Article

A Risk Management Framework for IoT Devices and Networks

Syed Rizvi * and Ephraim Govere

Posted Date: 14 October 2024

doi: 10.20944/preprints202410.1083.v1

Keywords: risk assessment; IoT security; control strategies; vulnerabilities management; security threats and attacks; device-level security

 doi:10.20944/preprints202410.1083.v1

Article

A Risk Management Framework for IoT Devices and Networks

Syed Rizvi [1,*] and Ephraim Govere [2]

[1] The Pennsylvania State University
[2] Queen's University
* Correspondence: srizvi@psu.edu

Abstract: The Internet of Things (IoT), as a technology, transforms every day, consumer devices into devices capable of collecting and transmitting data. This momentous progress highlights the need for reliable risk management frameworks that address the potential risks associated with IoT devices across all aspects of life. Traditionally, the feasibility of IoT was limited by the high costs of sensors and their connectivity. Although, recent advancements have greatly reduced costs, enabling widespread connectivity of devices to the Internet. Consequently, numerous IoT devices and networks are left vulnerable without a comprehensive framework for managing these risks effectively. This paper introduces a more systematic framework designed to counter security risks and safeguard IoT devices. This framework takes a step-by-step approach for focusing on mitigating risks arising from inadequate security designs for IoT devices. It involves procedures for risk identification, evaluation, and prioritization which is followed by comprehensive risk analysis and control measures, and because risk evaluation is tedious, we suggest using machine learning (ML) to accelerate the risk evaluation process, boost the precision and consistency of risk assessments, and provide valuable insight, which ultimately enables risk analysts to make better informed and timely decisions. Through multiple case studies, we demonstrate the practicality and efficacy of the framework for evaluating IoT device risks and guiding the implementation of appropriate controls to safeguard devices and networks. We also develop security dashboards that provide visual summaries comparing device values, threat assessments, and risk mitigation costs, aiding in clear communication and prioritization of security measures.

Keywords: risk assessment; IoT security; control strategies; vulnerabilities management; security threats and| attacks; device-level security

1. Introduction

The pervasive influence of the IoT in multiple domains, including businesses, homes, and daily life, requires a greater awareness of security risks and privacy implications with which they are involved. These interconnected devices profoundly impact transportation, schedules, well-being, communication with loved ones, and entertainment, while also enabling process optimization through data analytics applied to IoT data streams. Moreover, the cyber-physical attributes of IoT present new avenues for business growth and cross-cutting applications. Modern industries are moving towards solutions which enable artificial intelligence services for data demanding applications [1]. This expanding landscape presents the challenge of preserving privacy and addressing security risks without stifling IoT's ongoing development. Recognizing the significance of risk management, it becomes increasingly crucial to adopt proactive measures in understanding and mitigating the associated risks within the IoT ecosystem.

The IoT has made significant advancements through the adoption of various technologies, often relying on proprietary standards. However, the absence of standardized practices and regulations across IoT devices has led to numerous challenges concerning security and privacy. Consequently, technicians face difficulties in managing, maintaining, and addressing issues that arise with IoT devices due to the lack of guidelines and essential information. The absence of structured approaches in the development of IoT devices has further complicated security risk analysis, risk assessment, and the implementation of countermeasures. While there are common themes in modeling threats and

 doi:10.20944/preprints202410.1083.v1

evaluating risks within the IoT sector, each field presents its distinct set of risks. Instead of solely focusing on cybersecurity at the domain level, a comprehensive examination of numerous IoT applications at the inter-domain level is essential to ensure effective risk mitigation.

The Department of Homeland Security (DHS) highlights a concerning trend where many devices lack even the most fundamental security measures. According to DHS, this problem arises due to the complex nature of IoT, where different entities are involved in the device's design, software components, network operation, and deployment. This fragmented structure often results in ambiguity regarding the responsibility for security decisions [2]. Furthermore, DHS identifies a lack of incentives for IoT device developers to adhere to security standards since they are not directly liable for the consequences of inadequate security measures. Additionally, consumers' limited awareness regarding the evaluation of competing IoT options exacerbates the issue. To address these challenges, DHS suggests integrating security measures during the design phase of IoT devices. Furthermore, DHS emphasizes the importance of economic considerations and awareness to risk, urging businesses to prioritize security throughout the whole process rather than retroactively addressing vulnerabilities after launch. By incorporating security into the design, the need for expensive and complicated post-design security enhancements can be mitigated. The overall impact of IoT has exposed numerous vulnerabilities and challenges associated with these devices. Although, the absence of a risk management framework has exacerbated the severity of these vulnerabilities. One critical problem relates to ensuring the security of the extensive number of interconnected devices and preventing unauthorized access. Hackers can exploit entry points to compromise devices and access sensitive information. Vulnerabilities such as this stem from the trade-off between reducing production cost and compromising system security and performance. Another significant issue arises from firmware updates, which struggle to keep pace with the rapid advancement of technology. Hackers keenly target emerging technologies during their early stages, taking advantage of potential loopholes. Addressing these challenges is crucial for the success and resilience of the IoT network.

The main research contribution is the development of a methodical risk management framework, specifically designed for IoT devices. A framework that addresses potential security risks and vulnerabilities associated with IoT devices in many aspects of life. Its uniqueness lies in its exhaustive approach to risk management, with a process that includes risk assessment, identification, evaluation, prioritization, and risk analysis with additive control measures. Given that risk evaluation is an intensive process, we suggest the use of ML to streamline risk evaluation. ML can increase the accuracy of risk assessments and provide valuable insight, which ultimately enables risk analysts to make better informed decisions. The impact of this research also extends to stakeholders. For device manufacturers, the framework offers guidance on designing and implementing secure IoT devices, to mitigate potential risks and vulnerabilities. IoT network operators and service providers may utilize the framework to assess security posture of networks and devices, enhancing overall security and reliability of their services. Additionally, consumers and end-users benefit from this research by having a framework that accentuates the importance of securing IoT devices, ensuring the privacy and safety of data and interactions with these devices.

2. Related Works

AI and ML are being integrated, and show significant promise, in risk management. Specifically, AI is being applied in IoT devices across an array of domains. From healthcare to retail, these devices create opportunities for optimization and simplification of complex, organizational tasks. Furthermore, these devices, although incredibly useful, are just as extremely vulnerable to attack. Moreover, there are a plethora of security challenges that exist within the dominion of IoT. Node security is a great challenge that network engineers struggle with to this day [17]. Thus, it is paramount to protect these devices with resilient security frameworks.

AI in risk management for these devices is capable of, and novel at, detection, analyzation, and protection for these devices across the various domains in which they are implemented [4]. Additionally, the advent of AI has created a volatile environment in which both attackers and those

 doi:10.20944/preprints202410.1083.v1

applying controls must utilize AI to cope with the amount of data that is necessary to be analyzed to ensure network security [3]. This new role for AI has incorporated ML, decision trees, K-NN techniques, support vector machines (SVMs), and artificial neural networks (ANNs) which allow for immense capabilities and a significant number of options for application [8]. These options even include edge computing to shift data processing to edge nodes (ENs) which are highly vulnerable to attacks. These networks of interconnected nodes provide a significant benefit in their quality of service (QoS) for IoT applications with low-latency requirements [20]. Here, AI can be utilized to find security gaps and associate them with appropriate controls to be put in place. It is critical to monitor and update the given data to prevent issues. These issues can arise from improper data within the AI's dataset for determining risk management options. It also finds a place in banking operations as anomaly detection, pattern recognition, and predictive modelling capabilities are incredibly complex analyses that AI can manage much more efficiently [14]. Even the supply chain finds a use for AI in risk management as, again, the amount of data is immense and computationally challenging which makes AI a perfect fit [7]. One study [9] recognizes that IoT plays a critical role in ameliorating asset management capabilities. These devices are very capable and, in combination with AI, it can ensure security, stability, and compatibility for users [9]. AI also finds uses in IoT and big data in improving supply chain risk management systems. They prove incredibly efficient as well as useful for applications wherein they utilize real-time information to allow for more informed decision-making [10].

In AI's advent, government bodies have developed guidelines and frameworks to perform risk assessment for IoT devices. These bodies have developed indispensable tools for conducting assessments that act as a standard for risk management. Explicitly, NIST has developed a risk management framework which provides a process which integrates security, privacy, and risk management activities into the system development life cycle including IoT devices [12]. In their publication, they describe steps in following the Risk Management Framework (RMF). It is significant to all domains which utilize devices. Especially, they have information pertinent to all aspects of risk management, assessment, controls, configuration, authorization, and monitoring. It is exhaustive in its efforts to allow individuals, organizations, and government bodies to secure themselves and their IoT devices in the event of an incident. It contains countless documents which provide an invaluable resource for creating and maintaining a secure network.

NIST's impressive RMF has sparked innovation in research for the development of frameworks for managing risk. Numerous frameworks have been developed which expand on more niche and upcoming risks to be addressed. This is particularly significant in the onset of AI and its rapid development. One instance of a proposed framework seeks to improve existing methodologies in approaching risk. Therein, it incorporates a multitude of parameters to determine risk score for several device profiles to produce further insight into risk assessment [11]. Although, the proposed framework recommends scenario specific tuning to provide a more accurate assessment of risk; through this, it builds on the existing recommendations and guidelines outlined in the NIST RMF. Furthermore, one contribution proposes a model for IoT cybersecurity architecture comprised of a layered structure. Utilizing components that ensure compliance with a proposed set of controls, the architecture efforts in detecting cyber threats for IoT wearable devices [5].

An additional development focuses the scope on developing metrics to quantify systemic risk in supply chain IoT security systems. I-SCRAM, efforts in specifically analyzing risks in supply chain within the realm of IoT to support the decision-making process associated with risk. It details minimization in risk as reliable sources for components become more affordable [18]. In an extension of NIST's framework, a study reviews IoT risks in terms of their risk category and impacted industry. Moreover, it entails a ranking system to quantify risk vectors which lead to effective mitigation strategies and techniques [6]. A journal review of security frameworks for IoT-based smart environments identifies potential security needs based on ISO/IEC, ETSI, NIST, and a multitude of other security standards to culminate in an all-inclusive review of published security standards; standards that were shown to not directly address the needs of smart environments. Therefore, providing insight into the current state of security standards and opportunities for developing a

 doi:10.20944/preprints202410.1083.v1

greater foundation of IoT device security for risk management [13]. It directly addresses areas for improvement for the broader, pre-existing risk management frameworks. A distinct development gives to a multilayered technology-organization-environment (TOE-based) risk management framework for smart city governance. Risks are grouped into TOE categories to identify and manage risks that are pertinent to smart cities where it can illuminate significant risks to provide opportunities to develop effective responses and controls to enhance privacy and prevent incidents [19].

A notable instance effort in tailoring a risk management framework to individual users. It seeks to provide guidance and a novel Digital Security Management Framework to detail threats and corresponding risk responses for individuals [15]. It prioritizes providing measures for mitigation to prove a significant utility to individual users which allows for greater privacy and security, including common IoT devices. Another significant framework details governance in IoT for the ever-rising number of cyber-attacks. It builds off previous national standards specializing in the mitigation of cyber-attacks for organizations and their associated consumers, ensuring security of IoT resources as well as safeguarding personal information [16]. Real-time attack detection and mitigation is a prodigious task that only becomes further complicated by the immeasurable attack vectors to address to accomplish real-time protection. This framework suggests the use of blockchain to bolster security and incorporate logging, monitoring, machine learning-assisted intrusion detection systems, and indicators of compromise [3]. A colossal burden that efforts in providing a holistic approach to IoT security for a resilient, flexible, and scalable framework to address the changing threat landscape.

3. Proposed Risk Management (RM) Framework for IoT Devices and Networks

This research's main objective is presenting an extensive process for identifying, evaluating, and mitigating security threats to IoT devices and networks. The framework, as depicted in Figure 1, is organized into distinct sections that focus on risk identification, evaluation, prioritization, analysis, and control. Initially, the process of risk identification involves identifying potential attack vectors that adversaries may exploit to compromise the devices, determining the critical IoT devices that necessitate protection, and recognizing vulnerabilities associated with these devices that could pose significant threats. Subsequently, the risk assessment phase entails evaluating the identified devices to ascertain their value and importance within the organizational infrastructure. This assessment entails analyzing each identified threat to determine the urgency of implementing security controls to mitigate potential substantial harm. Following that, the identified threats are ranked based on their impact on the organization, thereby providing the Risk Analyst with quantitative data through a prioritized list of IoT devices and security threats. Moving on to risk analysis, each identified threat is carefully examined to determine the appropriate security policies, procedures, and technologies that should be designed, implemented, and maintained within the organization to mitigate future risks effectively. Finally, the recommended security strategies are implemented and diligently maintained across the organization.

 doi:10.20944/preprints202410.1083.v1

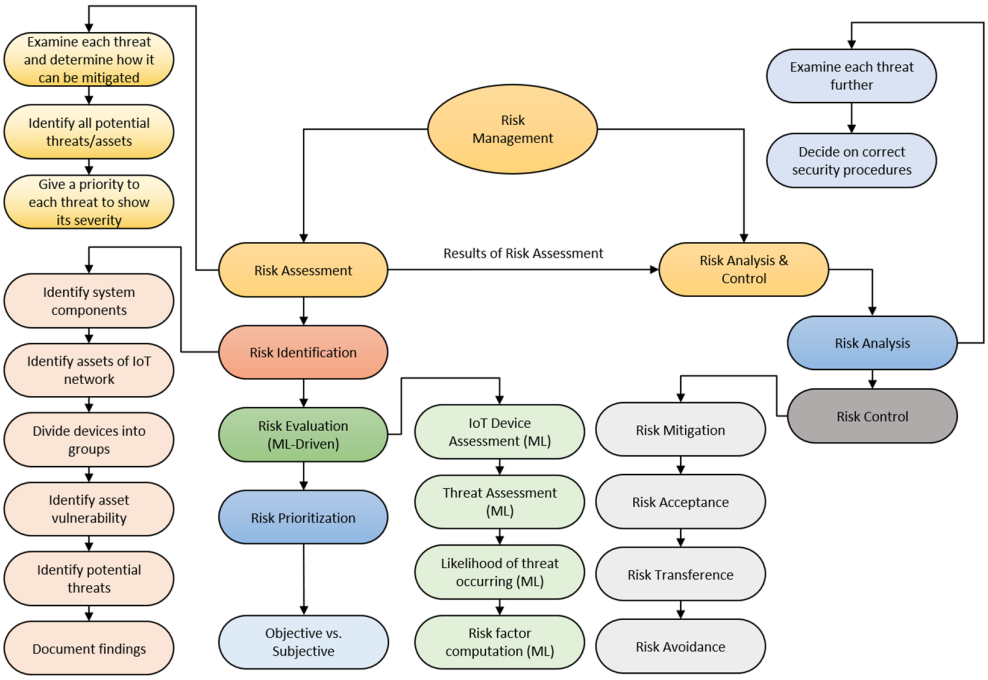

Figure 1. Illustration of Risk Management Framework for IoT Devices.

