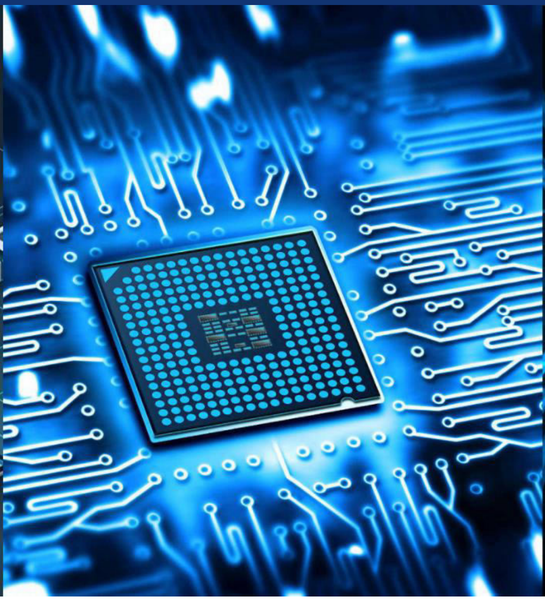
IJIRCCE

ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Impact Factor: 8.771

Volume 13, Issue 5, May 2025

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

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

Prajwal S P, Dr. Mohammed Rafi R

PG Student, Department of Computer Science and Engineering, University B.D.T College of Engineering, Davanagere, Karnataka, India

Professor, Department of Computer Science and Engineering, University B.D.T College of Engineering, Davanagere, Karnataka, India

ABSTRACT: This paper describes the creation and implementation of a Python system for evaluating the obsolescence and possible vulnerabilities in a simulated 150 varied IoT sensor deployment. The system creates artificial sensor data, including essential features like sensor ID, type (ranging from environmental, wearable, industrial, and automotive types), current firmware version, hardware model, and last communication timestamp. It then uses a set of simulated functions to determine the most recently available firmware for a given sensor's hardware and type, measure the difference between current and most recent firmware, calculate the time elapsed since the last sensor contact, and flag potential security exposures, using a basic CVE database indexed on hardware model and firmware version. The analysis is centered on determining an "outdatedness score" per sensor, derived from the combined effect of firmware version mismatch and communication inactivity. In addition, a "vulnerability score" is computed by the number of recognized Common Vulnerabilities and Exposures (CVEs). The two scores are combined to calculate a complete "risk score," allowing an overall measurement of each sensor's operational and security status. The system alerts sensors requiring firmware updates and classifies the entire risk distribution over the simulated sensor network into Low, Medium, and High tiers.The report illustrates major findings through descriptive pie charts, graphically depicting the percentage of sensors marked for immediate firmware updates and the breakdown of calculated risk scores within the simulated IoT setting. This analysis provides a basic framework for proactive lifecycle management and increased security within IoT sensor networks, accurately identifying devices in need of immediate action because of obsolete software or publicly reported security vulnerabilities. Although based on modeled data and working implementations, this process easily illustrates an effective methodology that can be applied to real-world management of IoT devices and overall security audits, providing useful information regarding possible threats and required maintenance procedures.

KEYWORDS: IoT Sensors, Synthetic Sensor Data, Firmware Version Assessment, Risk Score Aggregation, Firmware Upgrade Requirement, Simulated IoT Network Analysis, Security Testing Framework, IoT Device Management

I. INTRODUCTION

Internet of Things or IoT is designed to be the future of today's Internet. It is typically described as a network of physical and virtual objects, devices, or things that are able to gather surrounding data and share it among them or over the Internet. In order to facilitate data gathering, devices are equipped with sensors, software, and electronics; their exchange capability is provided by making them accessible through local area networks or the Internet.

The history of the Internet of Things is spread out. Although the term was originally used in 1999 by Kevin Ashton, co-founder and executive director of the Auto-ID Centre at MIT, for organizations like CISCO, the IoT was born in 2009, when there were more devices than humans on the Internet. The number of connected devices at that time was 10 billion, but the expectations are benevolent. It is estimated that by 2020, there will be more than 50 billion devices connected to the Internet. As one can see from the statistics, in recent years, the Internet of Things has witnessed an unforeseen rise in popularity.

IoT Architecture

The definition of IoT architecture is the structure that outlines how different IoT components (e.g., devices, networks, sensors, apps) that interact in an IoT environment. IoT architecture usually comprises a number of layers and elements which serve a range of operations from physical devices, and data acquisition systems, to network devices transmitting IoT data to data processing applications, and IoT data storage.

Layers of IoT architecture

To realize IoT architecture and identify the correct IoT solutions for an organization, it's important to learn about IoT layer architecture. In this case, an example of a five-layer IoT architecture will be employed for discussion. Perception layers the perception layer exchanges data with the physical environment to collect raw data.

Such IoT devices as sensors and cameras collect information and images passively that will be transported through the transport layer (e.g., network layer), whereas actuators tell devices to do things based on sensor readings or other commands in IoT systems. (Actuators are physical devices that transform energy into motion.)

