Camera with the Wireless router. Figure 4 presents the IP Camera Security 'WPA2-Personal' with AES encryption passphrase. This remote monitoring device is a High-Definition camera for two-way audio and Wi-Fi capabilities with pan and tilt and motion detection.

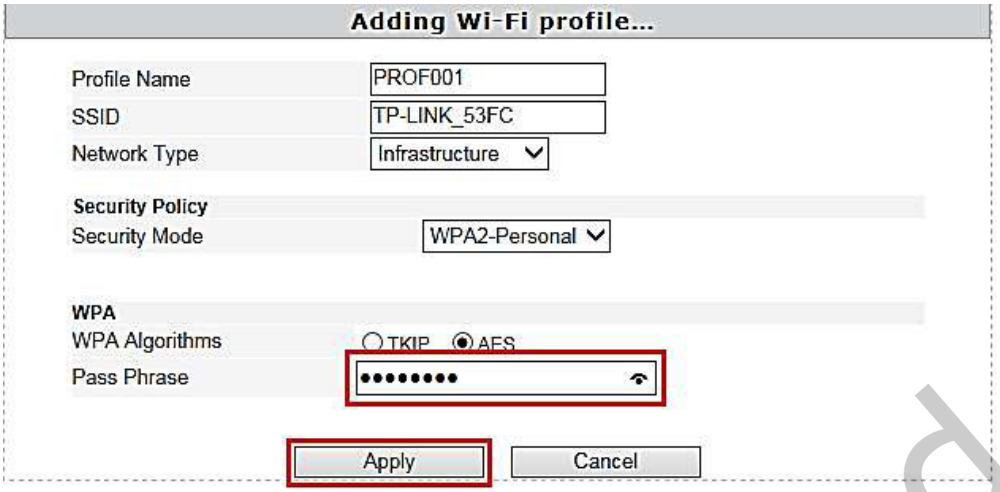


Figure 4: Keekoon IP Camera Wifi Profile Security

Figure 5 illustrates the secure connectivity of the IP Camera with the wireless router over TCP/IP network for accessing the external networks and the Internet. A group of routing protocols called TCP/IP, or Transport Management Protocols Connection, are employed to communicate networking gadgets on the network. Additionally, a personal network device uses TCP/IP as its transmission medium. This configuration enables the device owners can access the IP Camera video stream or configure the device externally.


Figure 5: IP Camera connectivity with Wifi Router

The firmware analysis, vulnerability scan, and potential attack scenarios are discussed in the next section.

For the second stage of research, gaps determined from the Literature survey revealed no all-inclusive research studies published to date on IoT Firmware attacks and heterogeneity relying on real-time IoT devices search engines on the Internet, mapping firmware updates with versions against keyword-based search lists. The authors proposed the following hypothesis as

H-1: Difference in IoT Firmware version being up to date
H-2: Installed Firmware versions by different vendors differ regardless of devices
H-3: IoT vendors do not provide regular security patches and Firmware updates
H-4: Owners immediately on release do not install Firmware updates

The authors referred to real-world data analysis portals like Shodan [40] and Censys [41], involving regular search expressions and keywords to filter the dataset and then amped the firmware versions for the various device

models. AWS Cloud is utilized for storage services. One can choose the web application architecture, software package, file system, databases, as well as other things that require with AWS. So, get a simulated reality through AWS that you may fill with the programs as well as services the program needs.