3.1. Risk Identification

Risk Assessment constitutes an initial stage within our proposed Risk Management (RM) framework, aiming to deliver systematic procedures for: (a) identifying security risks and valuable IoT devices that necessitate safeguarding within the organization, (b) evaluating each IoT device and security threat, and (c) prioritizing them based on the evaluation outcomes. With the objective of accomplishing this aim, the initial phase involves risk identification, which entails a six-step process for recognizing critical threats and valuable IoT devices.

3.1.1. Identify IoT Network Components and Assets

To conduct a thorough assessment of the organization, it is crucial to identify all system components, including the IoT devices within the network. These components have various assets such as data, software, hardware, personnel, procedures, and the IoT network itself. Notably, in the event of a network breach, these devices hold data that may be vulnerable to unauthorized access. Once the network components are properly acknowledged, attention turns to identifying the assets specific to the IoT network. These assets encompass software, hardware, databases, the network infrastructure, and the personnel involved. Software refers to the procedures or programs utilized within the organization, while hardware encompasses input/output devices, operating systems, and processors. Databases contain organized data pertaining to the IoT devices, and the network refers to hubs, network devices, and communication media. Figure 2 illustrates a deconstructed approach to asset identification and categorization for a clearer understanding.

 doi:10.20944/preprints202410.1083.v1

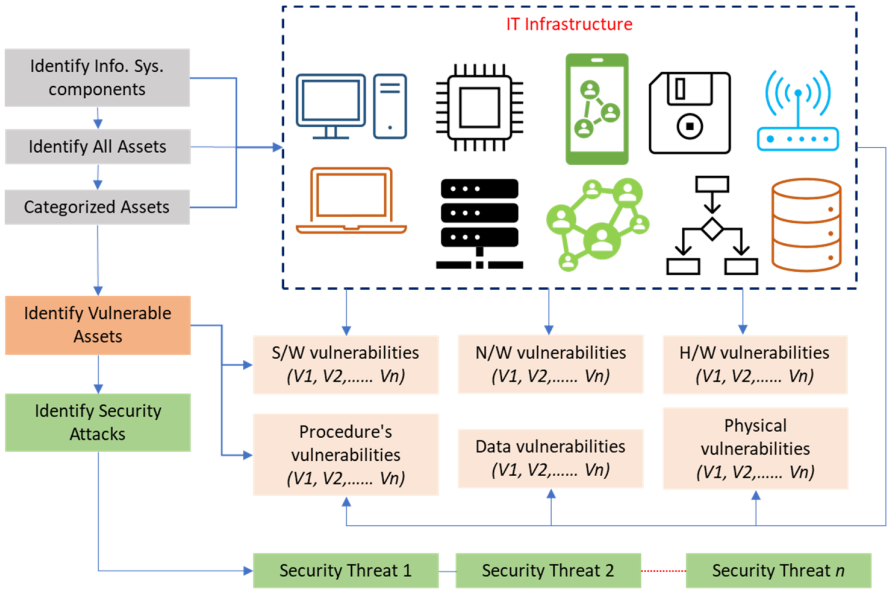

Figure 2. A Step-By-Step Approach for Risk Identification. S/W: Software; N/W: Network; H/W: Hardware.

3.1.2. Divide IoT Devices into Groups

The IoT devices will be systematically classified based on their respective contributions to the overall network infrastructure. Within the hardware category, input devices comprise computer equipment that provide data input and control signals to the network, and these input devices consist of keyboards, mice, and scanners. An output device points to the equipment that will transform input data into a readable format.

In the software category, procedures or coded instructions for computers within the system or network are included. The database group comprises commonly used database management systems such as SQL or Microsoft Access. The network group encompasses physical devices employed for communication between devices in a computer network. Finally, the people category comprises individuals responsible for operating the devices, network administrators, and system specialists within the organization.

3.1.3. Identification of Vulnerable Assets and Potential Security Threats

Once the IoT devices have been identified and classified into their respective categories, a thorough analysis is conducted to determine their vulnerability to potential attacks. Each category, including the people category, has the potential to exhibit vulnerabilities. Examples of vulnerabilities that may be present in each category include coding errors, unprotected communication lines in network devices, and social engineering threats. Figure 3 provides a visual representation of the proposed approach for assessing risks associated with each IoT device within the network. The identification process applies to the identification of IoT devices vulnerable to targeting and assessing potential attacks that the network may encounter due to device-level vulnerabilities. Social engineering is significant in that people may be deceived into revealing sensitive information which compromises organizational security. The threats identified include botnets, viruses, DDoS attacks, phishing, ransomware, and worms. The concluding step in risk identification entails the documentation of findings to create a record of issues and potential solutions to be implemented in addressing future incidents.

 doi:10.20944/preprints202410.1083.v1

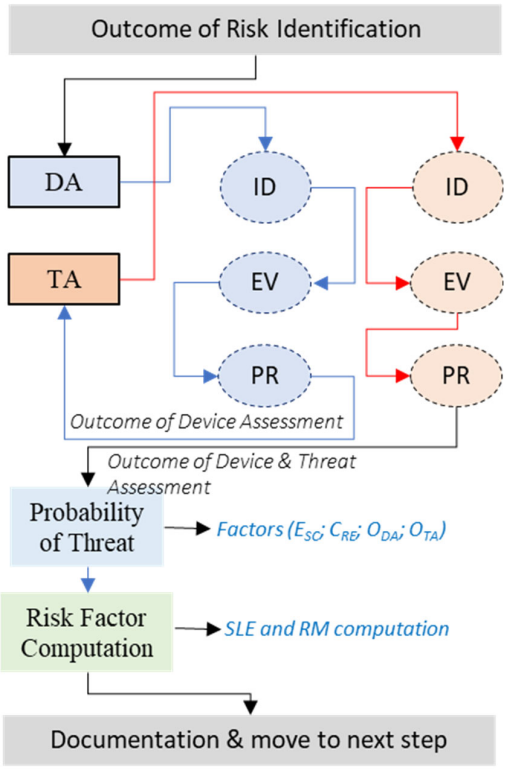

Figure 3. A Step-By-Step Approach for Risk Evaluation. DA: Device Assessment; TA: Threat Assessment; ID: Identification; EV: Evaluation; PR: Prioritization; E_{SC}: Existing security controls; C_{RE}: Current risk environment; O_{DA}; Outcome of Device Assessment; O_{TA}: Outcome of Threat Assessment.

3.2. Risk Evaluation

During this phase, a comprehensive examination is conducted on each threat that was identified in the previous phase, aiming to determine its potential impact on the IoT network. At this stage, all possible attack paths have been uncovered, necessitating an evaluation of their potential severity and the prioritization of necessary mitigation measures. This phase will incorporate ML models into each step to improve the accuracy and efficiency of this process. ML analyzes historical data and real-time assessments to predict criticality, potential impacts, and risks on IoT devices.

Leveraging automated systems and ML will help make the evaluation process more dynamic and accurate, allowing for continuous risk assessment as the organization obtains new data. To enhance visual comprehension of the attacker's routes to different network components, a tree map is utilized to display all possible attack paths. This step is crucial as it entails enumerating all identified threats and assigning priorities based on their associated level of risk

3.2.1. IoT Device Assessment (DA)

To assess the risks confronting your organization, it is necessary to examine the assets that require protection and assign them a ranking based on their significance. This evaluation involves categorizing the assets to identify those of critical importance, which demand the highest level of safeguarding. The objective is to ensure that any potential damage inflicted will not have a severe impact on the IoT network, while prioritizing the protection of the most essential assets. Recognizing that certain assets hold greater value than others, this approach allows for the safeguarding of key IoT devices during an attack and facilitates the reconstruction of any lost components. Given the subjective nature of asset valuation, it is essential to adopt a more universal approach that can be applied across various IoT domains. As part of the risk management framework, we have developed a set of questions to be posed by the security management group (SMG) or the IT department for each identified IoT device. Within each question, specific criteria are established to evaluate the

 doi:10.20944/preprints202410.1083.v1

identified IoT devices from the previous step. ML algorithms and predictive analytics are incorporated. These models analyze historical data, real-time inputs, and various operational parameters to assess the criticality, usage patterns, and vulnerability levels of IoT devices. This automated evaluation provides a comprehensive understanding of each device's risk profile, ensuring the most critical assets receive the highest level of protection. The SMG will review the outputs generated by the automated system at the end of the DA process.

A. Template Questions for DA

Template 1 presents a set of device assessment questions aimed at evaluating various aspects of IoT devices, including their criticality, revenue generation, replacement and protection costs, vulnerability to attacks, data characteristics, backup/redundancy measures, and impact on downtime cost. Additional columns provide information on the goal/objective of each question, data type, backup/redundancy status, sensitivity of data, and data connectivity. Automated systems will use these questions to gather comprehensive data points and provide a detailed assessment of each IoT device, making the evaluation process more thorough and data driven.

B. Explanation of DA Template Questions

Q1: This question assesses IoT devices based on the organization's goals and objectives. ML algorithms will analyze operational data, historical usage, and impact metrics to determine device criticality. Devices that are less essential will receive a lower score compared to the most critical devices.

Q2: This question evaluates IoT devices based on their contribution to revenue. Each device's impact on total revenue is considered using its net value (revenue generated minus upkeep costs) over a specific time period (e.g., year, quarter, month). Predictive analytics will process financial records and revenue data to identify and rank devices based on their revenue generation.

Q3: This question examines IoT devices based on their replacement cost, taking into account the initial cost of replacing the device, costs associated with physical installation or removal, and any expenses required to ensure the device operates at its maximum effectiveness (e.g., backups). ML models will estimate replacement expenses by analyzing market prices, installation costs, and maintenance data.

Q4: This question considers IoT devices in terms of their protection cost, focusing on the total cost required to fully secure the device. Predictive models will evaluate the cost-effectiveness of various protection measures by analyzing security implementation costs and their potential Return on Investment (ROI).

Q5: This question highlights the frequency of usage of a particular IoT device for various operations within the organization. The evaluation is based on the total usage time of the device. ML algorithms will detect usage patterns by analyzing operational logs and real-time usage data.

Q6: This question assesses the potential harm to the organization in financial and operational terms if a specific device is impacted. The evaluation measures the projected loss, which takes into account the loss of revenue directly or indirectly generated by the device minus the device's upkeep costs. Predictive analytics will quantify potential harm by evaluating historical incident data and projecting future impact scenarios.

Q7: This question identifies IoT devices that are most vulnerable to attacks, either from the internal network or physical security measures. The evaluation considers the level of security access required to interact with the device and the number of vulnerabilities affecting the device within the internal network. Vulnerability assessment models will identify internal vulnerabilities by analyzing security logs and conducting real-time threat simulations.

Q8: This question focuses on IoT devices that are most vulnerable to external threats. The evaluation considers the number of external vulnerabilities that affect the device. Threat intelligence systems will assess external threat vectors by analyzing threat intelligence feeds and historical breach data.

 doi:10.20944/preprints202410.1083.v1

Template 1. IoT Device Assessment Questions and Attributes.

Question	Description	Data Type	Backup & Redundancy	Sensitivity	Data Connectivity
DA-Q1	Which IoT Device is most critical to the organization's success?		x		
DA-Q2	Which IoT Device generates the most revenue?	x		x	
DA-Q3	Which IoT Device would be the most expensive to replace?				
DA-Q4	Which IoT Device would be the most expensive to protect?				
DA-Q5	Which IoT Device is used most often?				x
DA-Q6	Which IoT Device would hurt the organization the most if impacted?				
DA-Q7	Which IoT device is most vulnerable to an internal attack?				
DA-Q8	Which IoT device is most vulnerable to an external attack?		x		
DA-Q9	Which IoT Device is most susceptible to risk?				
DA-Q10	What are the operational characteristics of the IoT device, and how does it currently fit within the environment described?				
DA-Q11	What kind of data does the IoT device contain, and what data passes through it? Public? Private? Proprietary?			x	
DA-Q12	Are there backup locations for these IoT devices in the event of their compromise or failure? Are there redundant devices connected to the same system that current devices are placed in?				
DA-Q13	Is there sensitive data on this IoT device?		x		
DA-Q14	Is this IoT device connected to data that may be considered desirable?				x
DA-Q15	How would you rank the importance of accessible data?				
DA-Q16	Who are the authorized users of IoT devices?				x
DA-Q17	What other parties, including employees, customers, or business partners, might be affected if IoT devices are functionally impaired?				
DA-Q18	Which IoT device has the greatest impact on downtime cost?	x			

Q9: This question examines IoT devices based on the total number of vulnerabilities they possess. The evaluation takes into account the sum of internal and external vulnerabilities affecting the device. ML models will aggregate and analyze vulnerability data from various sources to provide a comprehensive risk profile.

Q10: This question evaluates how an IoT device fits into the organization's current operational framework. It considers factors such as the device's use in business transactions, the specific network traffic flowing through it, and the potential operational impact if the device is compromised. Predictive analytics will analyze operational data, network traffic, and business processes to evaluate the device's integration and significance.

Q11: This question examines the type of information flowing through the IoT device, such as customer data, proprietary organization data, sensitive documents, or other potentially compromising data if breached. Data classification algorithms will evaluate data types and their sensitivity and potential exposure risks.

Q12: This question assesses whether there is a backup infrastructure in place for the IoT device. It considers factors such as backup processes, failover mechanisms, data redundancy, and the device's operating framework. Redundancy analysis models will evaluate backup measures by analyzing system configurations and redundancy protocols.