Transport layer

The transport layer, also referred to as the network layer, manages the flow and data transfer between the sensors in the perception layer and the processing layer through multiple networks (e.g., data transfer) between IoT devices and backend systems by Wi-Fi, Bluetooth, etc.).

Processing layer

Data processing layer, also known as the middleware layer, stores, analyzes, and pre-processes. The information received from the transport layer. These involve such processes as data aggregation, protocol translation, and security enforcement to ready data for the application layer. Additionally, message brokers, IoT platforms, and edge computing nodes can also be added in this layer.

Application layer

The application layer includes software applications that utilize the processed data collected in the perception layer to complete tasks or gain insights using advanced analytics. Databases, data warehouses, and data lakes are all covered under the application layer.

Business layer

The business layer is most likely the most universally found IoT architecture layer in that it encompasses user interfaces, dashboards, and data visualization software which most business individuals are used to employing on a daily basis. It's in the business layer that all the data gathered and processed generates value by offering insights and fuelling business decisions.

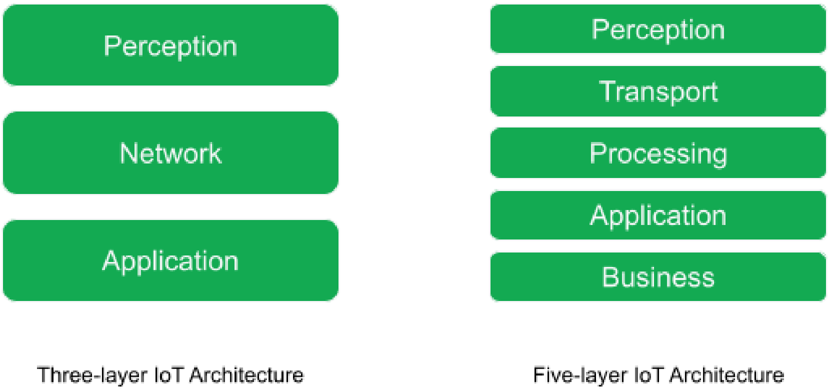


Fig: IoT Architecture

IoT Network Protocols

Bluetooth

Bluetooth operates in the frequency band of 2.4GHz. It has a range of 10m to 100m, and its data rate increases up to 1MBPS. It supports two network topologies point-to-point and mesh. It is suitable to send a small amount of information to personal devices such as speakers, earphones, smart watches, smart shoes, etc. The protocol can also use by Smart Homes, such as Alarms, HVAC, lighting, etc.

Zigbee
This is done following the IEEE802.15.4 standard. Its range frequency is as low as Bluetooth is, 2.4GHz. It has a maximum range of 100 meters with a maximum data rate of 250KBPS. The zigbee protocol will send small-sized data across short distances. It can be used in those systems where it's necessary for more authentication and sturdiness. It is supported by star topology, mesh topology, and cluster tree topology. Significant applications seen are monitoring device health in industries, smart homes, etc.

6LoWPAN
PAN is an abbreviation for Personal Area Network, and 6LoWPAN is an abbreviation for IPV6 Low Power PAN. It operates in a frequency of 900 to 2400MHz. The data rate is 250KBPS with two network topologies - star and mesh.

Wireless LAN - Wi-Fi
Wi-Fi provides a high band and supports the data rate of 54MBPS and goes as high as 600MBPS. The range is up to 50m in local area were providing individual antennas up to 30 km. Wi-Fi can connect IoT devices very easily and have a lot of data to be shared. Smart homes, smart cities, office spaces, etc. use this protocol.

LoRaWAN
This is the acronym for Long Range Wide Area Network. The range is about 2.5km and goes up to 15km. The data rate is very slow, which is 03, and KBPS and reaches up to a maximum of 50KBPS. It supports lots of connected devices and is used in applications such as Smart City, Supply Chain Management, etc.

LTE-M
LTE-M is an abbreviation for Long Term Evolution for Machines. It is a form of LPWAN Low Power Wide Area Network. It is utilized in combination with cellular networks to offer security. LTE-M operates within a frequency band of 1.4MHz-5MHz, and the data rate can reach up to 4MBPS.

Sigfox
Sigfox is employed when a wide area is needed to be covered with minimal power consumption. It is intended to connect billions of IoT devices. The frequency range of this protocol is 900MHZ with a range of 3km to 50km. The data rate is very low with a maximum of 1KBPS.

Cellular
It is also referred to as a mobile network. Cellular networks are 2G, 3G, 4G, and 5G. It has frequency ranges of 900MHz, 1.8/1.9/2.1 GHz. The range is about 35km and reaches up to 200km. The average data rate is 35KBPS 170KBPS. Cellular networks require high power consumption. It is not employed for the majority of IoT devices owing to security and frequency concerns. It can be employed in IoT applications such as connected cars.

MQTT (Message Queuing Telemetry Transport)
MQTT is a light protocol that supports communication among nodes in reliable and unreliable networks and still works in networks with very limited bandwidth. It supports a publisher subscriber messaging model enables effortless exchange of information among disparate hardware nodes. Internet of Things data standards was created to address unstable connections. MQTT design is its core selling point. Due to its lightweight and simple genetic makeup, it uses less power to operate devices.