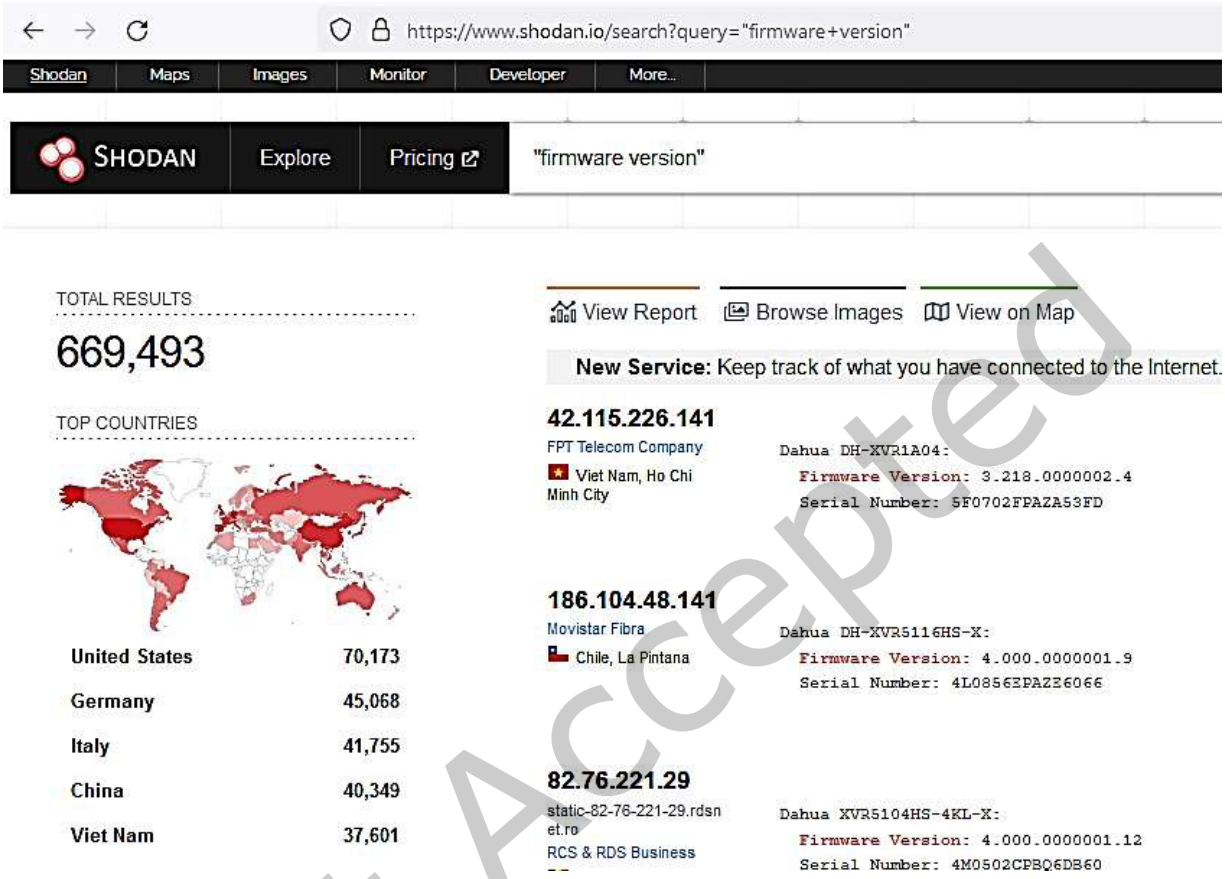


Figure 6: Shodan search for 'Firmware version' keyword

An iterative process was executed on Shodan to perform a keyword search for 'firmware version', this resulted in a raw dataset of 669,493 devices as illustrated in Figure 6 while a similar search query resulted in 204,521 results from Censys as presented in Figure 7.


Figure 7: Censys search for 'Firmware version' keyword

This dataset includes the Telnet access and HTML code for IoT Admin interface login. Using a sequential pattern mining algorithm keyword analysis is performed to determine information about IoT firmware versions. The GSP method seeks to explore the vast dataset for set of instances. The combinations are what make up the databases. whenever the recurrence of a substring exceeds the supporting threshold. Forecasting, linkage, as well as grouping are the three broad categories into which information excavation or structures can usually be divided. Trees, structures, utilized to support, and networking are examples of sequential or structure data that have been analyzed using pattern mining. Coherence continuous or cracked codes in program execution have been studied in computer engineering as frequent patterns that help detect system failures. As it enables companies to identify periodic trends for direct advertising, customer loyalty, or a variety of other duties, it is very beneficial for firms in the retail, telecoms, as well as other industries. The uses, kinds, techniques, and difficulties of sequence pattern mining will all be covered in this study. A list of IoT models and manufacturers which were known to be vulnerable to botnet attacks is researched and added to the searched keywords on Censys. These are translated into regular search expressions with duplicate device models removed. From the working hypothesis, manufacturer and device were analyzed resulting in Internet routers having the highest count. Next data fields were modified with a unique identifier for each dataset across the fields in form of a hash. To determine the firmware version, regular search expressions were executed in form of database queries and patterns extracted that matched the versions. Then the mapping table is created having device, manufacture, install date, model, existing and previous firmware version. The results obtained are presented in the next section.

## 4 EXPERIMENTAL RESULTS AND ANALYSIS

IoT vendors tend to push updates and firmware notifications to update the device OS, sensor app services and provide information about new and upcoming releases. This typically follows a set pattern with most devices running Linux OS kernel in a SquashFS as the file system, which includes compressed Linux files and directories. Linux has a compacted read-only file structure called SquashFS. It offers higher reduction by supporting block sizes ranging between 4 KiB to 1 MiB for folders, i-nodes, and domains. There are various possible compressing techniques. The clustered file tree starts at the root file structure. The devices subdirectory as well as programs used to start the platform are among the documents and directories that are essential for control system.

This research focused on Smart IoT devices found in homes today. From the IoT home setup, the authors downloaded the firmware from the vendor support portal for the TP-Link Router (TLMR3030v3) [42] and the Keekoon IP Camera (KK005 V1.94) [43] as illustrated in Figure 8. The terminal velocity for a rapid Ethernet cable is 100Mbps, whereas the fastest capacity for a gigabit Ethernet connection is 1000Mbps. The authors also extracted the firmware BIN files from the devices are usually in compressed format as. BIN, GZIP or .TAR.