Q13: This question identifies IoT devices that contain sensitive data, including financial account numbers, social security numbers, biometric data, and compliance-related information such as HIPAA or FISMA. ML models will analyze and perform privacy risk evaluation.

Q14: This question focuses on IoT devices connected to a network that contains sensitive data. Network analysis ML models will assess data connectivity and sensitivity by analyzing network configurations and data types.

Q15: This question considers the importance of the data flowing through the IoT device, ranging from low importance (e.g., addresses, phone numbers) to high importance (e.g., social security

 doi:10.20944/preprints202410.1083.v1

numbers, biometric data). Learning to rank (LTR) algorithms will classify data types and evaluate and rank their potential impact.

Q16: This question evaluates the probability of an attack based on the number of authorized users with access to the IoT devices. A lower number of authorized users reduces the probability of an intrusion, while a higher number increases the probability. ML algorithms will analyze user access patterns and evaluate the risk associated with the number of authorized users.

Q17: In the event of device failure or attack, this question quantifies the total number of impacted parties, including employees, customers, or business partners, with regard to the operations and data contained within the IoT device. ML algorithms will analyze organizational relationships and data dependencies to assess potential impact.

Q18: This question focuses on recovery costs by identifying IoT devices with the highest maximum downtime. The maximum downtime refers to the maximum acceptable outage (MAO) for a particular device. ML models will analyze historical downtime data and identify the potential recovery costs.

C. Device Score Computation

For each identified device, the automated system calculates the device score by assigning weights to each criterion. The importance given to each criterion may vary depending on the organization's priorities. For example, some organizations may prioritize protection cost over profit, resulting in a different device score during the assessment process. The formula computes the final device score for a given IoT device is as follows:

$$Device\ Score\ (Ds) = \frac{\sum_{i=1}^{n} DAQ_i \times W_i}{n} \quad (1)$$

where *W* is the specific weight assigned by the SMG after performing a careful device assessment (*DA*) and n is the number of questions in the template.

3.2.2. IoT Threat Assessment (TA)

The subsequent phase in risk evaluation entails identifying and ranking all the threats that pose a risk to your network. This process allows us to prioritize the threats and assets by assigning them rankings, enabling us to address the ones that require immediate attention. By doing so, we aim to anticipate potential attacks, determine their targets, and implement necessary safeguards to prevent their destruction. This step holds immense significance in safeguarding our IoT infrastructure and comprehending the nature of the threats and their potential consequences. Without adequately assessing the threats, we would remain oblivious to their magnitude and the extent of potential damage they could inflict. In this section of our risk management framework, we recommend that the SMG pose the following questions. Each question serves as a basis for evaluating the identified IoT devices. ML are integrated into each step of the threat assessment to automate and enhance the accuracy of this process, machine. These models analyze historical incident data, real-time threat intelligence, and various environmental factors to predict and prioritize threats effectively. By leveraging ML, the evaluation becomes more dynamic and precise, allowing for continuous updating and refinement of threat assessments as new data is gathered. The SMG will review the outputs generated by the automated system at the end of the TA process. The insights gained from these questions also assist in informed decision-making regarding security investments, risk management strategies, and resource allocation. It enables the organization to make informed choices based on the identified threats and their potential consequences.

A. Template Questions for TA

Template 2 presents the Threat Assessment (TA) questions related to the risks and impacts on devices and information in an organization's environment. It includes additional columns for device and information impact, cost considerations, single loss expectancy (SLE), impact on the organization, and system vulnerability. Automated systems will use these questions to gather comprehensive data points and provide a detailed assessment of each threat, making the evaluation process more thorough and data driven.

 doi:10.20944/preprints202410.1083.v1

B. Explanation of TA Template Questions

Q1: This question evaluates the potential harm posed by threats to the devices in their specific environment. By estimating the probability of each threat occurring, ML algorithms can identify and eliminate threats with the lowest probability, ensuring that resources are focused on addressing more significant risks.

Q2: This question aims to determine which threats pose the greatest danger to the organization's information integrity. By evaluating the impact of each threat on the organization's information assets, ML algorithms can prioritize measures to safeguard sensitive data, assess threat data and identify risks to information security based on vulnerability scans and incident reports, and mitigate risks to information security.

Q3: The goal of this question is to assess the cost of recovery from a successful attack. By using the "Recovery Cost" as a criterion, predictive analytic tools will estimate the expenses associated with recovering from each identified threat. Identifying threats with higher recovery costs allows the organization to prioritize the mitigation of those threats posing a more substantial financial impact.

Q4: This question aims to determine the cost of preventing the identified threats. By calculating the prevention cost for each threat and device, cost estimation ML algorithms can assess the resources required to implement preventive measures. Identifying threats with higher prevention costs helps allocate resources effectively to address serious risks.

Q5: This question aims to identify the threat that results in the highest SLE for the organization. Risk assessment ML algorithms will calculate SLE by evaluating potential impact and exposure.

Q6: This question aims to identify the threat with the highest annual rate of occurrence. Statistical ML models will predict annual occurrence rates by analyzing historical threat data. By examining the frequency of each threat's occurrence, the statistical ML models can prioritize measures to address threats that pose a higher risk.

Q7: This question is designed to identify threats that have the most substantial impact on the organization. These threats can harm the organization financially, affect operational time, and impact productivity. ML models will analyze potential threat scenarios and their consequences. Identifying such threats allows the organization to prioritize mitigation efforts to minimize their impact.

Template 2. IoT Device Level Threat Assessment (TA) Questions and Attributes.

Question	Description	DI	Rc	Mc	IO	Vs
[TA-Q1]	Which threats pose a risk to the organization's devices in the current environment?		x			
[TA-Q2]	Which threats pose the greatest risk to the organization's information?			x		
[TA-Q3]	What would be the cost of recovering from a successful attack?					
[TA-Q4]	What would be the cost of mitigating these threats?		x			
[TA-Q5]	Which threat would result in the highest single loss expectancy (SLE)?					
[TA-Q6]	Which threat has the highest annual occurrence rate?			x		x
[TA-Q7]	Which threats would have the most significant impact on the organization?					
[TA-Q8]	What is the likelihood of a natural threat occurring?		x			
[TA-Q9]	How well-prepared is the organization to handle device failures or power outages?					
[TA-Q10]	How severely would this threat impact daily operations?	x				
[TA-Q11]	What is the existing infrastructure for threat prevention?	x				
[TA-Q12]	Is the system vulnerable to hardware or software failures?					
[TA-Q13]	How many users have access to each device, and how many can modify device functions or access device data?				x	x

 doi:10.20944/preprints202410.1083.v1

[TA-Q14]	Are there firewalls and other device monitoring software in place to detect breaches or potential tampering?			x		
[TA-Q15]	Are there hardware protections such as surge protectors, backup generators, redundancies, or other measures to prevent physical damage?				x	

DI: Device Impact; Rc: Recovery Cost; Mc: Mitigation Cost; IO: Impact on organization; Vs: System Vulnerability.

Q8; This question focuses on assessing the chance of natural disasters based on the organization's geographical location. Predictive ML models will use geographical and historical data to estimate the likelihood of natural threats. By considering historical data on natural disasters, such as floods, fires, or tornadoes, the organization can plan and prepare for these events accordingly.

Q9: The objective of this question is to evaluate the accessibility of device and power backups within an acceptable timeframe known as Maximum Acceptable Outage (MAO). ML algorithms can help determine the duration the organization can operate without electricity or critical functions and help assess the availability and timeliness of backups for resuming normal operations.

Q10: This question aims to assess the impact of threats on everyday operations. The objective is to determine whether the organization can continue operating and resume daily functions without a loss of critical assets. Operational ML models can simulate threat scenarios to evaluate their impact on daily operations.

Q11: This question focuses on quantifying the effectiveness of the current threat prevention infrastructure. Infrastructure analysis ML tools can help evaluate the performance of firewall systems, anti-virus software, and user authorization controls, helping to determine the level of protection provided by the existing infrastructure and suggest necessary improvements.

Q12: The goal of this question is to evaluate the vulnerability of hardware and software components to failure. ML based vulnerability assessment can help conduct diagnostic tests, identifying potential weaknesses and assign ratings based on performance, enabling targeted efforts to address vulnerabilities.

Q13: This question determines the number of users with access to each device and their ability to alter device functions or access device data. Access control automated systems will analyze user permissions and monitor access patterns to identify risks. Understanding user interactions helps identify potential compromises and reinforces the importance of limiting access to as few users as possible for improved threat protection.

Q14: The objective of this question is to assess the presence of firewalls and other device monitoring software that can detect breaches or potential tampering. Security monitoring systems will evaluate the deployment and performance of firewalls and other monitoring tools. Proper monitoring enhances device traffic control and facilitates the interception and prevention of breaches. The absence of firewall protection or inadequate physical safeguards can leave devices vulnerable to external attacks and tampering.

Q15: This question focuses on evaluating the implementation of hardware protections such as surge protectors, backup generators, redundancies, and other measures to prevent physical damage. Physical security assessment ML models will analyze the presence and effectiveness of hardware protections. By having appropriate countermeasures in place, the organization can safeguard hardware from undetectable physical events like power surges, leaks, fires, and emergencies.

C. Threat Score Computation

For each identified threat, the automated system will calculate the threat score by assigning weights to each criterion. For instance, some organizations give more preference to recovery cost than the probability of the threat, which may change the threat score during the evaluation process. The formula to compute the final threat score for a given IoT device is as follows:

$$Threat\ Score\ (Ts) = \frac{\sum_{i=1}^{n} TAQ_i \times W_i}{n} \quad (2)$$

(2)

 doi:10.20944/preprints202410.1083.v1

where *W* is the specific weight assigned by the SMG after performing a careful threat assessment (*TA*) and n is the number of questions in the template.

- ***Ts***: Threat Score, which is the final score assigned to the identified threat.
- ***TAQi***: Threat Assessment Question (TAQ) score for each criterion. This score represents the evaluation of the threat based on a specific criterion.
- ***Wi***: Weight assigned by the SMG to each criterion i. This weight reflects the relative importance or preference given to the criterion during the threat assessment process.

To calculate the threat score, the equation sums up the products of the TAQ scores and their corresponding weights for each criterion. The resulting sum is then divided by the total number of questions or criteria, n, to obtain the average score, The purpose of this equation is to provide a quantitative measure of the threat's severity and potential impact based on the assessment criteria and their assigned weights. By assigning weights to different criteria, the automated system can prioritize certain aspects of the threat evaluation process, such as recovery cost or probability. This allows for a tailored assessment that aligns with the specific preferences of the organization conducting the evaluation.

3.2.3. Likelihood of Threat Occurring

The third phase in the risk evaluation process involves determining the probability of each identified threat occurring. The probability assessment is typically categorized on a scale, and we propose a five-step scale: frequent, probable, occasional, remote, and improbable. It is vital to assess threat likelihood because of the varying impacts that different threats can have. Several threats may bring high impact but a low probability of occurrence; regardless, these threats must be addressed, as even infrequent incidents can result in significant harm. Thus, it is paramount to be prepared for an incident as such. Although, there are threats that pose low risk and have low probability indicating that they do not pose substantial risk. The highest level of risk is associated to threats with a high probability of occurrence and capability for significant damage. In estimating threat event probability, ML models consider the outcomes of the device and threat assessments conducted in the previous steps of the risk management framework. Initially, ML models consider the outcomes of the previous two steps of the risk management framework, which involve device and threat assessments Additionally, the existing security controls implemented as part of the organization's security infrastructure should be considered. Conclusively, the overall risk environment and health of the organization play a crucial role. It is important to note that the probability of a threat is inversely related to the effectiveness of existing security controls and the overall risk environment within the organization.

3.2.4. Risk Factor Computations

The fourth step is to calculate relative risk factors for each IoT device. The relative risk factors are found by utilizing SLE and Risk Magnitude (RM). SLE is used to represent how much money we can expect to lose if a risk occurs. This can be found by multiplying the device value by the exposure factor percentage, as shown in (3).

$$\boldsymbol{Single\ Loss\ Expectancy\ (SLE)}: \boldsymbol{SLE\ =\ DV\ x\ EF\%} \tag{3}$$

where *DV*: Device Value and *EF*: Exposure Factor. Since Exposure Factor is a subjective value, it is possible that a risk analyst or SMG may not have a good estimate of EF or it is not available at all. In this case, we compute risk magnitude (RM) to estimate the impact of a potential security risk. We use RM to combine how significant the effects of risk are with the probability of that risk occurring. This can be found by multiplying the asset value and the probability of a threat, as shown in (4).

$$\boldsymbol{Risk\ Magnitude\ (RM)}: \boldsymbol{RM\ =\ DV\ x\ T\rho} \tag{4}$$

where *DV*: Device Value and *Tρ*:Threat Probability.

To enhance the accuracy and precision of threat impact estimation, machine learning (ML) models are used to compute the relative risk factor (RRF) for each IoT device. ML models analyze

 doi:10.20944/preprints202410.1083.v1

historical data, real-time threat intelligence, and environmental factors to provide dynamic and precise risk evaluations. When calculating the RRF for a device, we must first consider what the threat is, how vulnerable the device is, and the importance of the asset that could be made unavailable. In addition, we also consider the existing security controls ($\boldsymbol{E_{sc}}$) and the uncertainty factor ($\boldsymbol{U_F}$) as part of RRF computation since both ($\boldsymbol{E_{sc}}$) and ($\boldsymbol{U_F}$) play a role in neutralizing the impact of a threat. For instance, a higher value of $\boldsymbol{E_{sc}}$ reduces the RRF whereas a higher value of $\boldsymbol{U_F}$ increases the RRF.

