International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Mechanism to Identify and Upgrade Legacy Components in IoT Devices to Enhance Cybersecurity

Sahana G S[1], *Prakruthi R*[2], *Dr. Mohammed Rafi R*[3]

[1,2] PG Student, Dept. Of CSE, University B.D.T College of Engineering, Davanagere, Karnataka, India
[3] Professor Department of Computer Science and Engineering, University B.D.T College of Engineering, Davanagere, Karnataka, India

ABSTRACT:

This report outlines the creation and usage of a Python system to evaluate the obsoleteness and possible vulnerabilities in a simulated 100 varied IoT sensor deployment. The system produces fake sensor data, including important characteristics like sensor ID, type (covering environmental, wearable, industrial, and automobile categories), current firmware version, hardware model, and timestamp of the last communication. Next, it uses a set of simulated functions to determine the most recent available hardware-specific firmware for each sensor's model and type, measure the difference between current and most recent firmware, calculate the time elapsed since the last communication with a sensor, and infer possible security flaws, referencing a basic CVE database by hardware model and firmware number. It then employs a collection of mocked functions to identify the most recently released firmware for some sensor's hardware and model, compute current-most recent firmware difference, compute time since last sensor contact, and mark possible security exposures, from a simplistic CVE database accessed by hardware model and firmware version. The calculation is focused on creating an "outdatedness score" for each sensor based on the combined result of firmware version mismatch and communication idle time. Also, a "vulnerability score" is calculated by the number of identified Common Vulnerabilities and Exposures (CVEs). The two scores are then merged to compute a total "risk score," enabling a global measurement for the operation and security status of each sensor. The system notifies sensors that need firmware updates and puts the whole risk distribution across the simulated sensor network into Low, Medium, and High levels. The report demotes significant findings in descriptive pie charts, visually representing the proportion of sensors labeled for forthwith firmware updates and the division of calculated risk scores in the simulated IoT environment. The analysis demotes a rudimentary framework for proactive lifecycle management and enhanced security in IoT sensor networks, correctly demoting devices requiring instantaneous attention due to outdated software or publicly disclosed security vulnerabilities. While derived from modelled data and operational implementations, this operation readily demonstrates an effective methodology that can be used in real-world management of IoT devices and general security audits, giving valuable information for potential threats as well as maintenance processes necessary.

KEYWORDS: IoT sensor, Firmware analysis, Hardware analysis ,Obsoleteness detection ,Vulnerability assessment, Security mechanism, Scalable system ,Risk scoring, Firmware update.

I. INTRODUCTION

Internet of Things or IoT has been designed to be tomorrow's Internet today. It is generally characterized as a web of physical and virtual objects, devices, or things that can capture data around them and exchange it amongst themselves or through the Internet. To enable data collection, devices have sensors, software, and electronics; their ability to exchange is enabled by making them available over local area networks or the Internet. The past of the Internet of Things is stretched out. While the terminology was first employed in 1999 by Kevin Ashton, co- founder and executive director at the Auto-ID Centre at MIT, for such groups as CISCO, the IoT came into existence in 2009, where there were more objects than people on the Internet. The number of devices connected then was 10 billion, yet the aspirations are good. It is predicted that by the year 2020, there will be over 50 billion Internet-connected devices. As can be seen from the figures, in recent times, the Internet of Things has experienced an unexpected surge in popularity.

IoT Architecture

The IoT architecture definition is the design that defines how various components of IoT (e.g., networks, devices, sensors, apps) interrelate in an IoT system. IoT architecture typically consists of several layers and components which perform a variety of operations from physical devices, and data collection systems, to network devices routing IoT data to data processing software, and storage of IoT data.

Layers of IoT architecture

To achieve IoT architecture and determine the right IoT solutions for an organization, it is crucial to learn about IoT layer architecture. Here in this example, an example of five-layer IoT architecture will be used for discussion purposes. Perception layers the perception layer interacts with the physical world to gather raw data. Such IoT devices like cameras and sensors gather data and images passively that will be carried in the transport layer (e.g., network layer), while actuators instruct devices to perform actions based on sensor measurements or other instructions in IoT systems. (Actuators are tangible devices that convert energy into movement.)

Transport layer

The transport layer, or network layer, regulates flow and data exchange between the sensors of the perception layer and the processing layer across multiple networks (e.g., data transfer) between backend systems and IoT devices via Wi-Fi, Bluetooth, etc.).

Processing layer

Data processing layer, or the middleware layer, stores, analyses, and pre-processes the information received from the transport layer. These include such activities as data aggregation, protocol translation, and security enforcement to prepare data for the application layer. Message brokers, IoT platforms, and edge computing nodes may also be included in this layer.

Application layer

The application layer consists of software applications that make use of processed data gathered in the perception layer to perform tasks or derive insights with the help of sophisticated analytics. Databases, data warehouses, and data lakes are encompassed under the application layer.

Business layer

The business layer is probably the most widely occurring IoT architecture layer in that it includes user interfaces, dashboards, and data visualization software which most business people are accustomed to using on a day-to-day basis. It's within the business layer that all the data collected and processed comes into value by providing insights and driving business decisions.