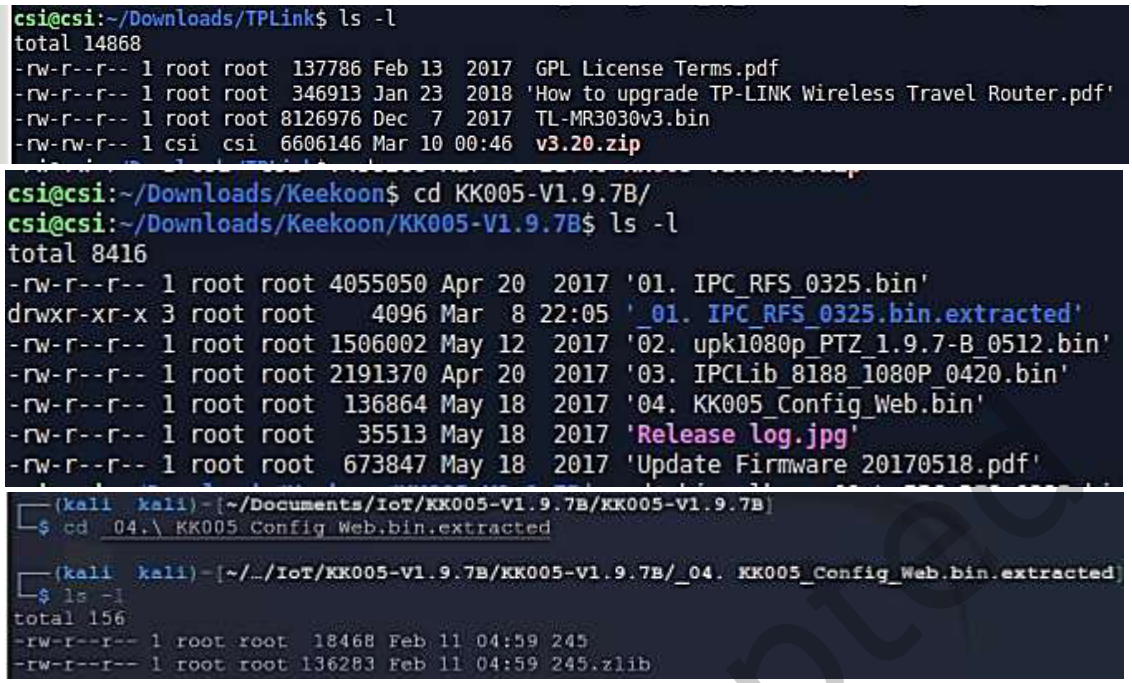


Figure 8: TP-Link and Keekoon Firmware

For analyzing the firmware, Binwalk [44] is used for this research, this is an open-source tool to analyze, extract and reverse engineer firmware images. The reason for using Binwalk is the signature scan feature and search for embedded files and file systems inside the firmware BIN files of different IoT is extracted in a recursive manner using the 'binwalk' tool as illustrated in Figure 9. This reveals the 'squashfs' Filesystem with the compression and Linux version 2.4.25.

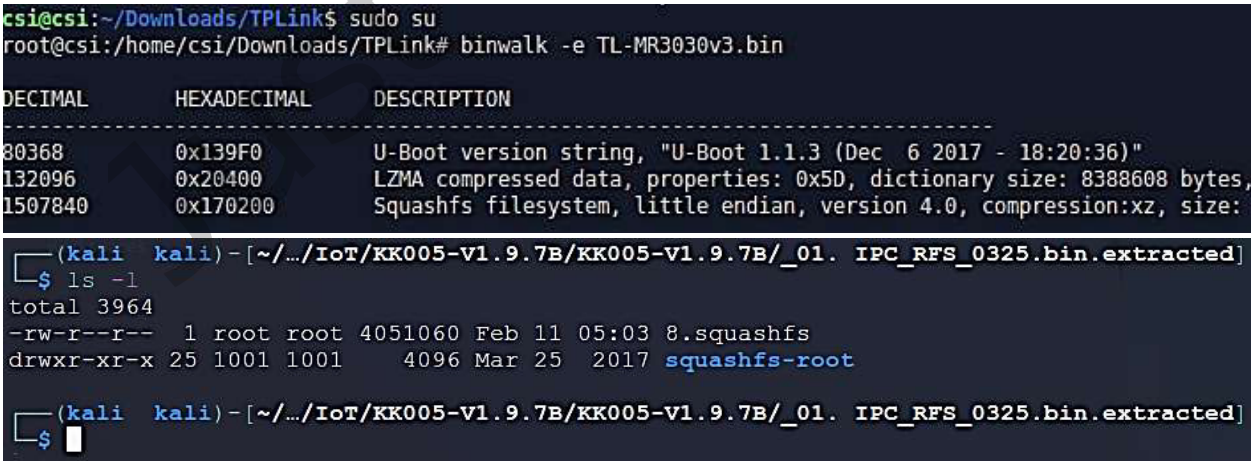


Figure 9: Extracting Firmware Images Binwalk

Using the 'Binwalk' tool with the '-A' option, the authors scanned to determine the common executable op-code signatures in the BIN file. Figure 10 illustrates the IP Camera has ARM in the offset 0x37B4E8.

```
┌──(kali  kali)-[~/Documents/IoT/KK005-V1.9.7B/KK005-V1.9.7B]
└─$ sudo binwalk -A 01.\ IPC_RFS_0325.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
3650792       0x37B4E8        ARM instructions, function prologue
```