AMQP (Advanced Message Queuing Protocol)
AMQP is a software layer protocol that provides to queue and route in a message-oriented middleware environment. It has, however, limited adoption in other environments. AMQP was initially designed for financial institutions and not the Internet of Things. AMQP is too power-hungry to be utilized by low-powered IoT sensors. The banking industry is the most significant user of the AMQP protocol.

CoAP (Constrained Application Protocol)
IoT devices running on the HTTP protocol will be advantageous with this strategy. Although any IoT device is capable of leveraging the existing internet infrastructure, it tends to be too resource-intensive and cumbersome for IoT applications. It's a client-server, similar to HTTP, and it accommodates the REST architecture, so servers will make resources available by URL, and users will be permitted to issue GET, POST, PUT, and DELETE requests.

XMPP (Message Protocol and Presence Expansion)
XMPP is flexible and can readily adapt to new situations. How XMPP identifies and addresses nodes is one of its standout characteristics. XMPP is a straightforward and simple protocol that is openly are available at no charge. XMPP provides a unique identifier for each device, similar to an email address. A presence indicator, XMPP, was constructed using the extensible markup language (XML) to indicate whether servers or gadgets can be used to send or receive messages.

HTTP (Hyper Text Transfer Protocol)
The HTTP framework was discussed briefly earlier. The Hypertext Transfer Protocol (HTTP) was are created so that a single computer can send data to another computer (server). Using this software, users can print 3-D objects from any connected computer to any 3-D printer on a network.

DDS (Data Distribution Service)
DDS uses a publish-subscribe strategy similar to MQTT, except for the difference in not having brokers. As in other scalable IoT protocols, DDS ensures high-quality communication in IoT. It contains numerous potential deployment environments, ranging from the cloud to small devices.

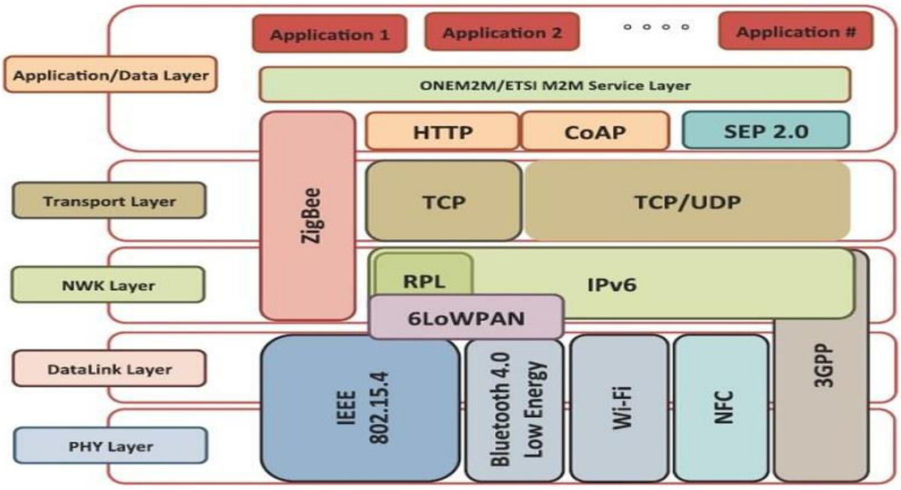


Fig: IoT Network Protocols

Different categories of IoT sensors used are:
1. Environmental Sensors
Environmental sensors monitor the environmental conditions of the data centre including the temperature and humidity. Real-time data from environmental sensors is gathered, monitored, and reported by Data Centre DCIM (Infrastructure Management) software to enable data centre managers to observe trends, receive notifications, save power, and maximize uptime.

2. Motion and proximity sensors
Motion and proximity sensors sense the presence or movement of objects without touching them, employing a variety of technologies such as infrared, electromagnetic fields, or sound waves and are applied to various uses 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 play a key application in environmental monitoring, safety purposes, and different industries.

4. Optical and imaging sensors

Optical and imaging sensors are sensors that sense and record light, creating images or giving information for the environment, employing technologies such as CCD and CMOS chips, and utilized in different applications, such as cameras, medical imaging, and remote sensing.

5. Biometric sensors

Biometric sensors are sensors that detect and measure distinctive biological or behavioural traits, such as fingerprints, facial appearance, or voice characteristics, to recognize or authenticate a person's identity.

6. Industrial and structural monitoring sensors

Structural and industrial monitoring sensors, utilized in fields such as bridges, buildings, and industry equipment detect variations in other parameters such as vibration, strain, and temperature, assisting to ensure structural integrity and safety.

7. Smart sensors

Smart sensors, those tiny, invisible machines, play a vital part in making homes smarter. They detect fire, water leakage, and intrusion, immediately send an alert via the wireless link as soon as possible - every second accounts in time-critical emergencies. Correct connected sensors can save time and lives, safeguard property, and provide peace of mind to users.

8. Automotive and transportation sensors

Automotive and transportation sensors play a vital role in safety, efficiency, and performance, tracking numerous vehicle parameters and sending data to control systems, to facilitate options such as ABS, airbags, and advanced driver-assistance systems.