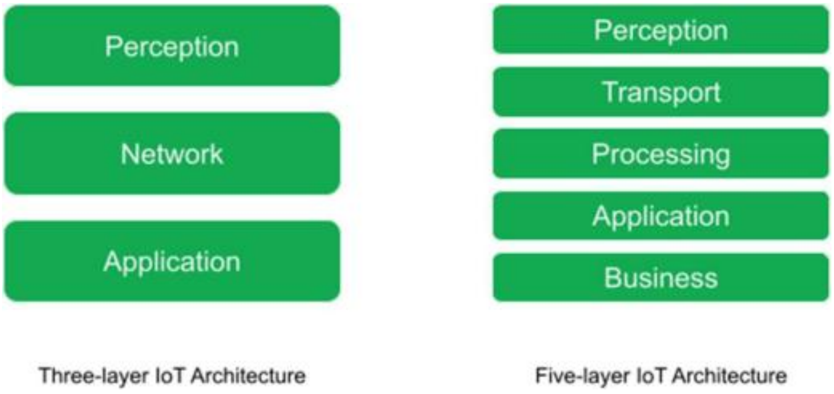

Fig: IoT Architecture

IoT Network Protocols

Bluetooth

Bluetooth works in the 2.4GHz frequency band. It can work in a range of 10m to 100m, and its data rate goes up to 1MBPS. It is supportive of two network topologies point-to-point and mesh. It can be used to send small information to personal devices like speakers, earphones, smart watches, smart shoes, etc. The protocol can also be used by Smart Homes, like Alarms, HVAC, lights, etc.

Zigbee

This is achieved according to the IEEE802.15.4 standard. Its frequency range is as low as Bluetooth, 2.4GHz. It has a maximum distance of 100 meters with a maximum data rate of 250KBPS. The zigbee protocol will transmit small-sized data for short distances. It can be applied in those systems where more authentication and robustness is required. It is supported by star topology, mesh topology, and cluster tree topology. Important use cases observed are device health monitoring in industries, smart homes, etc.

6LoWPAN

PAN stands for Personal Area Network, and 6LoWPAN stands for IPV6 Low Power PAN. It works in a frequency range of 900 to 2400MHz. Data rate is 250KBPS with two topologies of networks - star and mesh.

Wireless LAN - Wi-Fi

Wi-Fi offers a greater band and accommodates the data rate of 54MBPS and reaches up to 600MBPS. The range is 50m in local area were giving individual antennas ranging up to 30 km. Wi-Fi easily connects IoT devices and has a lot of data to share. Smart homes, smart cities, office spaces, etc. utilize this protocol.

LoRaWAN

This is the abbreviation of Long-Range Wide Area Network. The range is approximately 2.5km and extends up to 15km. Data rate is extremely slow, i.e., 03, and KBPS and reaches a maximum of 50KBPS. It supports a large number of connected devices and is utilized in applications like Smart City, Supply Chain Management, etc.

LTE-M

LTE-M stands for Long Term Evolution for Machines. It is a type of LPWAN Low Power Wide Area Network. It is used along with cellular networks to provide security. LTE-M runs on a frequency band of 1.4MHz-5MHz and the data rate is up to 4MBPS.

Sigfox

Sigfox is utilized where a large area has to be covered with little use of power. Sigfox is used for connecting billions of IoT devices. The frequency band for Sigfox is 900MHZ with a range of 3km to 50km. Data rate is extremely low with a limit of 1KBPS.

Cellular

It is also known as a mobile network. Cellular networks are 2G, 3G, 4G, and 5G. It has frequency bands of 900MHz, 1.8/1.9/2.1 GHz. The coverage is around 35km and goes up to 200km. The data rate is average 35KBPS 170KBPS. Cellular networks need high power consumption. It is not used for most IoT devices due to security and frequency issues. It can be used in IoT applications like connected cars.

MQTT (Message Queuing Telemetry Transport)

MQTT is a lightweight protocol that accommodates communication between nodes in stable and unstable networks and still functions in networks where the bandwidth is extremely low. It accommodates a publisher subscriber message pattern makes information exchange between different hardware nodes easy. Internet of Things data standards was designed in order to solve the unstable connections. Its design is its main selling point. As a result of its light and minimalist genetic construction, it consumes less energy to power devices

AMQP (Advanced Message Queuing Protocol)

AMQP is a layer protocol for software that offers to route and queue in a message-oriented middleware system. It enjoys limited usage outside middleware environments. AMQP was not developed for the Internet of Things but for financial institutions. AMQP is too power-wasteful to be used by low-powered IoT sensors. The banking sector is the largest consumer of the AMQP protocol.

CoAP (Constrained Application Protocol)

IoT devices based on the HTTP protocol will be favored with this approach. While any IoT device can take advantage of the available internet infrastructure, it is normally too resource-hungry and clumsy for IoT use. It's client-server, as with HTTP, and it supports the REST architecture, so servers will provide resources by URL, and users will be allowed to send GET, POST, PUT, and DELETE requests.

XMPP (Message Protocol and Presence Expansion)

XMPP is highly adaptable and can easily accommodate new circumstances. One of XMPP's best features is how it identifies and addresses nodes. XMPP is a simple and plain protocol that is freely available at no cost. XMPP assigns a unique identifier for every device, much like an email address. A presence indicator, XMPP, was built utilizing the extensible markup language (XML) to show whether servers or devices can be utilized for sending or receiving messages.