Figure 10: ARM Architecture confirmed

The squashed filesystem has several folders and the root file system can be searched for any sensitive information. To perform this, the authors decided to search for root passwords by filtering for sensitive keywords (such as root or telnet) using the 'grep' and recursive as illustrated in Figure 11.

```
csi@csi:~/Downloads/TPLink/_TL-MR3030v3.bin.extracted$ grep -iRn 'telnetd'
Binary file squashfs-root/bin/chmod matches
Binary file squashfs-root/bin/sed matches
Binary file squashfs-root/bin/ping6 matches
Binary file squashfs-root/bin/ping matches
Binary file squashfs-root/bin/sleep matches
Binary file squashfs-root/bin/mkdir matches
Binary file squashfs-root/bin/echo matches
Binary file squashfs-root/bin/netstat matches
Binary file squashfs-root/bin/cat matches
csi@csi:~/Downloads/TPLink/_TL-MR3030v3.bin.extracted$ grep -iRn 'root'
Binary file squashfs-root/bin/chmod matches
Binary file squashfs-root/bin/sed matches
Binary file squashfs-root/bin/ping6 matches
Binary file squashfs-root/bin/ping matches
Binary file squashfs-root/bin/sleep matches
Binary file squashfs-root/bin/mkdir matches
Binary file squashfs-root/bin/echo matches
Binary file squashfs-root/bin/netstat matches
Binary file squashfs-root/bin/cat matches
Binary file squashfs-root/bin/umount matches
Binary file squashfs-root/bin/egrep matches
```

Figure 11: Search for Sensitive keywords in Squashfs filesystem

Next, the contents of the passwd file are displayed, this file contains user account information required during login, i.e., the User ID, Group ID, and Password hash. Using password cracking tools like 'media' and 'john' the authors can crack the root password as illustrated in Figure 12. A similar process can be performed for other firmware to determine the root of SSH and Telnet User ID and Passwords.

```
csi@csi:~/Downloads/Keekoon/KK005-V1.9.7B/_01. IPC_RFS_0325.bin.extracted/squashfs-root/etc_ro$ cat passwd
root:$1$$qRPK7m23GJusamGpoGLby/:0:0::/root:/bin/sh
csi@csi:~/Documents/Passwords$ sudo medusa -u root -P passw.txt -h 10.9.1.34 -M http
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [http] Host: 10.9.1.34 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: root xc3511 (1 of 59 complete)
ACCOUNT FOUND: [http] Host: 10.9.1.34 User: root Password: root xc3511 [SUCCESS]
```

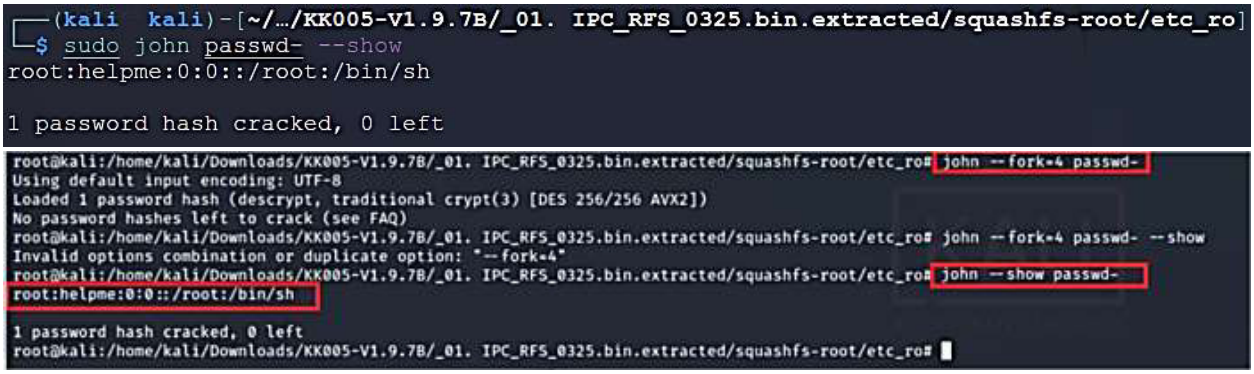


Figure 12: Contents of Passwd File displayed & cracked

The authors found only a few IoT manufacturers encrypt the firmware, while most vendors have unencrypted firmware versions. When the firmware is uploaded to the device for an upgrade, the file is decrypted and then the normal update process starts. Entropy is a measure of the unpredictability or instability of the data that machine learning algorithms are analyzing. It is the computational intelligence measurement that evaluates the randomness or impurities in the network, to put it another way. Through determining how much heat necessary to increase the temperature by a specific number utilizing a reversible procedure, one can determine the entropy of a material. Entropy has a scale from 0 to 1. At times the firmware version is not mentioned in the release notes, for which the authors propose using the 'Entropy Visualization' method to determine the randomness for values between 0 and 1. Near one value is considered high entropy and the firmware data is compressed as presented in Figure 13 for the IP Camera and Wireless router.