9. Wearable sensors

The wearable sensors are the hardware aspect that record various kinds of signals including, physiological and environmental cues and are integrated into our everyday devices like smartphones, smart, watches, head-worn, etc., and other wearable medical devices.

10. Agricultural and livestock sensors

Agricultural and livestock sensors are instruments used to monitor and gather information concerning crops, soil, weather, and livestock for enhancing farming processes and ensuring the well-being of animals. These sensors assist in monitoring in real-time, Early problem detection, and making informed choices for enhanced efficiency and productivity.

11. Smart city sensors

Intelligent city sensors driven by the Internet of Things (IoT) gather information in order to make city services better, track resources, and improving citizen life, with themes such as traffic, environment, and infrastructure.

12. Retail and Supply Chain Sensors

Sensors have a very important function in today's retail and supply chain management through providing real-time data gathering and analysis, resulting in increased efficiency, inventory control, and customer service.

13. Healthcare and Medical Sensors

Medical and healthcare sensors are equipment that measure, detect, and monitor environmental or physiological health-related parameters, which allow for monitoring of vital signs, diagnostics, and treatment, and remote patient care.

14. Communication and Networking Sensors

Communication and networking sensors, or Wireless Sensor Networks (WSNs), are networks of connected wireless sensor nodes that exchange information to collect and report data from their surroundings, allowing monitoring and control for diverse applications.

II. LITERATURE REVIEW

Mofareh Waqdan, Habib Louafi, Malek Mouhoub, 2025, [1] "Security risk assessment in IoT environments: A taxonomy and survey" suggested Internet of Things (IoT) applications are a necessary part of our everyday life. But due to the increasing frequency of cybercrimes, it has become necessary to ensure cyberspace security. The security and privacy of IoT applications are paramount because they are implemented in mission-critical domains, such as healthcare, transportation systems, and energy generation. Due to this reason, numerous studies are also addressing the security and privacy of the IoT revolution. The requirement for evaluating IoT security threats is growing. This paper also offers a survey and taxonomy of risk management, analysis, and evaluation approaches implemented on systems comprising IoT devices. Specifically, the paper discusses and categorizes current IoT risk management and assessment frameworks, and various assessments techniques, risk viewpoints, and methodologies. The paper concludes with an in-depth analysis of these frameworks, solutions, and guidelines, and elaborates on future research trends.

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", suggested developed SAFER, an approach to carry out security risk assessments of IoT devices. And tested SAFER in the vast and diverse network infrastructure of the European Organization for Nuclear Research (CERN), where approximately 312,000 network devices are registered. they utilized SAFER to scan the IoT devices in this network and analyse them in a security critical manner. To allow SAFER to give a holistic risk analysis for its users, our framework simply requires the host-name of a device to begin with. So, in order to assess whether users are able to interpret SAFER's risk analysis in an understandable way, they ran a study involving 10 technical and 10 non-technical CERN workers.

Mohammad Beyrouti, Ahmed Lounis, Benjamin Lussier, Abdelmadjid Bouabdallah, Abed Ellatif Samhat, 2024, [3] "Vulnerability-oriented risk identification framework for IoT risk assessment", suggested that the spread of Internet of Things (IoT) systems over various applications has resulted in a significant rise in interconnected smart devices. However, this connectivity growth has caused a wide range of vulnerabilities and threats to undermine the security and safety of IoT applications. Security risk assessment techniques are widely utilized to evaluate risks. Nevertheless, conventional IT and the current IoT-specific security assessment techniques tend not to deal comprehensively with critical aspects of IoT: intercommunication between complex assets, system changes dynamically, prospective use of assets as attack platforms, security breach effects on safety, and resource limitations of assets. Through such gaps, major risks are being omitted in the IoT environment. We present in this paper a new vulnerability-focused risk identification process that involves a four-step procedure as a fundamental component of IoT security risk assessment, transferable to any IoT system. Our process upgrades both conventional and IoT-centred security risk assessment procedures by offering customized methods that counter their essential shortcomings for holistic IoT risk assessment. We verify our process through a case study on an IoT smart healthcare system based on a suggested expert-driven method. The findings prove our process clearly recognizes significant attack scenarios from the absence of adequate security practices, mobility, and intercommunication processes among the IoT devices in the healthcare system. In addition, our analysis shows likely attacks exploiting the IoT devices as platforms for attacking the backend and user domains. They proved the efficacy of our risk identification process with simulations of two attack scenarios derived 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", suggested that the wide-scale adoption of Industrial Internet of Things (IIoT) devices has transformed industrial systems but has brought with it immense security concerns, especially concerning firmware protection. This review explores the essential vulnerabilities with IIoT firmware, identifying the significant need for automated detection methodologies and strong hardening measures. Core work in firmware security is covered, including technological innovations like static and dynamic analysis, machine learning, and policy-based systems. The paper critiques new methods of securing IIoT firmware, highlighting the efficiency of handling real-world problems. Practical advice for researchers and industry professionals is offered, basing itself on scalable solutions and collaborative frameworks to close existing gaps. They also ventured into future possibilities, such as embracing enhanced tools and standardization initiatives, this review seeks to assist in creating a resilient and secure IIoT ecosystem.