HTTP (Hyper Text Transfer Protocol)

The HTTP protocol was briefly mentioned above. The Hypertext Transfer Protocol (HTTP) is are developed so that one computer can transmit data to another computer (server). With the use of this software, people can print 3-D objects from any other computer in the network to any 3-D printer in a network.

DDS (Data Distribution Service)

DDS employs a publish-subscribe paradigm identical to that of MQTT, with only the exception of not employing brokers. Like other scalable IoT protocols, DDS provides high-quality communication in IoT. It includes many potential deployment scenarios from the cloud to small devices.

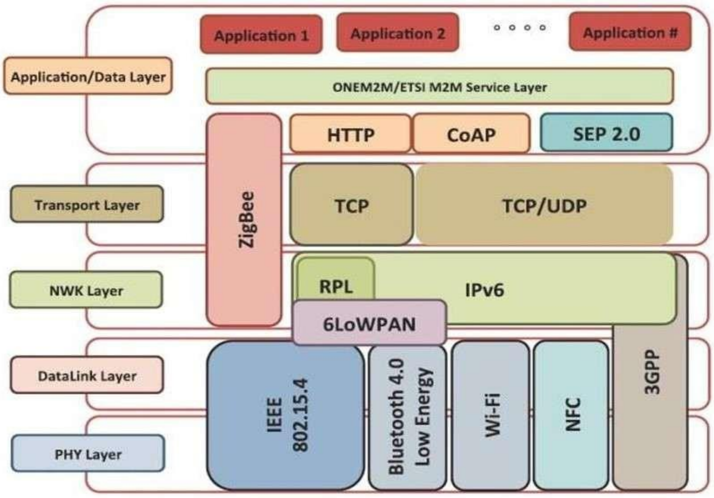

Fig: IoT Network Protocols

Different categories of IoT sensors used are:

1. **Environmental Sensors**

Environmental sensors monitor the environmental conditions of the data centre, whether it is the temperature or humidity. Data Centre DCIM (Infrastructure Management) software gathers, monitors, and reports real-time data from environmental sensors to allow data centre managers to view trends, notifications, power saving, and maximum uptime.

2. **Motion and proximity sensors**

Motion and proximity sensors detect the movement or presence of objects without coming into physical contact with them, using a range of technologies including infrared, electromagnetic fields, or sound waves and are used for many applications from security to automation.

3. **Gas and chemical sensors**

Gas and chemical sensors are equipment's that measure the existence and concentration of different gases and chemicals, utilizing physical or chemical reactions to convert chemical information into electrical signals. They are key applications in environmental monitoring, safety purposes, and different industries.

4. **Optical and imaging sensors**

Imaging and optical sensors are sensors that capture and record light to form images or provide information to the environment, using technologies like CCD and CMOS chips, and used in various applications, including cameras, medical imaging, and remote sensing.

5. **Biometric sensors**

Biometric sensors are sensors that sense and measure unique biological or behavioural characteristics, like fingerprints, facial appearance, or voice characteristics, to identify or authenticate an individual's identity.

6. **Industrial and structural monitoring sensors**

Structural and industrial monitoring sensors, used in applications including bridges, buildings, and industrial equipment, sense changes in other parameters like vibration, strain, and temperature to help maintain structural integrity and safety.

7. **Smart sensors**

Smart sensors, those small, invisible devices, have an important role to play in making the home smarter. They sense fire, water leakage, and intrusion, send an immediate warning through the wireless connection as quickly as possible - each second counts in time-sensitive emergency situations. Proper connected sensors can save time and lives, secure property, and bring peace of mind to users.

8. **Automotive and transportation sensors**

Automotive and transport sensors have an essential function in security, efficacy, and performance, monitoring many car parameters and reporting to control systems, in order to allow choices like ABS, airbags, and advanced driver-assistance systems.

9. **Wearable sensors**

The wearable sensors are the hardware component that capture different types of signals such as, physiological and environmental stimuli and are embedded in our daily devices such as smartphones, smart, head-worn, watches, etc., and other wearable medical devices.

10. **Agricultural and livestock sensors**

Agric and livestock sensors are tools employed to sense and acquire data related to crops, soil, climate, and cattle for improving agricultural processes and the welfare of livestock. Such sensors aid in real-time tracking, Early issue detection, and decision- making for increased efficiency and performance.

11. **Smart city sensors**

Smart city sensors fuelled by the Internet of Things (IoT) collect data in a bid to improve city services, monitor resources, and enhance life for citizens, with themes revolving around traffic, environment, and infrastructure.

12. **Retail and Supply Chain Sensors**

Sensors play a critical role in the retail and supply chain management of today by offering real-time data collection and analysis, leading to greater efficiency, inventory management, and customer service.

13. **Healthcare and Medical Sensors**

Medical and healthcare sensors are devices that detect, measure, and monitor environmental or physiological health-related parameters, through which vital signs can be monitored, diagnosed, and treated, and remote patient monitoring.

14. **Communication and Networking Sensors**

Communication and networking sensors, or Wireless Sensor Networks (WSNs), are groups of wireless sensor nodes that are connected and communicate to gather and report data from their environments, enabling monitoring and control for various applications.