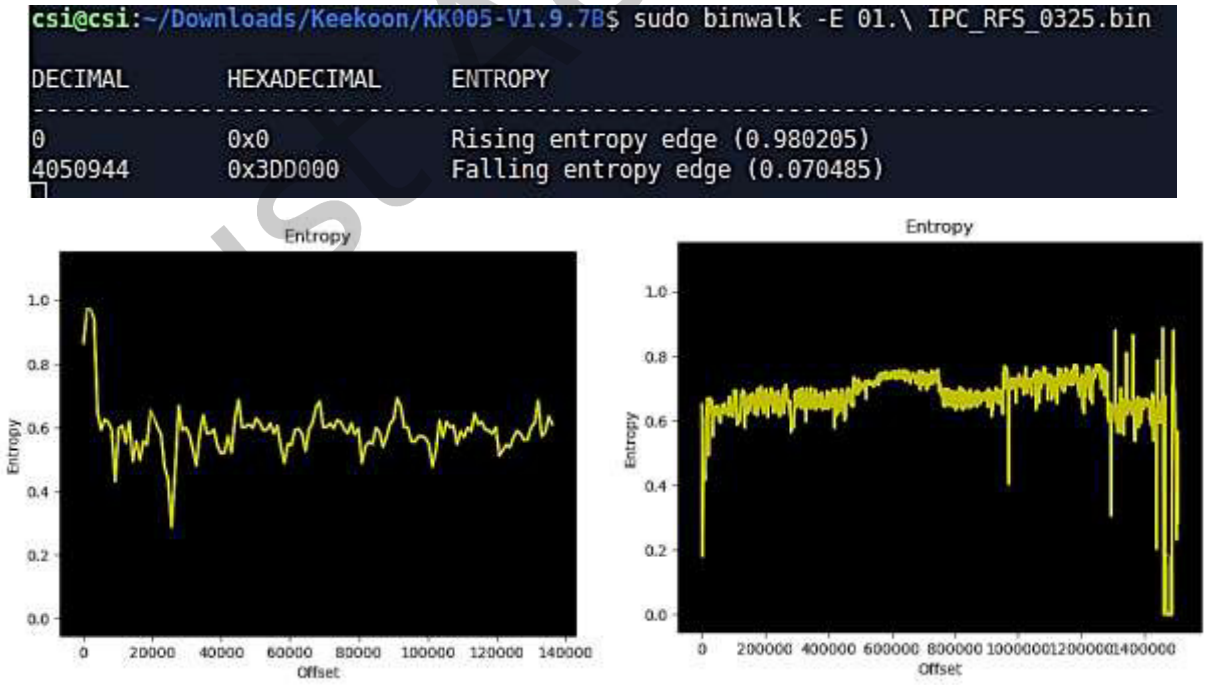


Figure 13: Entropy Visualization

After extracting the firmware, the authors used the 'firmwalker' [45] tool to scan the files and search for possible vulnerabilities. The tool generates a list of possible vulnerabilities as illustrated in Figure 14. Analyzing the files for access-related and sensitive details are gathered and validating the above information gathered.

```
csi@csi:~/Downloads/firmwalker$ sudo ./firmwalker.sh ~/Downloads/Keekoon/Keekoon/OpenWrt/openwrt-18.06.2/files/
***Firmware Directory***
/home/csi/Downloads/Keekoon/Keekoon/OpenWrt/openwrt-18.06.2/files/
***Search for password files***
################################## passwd
/etc/passwd

################################## shadow
/etc/shadow

################################## *.psk

***Search for Unix-MD5 hashes***
/home/csi/Downloads/Keekoon/Keekoon/OpenWrt/openwrt-18.06.2/files/etc/shadow:$1$Jl7H1VOG$Wgw2F/C.nLNTC.4pwDa4H1
/home/csi/Downloads/Keekoon/Keekoon/OpenWrt/openwrt-18.06.2/files/etc/shadow:$1$79bz0K8z$Ii6Q/if83F1QodGmkb4Ah.
/home/csi/Downloads/Keekoon/Keekoon/OpenWrt/openwrt-18.06.2/files/etc/shadow.bak:$1$KzoHhzG9$wGyFXbWOcRChy3e.Ep2NY1
```

Figure 14: Firmwalker validating sensitive details

This tool also confirms the presence of hardcoded User IDs and passwords inside the IoT device firmware as illustrated in Figure 15.

```
-------------------- root --------------------
/etc/shadow
/etc/passwd
/etc/shadow.bak
/usr/lib/lua/luci/view/themes/bootstrap/header.htm
/usr/lib/lua/luci/view/iotgoat/cmd.htm
-------------------- root pattern with line numbers----
/etc/shadow:1:root
/etc/passwd:1:root
/etc/passwd:7:root
/etc/shadow.bak:1:root
/usr/lib/lua/luci/view/themes/bootstrap/header.htm:192:root
/usr/lib/lua/luci/view/themes/bootstrap/header.htm:195:root
/usr/lib/lua/luci/view/iotgoat/cmd.htm:5:root

-------------------- password --------------------
/www/luci-static/bootstrap/cascade.css
/usr/lib/lua/luci/view/themes/bootstrap/header.htm
/usr/lib/lua/luci/model/cbi/admin_network/wifi.lua
-------------------- password pattern with line numbers----
```

Figure 15: User ID and Password details found on Firmware

The firmwalker tool further revealed hardcoded Email IDs and Network IPs inside the Keekoon firmware as presented in Figure 16. Similar sensitive details are found inside most IoT Firmware files which reveal and confirm the low-security level inside IoT devices.


Figure 16: Hardcoded Email IDs, IP addresses, and URLs found inside the firmware

As part of the second stage, the authors analyzed the IoT manufacturer, model, and device type, related to the firmware version. It was found that not every IoT device displayed the information, the below equations are applied for calculating the variance analysis for the IoT device firmware.