Pascal Oser, Rens W. van der Heijden, Stefan Lüders, Frank Kargl, 2022, [5] "Risk Prediction of IoT Devices Based on Vulnerability Analysis", suggested SAFER, the Security Assessment Framework for Embedded-device Risks, to allow a semi-automated risk assessment of IoT devices across any network. SAFER brings together data from network device discovery and automated analysis of firmware to provide an estimated current risk from the device. On the basis of historical vulnerability information and vendor patch cycles for device models, SAFER extrapolates those findings into the future based on various automatically parameterized prediction models. On the basis of that, SAFER also predicts an indicator of future security threats. This allows users to know about devices posing high risks in the future. Results show that SAFER successfully identified 531 out of 572 devices and achieved a rate of device identification of 92.83 %, analysed 825 firmware images, and predicted 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", suggested that the current large-scale production and application of the Internet of Things (IoT) have raised serious issues because of the inevitable security challenges. The firmware of IoT devices is one of the most important elements in IoT security. While various organizations have published security best practices, few IoT suppliers are implementing these best practices effectively due to a lack of responsibility or access to proper resources. Some of these tools can apply static, dynamic, or fuzzing methods for testing the security of IoT firmware, and these may yield false positives or miss vulnerabilities. In addition, most of the resources are allocated to one topic, e.g., networking protocols, web interfaces, or computer applications of Internet of Things. This paper intends to introduce a new approach to performing compliance testing and vulnerability assessment on IoT system firmware, communication interfaces, and networking services based on static and dynamic analysis. The suggested system identifies a wide variety of security flaws on a large variety of hardware architectures and platforms. To actually test and verify our prototype, they tested 4300 firmware images and identified 13,000+ compliance problems.

Samira A. Baho, Samira A. Baho, 2023,[7] "Analysis of Consumer IoT Device Vulnerability Quantification Frameworks", suggested that the growing use of Internet of Things (IoT) devices in mission-critical systems made them even more attractive to attackers. Cyberattacks targeting IoT devices can potentially disclose sensitive information, suspend operations, and even risk lives. Consequently, IoT security has recently gained prominence in industry and academia. Yet, there is no systematic and comprehensive research on existing IoT vulnerability assessment frameworks. In response to this shortcoming, this paper methodically examines and evaluates the research challenges and state-of-the-art IoT vulnerability assessment frameworks with consideration of both depth and breadth. The research sheds light on present IoT vulnerability assessment methodologies that can contribute to continued efforts in characterising cybersecurity threats and coping with IoT vulnerabilities. It will be of interest to a range of readers, including the IoT research community, cybersecurity researchers, risk and vulnerability management experts, and others. By providing the most recent view of the current IoT vulnerability assessment methods, this research will enhance IoT security awareness and enable research into IoT vulnerability assessment methods. The information gained from this research will also be helpful to upcoming scholars interested in IoT security problems and solutions. They also help comprehend the research focus in IoT vulnerability assessment methods, hence making it useful for scholars interested in developing new techniques to identify IoT vulnerabilities.

Mohammad Monjur, Joshua Calzadillas, Qiaoyan Yu, 2023,[8] "Hardware Security Risks and Threat Analyses in Advanced Manufacturing Industry" suggested that the advanced manufacturing industry (AMI) is confronted with numerous special challenges in the cyber-physical field. Security threats are derived from two essential components: software and hardware. Software security has been given full attention over the last decade, while hardware security has not been adequately noticed.

This paper examines the security weaknesses of common electronic chips implemented to AMI and suggests three models for attacks on sensing nodes, local processing and storage edge devices, and wired/wireless communication interfaces, respectively. Realistic security attacks on hardware are presented in this paper to motivate the creation of viable countermeasures against hardware Trojans, fault injection attacks, and external signal interference. In addition, this paper emphasizes novel security threats from advanced manufacturing applications. To address those security attacks in AMI, this paper proposes guidelines for designing the defence method to help effectively defend against hardware in AMI.

Muhammad Ibrahim; Andrea Continella; Antonio Bianchi, 2023, [9] "AoT - Attack on Things: A security analysis of IoT firmware updates" suggested that the IoT devices have firmware update mechanisms to patch security vulnerabilities and roll out new functionalities. These mechanisms are usually initiated and brokered by mobile companion apps executed on the users' smartphones. Although it is important to update devices, these processes can lead to serious security vulnerabilities if they are not properly implemented. Due to their importance, in this paper we conduct a systematic security analysis of the firmware update processes used by IoT devices through their companion apps. We first establish a threat model for IoT firmware updates, and we classify the various possible security issues that impact them. Next, we examine 23 popular IoT devices (and their companion apps) to find vulnerable devices and the SDKs that these devices employ to integrate the update functionality. We find that 6 popular SDKs have dangerous security vulnerabilities. We also fingerprint each vulnerable SDK and they use our fingerprints to conduct a large-scale analysis of companion apps from the Google Play Store. Their findings indicate that 61 top devices and 1,356 applications depend on insecure SDKs, therefore, they may employ an insecure firmware update model.