II. LITERATURE REVIEW

Mofareh Waqdan, Habib Louafi, Malek Mouhoub, 2025, [1] "Security risk assessment in IoT environments: A taxonomy and survey" proposed Internet of Things (IoT) applications are an essential aspect of our daily life. But with the growing trend of cybercrimes, it is required to secure cyberspace. Security and privacy of IoT applications are of utmost importance since they are being deployed in mission-critical areas, including healthcare, transportation networks, and power generation. For this reason alone, many studies are also focusing on the security and privacy of the IoT revolution. The need to analyze IoT security threats is increasing. This paper also provides an overview and taxonomy of risk management, analysis, and evaluation methods applied on systems that include IoT devices. More particularly, the paper addresses and classifies existing IoT risk management and assessment frameworks, and types of assessment techniques, risk perspectives, and methodologies. The paper concludes by thoroughly analyzing such frameworks, solutions, and guidelines, and further discusses future research direction. Prof. Dr. Anke Huckauf, Prof. Dr. Frank Kargl, Prof. Dr. Marc Dacier, 2022, [2] "Security risks of IoT devices: from device characteristics of future risk score predictions," proposed developed SAFER, a method to perform security risk analysis of IoT devices. And validated SAFER in the enormous and diverse network infrastructure of the European Organization for Nuclear Research (CERN), where around 312,000 network devices are registered. they used SAFER to scan the IoT devices in this network and process them in a security critical way. To enable SAFER to provide a holistic risk analysis for its users, our framework only needs the host-name of a device to start with. Therefore, to be able to gauge if the users can understand SAFER's risk analysis in a comprehensible manner, they conducted a study on 10 technical and 10 non-technical employees of CERN. Mohammad Beyrouti, Ahmed Lounis, Benjamin Lussier, Abdelmadjid Bouabdallah, Abed Ellatif Samhat, 2024, [3] "Vulnerability-oriented risk identification framework for IoT risk assessment", proposed that the proliferation of Internet of Things (IoT) systems across different applications has led to an alarming increase in interconnected smart devices. But growth in connectivity has created a myriad of vulnerabilities and threats to compromise the security and safety of IoT applications. Security risk assessment methods are commonly used to assess risks. However, traditional IT and present IoT-specialized security testing methods do not address thoroughly important factors of IoT: complex asset intercommunication, system dynamic change, future use of assets as attack platforms, effects of security breaches on safety, and asset resource constraints. Such gaps allow serious risks to be left out of account in the IoT scenario. We introduce here a novel vulnerability-centered risk identification process comprising a four-step procedure as the essential part of IoT security risk assessment, applicable to any IoT system. Our process enhances both traditional and IoT-based security risk assessment procedures through providing tailored methods that overcome their intrinsic deficiencies for comprehensive IoT risk assessment. We validate our process with a case study on an IoT smart healthcare system based on a proposed expert-led method. The results demonstrate our process identifies notable attack scenarios from the lack of sufficient security practices, mobility, and intercommunication processes between the IoT devices within the healthcare system. Moreover, our analysis illustrates probable attacks leveraging the IoT devices as platforms for attacking the backend and user domains. They demonstrated the effectiveness of our risk detection process through simulations of two attack scenarios based on using the Contiki Cooja network simulator. Yewande Goodness Hassan, Anuoluwapo Collins, Gideon Opeyemi Babatunde,2022, "[4] Automated vulnerability detection and firmware hardening for industrial IOT devices", postulated that the mass deployment of Industrial Internet of Things (IIoT) devices has revolutionized industrial systems but has come with huge security issues, primarily related to firmware protection. This review delves into the critical vulnerabilities with IIoT firmware, recognizing the substantial need for automated detection strategies and stringent hardening efforts. Firmware security core work is addressed, such as technological advancements in the form of static and dynamic analysis, machine learning, and policy-based systems. New ways of IIoT firmware security have been criticized within the paper based on the effectiveness in addressing real-world issues. Practical recommendations are provided for researchers and practitioners alike based on scalable solutions and collaborative paradigms to bridge the gaps that currently exist. They also explored future prospects, like adopting advanced tools and standardization efforts, this review aims to help build a resilient and secure IIoT environment. Pascal Oser, Rens W. van der Heijden, Stefan Lüders, Frank Kargl, 2022, [5] "Risk Prediction of IoT Devices Based on Vulnerability Analysis", proposed SAFER, the Security Assessment Framework for Embedded-device Risks, to enable a semi- automated risk evaluation of IoT devices on any network. SAFER consolidates information from network device discovery and automated analysis of firmware to present an estimated current risk from the device. Based on past vulnerability data and vendor patch schedules for the device models, SAFER projects those results into the future using different automatically parameterized predictive models. Based on that, SAFER also forecasts a measure of future security risk. This enables users to be informed about devices with high risks in the future. Results indicate that SAFER identified 531 out of 572 devices successfully and recorded a device identification rate of 92.83 %, parsed 825 firmware images, and made forecasts about current and future security risk for 240 devices. Mohan Krishna Kagita, Giridhar Reddy Bojja, Mohammed Kaosar, 2021,[6] "A framework for intelligent IoT firmware compliance testing", proposed that the existing extensive production and usage of the Internet of Things (IoT) have created serious concerns due to the unavoidable security issues. The IoT device firmware is one of the most significant factors in IoT security. Although different organizations have made security best practices available, not many IoT vendors are successfully deploying these best practices as a result of lack of responsibility or availability of the right resources. Some of these tools are capable of using static, dynamic, or fuzzing techniques to test the security of IoT firmware, and these can sometimes report false positives or fail to detect vulnerabilities. Also, most of the effort is devoted to a single topic, such as networking protocols, web interfaces, or computer applications of Internet of Things. The current paper seeks to present a new method of conducting compliance testing and vulnerability assessment on IoT system firmware, communication interfaces, and networking services from static and dynamic analysis. The proposed system detects a broad range of security vulnerabilities on a broad range of hardware platforms and architectures. In order to actually test and validate our