The ML models can dynamically adjust these factors based on continuous learning from new data, improving the accuracy of the risk assessment over time. Lastly, in the documentation part of this step, ML models could calculate the risk factor and document all relevant findings. By incorporating ML into the computation of risk factors, the organization can achieve a more automated, precise, and dynamic approach to evaluating the risks associated with IoT devices. This approach ensures that the risk assessments are continuously updated and based on the most current data, enabling better preparedness and response strategies.

$$Relative\ Risk\ Factor\ (RRF): RRF\ =\ RM - (RM\ x\ E_{sc}) + (RM\ x\ U_F) \tag{5}$$

where RM: Risk Magnitude = $(DV\ x\ T\rho)$; E_{sc}: Existing security control; U_F: Uncertainty Factor

$$RRF\ =\ (DV\ X\ TP) - ((DV\ X\ T\rho)\ x\ E_{sc})\ +\ ((DV\ X\ TP)\ x\ U_F) \tag{6}$$

C. Template Questions for DA

For each identified threat, the automated system will calculate the threat score by assigning weights to each criterion. For instance, some organizations give more preference to recovery cost than the probability of the threat, which may

3.3. Risk Prioritization

During this phase, our focus shifts to the threats identified in the evaluation phase, aiming to determine which threats are the most critical and demand immediate attention from the SMG. In reference to Table 1, the threats are arranged in order of severity. The severity of a threat is determined by its potential for harm to the system, the extent of information accessible to potential attackers, the cost associated with resolving the issue, and the likelihood of its occurrence. The threats falling within the highest severity category become our primary priority as we move forward. Risk prioritization is a crucial step since it allows us to identify and protect the most vulnerable assets. By allocating more resources to safeguard certain devices over others, we incur a certain level of risk, but it is considerably lower than the risk posed by leaving those assets unprotected. Risk prioritization plays a pivotal role in safeguarding a significant number of assets when an attack becomes imminent.

In our approach, we adopt a subjective scale rather than an objective one. An objective scale ranks risks based on quantifiable and measurable factors. However, incorporating personal opinions and interpretations into the equation implies a subjective assessment. Subjective scale comprises five groups: minimal, minor, moderate, significant, and severe. The minimal group encompasses risks with a probability of 0-20% and negligible impact on the network. The minor group includes risks with a 21-40% probability and a minor impact on the network, yet still operating at an acceptable level. Risks falling into the moderate group have a 41-60% probability and a moderate impact on the network, necessitating adjustments to meet expectations. The significant group involves risks with a 61-80% probability and a notable impact on the network, requiring substantial changes as the network's performance falls below acceptable levels. Finally, the severe group encompasses risks with an 81-100% probability, severely impacting the network to the extent that no aspect operates at an acceptable level.

Table 1. Device and Security Threats Prioritization Scale.

Significance	Description	Range
Minimal	Extremely unlikely the risk occurs. Little to no impact on the	(0-20%)

 doi:10.20944/preprints202410.1083.v1

	network.	
Minor	Minor chance the risk occurs. Low impact on the network.	(21-40%)
Moderate	Moderate chance the risk occurs. Medium impact on the network.	(41-60%)
Significant	Significant chance the risk occurs. Notable impact on the network.	(61-80%)
Severe	Severe chance the risk occurs. Extreme impact on the network.	(81-100%)

3.4. Risk Analysis

During this phase, we further inestigate each threat to determine the appropriate security policies and procedures for managing the risks faced by IoT devices. This step allows us to identify any vulnerabilities in the IoT devices and strengthen their security measures. Conducting a comprehensive analysis enables us to devise effective countermeasures against the identified threats. To streamline the risk analysis process, this section offers a step-by-step approach outlined in Figure 4. Risk analysis can be a time-consuming aspect of the overall assessment process, particularly in the case of IoT devices. These devices often operate within multiple frameworks, making it challenging to apply a standardized framework. Consequently, they require diverse aspects of protection. The risk analysis phase is divided into two parts. In part 1, the SMG examines the mission-critical resources of the business and conducts a thorough analysis of the sources of threats. In part 2, the SMG analyzes each IoT device to define its operational framework, understanding the necessary measures to safeguard it from the known threat sources. For each part of this phase, we present a systematic methodology that the SMG can adopt during the risk analysis process.

3.4.1. Part 1: Mission-Critical and Threat Source Analysis

Step 1: Identify Mission-Critical Business Functions: This involves defining the current essential functions and activities that must be safeguarded during a threat event. To effectively mitigate or prevent threats, it is crucial to prioritize the protection of mission-critical activities and functions. Thus, before considering other device-related factors, it is necessary to determine the business's current objectives, critical functions, and mission statements in order to frame the risk analysis and ensure the preservation of these elements during threat events.

Step 2: Identify Relevant Threat Sources: Identify all known threat sources that are applicable to the organization and the devices under examination. Consolidate information about existing threats into a comprehensible document that outlines which devices or functions they may exploit and the potential consequences of successfully exploiting vulnerabilities in those devices or functions.

Step 3: Assess the Likelihood of Threat Sources: Evaluate the probability of threat sources posing credible threats to the organization and the likelihood of them exploiting assets or device functions. Each threat source presents a potential problem for the organization's operations. Therefore, it is necessary to examine the likelihood of their occurrence and weigh it against the potential negative impact if a threat event successfully exploits a vulnerability. Considering the potential rate of occurrence and the potential consequences of exploitation will enable more accurate risk management considerations for the assets.

3.4.2. Part 2: Device Analysis

Step 4: Define the operational framework of the threatened devices: It is necessary to examine how the device aligns with the organization's current operational framework. This entails understanding the device's role within the chain of operations, its interface with other devices, and its contribution to accomplishing the organization's mission statement or goals.

 doi:10.20944/preprints202410.1083.v1

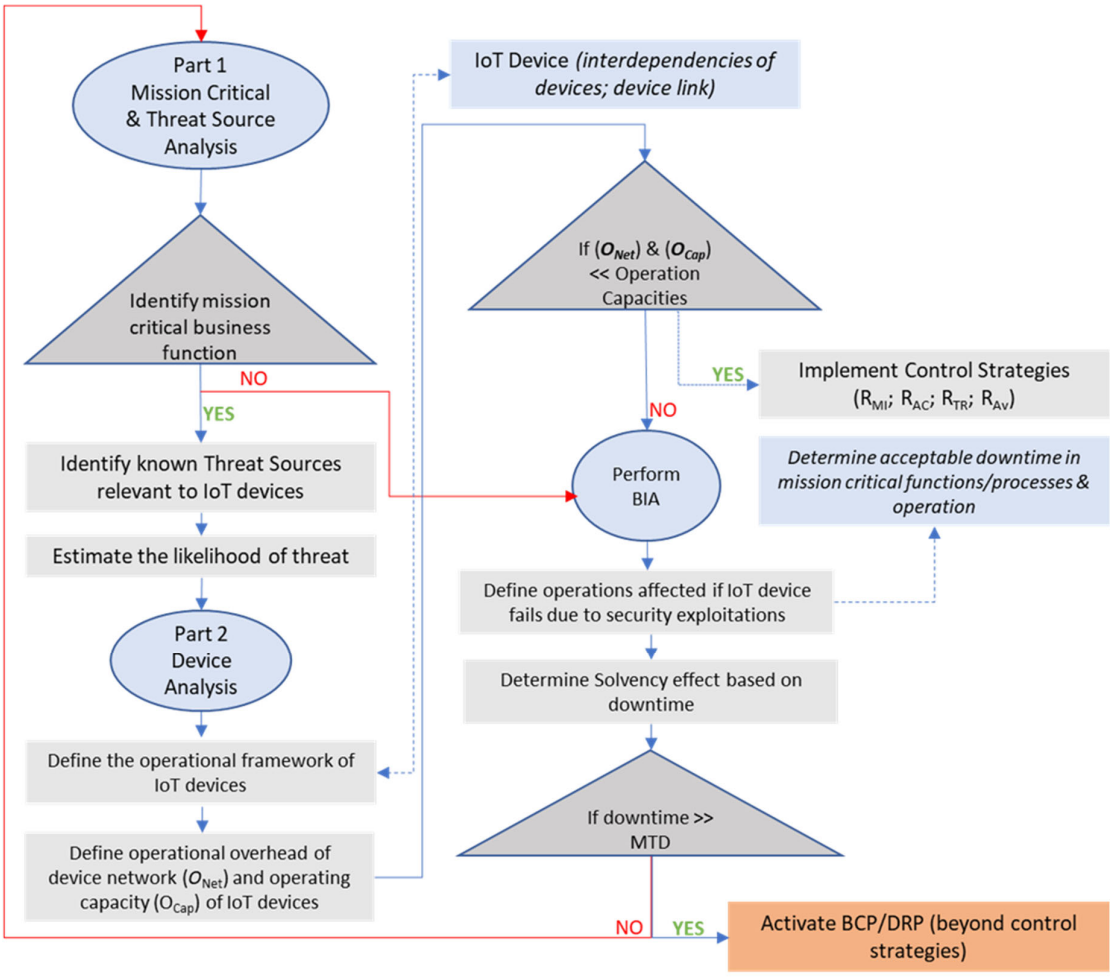

Figure 4. A Step-By-Step Approach for Risk Analysis. RMI: Risk Mitigation; RAC: Risk Acceptance; RTR: Risk Transference; RAV: Risk Avoidance; MTD: Maximum Tolerable Downtime; BCP: Business Continuity Plan; DRP: Disaster Recovery Plan.

Step 5: Define the current operational overhead and capacity of the device network: The network infrastructure of the organization requires a specific level of overhead to ensure efficient functioning. When implementing controls or risk management techniques on the device, it is essential to ensure that they do not exceed the operational capacity. Otherwise, it may negatively impact other services, slow down network activities, and potentially disrupt mission-critical functions due to increased overhead.

Step 6: Identify the operational impact of device failure due to exploitation by a threat: Once the device's position in the current operational framework is established, the next step is to determine the consequences of a device compromise resulting from a threat event. Will certain mission-critical functions and operations experience downtime? If so, to what extent? Will a failure in one device trigger a cascade of failures, or will the impact be contained within a closed system?

Step 7: Assess the financial implications of downtime caused by threat exploitation: IoT devices, given their interconnected nature, can have wide-ranging effects if they fail and cause disruptions or delays in operational performance. It is crucial to determine the acceptable duration of such delays before the organization starts incurring financial losses and potentially suffers damage to factors such as consumer trust and reputation due to service outages or failures.

Step 8: Evaluate information security risks: In addition to threats to assets, operations, and individuals, it is necessary to examine information security risks. These risks involve the likelihood

 doi:10.20944/preprints202410.1083.v1

and potential impact of occurrences such as the exposure of user data, personal data, and other confidential information due to device failures or the exploitation of vulnerabilities.

3.5. Risk Control

In this final phase, we formulate and implement security policies to address the challenges and threats faced by the IoT network. These policies are continually monitored to ensure their effectiveness in safeguarding the system against future security threats. Mitigating vulnerabilities within IoT poses a significant challenge due to the multitude of end-users who can create potential attack vectors. As an attacker, exploiting a singular vulnerability can cause a breach; as a defender, it is pertinent to address every avenue of attack. User behavior plays a crucial role in promoting best practices, such as avoiding default usernames and passwords, to make it more challenging for attackers. Although, it does not completely resolve the issue. Additionally, it is vital to control the proliferation of unaccounted devices, which poses a significant risk.

3.5.1. Control Strategies

Once the risk analysis is completed in the preceding step, one of the crucial decisions to be made by the SMG is the selection of an appropriate control strategy, coupled with the implementation of recommended security policies, procedures, and technologies, to counter the identified threats. Determining the suitable control strategy depends on several factors and can sometimes pose a challenge for the SMG in making the correct decision. To simplify this process, we provide guidelines that can be followed to adopt the most effective control strategy, as shown in Algorithm 1.

When should Risk Mitigation be used? Risk mitigation is employed when the potential impact of an attack is significant and poses a serious threat to the continuity of business processes or functions. In such cases, we aim to reduce the risk by addressing vulnerabilities. Closing out vulnerabilities necessitates the implementation of controls or countermeasures. However, it is critical to ensure that the cost of deployment for a control does not exceed the benefits. Risk mitigation is chosen when the risk is unavoidable, but it cannot be accepted. If accepting the risk would result in a predetermined percentage of financial damage to the organization, we opt to implement controls to mitigate the risk. Risk mitigation is chosen when the company cannot progress if a risk avoidance approach is adopted.

When should Risk Acceptance be used? Risk acceptance occurs when an organization evaluates a risk, comprehends the potential loss (P), and decides to accept the risk. This is typically done when the cost of implementing a control (C) outweighs the potential loss. For instance, it would not be logical to invest $10,000 in a countermeasure if the potential loss is only $100.

When should Risk Transference be used? Risk transference involves sharing or transferring risk by shifting the responsibility to another party. It can involve transferring the entire responsibility or liability or shifting a portion of it (risk sharing). Organizations may choose to outsource certain activities to external entities or acquire insurance as means of transferring risk. Risk transference is commonly employed when dealing with sensitive data to avoid being held accountable in case of a compromise. The responsibility is entrusted to a third party to manage.

 doi:10.20944/preprints202410.1083.v1

Algorithm 1: Control strategy Selection: The below is a high-level algorithm that outlines the decision-making process for selecting the appropriate control strategy based on the provided guidelines.

```
# Input variables
potential_impact = input("Enter the potential impact of the attack: ")
cost_of_control = input("Enter the cost of control measures: ")
potential_loss = input("Enter the potential loss: ")
# Step 2: Risk Mitigation
if potential_impact == "significant":
    if float(cost_of_control) <= float(potential_loss):
        control_strategy = "Risk Mitigation"
        exit()
# Step 3: Risk Acceptance
if float(cost_of_control) > float(potential_loss):
    control_strategy = "Risk Acceptance"
    exit()
# Step 4: Risk Transference
if input("Is there a need to shift responsibility or liability? (yes/no): ") == "yes":
    control_strategy = "Risk Transference"
    exit()
# Step 5: Risk Avoidance
if input("Does the impact of risk outweigh the benefits of the asset? (yes/no): ") ==
"yes":
    control_strategy = "Risk Avoidance"
    exit()
# Step 6: Further analysis or considerations
# Add any additional calculations or assessments based on specific context or
requirements
# Default control strategy if no specific conditions are met
control_strategy = "Default Strategy"
# Output
print("Selected Control Strategy:", control_strategy)
```

When should Risk Avoidance be used? Risk avoidance focuses on eliminating any exposure to risks that carry potential losses. The primary factor in determining whether to avoid a specific risk is when the impact of the risk outweighs the benefits of the asset. An organization can avoid risk by eliminating the source of the risk, thereby ceasing the associated activity.