$F(LD) - F(ID) = TD$ …. Equation 1

If $F(LD) = F(ID) \rightarrow TD = 0$ → Firmware Up-To-Date…. Equation 2

where F(LD) = latest firmware date
F(ID) = installed firmware date
TD = time delay between installation and latest firmware

From the IoT search engine searches, a total of 874,014 device dataset lists is obtained (669,493 from Shodan and 204,521 from Censys) which fits the regular search expression. In sorting and classifying the devices, there are 120 models from 65 manufacturers that can be categorized into 15 device types. Devices are found to be installed in the US, Germany, China, and Vietnam locations among the top locations. From the variance analysis, 2,154 devices are analyzed in Table 1 for the lag in the number of days by users to update the firmware versions when released by the vendors. Table 2 presents the average delay in days for releasing a new firmware version based on the top vendors and the locations.

Table 1: Device Types & Lag times

| IoT Device | Days Lag |
|---|---|
| Smart Lock | 45 |
| Smart Doorbell | 105 |
| IP Camera | 116 |
| Voice Assistant | 175 |
| Industrial IoT | 205 |
| Enterprise IoT | 13 |
| Consumer IoT | 185 |
| Healthcare IoT | 192 |

Table 2: Manufacturer, Locations, and Release Lag

| Manufacturer | Location | Days Lag |
|---|---|---|
| HP | Texas, USA | 9 |
| Cisco | San Jose, USA | 11 |
| ARM | Vancouver, Canada | 12 |
| GE Digital | California, USA | 21 |
| Bosh Sensor | Michigan, USA | 18 |
| SAP | Walldorf, Germany | 34 |
| Siemens | Munich, Germany | 23 |
| IBM | New York, USA | 45 |

The authors further calculated the univariate ANOVA as the average days for the installed or upgraded IoT Firmware as per device types, Manufacturers and location. In reality, the Univariate General Linear Modeling is designed to assess theories with a single predictor variables and numerous explanatory variables. Since the regression model is unitary, ANOVA is regarded as a univariate study. At least one grouping average differs from the other team means if the testing is significantly positive. The multiple regression is said to be multimodal if every measurement contains a matrix of factors. In an ANOVA, there are three main suppositions: The reply shows a typical demography at every degree of the variable. The volatility of such models is identical. The information is impartial.

$$Firmware(Device\_Type)\ from\ 10{,}481145 = 3.15, p = 0.02, \mu < 0.001$$

$$Firmware(Manufacturers)\ from\ 11{,}461727 = 12.78, p = 0.01\ \mu < 0.05$$

$$Firmware(Location)\ from\ 211{,}406781 = 6.45, p = 0.01, \mu < 0.05$$

H-1: Difference in IoT Firmware version being up to date
H-2: Installed Firmware versions by different vendors differ regardless of devices
H-3: IoT vendors do not provide regular security patches and Firmware updates
H-4: Firmware updates are not installed by owners immediately on release

Analysis of the firmware versions released lag by various global IoT device manufacturers revealed HP and Cisco have the least number of days, as compared to IBM which has the maximum lag time to release IoT firmware updates.

- The difference between IoT firmware released being up-to-date proved the hypothesis H-1 for some vendors such as HP and Cisco
- Manufacturers deliver and release firmware update services better than others, which also indicates their devices are secured quickly against new-age cyberattacks. In other words, IBM IoT devices would tend to be less secure as compared to HP and Cisco as per the results and supported hypothesis H-2.
- The lag delay for the latest firmware version varies between different IoT device manufacturers even as the overall size is insignificant. Manufacturers tend to release patches slowly as well as device owners still use legacy devices that are already end-of-support, although hypothesis H-3 does not fully support this fact.

- Firmware releases and the installation time difference is also considered to be critical indicator for device adoption and user acceptance. Device firmware is known to be updated around 11-13 months, this is independent of the manufacturer and IoT device types, which supports hypothesis H-4. The users tend to buy the IoT, set it up, and forget to upgrade the devices. The device owners can be considered the weakest link in the IoT security ecosystem. Highlight the advantages of the proposed technique.

## 5 CONCLUSION

This research assessed new IoT devices that are commonly available in smart home environments. The outcome of this research on IoT firmware security risks emphasizes the broadening of the attack surface for threat actors. This implies that traditional defenses such as firewall rules against denial-of-service attacks or brute force are no longer effective against such new-age firmware and botnet attacks, which unfortunately have become common in diverse smart home environments. Ensuring the least delay in updating the IoT device firmware is just a step towards the overall IoT security. To the best of our knowledge, we have analyzed the IoT firmware proposing a new framework, and also performed comprehensive research on firmware distribution and up-to-date lag times for IoT devices using the real-time iterative dataset of various firmware versions from Shodan and Censys. The proposed hypothesis found empirical support validating this research.

## CONFLICT OF INTEREST

The authors have no conflict of interest relevant to this article.

## AUTHORSHIP

The authors have made substantial contributions to conception and design, or acquisition of data, or analysis and interpretation of data; and are involved in drafting the manuscript or revising it critically for important intellectual content

## ETHICS STATEMENT

The authors declare no conflicts of interest.