prototype, they tested 4300 firmware images and detected 13,000+ compliance issues. Samira A. Baho, Samira A. Baho, 2023,[7] "Analysis of Consumer IoT Device Vulnerability Quantification Frameworks", presented the hypothesis that the increased deployment of Internet of Things (IoT) devices in mission-critical applications rendered them all the more appealing to attackers. Cyberattacks against IoT devices can potentially reveal confidential information, halt operations, and even endanger lives. For these reasons, IoT security recently gained significant attention in industry and academia. However, no systematic and extensive study of the current IoT vulnerability assessment frameworks exists. To address this lack, this paper systematically explores and assesses the research challenges and state-of-the-art IoT vulnerability assessment frameworks taking both depth and breadth into account. The study enlightens on current IoT vulnerability assessment methods that can add to ongoing efforts in describing cybersecurity threats and dealing with IoT vulnerabilities. It will be useful to a variety of readers, including the IoT research community, cybersecurity researchers, risk and vulnerability management professionals, and others. By offering the latest perspective of existing IoT vulnerability assessment methods, this study will improve IoT security consciousness and facilitate research into methods for assessing IoT vulnerabilities. The knowledge obtained through this study will also benefit future researchers interested in IoT security issues and solutions. They also assist in understanding the research interest in IoT vulnerability evaluation techniques, thus being useful for researchers interested in formulating new methods to identify IoT vulnerabilities. Mohammad Monjur, Joshua Calzadillas, Qiaoyan Yu, 2023,[8] "Hardware Security Risks and Threat Analyses in Advanced Manufacturing Industry" proposed that the advanced manufacturing industry (AMI) also faces many special challenges in the cyber-physical domain. Security threats are contributed from two key elements: software and hardware. Software security has been fully focused upon during the past decade, but hardware security has not been paid enough attention. This paper analyzes the security vulnerabilities of ubiquitous electronic chips deployed to AMI and proposes three attack models for sensing nodes, local processing and storage edge devices, and wired/wireless communication interfaces, respectively. Realistic hardware security attacks are discussed in this paper to stimulate the development of effective countermeasures to hardware Trojans, fault injection attacks, and external signal interference. Apart from that, this paper highlights new security threats from advanced manufacturing implementations. In order to counter those attacks on security in AMI, this paper introduces guidelines for designing the defense approach in a way that it can effectively protect against hardware in AMI. Muhammad Ibrahim; Andrea Continella; Antonio Bianchi, 2023, [9] "AoT - Attack on Things: A security analysis of IoT firmware updates" proposed that the IoT devices possess firmware update mechanisms to close security loopholes and deploy new features. The mechanisms are typically triggered and mediated by mobile companion apps run on the smartphones of the users. While it is crucial to update devices, these operations can create severe security vulnerabilities if they are not correctly executed. Because of their criticality, in this paper we perform a systematic security evaluation of the firmware update processes employed by IoT devices via their companion apps. We first create a threat model for IoT firmware updates, and we categorize the different possible security issues affecting them. Then, we scan 23 most popular IoT devices (and their respective companion apps) for vulnerable devices and the SDKs that the devices use to incorporate the update functionality. We discover that 6 of the most widely used SDKs contain perilous security flaws. We further fingerprint every vulnerable SDK and they utilize our fingerprints to perform a large-scale study of companion apps on the Google Play Store. Their results show that 61 leading devices and 1,356 apps rely on insecure SDKs, thus they might use an insecure firmware update mechanism. Ibrahim Nadira, Haroon Mahmooda, Ghalib Asadullahb, 2021, [10] "A Taxonomy of IoT Firmware Security and Principal Analysis Techniques", had envisioned Internet of Things (IoT) has come a long way from where it began. However, the standardization process in IoT systems for a secure IoT solution is still in its nascent stage. Several quality review papers have been published by researchers on existing frameworks, architectures, as well as IoT threats on different layers. Nonetheless, most of the prior existing work has neglected the firmware security aspects in the IoT context. They wish to fill this gap by publishing, to our best knowledge, the first comprehensive review paper on IoT device firmware (in)security. Starting from the necessity of firmware security, this paper recognizes the rationale for firmware insecurity by addressing technical, commercial, standardization, and research-related issues. In particular, the scope, history, and inner workings of IoT firmware and their security implications are addressed. Besides, a taxonomy-based classification of IoT firmware vulnerabilities has been outlined to focus on the most common issues in IoT firmware. They also depict challenges in identifying firmware vulnerabilities before conducting thorough analysis of existing vulnerability assessment techniques and tools. Comparison of popular solutions is depicted in terms of vulnerabilities they identify, the process applied, and the platform and/or architecture they cater to. Finally, some research challenges have been pointed out to encourage and facilitate research in the firmware security domain of IoT. The system simulates an end-to-end risk assessment system for an IoT sensor network with focuses on firmware obsolescence, communication activity, and known security exploits. It generates synthetic data for 100 varied IoT sensors across various industries such as environmental monitoring, healthcare, agriculture, industrial automation, and smart homes. Each sensor is associated with a hardware model, firmware version, and last communication time. The current system demonstrates the benefits of utilizing lightweight device profiling along with firmware analysis-based risk prediction and show even greater analysis of dynamic intercommunications and attack surfaces, areas beyond that would enhance this system. Studies like "Attack on Things" (AoT) recognize the direct threat imposed by insecure firmware update processes and stresses the need to not only identify outdated firmware but also verify the integrity and security of the update protocols. Firmware Security Taxonomies note that the majority of firmware vulnerabilities remain undetected in the absence of extensive static and dynamic analysis, suggesting possible extensions for the current system to perform more extensive firmware security scanning. The detection of vulnerabilities is limited to pre-defined cases and fails to dynamically check unknown threats or perform extensive firmware inspection. The system does not mimic actual network behaviours, device dependencies, or mobile firmware update processes, which are new risk factors on the increase.