4. Implementation of the Proposed RM Framework Using Case Studies

The case studies presented in this context serve to illustrate the applicability of the proposed framework by presenting hypothetical scenarios. These case studies specifically demonstrate scenarios within the domains of home, healthcare, and retail. Within each domain, we employ the proposed risk management framework to analyze selected IoT devices, showcasing how the various phases of the framework can be utilized to evaluate and address the risks faced by these IoT devices.

4.1. Smart Home Scenario

Smart home devices have become popular recently as technology advances. Within a smart home, every device is connected to the main network. As a result, the compromise of a singular device may pose a risk to an entire network which potentially exposes sensitive information. A key vulnerability of these devices lies in inadequate attention to security during design. Wireless devices are quite vulnerable to risks due to the medium of data transmission, causing them to be prone to hijack and manipulation. Consider Dan's case, Dan's home contains smart home devices with have a vital role in his day-to-day life. Figure 5 provides an illustration of Dan's typical smart home setup, which includes various IoT devices such as a smart thermostat, an Amazon Alexa, a smart garage door, smart locks, smart doorbells, a smart vacuum, and a smart camera system for security purposes. It is critical to note that all these devices operate wirelessly, thereby amplifying their vulnerability to potential attacks.

 doi:10.20944/preprints202410.1083.v1

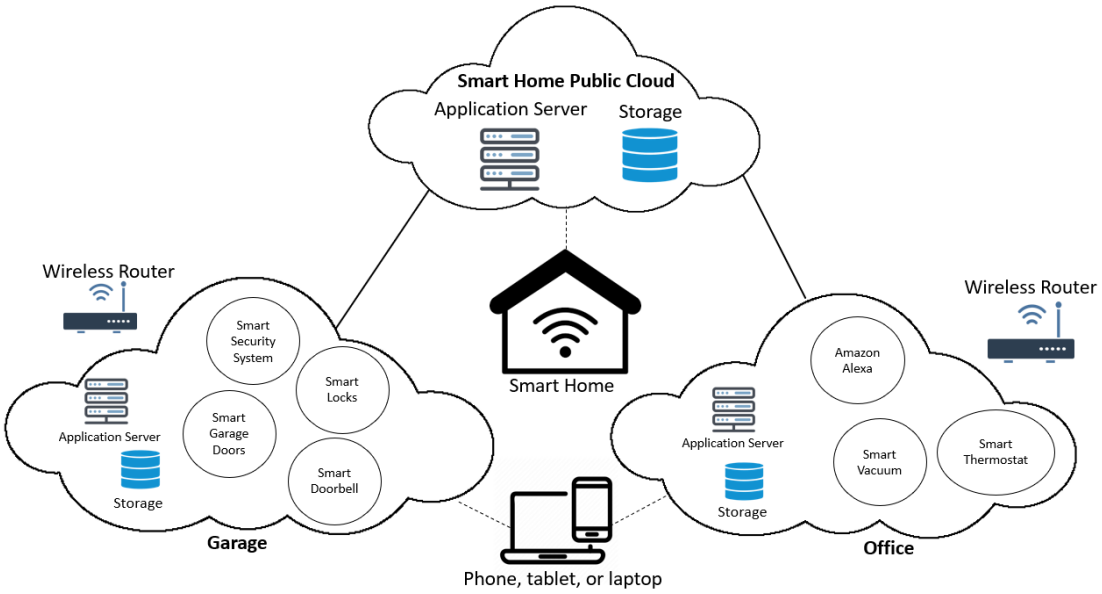

Figure 5. Illustration of a Smart Home IoT Network.

4.1.1. Risk Identification of the Smart Home Network

Dan's network comprises various components, including software, data, hardware, and device procedures. Unlike businesses or hospitals, a home is particularly susceptible to risks that can result in the exposure of personal data, burglary or robbery, and even damage to the property caused by malfunctions, such as thermostat failures. The interconnectedness of all home IoT devices through wireless means significantly amplifies their vulnerability to external attacks. The potential consequences of outside interference in Dan's IoT smart home network are concerning. Attackers may compromise, manipulate, steal, or alter the data of Dan's smart home devices, leading to havoc-inducing scenarios which can include physical attacks, fires, and property damage. For instance, if in-home security cameras are poorly secured, threat actors can obtain access to them, allowing them to spy on residents. An intrusion as such would result in the release of sensitive personal information such as debit card numbers, mailing addresses, social security numbers, and other exploitable information. Furthermore, smart locks and doors can be compromised which leaves the home vulnerable to break-ins or robberies. Given the risks, it is imperative for a smart home network with multiple IoT devices to address all known vulnerabilities and corresponding threats.

4.1.2. Risk Evaluation of the Smart Home Network

The risk evaluation process for a smart home network can be divided into two parts. In the first part, we focus on examining and evaluating each individual device within the network. This evaluation is conducted using a set of questions that have been developed and presented in the previous section. By applying these questions, we assess the specific vulnerabilities and risks associated with each device. Moving on to the second part, we conduct a comprehensive threat assessment. This assessment involves considering various factors and criteria to understand and evaluate the potential impact of each identified threat. By analyzing these factors, such as the likelihood of occurrence and the potential consequences, insights into severity and significance of each threat are revealed. This evaluation allows for identification and prioritization of the most critical vulnerabilities and threats, enabling development of effective risk mitigation strategies to safeguard the network and its connected devices.

A. Device Assessment (DA)

Upon identifying the risks associated with Dan's IoT devices, it is crucial to conduct a further assessment and prioritize these devices based on the questions presented in section 3.2. Additionally,

 doi:10.20944/preprints202410.1083.v1

other factors such as frequency of use and functionality can be considered in ranking these devices. The following devices are listed in order of importance, taking into account Dan's scenario and their impact on overall security:

- Smart home device (Amazon Alexa) [DA-Q1],[DA-Q5],[DA-Q6],[DA-Q12],[DA-Q13]
- Smart locks [DA-Q16] [DA-Q17]
- Smart cam system (security system) [DA-Q14], [DA-Q15]
- Smart garage doors [DA-Q3]
- Smart thermostat [DA-Q17]
- Smart doorbell [DA-Q14]

The most frequently used device in Dan's smart home network is the Amazon Alexa device, which holds significant value due to its multifunctionality. Serving as the central control system for other smart devices, it can perform various tasks and is akin to a secondary smartphone for managing the smart home. Dan utilizes his Amazon Alexa to place orders on Amazon, which implies that at least some account information is stored on the device, including credit card details. Smart locks are critical in physical security and are vital for home security. Compromise of the smart locks not only jeopardizes the security of the home but also compromises the safety of its occupants. The smart cam system serves as another essential component for maintaining overall security and data privacy within the home, as it has the capability to record and alert against suspicious activities. The recorded information on the security cameras could contain sensitive data depending on their placement. Smart garage doors, if directly connected to the home, can provide access to the interior. A compromise of the garage door would consequently compromise the security of those inside the home. A compromised smart thermostat can be exploited to manipulate temperature settings, leading to highly uncomfortable living conditions and potential spikes in gas or electric bills due to excessive heating. The smart doorbell, although useful for porch monitoring, has limited impact beyond that. It does not provide direct access to the home nor monitor activities inside. The smart vacuum has minimal impact on the network and does not perform any critical functions. To evaluate the device assessment final score for Amazon Alexa, Table 2 is utilized, considering the weight assigned to each question based on our discussion. It is important to note that these weights may vary depending on individual preferences.

Table 2. Device Assessment Score Evaluator.

Device Assessment	**Question Weight**	**Amazon Alexa**	**[DA-Q1]**	**[DA-Q2]**	**[DA-Q3]**
			0.0875	0.0658	0.0658
			97	80	30
[DA-Q4]	**[DA-Q5]**	**[DA-Q6]**	**[DA-Q7]**	**[DA-Q8]**	**[DA-Q9]**
0.0658	0.06	0.075	0.045	0.0575	0.045
30	90	80	95	70	70
[DA-Q10]	**[DA-Q11]**	**[DA-Q12]**	**[DA-Q13]**	**[DA-Q14]**	**[DA-Q15]**
0.0225	0.0675	0.035	0.065	0.025	0.0275
75	87	40	92	82	84
[DA-Q16]	**[DA-Q17]**	**[DA-Q18]**	**Final Score**		
0.065	0.07	0.0575	1		
51	54	22	68.27		

B. Threat Assessment (TA)

The subsequent phase involves the identification and prioritization of all the threats that the IoT devices face. These threats will be ranked based on their potential impact on the devices and the

 doi:10.20944/preprints202410.1083.v1

overall IoT network. Presented below is a numbered enumeration of the threats, starting with the most significant:

Botnets [TA-Q1]
Denial-of-Service (DoS) [TA-Q6], [TA-Q10]
Man-in-the-Middle [TA-Q1]
Physical Interference [TA-Q8], [TA-Q9]

A botnet is a type of malware that remotely takes control of devices within a victim's network and spreads rapidly. Cybercriminals use botnets to pilfer sensitive data and launch attacks, such as phishing and DDoS. This poses a considerable risk due to inadequate security controls for smart home devices. A DoS attack occurs when an attacker attempts to overload the information capacity of the victim's system, resulting in slowdowns or even system disablement. These attacks typically have a high frequency rate on an annual basis and can disrupt daily operations if services become unavailable to users. In a Man-in-the-Middle attack, the perpetrator compromises the transmission channel between two devices in a network to intercept the exchanged messages. By gaining control over the communication, the attacker can send illicit messages between systems and devices. This form of attack also poses a significant threat in the given context. Physical interference encompasses potential threats that can be accessed through the physical location of the device, leading to device damage or disruption of functionality. Three common classifications of physical threats include internal, external, and human factors. In the context of physical interference, concerns arise regarding natural threats and power outages. Following the threat identification and ranking, the next step in this framework involves determining the likelihood of each threat occurring. The likelihood of each threat is categorized as frequent, probable, occasional, remote, or improbable. Botnets and DoS are categorized as probable, Man-in-the-Middle as occasional, and Physical Interference as remote. Table 3 is utilized to calculate the final threat assessment score for a given device. Equation (2), derived earlier, is employed to compute the final score of the device as follows:

$$Threat\ Score\ (Ts) = \frac{\sum_{i=1}^{n} TAQ_i \times W_i}{n}$$

where W is the specific weight assigned by the SMG after performing a careful threat assessment (TA) and n is the number of questions in the template.

4.1.3. Risk Factor Computations and Prioritization

Utilizing our probability scale, as presented in Table 4, we assign a probability value to each threat, indicating the likelihood of its occurrence and its corresponding impact on the network. To prioritize the threats, we categorize them into different severity groups based on their potential consequences. In the Severe group, we place smart home devices and smart locks, as they pose a significant risk to Dan's physical security, potentially resulting in extreme impacts. Smart camera systems and smart garage doors are categorized in the Significant group, as their compromise would have notable effects on both the network and physical security. Smart thermostats fall into the Moderate group, given their medium-level impact on the network. On the other hand, smart doorbells and smart vacuums are assigned to the Minor and Minimal groups, respectively, due to their low or negligible impact on the network.

Table 3. Threat Assessment Score Evaluator.

Threat Assessment	Question Weight	Amazon Alexa	Threat Assessment	Question Weight	Amazon Alexa
[TA-Q1]	.0650	87	[TA-Q9]	.0650	27
[TA-Q2]	.0750	75	[TA-Q10]	.0750	50
[TA-Q3]	.0725	40	[TA-Q11]	.0450	20
[TA-Q4]	.0725	30	[TA-Q12]	.0575	86

 doi:10.20944/preprints202410.1083.v1

[TA-Q5]	.0725	65	[TA-Q13]	.0775	90
[TA-Q6]	.0525	73	[TA-Q14]	.0900	18
[TA-Q7]	.0800	79	[TA-Q15]	.0650	33
[TA-Q8]	.0350	15	Final Score	1	52.53

Table 4. Computation of SLE with impact on network.

DEVICE	DV	EF%	SLE	IMPACT ON NETWORK	SEVERITY GROUP
SMART VACUUM	$200	20%	$40	Low	Minimal
SMART DOORBELL	$250	35%	$87.5	Low	Minor
SMART THERMOSTAT	$300	60%	$180	Medium	Moderate
SMART GARAGE DOORS	$300	70%	$210	Notable	Significant
SMART CAM SYSTEM	$1,500	80%	$1200	Notable	Significant
SMART LOCKS	$250	90%	$225	High	Severe
SMART HOME DEVICE	$100	95%	$95	High	Severe

As shown in Table 5, we identify botnets and denial-of-service (DoS) threats as Probable, indicating a significant likelihood of occurrence and a notable impact on the network. Man-in-the-middle threats are classified as Occasional, reflecting a moderate chance of occurrence with a moderate impact on the network. Physical interference is placed in the Remote group, signifying a minor probability of the threat occurring and a low impact on the network. With the given configurations, we compute the SLE, RM, and Residual Risk Factor (RRF) by assuming the characteristics of the device. The values of Exposure Factor (*EF*) and Time period (*Tp*) are subjectively assessed based on the given scenario. Computations of SLE, comprehensive findings with results are summarized in Table 4, Table 5, and Table 6, providing an overview of the threat assessment and its implications. Table 7 represents an analysis of various smart devices in terms of their potential risks using factors such as *DV, Tρ, RM, ESC, UF,* and Residual Risk Factor (RRF).

4.1.4. Risk Analysis of Smart Home IoT Devices

The previously identified threats will undergo further evaluation to determine the most suitable security measures for the network. At this stage, the SLE of each device in the network has been calculated to obtain a better understanding of their value to the organization. The subsequent step involves developing strategies to manage the risks associated with each device, which can fall into categories such as risk mitigation, risk acceptance, etc. Firstly, the critical functions of the devices were identified. For instance, Amazon Alexa can interact with Dan's network, provide weather updates, set alarms, and facilitate product orders from Amazon. In the second step, all known threat sources were identified, revealing vulnerabilities in Amazon Alexa's speakers that could be exploited for eavesdropping and phishing attacks. Malicious software could be disguised and uploaded to Alexa, enabling covert audio recording within Dan's home.

Table 5. Smart Home Device Prioritization Scale.