## REFERENCES


[1] "What is IoT? Defining the Internet of Things (IoT) | Aeris." https://www.aeris.com/in/what-is-iot/ (accessed Mar. 25, 2022).

[2] K. Kaushik, S. Dahiya, and R. Sharma, "Internet of Things Advancements in Healthcare," *Internet of Things*, pp. 19–32, Aug. 2021, doi: 10.1201/9781003140443-2.

[3] "IoT: Opportunities and Use Cases for Life Sciences Organizations | Avalere Health." https://avalere.com/insights/iot-opportunities-and-use-cases-for-life-sciences-organizations (accessed Mar. 25, 2022).

[4] "Smart home automation - 7 use-case scenarios in an IoT (Internet of Things) world. - eGlu." https://wwww.myeglu.com/smart-home-automation-7-use-case-scenarios-in-an-iot-internet-of-things-world/ (accessed Mar. 25, 2022).

[5] "IoT in Manufacturing: Top Use Cases and Case Studies | MachineMetrics." https://www.machinemetrics.com/blog/iot-in-manufacturing (accessed Mar. 25, 2022).

[6] "How IoT is Shaping the Future of Transportation—Top Use Cases Explained." https://imaginovation.net/blog/iot-shaping-future-transportation-top-use-cases-explained/ (accessed Mar. 25, 2022).

[7] "Internet of Things in the Utilities Industry | SaM Solutions." https://www.sam-solutions.com/blog/iot-in-utilities/ (accessed Mar. 25, 2022).

[8] "The risks of the Internet of Things — CYBER STRIKE SOLUTIONS." https://cyberstrikesolutions.com/the-risks-of-the-internet-of-things/ (accessed Mar. 25, 2022).

[9] "How to find security gaps in IoT devices - IoT Inspector." https://www.iot-inspector.com/blog/how-to-find-security-gaps-in-iot-devices/ (accessed Mar. 25, 2022).

[10] "IoT Privacy & Security | Internet of Business." https://internetofbusiness.com/iot-privacy-security/ (accessed Mar. 25, 2022).

[11] K. Kaushik and S. Dahiya, "Security and privacy in iot based e-business and retail," *Proceedings of the 2018 International Conference on System Modeling and Advancement in Research Trends, SMART 2018*, pp. 78–81, Nov. 2018, doi: 10.1109/SYSMART.2018.8746961.

[12] "7 out of 10 Organizations Have Seen Hacking Attempts via IoT | Extreme Networks, Inc." https://investor.extremenetworks.com/news-releases/news-release-details/7-out-10-organizations-have-seen-hacking-attempts-iot (accessed Mar. 25, 2022).

[13] S. Jain, K. Kaushik, D. K. Sharma, R. Krishnamurthi, and A. Kumar, "Sustainable Infrastructure Theories and Models," *Digital Cities Roadmap*, pp. 97–126, Apr. 2021, doi: 10.1002/9781119792079.CH3.

[14] D. Bi, S. Kadry, and P. M. Kumar, "Internet of things assisted public security management platform for urban transportation using hybridized cryptographic-integrated steganography," *IET Intelligent Transport Systems*, vol. 14, no. 11, pp. 1497-1506, doi: 10.1049/iet-its.2019.0833.

[15] "What is WannaCry? WannaCry Ransomware Attack Case Study | Fortinet." https://www.fortinet.com/resources/cyberglossary/wannacry-ransomeware-attack (accessed Mar. 25, 2022).

[16] N. M. Karie, N. M. Sahri, W. Yang, C. Valli, and V. R. Kebande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," *IEEE Access*, vol. 9, pp. 121975–121995, 2021, doi: 10.1109/ACCESS.2021.3109886.

[17] M. G. Samaila, J. B. F. Sequeiros, T. Simoes, M. M. Freire, and P. R. M. Inacio, "IoT-HarPSecA: A Framework and Roadmap for Secure Design and Development of Devices and Applications in the IoT Space," *IEEE Access*, vol. 8, pp. 16462–16494, 2020, doi: 10.1109/ACCESS.2020.2965925.

[18] S. Siboni *et al.*, "Security Testbed for Internet-of-Things Devices," *IEEE Trans Reliab*, vol. 68, no. 1, pp. 23–44, Mar. 2019, doi: 10.1109/TR.2018.2864536.

[19] S. Verma, Y. Kawamoto, and N. Kato, "A Network-Aware Internet-Wide Scan for Security Maximization of IPv6-Enabled WLAN IoT Devices," *IEEE Internet Things J*, vol. 8, no. 10, pp. 8411–8422, May 2021, doi: 10.1109/JIOT.2020.3045733.

[20] C. Choi and J. Choi, "Ontology-Based Security Context Reasoning for Power IoT-Cloud Security Service," *IEEE Access*, vol. 7, pp. 110510–110517, 2019, doi: 10.1109/ACCESS.2019.2933859.

[21] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J*, vol. 5, no. 4, pp. 2483–2495, 2018, doi: 10.1109/JIOT.2017.2767291.

[22] G. Manogaran, R. Varatharajan, D. Lopez, P. M. Kumar, R. Sundarasekar, and C. Thota, "A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system," *Future Generation Computer Systems*, vol. 82, pp. 375-387, doi: org/10.1016/j.future.2017.10.045.