III. PROBLEM STATEMENT

In the IoT ecosystem with about 100 connected devices, it is important to provide cybersecurity. Obsolete hardware and software parts greatly raise the risk of cyber-attacks for the network. In order to eliminate this problem, it is necessary to create a systematic approach and algorithm that can detect obsolete hardware and software for all the devices. This solution should enable timely patches and upgrades in order to offset possible security vulnerabilities, improve system integrity, and ensure best-practice cybersecurity compliance.

Proposed Solution

The proposed solution aims to enhance security and maintenance of IoT sensor networks through a self-operating system for firmware outdatedness detection and security threats. The system, through simulation of a diverse set of 100 IoT sensors across all industries, continuously monitors key parameters such as firmware version, the time when it last communicated, and known weaknesses. It evaluates the individual sensor to calculate a total risk score considering firmware obsolescence, delay in communication, and exposure of vulnerabilities. The system then categorizes devices into low, medium, and high risk and also marks the devices that require an immediate firmware update. In addition to delivering actionable information, the system provides visual analytics in the form of pie charts to provide overall upgrade requirement status and sensor distribution according to risk levels such that network administrators can easily understand. Modular structure facilitates seamless extension to real sensor data and incorporation into large IoT device management frameworks. Future improvements can involve using more extensive dynamic vulnerability scanning, automating firmware patch suggestions, incorporating predictive risk analytics based on machine learning models, and mitigating next- generation attack surfaces investigated in ongoing studies. Ultimately, this solution will be aimed at facilitating proactive management of IoT device security, minimizing operational downtime, and quelling cybersecurity threats more efficiently.