Devices	Significance of Device	Description	Range
Smart Vacuum	Minimal	Extremely unlikely the risk occurs. Little to no impact on the network.	(0-20%)
Smart Doorbell	Minor	Minor chance the risk occurs. Low impact on the network.	(21-40%)
Smart Thermostat	Moderate	Moderate chance the risk occurs. Medium impact on the network.	(41-60%)

 doi:10.20944/preprints202410.1083.v1

SmartCam System Smart Garage Doors	Significant	Significant chance the risk occurs. Notable impact on the network.	(61-80%)
Smart Locks	Severe	Severe chance the risk occurs. Extreme impact on the network.	(81-100%)

Table 6. Smart Home Security Threat Prioritization Scale

Threats	Significance of Threat	Description	Range
	Improbable	Extremely unlikely the threat occurs. Little to no impact on the network.	(0-20%)
Physical Interference	Remote	Minor chance the threat occurs. Low impact on the network.	(21-40%)
Man-in-the-Middle	Occasional	Moderate chance the threat occurs. Medium impact on the network.	(41-60%)
Botnets	Probable	Significant chance the threat occurs. Notable impact on the network.	(61-80%)
Denial-of-Service	Frequent	Severe chance the threat occurs. Extreme impact on the network.	(81-100%)

Table 7. Threat Prioritization Using Factors (*Tρ*, *ESC*, and *UF*)**.**

Device	*DV*	*Tρ*	*RM*	*ESC*	*UF*	*RRF*	*Impact of RRF*
Smart vacuum	$200	5%	$10	70%	10%	$2.70	Low
Smart doorbell	$250	15%	$37.5	60%	10%	$11.25	Medium
Smart thermostat	$300	25%	$75	80%	10%	$21.00	Medium
Smart garage doors	$300	45%	$135	50%	10%	$54.00	High
Smart cam system	$1500	75%	$1125	40%	10%	$468.00	Very High
Smart locks	$250	90%	$225	20%	10%	$202.50	High
Smart home device	$100	95%	$95	10%	10%	$94.50	Low

The third step of the risk analysis involves assessing the likelihood of these threat sources posing credible risks to the organization and estimating the probability of exploiting assets or device functions. In the case of Amazon Alexa, a 95% threat probability was assigned during the calculation of Risk Mitigation (RM), indicating a high likelihood of a threat occurring. In the fourth step, the operational framework of the devices under threat is defined, with a particular emphasis on understanding the network connections of the identified devices. It is crucial to recognize that Amazon Alexa holds considerable influence within the network, as it can interact with multiple devices simultaneously. Therefore, compromising Amazon Alexa also exposes other devices to risk. The fifth step involves defining the current operational overhead and operating capacity of the device network. In the sixth step, the potential impact on operations is analyzed if a device fails due to exploitation by a threat. Since Amazon Alexa serves as a central device in the smart home, its compromise has the potential to affect every other device, leading to significant downtime. However, it should be noted that the downtime resulting from a threat exploiting Amazon Alexa in Dan's house may not have as severe financial implications as it would in a business setting.

In the seventh step, the financial effects, considering downtime resulting from the exploitation of vulnerabilities in devices or assets by threats, are determined. If a threat successfully exploits Amazon Alexa in Dan's house, the resulting downtime may not incur significant financial costs. Lastly, in the eighth step, information security risks must be examined, considering both their likelihood of occurrence and the potential impact they could have. It is evident that the likelihood of occurrence with Amazon Alexa is extremely high due to its relatively weak factory security settings. As previously discussed, compromising Amazon Alexa puts all other devices at risk.

 doi:10.20944/preprints202410.1083.v1

4.1.5. Risk Control of Smart Home IoT Devices

In situations where the exposure factor (EF) reaches 61% to 100% of the device value (DV), it becomes essential for organizations to mitigate the associated risks. This applies to devices such as Smart Garage Doors, SmartCam System, Smart Locks, and Smart home devices, which have exposure factors of 70%, 80%, 90%, and 95% respectively. In these cases, risk mitigation requires taking measures to minimize the probability of the identified threats occurring. Additionally, a contingency plan is enacted to minimize the potential impact on the network if any of these threats materialize. Devices with EF values ranging from 0% to 20% are categorized as minimal risk, and the organization can choose to accept the risk. For instance, Smart Vacuum falls into this category with an exposure factor of 20%. Accepting the risk is typically done when the threat's severity is deemed very low.

The organization considers it unwarranted to invest resources in protecting the device because, even in the event of a threat, the impact on the network would be minimal. Devices with EF values between 21% and 60% require the transfer of risk. This applies to the Smart Doorbell and Smart Thermostat in the aforementioned case study, with exposure factors of 35% and 60% respectively. Risk transfer is commonly achieved through a third-party, often an insurance company. By transferring the risk, the organization or individual can have the insurance company assume responsibility for the potential damage caused to the network, in exchange for paying an insurance premium. In cases where the impact on the network resulting from a threat would exceed the device's value by over 100%, the organization chooses to avoid the risk altogether. Avoiding the risk entails discontinuing the use of the specific IoT device as part of the network. This decision is based on the understanding that the potential damage outweighs any benefits or value associated with the device. In summary, managing the exposure factor of devices plays a crucial role in risk assessment and decision-making. Depending on the EF percentage, organizations can determine whether to mitigate, accept, transfer, or avoid the associated risks, thus ensuring the security and operational integrity of their IoT networks.

The results of the smart home domain are summarized in Figure 6 using a dashboard that visually compares various IoT devices based on their assessment question weights, device value, and associated risks. The pie charts on the left illustrate the weight distribution of device and threat assessment questions, emphasizing the relative importance of different factors in evaluating device security. The bar chart in the top-right compares the value of different devices, considering network impact and severity levels. The bar chart in the bottom-right contrasts the risk mitigation costs and SLE for each device, highlighting the financial implications of potential security incidents.

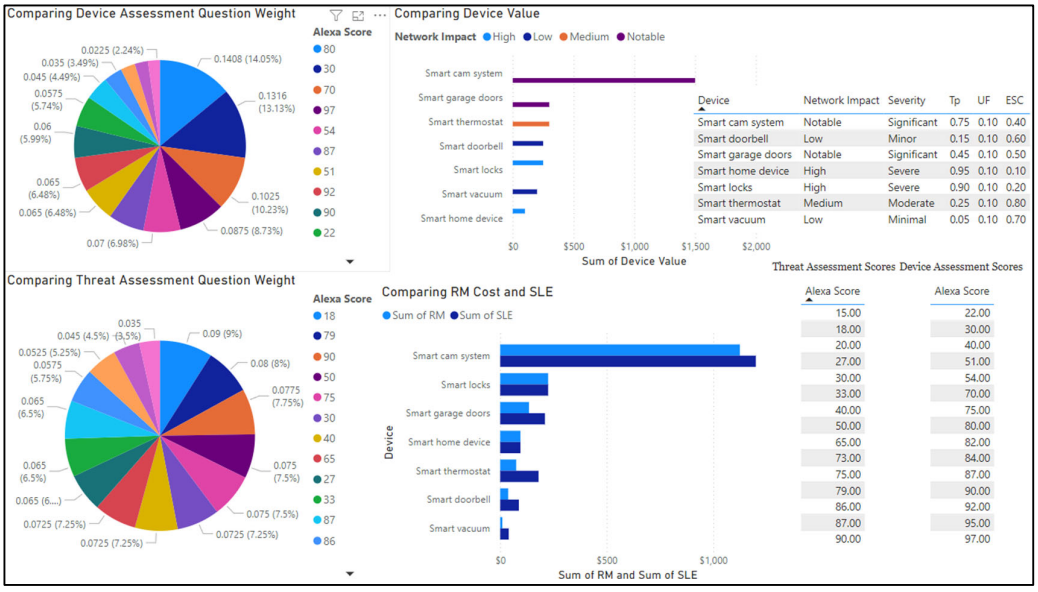

Figure 6. Summary of Smart Home Case Study.

 doi:10.20944/preprints202410.1083.v1

4.2. Healthcare Scenario

In a healthcare scenario, adopting an overarching framework is imperative due to inherent risks associated with IoT devices, which can jeopardize a patient's well-being. Additionally, these devices may reveal sensitive health information to unauthorized individuals.

The diagram presented in Figure 7 illustrates the wireless connectivity of various IoT devices, including ingestible sensors, smart contact lenses, the Open Artificial Pancreas System (APS), cochlear implants, foot drop implants, and pacemakers, all linked through wireless routers. The only device connected via a wired connection is the stationary medical device. Within a hospital setting, IoT devices play a vital role in daily operations, as they are employed to provide effective treatment to patients. The hospital's primary objective is to enhance security measures throughout the organization, safeguarding the integrity of both the patients' devices and their associated data from compromise and exploitation. By implementing robust security protocols and adhering to the established framework, the hospital aims to maximize the protection of patient devices and preserve the confidentiality and privacy of their medical information.

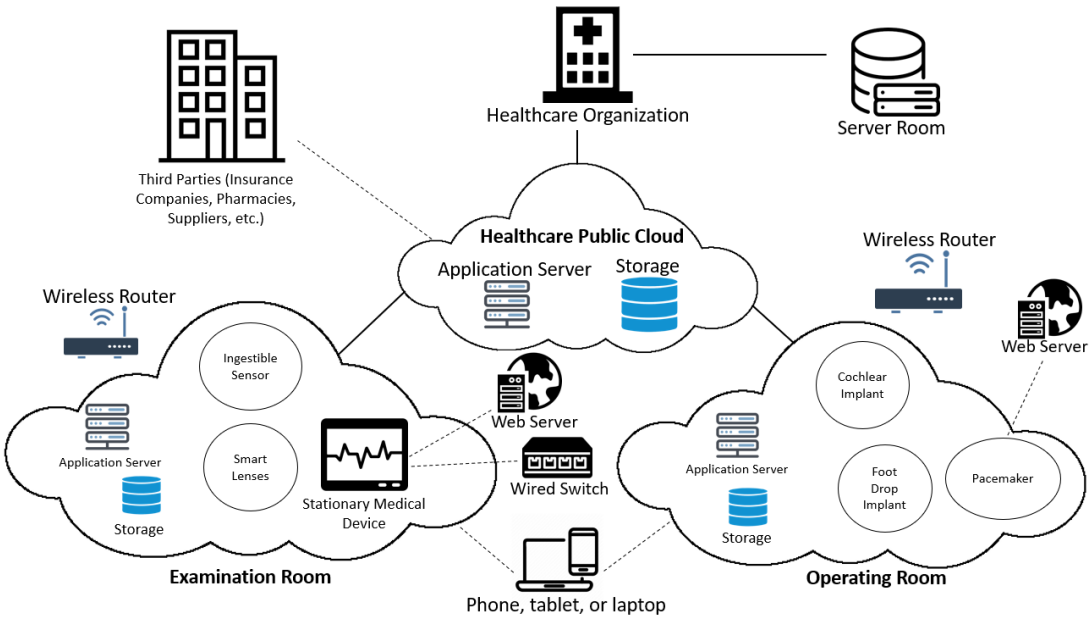

Figure 7. Illustration of a Healthcare IoT Network**.**

4.2.1. Risk Identification of Healthcare Network

Utilizing the proposed framework, the various components of the IoT network, including software, data, procedures, and hardware, are systematically identified. Within the hospital network, specific areas such as the surgery room and examination room are considered. The surgery room houses common IoT devices, namely the Open Artificial Pancreas System, Cochlear Implant, Foot Drop Implant, and Pacemaker, while the examination room comprises the Stationary Medical Device, Smart Contact Lenses, and Ingestible Sensor. Although categorized as hardware, each of these devices operates using embedded software programs. To facilitate analysis and organization, IoT devices are further classified into groups corresponding to specific components within the IoT network. The Stationary Medical Device, serving as an output device, transforms data into a readable format, positioning it as a hardware source. Additionally, the Open Artificial Pancreas System, Cochlear Implant, Foot Drop Implant, Pacemaker, Smart Contact Lenses, and Ingestible Sensor are also categorized as part of the hardware group. Vulnerabilities within each device are then systematically assessed, adhering to the evaluation criteria outlined in the proposed framework.

Notably, wireless devices present higher vulnerability due to the potential interception of transmitted data packets. Conversely, the Stationary Medical Device, being wired, is identified as the

 doi:10.20944/preprints202410.1083.v1

least vulnerable device within the hospital network. The final stage of risk identification involves identifying potential threats. IoT devices connected to smartphone applications pose a significant risk as they transmit protected health information. In the event of a cybercriminal hacking into the smartphone within the hospital premises, all transmitted data becomes susceptible to identity theft or financial exploitation. Unauthorized access to these devices allows for the alteration of messages intended for authorized users, potentially concealing critical health problems or misleading healthcare professionals Another scenario involves the Stationary Medical Device in the examination room displaying conflicting messages compared to the readings from a patient's pacemaker, posing a serious concern. Furthermore, post-procedure, wireless devices implanted in a patient's body require programming and are therefore prone to cyber-attacks, necessitating heightened security measures.

4.2.2. Risk Evaluation of Healthcare Network

The initial stage of risk evaluation involves assessing the IoT devices present in the hospital and prioritizing them based on various factors, including revenue generation, replacement costs, and the devices' significance to patient health and network operations. The following list presents the IoT devices in descending order of importance: Pacemaker, Cochlear Implant, Open Artificial Pancreas System, Foot Drop Implant, Stationary Medical Device, Smart Lenses, and Ingestible Sensor. The Pacemaker and Cochlear Implant are the most expensive devices to replace, and along with the Open Artificial Pancreas System, they hold the highest significance in terms of life or death for patients. The Foot Drop Implant, requiring surgery and significant replacement costs, holds considerable importance. The Stationary Medical Device plays a crucial role in monitoring a patient's health and is vital to both the patient and the entire network. Smart Lenses and Ingestible Sensors, while useful, are less vital and more affordable to replace, placing them lower on the list. The subsequent step involves identifying and ranking the threats facing these IoT devices, considering the potential damage to both the devices and the IoT network. The following list presents the threats in descending order of importance: User Authentication Deficiencies, Insider Threat, Endpoint Data Leakage, and Excessive User Permissions.