Ibrahim Nadira, Haroon Mahmooda, Ghalib Asadullahb, 2021, [10] "A Taxonomy of IoT Firmware Security and Principal Analysis Techniques", envisioned Internet of Things (IoT) has evolved a long way from its birth. Nevertheless, the standardization process in IoT systems for a secure IoT solution is in the initial stages. Various quality review papers have been authored by researchers on currently available frameworks, architectures, as well as IoT threats on various layers. Nonetheless, the majority of the previously available work has overlooked the firmware security aspects within the IoT landscape. They want to bridge this gap by presenting, to our knowledge, the first thorough review paper of IoT device firmware (in)security. Beginning with the need for firmware security, this article acknowledges the compelling reasons for firmware insecurity by covering technical, commercial, standardization, and research-oriented aspects. Specifically, the scope, evolution, and internals of IoT firmware and their security implications are covered. In addition, a taxonomic classification of IoT firmware vulnerabilities has been described to emphasize the most prevalent problems in IoT firmware. They also present complications in detecting firmware vulnerabilities prior to performing in-depth analysis of current vulnerability assessment tools and methods. Comparative analysis of widely known solutions is presented in terms of the vulnerabilities they find, the methodology used, and the platform and/or architecture they support. At the end, certain research problems have been highlighted to promote and enable research in the firmware security area of IoT.

The system emulates an end-to-end risk assessment framework for an IoT sensor network, with emphases on firmware obsoleteness, communication activity, and known security exploits. It creates synthetic data for 150 diverse IoT sensors in different industries, including environmental monitoring, healthcare, agriculture, industrial automation, and smart homes. Each sensor is linked to a hardware model, firmware version, and last communication time. The present system illustrates the merits of using lightweight device profiling in conjunction with risk prediction based on firmware analysis and highlight even more analysis of dynamic intercommunications and attack surfaces, regions further that could improve this system. Research such as "Attack on Things" (AoT) identifies the immediate risks brought upon by insecure firmware update procedures and emphasizes the requirement to not just detect old firmware but also check for the integrity and security of the update protocols.

Firmware Security Taxonomies emphasize that most firmware vulnerabilities go undetected in the absence of intensive static and dynamic analysis, indicating potential extensions for the existing system to carry out more intensive firmware security scanning. Vulnerability detection is confined to pre-defined cases and does not dynamically evaluate unknown threats or carry out intensive firmware inspection. The system fails to emulate real network behaviours, device dependencies, or mobile firmware update processes, which are new risk factors on the rise.

III. PROBLEM STATEMENT

In an IoT environment comprising approximately 150 connected devices, ensuring cybersecurity is a critical challenge. Outdated hardware and software components significantly increase the vulnerability of the network to cyber-attacks. To address this issue, there is a need to develop a systematic mechanism and algorithm capable of identifying outdated hardware and software across all devices. This solution should facilitate timely upgrades and patches to mitigate potential security threats, enhance system integrity, and maintain compliance with best cybersecurity practices.

Proposed Solution

The solution proposed intends to improve security and maintenance in IoT sensor networks by implementing an automated system for detection of firmware outdatedness and security risks. The system, through simulation of a varied range of 150 IoT sensors representing all industries, constantly tracks important parameters like firmware version, last communication time, and known vulnerabilities. It assesses each sensor in isolation to compute an overall risk score, taking into account firmware obsolescence, communication delay, and vulnerability exposure. Based on the risk scores, the system classifies devices into low, medium, and high-risk categories and highlights those that need to be firmware-updated urgently.

Alongside producing actionable insights, the system offers visual analytics via pie charts to present overall upgrade requirement status and sensor distribution by risk levels, allowing for easy comprehension by network administrators. Modular architecture supports easy extension to real-world sensor data and integration into larger IoT device management platforms. Subsequent enhancements may include applying more comprehensive dynamic vulnerability scanning, automating firmware patch recommendations, integrating predictive risk analytics based on machine learning models, and countering next-generation attack surfaces explored in current studies. Ultimately, this solution will be directed toward enabling proactive management of IoT device security, reducing operational downtime, and suppressing cybersecurity threats with greater efficiency.