System Design

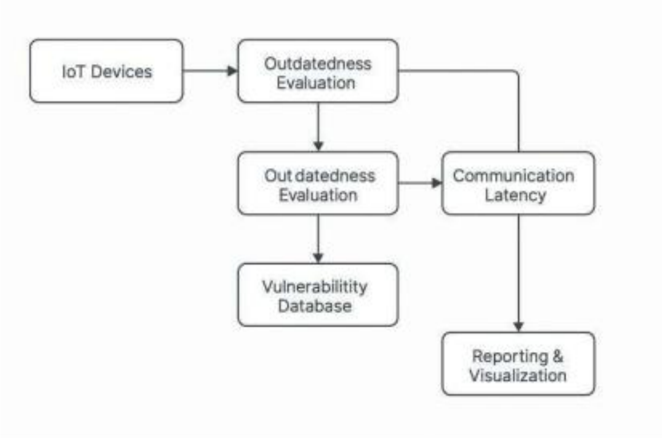

Fig: System Architecture Diagram

IV.METHODOLOGY

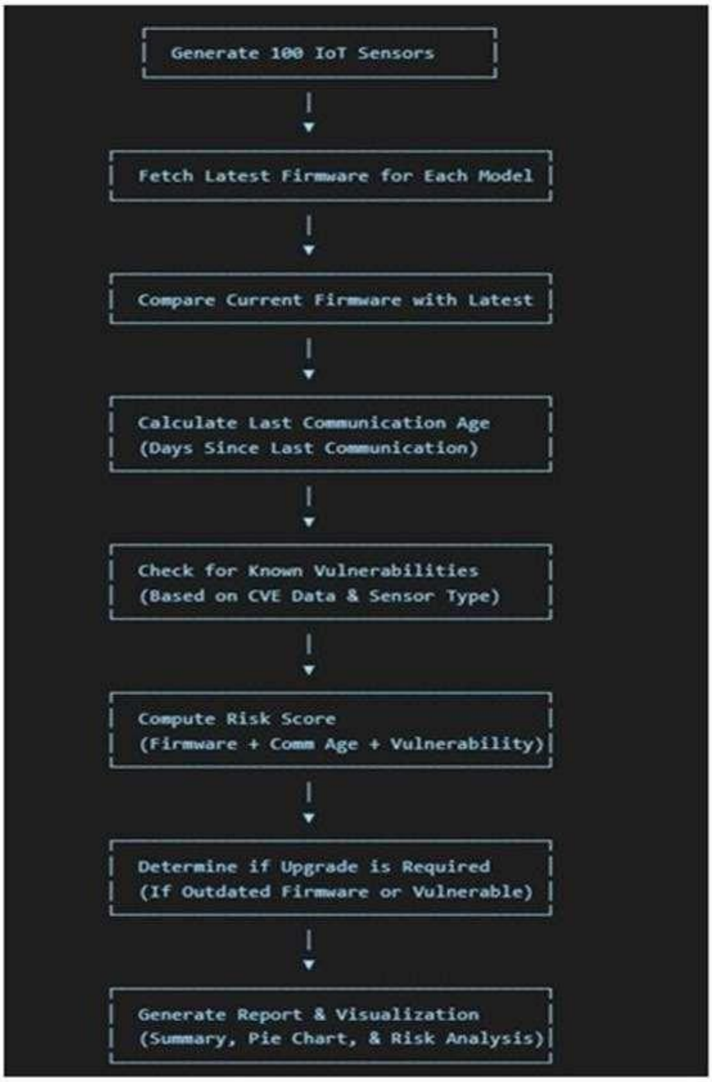
Generate 100 IoT Sensors
Fetch Latest Firmware for Each Model
Compare Current Firmware with Latest
Calculate Last Communication Age (Days Since Last Communication)
Check for Known Vulnerabilities (Based on CVE Data & Sensor Type)
Compute Risk Score (Firmware + Comm Age + Vulnerability)
Determine if Upgrade is Required (If Outdated Firmware or Vulnerable)
Generate Report & Visualization (Summary, Pie Chart, & Risk Analysis)

Fig: Methodology Diagram

Detailed Description of methodology

Methodology describes the process of analysis of IoT sensor data, establishing their obsolescence, identifying vulnerabilities, and whether an upgrade should be necessary. The audit is firmware version based, last communication timestamp, and potential security threat. To simulate a real IoT network, we have considered 100 IoT sensors with random features, such as sensor ID, which is treated as a unique identifier for a sensor, and sensor type, which represents the kind of sensors used, along with the present firmware and hardware type, which represents the firmware versions and hardware models used, and the last communication time, which is the days since the last communication, between 0 to 90 days back, to simulate inactive devices. The latest firmware for each sensor is computed based on its hardware model, i.e., Model A as 2.0, Model B as 1.5, Model C as 2.3, and Model D as 1.8. The latest firmware is then compared with the latest version; if they are the same, there is no update; otherwise, the update is necessary. Then, the difference between the current date and the last comms date will be computed to check if the sensor is idle. If the last comms date is higher, then it is highly likely that the sensor has broken down or that it won't show the proper result. After that, we will compute the risk score to determine whether the A sensor has to be upgraded or not.

Implementation

The application process of this IoT sensor firmware analysis system involves a series of significant steps in order to conduct monitoring and evaluation efficiently. Data is initially generated through the emulation of 100 IoT sensors with randomly selected attributes from various categories. Subsequently, the most recent firmware is loaded in each piece of hardware in order to compare with existing firmware in order to determine whether it requires updating. Outdated firmware status and communication age are calculated, and stale sensors are marked. A risk score is then determined by giving firmware outdatedness, communication age, and vulnerability information weight to help decide on the risk level each sensor poses. Based on this calculation, sensors that require updating are identified to help ensure devices that possess outdated firmware or have security concerns are updated first. The final result is a structured output displaying the risk level, vulnerabilities, and upgrade requirement of each sensor, and then an overview indicating the number of sensors scanned and those needing an upgrade. A pie chart visualization is also produced to provide a clear picture of the percentage of sensors requiring attention.

Pseudo code

Input: A list of IoT sensors (100 devices), each with sensor id, sensor type, current firmware, hardware model, and last communication timestamp.

Output: Upgrade status and risk score for each sensor and Summary statistics. Step 1: For each of the 100 IoT sensors:

```
    • Randomly assign a sensor_type from a predefined list
    • Randomly assign a hardware_model from available models
    • Generate a current_firmware version
    • Simulate last_comm (last communication timestamp) within the past 90 days
Step 2: Define a function get_latest_firmware(model, type) that returns the latest known firmware version for each hardware_model
Step 3: For each sensor:
• Compare the current_firmware with latest_firmware
    ➢ If different → set firmware_diff = 1, else firmware_diff = 0
• Calculate comm_age = days_since(last_comm)
• Identify known vulnerabilities (e.g., CVEs) based on firmware/hardware/type
    ➢ Count vulnerabilities to get vulnerability_score
Step 4: Calculate the following for each sensor:
• outdatedness_score = firmware_diff + comm_age
• risk_score = outdatedness_score + vulnerability_score
• upgrade_required = True if firmware_diff > 0 or vulnerability_score >
Step 5: Aggregate and display results:
• Print sensor details with risk_score, upgrade_required, vulnerabilities
  Count and display:
  ➢ Number of sensors requiring upgrades
  ➢ Pie chart of upgrade vs. non-upgrade
  ➢ Risk score distribution: Low (≤30), Medium (31–60), High (>60)
```