User Authentication Deficiencies are frequently observed in healthcare organizations, typically arising from weak password requirements or improper handling of passwords, such as leaving them visible in workspaces or utilizing single sign-on logins. An authorized user with malicious intent can pose a significant risk by leaking sensitive information outside the network. Ransomware, phishing, and malware attacks are common and can lead to data loss. It is crucial to restrict authorized user access to only the necessary systems and data. When access exceeds what is required, potential security issues may arise. The subsequent step in the framework involves determining the likelihood of each threat occurring. Each threat is categorized as frequent, probable, occasional, remote, or improbable. User Authentication Deficiencies are considered probable, while Insider Threats and Endpoint Data Leakage are categorized as occasional. Excessive User Permissions are labeled as remote in terms of likelihood.

4.2.3. Risk Factor Computations

Table 8 provides the results of computations and gives information about IoT devices in terms of their Device Value (*DV*), Exposure Factor (*EF%*), Single Loss Expectancy (*SLE*), Risk Category, and Risk Mitigation Strategy. It highlights the level of risk associated with each device and suggests appropriate strategies to mitigate the identified risks. The Risk Mitigation Strategy column suggests the approach to mitigate the identified risks, which is Risk Acceptance for devices in the Minimal Risk category and Risk Mitigation for devices in the Moderate and High-Risk categories. Figure 8 depicts an IoT environment comprising multiple devices (*D1, D2, ...Dn*), where each device (Di) may possess multiple vulnerabilities (*V1, V2, ….Vn*). Each vulnerability gives rise to one or more threats (T1, T2, ….Tn), which can be executed by an attacker through successful exploitation of the device's vulnerability, consequently leading to undesirable outcomes for the IoT network. The exposure factor

 doi:10.20944/preprints202410.1083.v1

(*EF*%) quantifies the device's susceptibility to a threat in the event of a successful attack, while Tp represents the likelihood of a threat occurring.

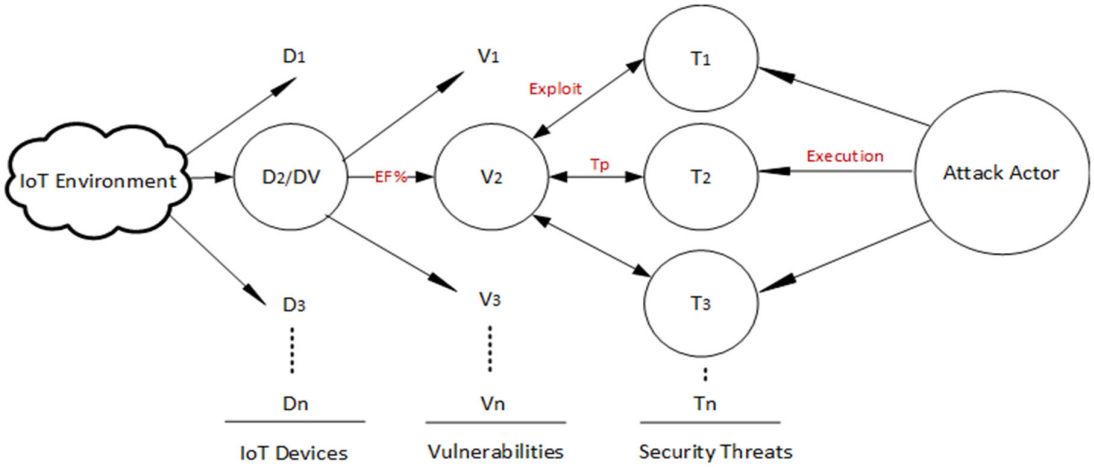

Figure 8. Risk Factor Computation Diagram for IoT Devices.

Table 8. Device Risk Assessment and Mitigation Strategies for Healthcare IoT.

IoT Device	Device Value (DV)	EF%	SLE	Risk Category	Risk Mitigation Strategy
Ingestible Sensor	$55	40%	$22	Minimal Risk	Risk Acceptance
Smart Lenses	$500	45%	$225	Moderate Risk	Risk Mitigation
Foot Drop Implant	$5,000	50%	$2,500	Moderate Risk	Risk Mitigation
Stationary Medical Device	$550	55%	$302.5	Moderate Risk	Risk Mitigation
Open APS	$6,500	60%	$3,900	Moderate Risk	Risk Mitigation
Cochlear Implant	$40,000	70%	$28,000	High Risk	Risk Mitigation
Pacemaker	$58,000	80%	$46,400	High Risk	Risk Mitigation

It is important to emphasize that the value of *Tp* is contingent upon the existing security controls and the prevailing risk environment. Figure 9 demonstrates the practical application of the diagram presented in Figure 8, specifically by employing the IoT devices from the healthcare case study. Eq (3), derived earlier, is utilized to calculate the SLE for each healthcare IoT device by incorporating appropriate values of *DV* and EF%

 doi:10.20944/preprints202410.1083.v1

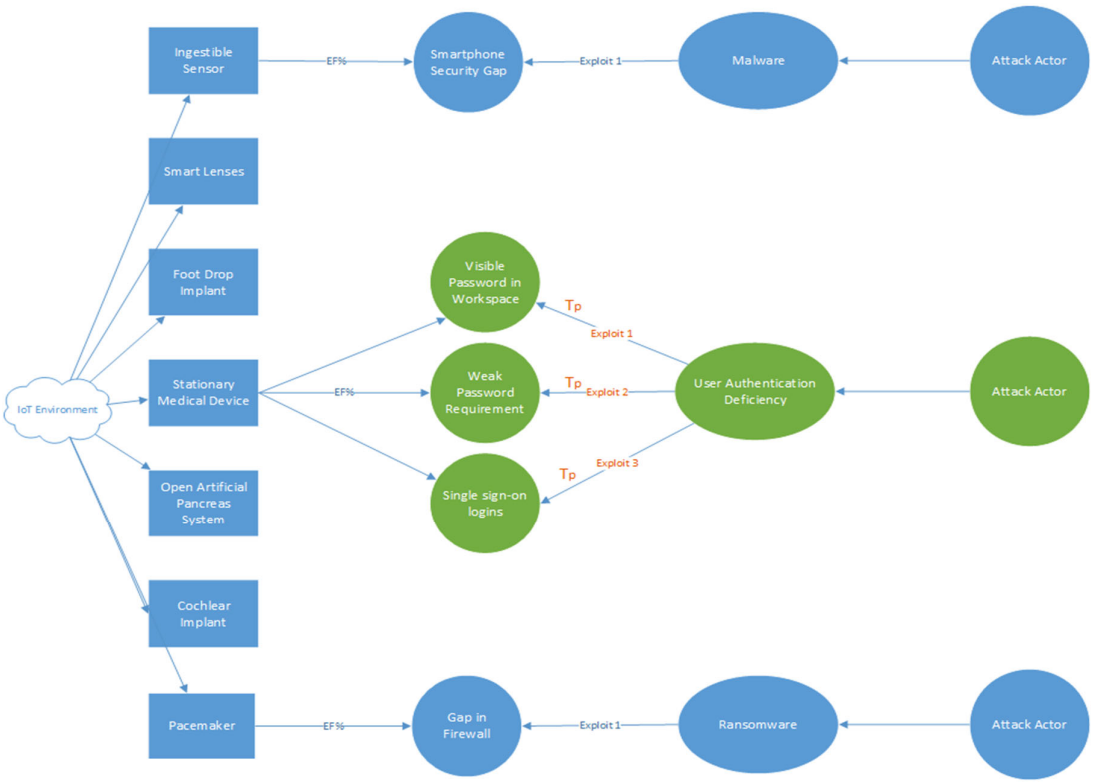

Figure 9. Healthcare Risk Factor Computation for Multiple IoT Devices.

4.2.4. Risk Prioritization of Healthcare IoT Devices

By utilizing the probability scale within the framework, the assessment determines the likelihood and impact of each threat on the network. User Authentication Deficiencies, as displayed in Table 10, fall into the probable category due to the likelihood of occurrence and potential impact. Insider Threats and Endpoint Data Leakage are classified as occasional since they have a moderate likelihood and significant consequences. Excessive User Permissions are considered remote as the chances of their occurrence are minimal. As shown in Table 9, the devices are categorized based on their importance.

Table 9. Healthcare Device Prioritization Scale.

Devices	Significance of Device	Description	Range
Ingestible Sensor	Minimal	Extremely unlikely the risk occurs. Little to no impact on the network.	(0-20%)
	Minor	Minor chance the risk occurs. Low impact on the network.	(21-40%)
Smart Lenses, Foot Drop Implant, Stationary Medical Device, Open APS	Moderate	Moderate chance the risk occurs. Medium impact on the network.	(41-60%)
Cochlear Implant, Pacemaker	Significant	Significant chance the risk occurs. Notable impact on the network.	(61-80%)
	Severe	Severe chance the risk occurs. Extreme impact on the network.	(81-100%)

Table 10. Healthcare Security Threat Prioritization Scale.

Threats	Significance of Threat	Description	Range
	Improbable	Extremely unlikely the threat occurs. Little to no impact on the network.	(0-20%)

 doi:10.20944/preprints202410.1083.v1

Excessive User Permissions Insider Threat, Endpoint Data Leakage User Authentication Deficiencies	Remote	Minor chance the threat occurs. Low impact on the network.	(21-40%)
	Occasional	Moderate chance the threat occurs. Medium impact on the network.	(41-60%)
	Probable	Significant chance the threat occurs. Notable impact on the network.	(61-80%)
	Frequent	Severe chance the threat occurs. Extreme impact on the network.	(81-100%)

4.2.5. Risk Analysis of Healthcare IoT Devices

During this phase, a detailed analysis of each threat is conducted, and the corresponding security policies and procedures are established. The SLE of each network device is evaluated to gauge the potential impact of the threat. Based on this assessment, security recommendations are formulated and examined. Using the proposed risk probability table, it is determined that none of the devices fall into the minimal or severe risk categories. This indicates that each device will require a risk mitigation or risk transfer plan, possibly involving a third party.

Figure 10 provides a comprehensive summary of the Healthcare Case Study by visually representing the comparison between device value and Single Loss Expectancy (SLE) for various IoT medical devices. The bar chart on the left side displays the device value and SLE for devices like pacemakers, cochlear implants, and smart lenses, highlighting the financial impact of potential security breaches. The threats associated with each device are listed in the top-right table, categorized by their significance and described in detail. This information helps in understanding the potential risks and their severity. The pie chart at the bottom-right illustrates the distribution of device values across different IoT medical devices, emphasizing the relative importance of each device. Overall, this dashboard is crucial for identifying high-risk devices and prioritizing risk mitigation strategies effectively.

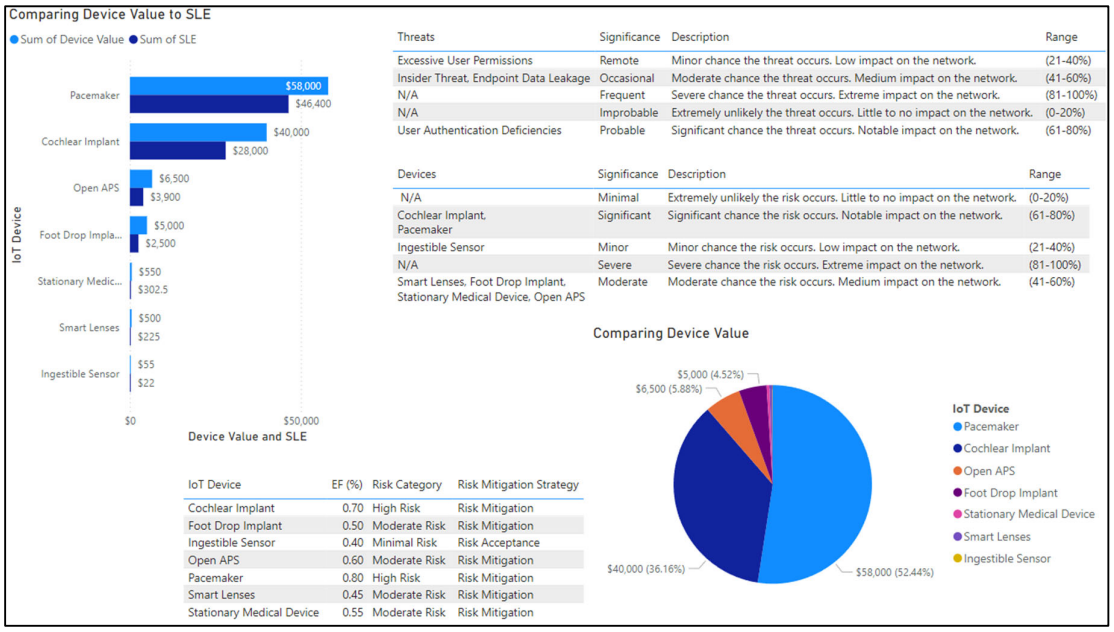

Figure 10. Summary of Healthcare Case Study.

4.2.6. Risk Control of Healthcare IoT Devices

When the exposure factor (EF) of an IoT device reaches 60%-100% of its device value (DV), it is imperative for the organization to proactively mitigate the associated risk. This requirement applies

 doi:10.20944/preprints202410.1083.v1

to pertinent devices such as the Open APS, Cochlear Implant, and Pacemaker, with EFs of 60%, 70%, and 80% respectively. Risk mitigation is comprised of implementing measures to reduce the probability of the identified threats occurring and developing an extensive contingency plan to minimize their potential impact on the network. Furthermore, devices exhibiting EFs ranging from 0%-20% are classified as minimal risk, prompting the organization to accept the risk due to the relatively low severity of the potential threats. Conversely, devices with EFs falling within the range of 21%-59% (e.g., the Ingestible Sensor, Smart Lenses, Foot Drop Implant, and Stationary Medical Device in our case study, with EFs of 40%, 45%, 50%, and 55% respectively) warrant a risk transfer strategy, which involves shifting the risk responsibility to a trusted third party through contractual or legislative means, as expounded in Section 3.