System Design

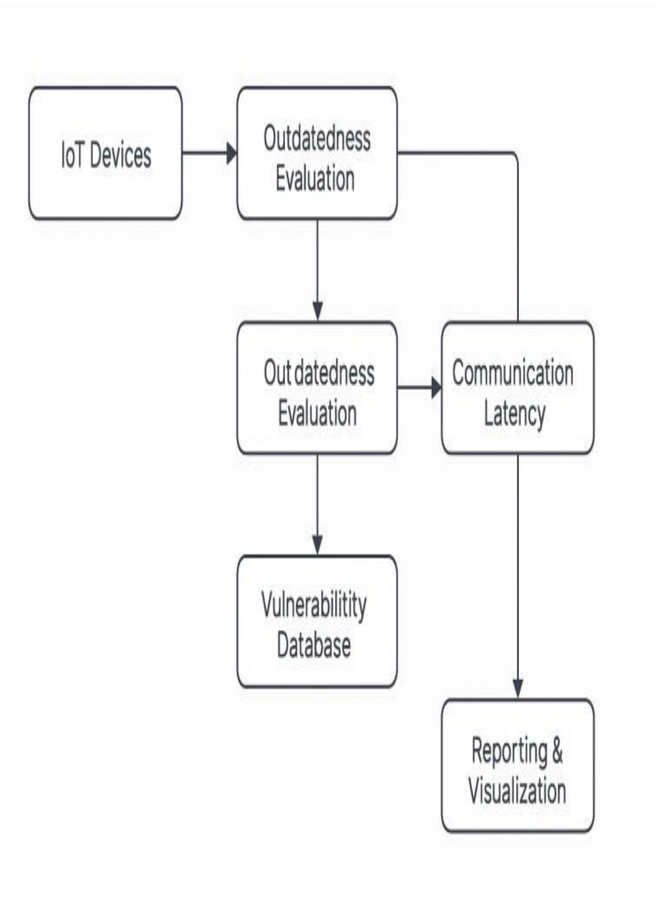


Fig: System Architecture Diagram

IV. METHODOLOGY

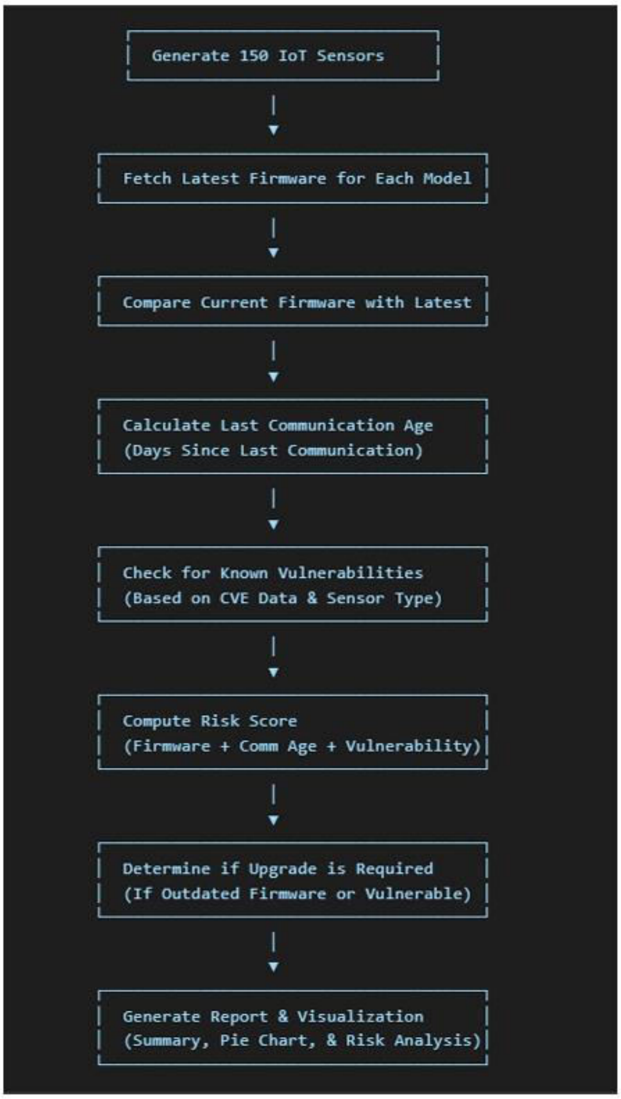

Generate 150 IoT Sensors
Fetch Latest Firmware for Each Model
Compare Current Firmware with Latest
Calculate Last Communication Age (Days Since Last Communication)
Check for Known Vulnerabilities (Based on CVE Data & Sensor Type)
Compute Risk Score (Firmware + Comm Age + Vulnerability)
Determine if Upgrade is Required (If Outdated Firmware or Vulnerable)
Generate Report & Visualization (Summary, Pie Chart, & Risk Analysis)

Fig: Methodology Diagram

Detailed Description of methodology

Methodology outlines the procedure of the analysis of IoT sensor data, determining their obsolescence, detecting vulnerabilities, and whether an upgrade will be needed. The review is firmware version based, last timestamp of communication, and possible security threat.

In order to mimic an actual IoT network, we have taken into account 150 IoT sensors with random characteristics, including sensor ID, which is used as a distinct identifier for a sensor, and sensor type, which describes the type of sensors involved, together with the existing firmware and hardware type, which describes the firmware revisions and hardware models employed, and the timestamp of the last communication, which is the number of days since the last communication, between 0 and 90 days ago, to mimic idle devices.

The newest firmware for every sensor is calculated according to its hardware model, such as Model A being 2.0, Model B being 1.5, Model C being 2.3, and Model D being 1.8. The newest firmware is compared to the newest version; if both are equal, there is no update; if not, the update is required. Afterwards, the discrepancy between the current date and the last comms date will be calculated in order to verify if the sensor is not in use. In case the last comms date is greater, then it is more possible that the sensor has failed or that it will not display the correct result. Then we will calculate the risk score to ascertain if the A sensor needs upgrading or not.