V. RESULTS AND DISCUSSION

Implementation is able to mimic 100 IoT sensors, and each sensor has a unique set of sensor types, hardware model, and firmware level. The system monitors the firmware status of every sensor, communication age, risk, and risk score for determining whether an upgrade is required. Through the implementation, it was found that 134 sensors out of 100 require upgrade. The results also indicate that risk scores vary based on firmware obsolescence, communication era, and vulnerabilities. An upgrade status pie chart provides a quick view of the percentage of sensors due for an upgrade compared to those which are up to date.

A pie chart diagram of risk scores categorizes sensors based on their risk levels, providing a sense of the gravity of potential security issues.

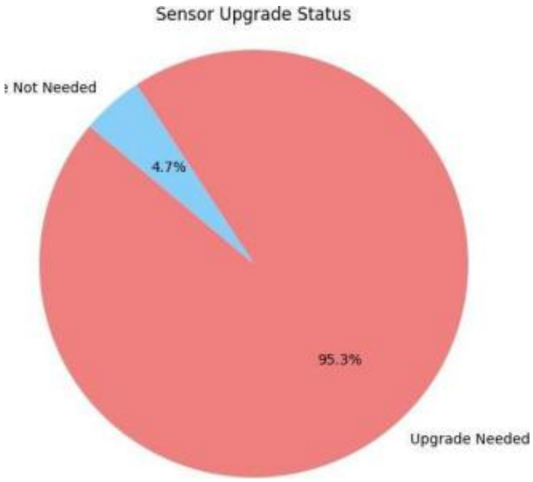

Fig: Pie chart for Sensor Upgrade Status

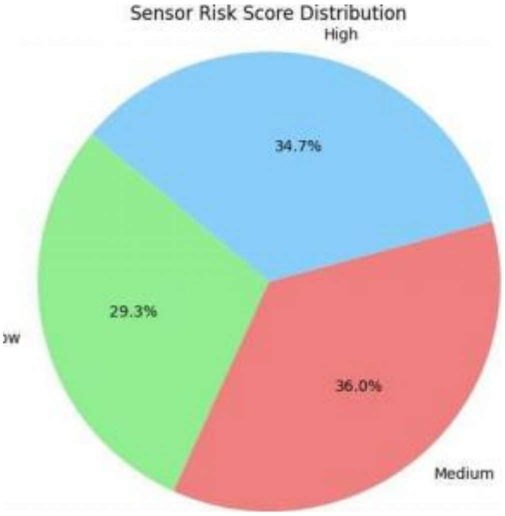

Fig: Pie chart for Sensor Risk Score Distribution

VI. CONCLUSION

The successfully installed system evaluates firmware status, communication history, and 100 IoT simulated sensor vulnerabilities. Examining firmware versions, the timestamp of last communication, and potential security threats, the model calculates which sensors need updating. The result shows that the majority of sensors (134 out of 100) need to be updated due to outdated software and long periods of communication disconnection.

The automated risk assessment model provides a structured approach to sensor update ranking to ensure timely performance and security optimization. Having the aid of a risk score makes decision-making efficient, with the allocation of resources on the most vulnerable devices. In addition, the use of pie chart visualization aids the interpretability of results through clearly showing the percentage of sensors to be addressed.

Risk score distribution pie chart categorizes sensors based on their risk levels, providing information about the gravity of potential security threats. Most of the high-risk sensors are associated with outdated firmware and large communication gaps.

This study highlights the importance of autonomous firmware testing and risk analysis in IoT security. Future development may also involve real-time monitoring and auto-firmware updates to enable continuous security and performance enhancement.

REFERENCES

1 F. Ebbers, “A Large-Scale Analysis of IoT Firmware Version Distribution in the Wild,” 2022.
2 K. Oliynyk, “Firmware Analysis for IoT Devices,” 2024.
3 H. M. G. A. Ibrahim Nadira, “A taxonomy of IoT firmware security and principal firmware analysis techniques,” 2022.
4 Q. N. M. A. T. Meriem Bettayeb, “Firmware Update Attacks and Security for IoT Devices,” 2019.

5 H. M. G. A. Ibrahim Nadir, “A taxonomy of IoT firmware security and principal firmware analysis techniques,” 2022.

6 B. G. Taimur Bakhshi, “A Review of IoT Firmware Vulnerabilities and Auditing Techniques,” 2024.

7 B. S. D. Keshav Kaushik, “Framework to analyze and exploit the smart home IoT firmware,” 2024.

8 G. R. B. Mohan Krishna Kagita, “A framework for intelligent IoT firmware compliance testing,” 2021.

9 M. E. O. Marco Grossi, “Security Issues and Solutions for the Internet of Things,” 2025.

10 10 S. R. G. Yashwant Singh, “A survey on IoT & embedded device firmware security: architecture, extraction techniques, and vulnerability analysis frameworks,” 2023.