[23] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang, and D. Chen, "Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach," *IEEE Access*, vol. 7, pp. 9368–9383, 2019, doi: 10.1109/ACCESS.2018.2890432.

[24] G. George and S. M. Thampi, "A Graph-Based Security Framework for Securing Industrial IoT Networks from Vulnerability Exploitations," *IEEE Access*, vol. 6, pp. 43586–43601, Aug. 2018, doi: 10.1109/ACCESS.2018.2863244.

[25] Z. Han, X. Li, K. Huang, and Z. Feng, "A software defined network-based security assessment framework for cloudIoT," *IEEE Internet Things J*, vol. 5, no. 3, pp. 1424–1434, Jun. 2018, doi: 10.1109/JIOT.2018.2801944.

[26] M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, "A Machine Learning Security Framework for Iot Systems," *IEEE Access*, vol. 8, pp. 114066–114077, 2020, doi: 10.1109/ACCESS.2020.2996214.

[27] L. Mao, F. Sheng, and T. Zhang, "Face Occlusion Recognition with Deep Learning in Security Framework for the IoT," *IEEE Access*, vol. 7, pp. 174531–174540, 2019, doi: 10.1109/ACCESS.2019.2956980.

[28] K. Kaushik and K. Singh, "Security and Trust in IoT Communications: Role and Impact," *Advances in Intelligent Systems and Computing*, vol. 989, pp. 791–798, 2020, doi: 10.1007/978-981-13-8618-3_81.

[29] J. Bhayo, S. Hameed, and S. A. Shah, "An Efficient Counter-Based DDoS Attack Detection Framework Leveraging Software Defined IoT (SD-IoT)," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3043082.

[30] L. Wang, Y. Ali, S. Nazir, and M. Niazi, "ISA Evaluation Framework for Security of Internet of Health Things System Using AHP-TOPSIS Methods," *IEEE Access*, vol. 8, pp. 152316–152332, 2020, doi: 10.1109/ACCESS.2020.3017221.

[31] K. Singh, K. Kaushik, Ahatsham, and V. Shahare, "Role and Impact of Wearables in IoT Healthcare," *Advances in Intelligent Systems and Computing*, vol. 1090, pp. 735–742, 2020, doi: 10.1007/978-981-15-1480-7_67.

[32] K. Sood, K. K. Karmakar, S. Yu, V. Varadharajan, S. R. Pokhrel, and Y. Xiang, "Alleviating Heterogeneity in SDN-IoT Networks to Maintain QoS and Enhance Security," *IEEE Internet Things J*, vol. 7, no. 7, pp. 5964–5975, Jul. 2020, doi: 10.1109/JIOT.2019.2959025.

[33] S. Vijayarangam, G. Chandra Babu, S. Ananda Murugan, N. Kalpana, and P. Malarvizhi Kumar, "Enhancing the security and performance of nodes in Internet of Vehicles," *Concurrency and Computation: Practice and Experience,* vol. 33, no. 7, pp. 1-1, 2021, doi: org/10.1002/cpe.5080.

[34] B. Maram, J. M. Gnanasekar, G. Manogaran, and M. Balaanand, "Intelligent security algorithm for UNICODE data privacy and security in IOT," *Service Oriented Computing and Applications*, vol. 13, no. 1, pp. 3-15, 2019, doi: org/10.1007/s11761-018-0249-x.

[35] R. Zhang, S. VE, and R. D. Jackson Samuel, "Fuzzy efficient energy smart home management system for renewable energy resources," *Sustainability,* vol. 12, no. 8, pp-3115, doi: org/10.3390/su12083115.

[36] "What is the Mirai Botnet? | Cloudflare." https://www.cloudflare.com/en-in/learning/ddos/glossary/mirai-botnet/ (accessed Mar. 29, 2022).

[37] "Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution." https://www.kali.org/ (accessed Mar. 29, 2022).

[38] "TL-MR3020 | Portable 3G/4G Wireless N Router | TP-Link India." https://www.tp-link.com/in/home-networking/3g-4g-router/tl-mr3020/ (accessed Mar. 29, 2022).

[39] "KK005 | Keekoon - A Smart Wireless Video Monitoring IP Camera Manufacturer." https://www.keekoonvision.com/KK005 (accessed Mar. 29, 2022).

[40] "Explore." https://www.shodan.io/explore (accessed Mar. 29, 2022).

[41] "Censys Search." https://search.censys.io/ (accessed Mar. 29, 2022).

[42] "Download for TL-MR3020 | TP-Link India." https://www.tp-link.com/in/support/download/tl-mr3020/ (accessed Mar. 29, 2022).

[43] "Firmware Download A | Keekoon - A Smart Wireless Video Monitoring IP Camera Manufacturer." https://www.keekoonvision.com/firmware-download-a (accessed Mar. 29, 2022).

[44] "GitHub - ReFirmLabs/binwalk: Firmware Analysis Tool." https://github.com/ReFirmLabs/binwalk (accessed Mar. 29, 2022).

[45] "GitHub - craigz28/firmwalker: Script for searching the extracted firmware file system for goodies!" https://github.com/craigz28/firmwalker (accessed Mar. 29, 2022).