Implementation

The process of applying this IoT sensor firmware analysis system consists of a number of important steps for effective monitoring and evaluation. Data is first created by emulating 150 IoT sensors with randomly chosen attributes from different categories. Then, the latest firmware is assigned to every hardware model for comparison with current firmware to identify if it is necessary to update it. Obsolete firmware status and communication age are determined, and outdated sensors are indicated. A risk score is calculated by weighting firmware outdatedness, communication age, and vulnerability data to assist in determining the risk level each sensor presents. According to this analysis, sensors that need updating are determined to ensure devices that have outdated firmware or present security issues are updated as a priority. The final outcome is a formatted output showing each sensor's risk level, vulnerabilities, and upgrade needs, followed by an overview showing the number of sensors analysed and those that require an upgrade. A pie chart visualization is also created to offer a clear view of the proportion of sensors that need attention.

Pseudo code

Input: A list of IoT sensors (150 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 150 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 > 0

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 proves to emulate successfully 150 IoT sensors, where each sensor carries a different set of sensor types, hardware model, and firmware level. The system checks the firmware status of each sensor, communication age, risks, and risk score to identify if an upgrade is needed. From the implementation, it was discovered that 134 out of 150 sensors need to be upgraded. The findings also show that risk scores differ depending on firmware obsolescence, communication era, and vulnerabilities.

A pie chart for upgrade status gives a clear display of the percentage of sensors that need an upgrade against those which are current.

A pie chart graph of risk scores classifies sensors according to their risk levels, giving an indication of the seriousness of possible security problems.

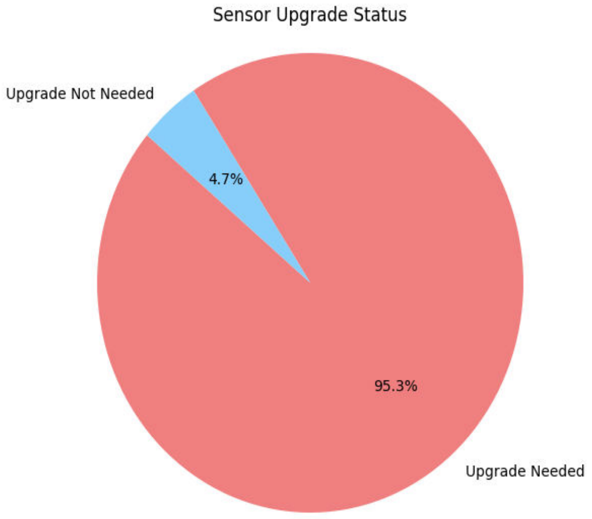


Fig: Pie chart for Sensor Upgrade Status

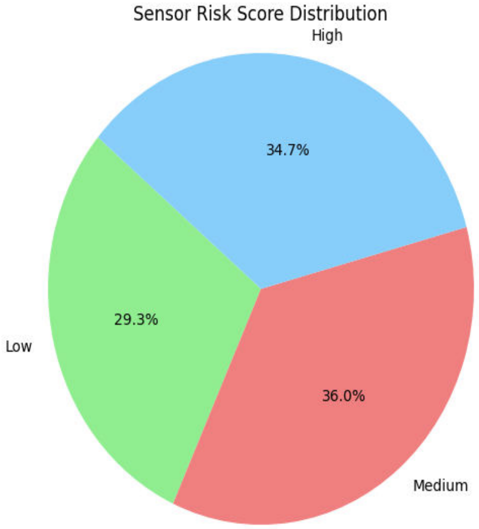


Fig: Pie chart for Sensor Risk Score Distribution

VI. CONCLUSION

The system installed successfully assesses firmware status, communication history, and vulnerabilities of 150 IoT simulated sensors. Analysing firmware versions, last communication timestamps, and possible security risks, the model computes which sensors must be updated. The outcome reveals that a vast majority of sensors (134 out of 150) require firmware updates because of obsolete software and extended communication gaps.

The risk assessment model using automation offers a systematic method of ranking sensor updates to guarantee timely performance and security enhancements. The utilization of a risk score facilitates effective decision-making, prioritizing resources on the most at-risk devices. Furthermore, the pie chart visualization makes the interpretability of the results through clearly illustrating the percentage of sensors that need attention.

Risk score distribution pie chart classifies sensors according to their risk levels, giving insight into the severity of possible security risks. The majority of high-risk sensors are connected to old firmware and extended communication gaps.

This research emphasizes the significance of autonomous firmware testing and risk analysis for IoT security. Future enhancements may include real-time monitoring and automatic firmware updates to allow for ongoing security and performance improvements.

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] A. B. S. D. Keshav Kaushik, “Framework to analyze and exploit the smart home IoT firmware,” 2024.
[8] Seethala, S. C. (2024). AI-Infused Data Warehousing: Redefining Data Governance in the Finance Industry. International Research Journal of Innovations in Engineering & Technology, 5(5), Article 028. https://doi.org/10.47001/IRJIET/2021.505028
[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] A. S. R. G. Yashwant Singh, “A survey on IoT & embedded device firmware security: architecture, extraction techniques, and vulnerability analysis frameworks,” 2023.

INTERNATIONAL JOURNAL
OF INNOVATIVE RESEARCH
IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details