4.3. Retail Scenario

The application of this framework is crucial in a retail setting due to the widespread use of mobile devices by customers. In order to enhance sales and improve customer experience, a convenience store has incorporated IoT devices within its premises. However, the presence of these IoT devices exposes every customer with a device in proximity to potential cyber threats. The security of customers' private information becomes vulnerable as a consequence. As depicted in Figure 11, the digital kiosk, beacon, Radio Frequency Identification (RFID) reader, and heat sensor are all wirelessly connected to the network through wireless routers. The wireless nature of these devices renders them more susceptible to malicious attacks, making the occurrence of such attacks highly probable. Conversely, the surveillance camera, being a wired device, presents comparatively greater difficulty for exploitation when compared to the wireless devices utilized within the store.

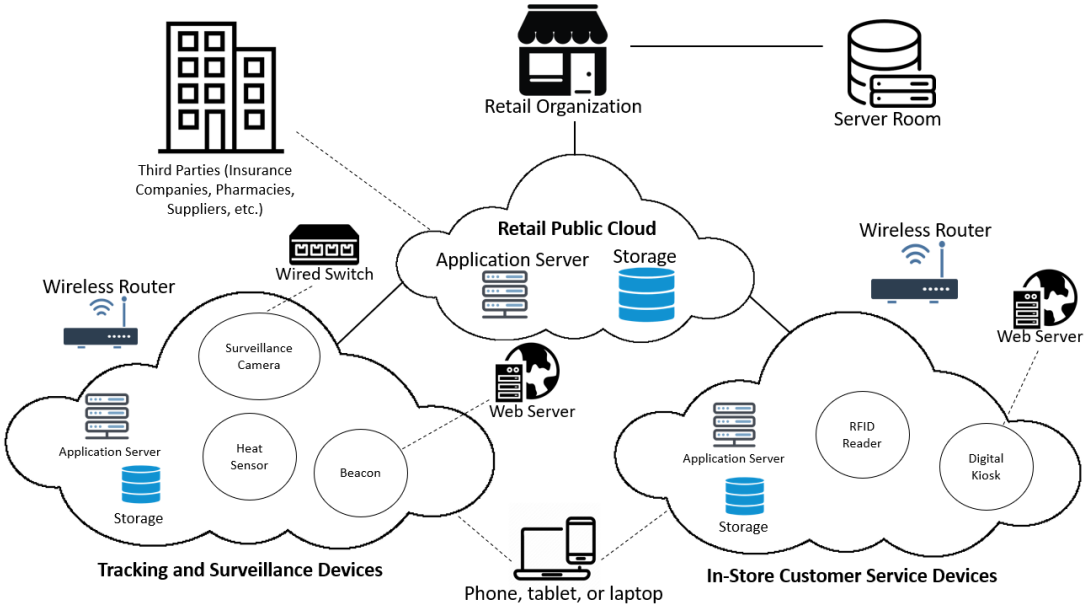

Figure 11. Illustration of Retail Organization IoT Network.

4.3.1. Risk Identification of Retail Organization

Initially, the IoT network components in the store are comprehensively documented. The devices include digital kiosks, beacons, RFID readers, heat sensors, and surveillance cameras, many of which integrate software functionalities. Digital kiosks serve as output devices, transforming data into readable formats, while the others fall into the hardware category. Vulnerabilities are identified and evaluated, revealing that wireless devices are more susceptible than wired ones. Consequently, surveillance cameras exhibit the least vulnerability due to their wired nature. The next step involves identifying potential threats and implementing security measures during the design phase. Digital kiosks face threats related to user authentication deficiencies, and communication between beacons

 doi:10.20944/preprints202410.1083.v1

and smartphones lacks encryption, enabling unauthorized access. RFID systems pose eavesdropping risks, while surveillance cameras are vulnerable to brute force attacks, leading to privacy breaches.

4.3.2. Risk Evaluation of Retail Organization

The initial step in risk evaluation involves assessing IoT devices and assigning them rankings based on their importance to the organization. This ranking is determined by considering factors such as revenue generation, replacement costs, and protection requirements, as outlined in Section 3. The devices are listed in descending order of importance: Digital Kiosk, RFID Reader, Surveillance Camera, Heat Sensor, and Beacon. A digital kiosk holds significant value for the business, as it is both expensive to replace and provides customers with immediate self-service options, greatly enhancing their experience. An RFID reader is also costly to replace but offers the advantage of efficient object tracking, allowing for quick scanning of multiple items simultaneously. Surveillance cameras play a vital role in ensuring physical security, acting as a deterrent to shoplifters. While a heat sensor may not be expensive to replace, it aids in determining areas of high customer traffic within the store, offering invaluable insight into store design and modification. Beacons, although easily replaceable, serve a vital function in attracting customers by sending notifications to their phones, informing them about enticing deals and encouraging store visits. The subsequent stage in risk evaluation involves ranking the threats faced by the IoT devices. This ranking is determined by considering the questions raised earlier regarding the potential risks to the organization's information and the associated costs of recovery and prevention. The threats are presented below in descending order of importance: User Authentication Deficiencies, Data Leakage, and Brute Force Attacks.

User Authentication Deficiencies pose significant risks to retailers, as unauthorized access can allow threat actors to manipulate critical infrastructure. Data Leakage concerns both retailers and customers, as it involves protecting personal information and passwords. Without encryption, eavesdropping can exploit sensitive data. Brute Force Attacks exploit vulnerabilities, enabling unauthorized access to devices like surveillance cameras, allowing theft of footage and unauthorized monitoring, violating customer and staff privacy. The next step assesses the likelihood of these threats. Table 12 categorizes the likelihood as frequent, probable, occasional, remote, or improbable. Brute Force Attacks are classified as frequent, User Authentication Deficiencies as probable, and Data Leakage as occasional.

4.3.3. Risk Prioritization of Retail Organization

The proposed framework probability scale, as depicted in Table 12, is utilized to assess the probability and impact of each threat on the network. Brute Force Attacks are classified as frequent since they occur most frequently compared to other threats. User Authentication Deficiencies are categorized as probable due to the likelihood of their occurrence. Data Leakage, while not as frequent as other threats, falls into the occasional group. The prioritization of devices is presented in Table 11 based on their significance to the organization.

Table 11. Retail Device Prioritization Scale.

Devices	Significance of Device	Description	Range
Beacon	Minimal	Extremely unlikely the risk occurs. Little to no impact on the network.	(0-20%)
	Minor	Minor chance the risk occurs. Low impact on the network.	(21-40%)
Heat Sensor, Surveillance Camera	Moderate	Moderate chance the risk occurs. Medium impact on the network.	(41-60%)
RFID Reader, Digital Kiosk	Significant	Significant chance the risk occurs. Notable impact on the network.	(61-80%)
	Severe	Severe chance the risk occurs. Extreme impact on the network.	(81-100%)

Table 12. Retail Security Threat Prioritization Scale.

Threats	Significance of Threat	Description	Range

 doi:10.20944/preprints202410.1083.v1

	Improbable	Extremely unlikely the threat occurs. Little to no impact on the network.	(0-20%)
	Remote	Minor chance the threat occurs. Low impact on the network.	(21-40%)
Data Leakage	Occasional	Moderate chance the threat occurs. Medium impact on the network.	(41-60%)
User Authentication Deficiencies	Probable	Significant chance the threat occurs. Notable impact on the network.	(61-80%)
Brute Force Attacks	Frequent	Severe chance the threat occurs. Extreme impact on the network.	(81-100%)

Equation (3), derived earlier, is employed to calculate the Single Loss Expectancy (SLE) for each IoT device used in the retail domain, considering appropriate values of *DV* and *EF%*. The computations and results are presented in Table 13. The Risk Category column categorizes the level of risk associated with each device, ranging from Medium to High to Critical, as shown in Table 13. Moreover, the Risk Mitigation Plan column outlines the measures to mitigate the identified risks for each device whereas the Contingency Plan column specifies the backup plans or alternative strategies in case the threat occurs and impacts the device or network.

4.3.4. Risk Analysis of Retail IoT Devices

During this phase, a comprehensive assessment of each threat is conducted to determine the most suitable security procedures for the network. The *SLE* of every device is calculated to assess their value to the organization. Subsequently, decisions are made regarding the management of risks going forward. As previously mentioned, the options include risk mitigation, risk acceptance, risk transference, and risk avoidance. Since none of the devices fall into the improbable or remote category, the decision is made not to accept the risk for any device.

4.3.5. Risk Control of Retail IoT Devices

There are no devices categorized as minimal risk, but if there were, the organization would opt to accept the risk due to the minimal impact of any potential threats. Devices with *EF* ranging from 21% to 60% would have their risks transferred. This applies to the beacons, heat sensors, and surveillance cameras in our case study, with *EF* values of 40%, 50%, and 60% respectively.

Table 13. IoT Device Risk Assessment and Mitigation Strategies for Retail Domain.

Device	Device Value (DV)	Exposure Factor (EF)	Single Loss Expectancy (SLE)	Risk Category	Risk Mitigation Plan	Contingency Plan
Beacon	$25	40%	$10	Medium	Improve encryption and authentication	Implement backup beacons
Heat Sensor	$100	50%	$50	Medium	Enhance data encryption	Deploy redundant heat sensors
Surveillance Camera	$200	60%	$120	High	Regular firmware updates	Store backup footage in secure location
RFID Reader	$1200	70%	$840	High	Implement access control measures	Maintain offline inventory tracking system
Digital Kiosk	$2500	80%	$2000	Critical	Implement strong user authentication	Establish alternative customer service

Insurance or third-party entities would assume responsibility for managing the risks associated with these devices. For devices with EF values between 60% and 100%, such as the RFID Reader and Digital Kiosk (with EF of 70% and 80% respectively), the focus would be on mitigating the risks by reducing the probability of threats and implementing contingency plans. If a device's exposure factor indicates that the potential impact on the network would exceed the device's value, the organization would choose to completely avoid the risk by discontinuing the device in the convenience store.

 doi:10.20944/preprints202410.1083.v1

Figure 12 provides a detailed summary of a retail case study, showcasing the value of various IoT devices and their associated security risks. The bar chart on the left displays the sum of device values and SLE for different devices. The pie chart below highlights the distribution of device values, with the Digital Kiosk representing the highest value. The table on the right details the exposure factors, risk mitigation plans, and contingency plans for each device. Additionally, it categorizes the risks and their significance, explaining the potential impact on the network.

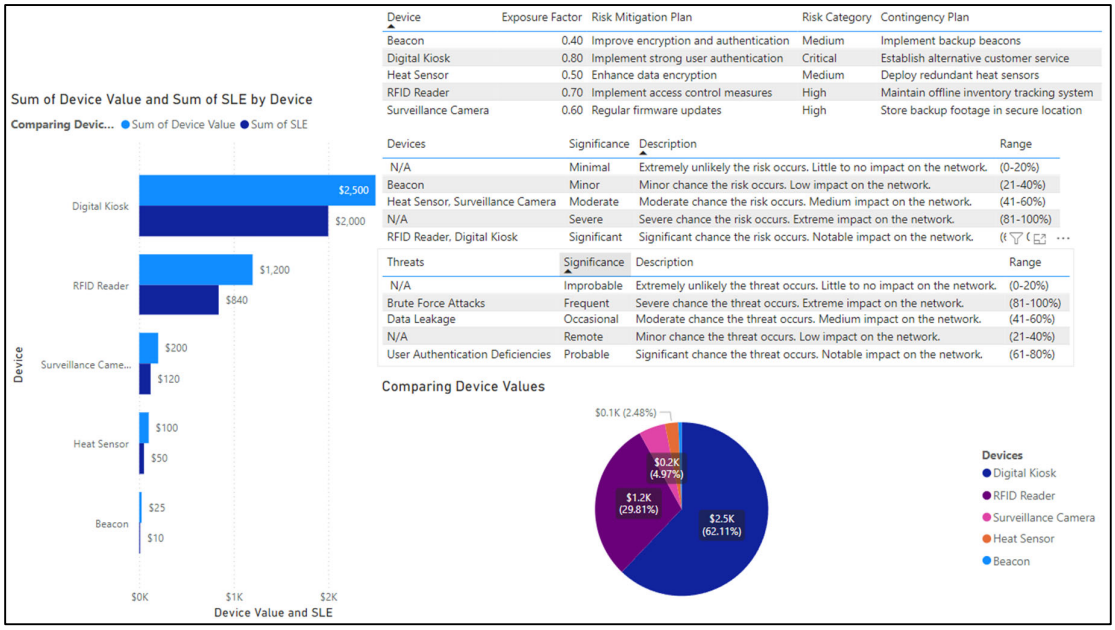

Figure 12. Summary of Retail Case Study.

5. Conclusions

The paper presents a complete framework for managing risks associated with the adoption of IoT devices. Unique contributions of this research consist of addressing security deficiencies in IoT designs and providing a detailed approach for risk assessment, identification, evaluation, and control. We have developed specific methodologies for risk identification and evaluation, supported by illustrative examples and evaluation tables applicable to various IoT devices. By computing key metrics such as SLE, RM, and RRF for each device, the paper accurately portrays the value provided by individual devices. We have also devised tables for prioritizing risks based on their significance and description, enabling organizations to make informed decisions. Furthermore, the paper introduces an innovative 8-step risk analysis approach encompassing mission-critical, threat source, and device analysis, leading to effective security policy recommendations and controls. The integration of IoT devices into real-world case studies is demonstrated through diagrams, highlighting the practicality of the proposed framework. Overall, our research emphasizes the importance of the framework in evaluating and safeguarding IoT devices, making it relevant and beneficial for organizations and households utilizing IoT technology. In future, we would like to further extend our proposed framework to support the implementation of AI-based security mechanisms, such as anomaly detection, behavioral analysis, and adaptive access control, each step in the risk framework. These AI-driven security measures can dynamically adapt to changing environments and user behavior, providing a higher level of protection for IoT devices during the assessment, identification, and control phases of our risk management framework.

Author Contributions: For research articles with several authors, a short paragraph specifying their individual contributions must be provided. The following statements should be used Conceptualization, E.G. and S.R.; methodology, E.G.; software, E.G.; validation, E.G. and S.R..; formal analysis, E.G.; investigation, E.G.; resources, E.G.; writing—original draft preparation, E.G.; writing—review and editing, E.G. and S.R.; visualization, E.G. and S.R.; supervision, S.R.; project administration, E.G. and S.R.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Acknowledgments: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Hernandez, B. Xiao and V. Tudor, "ERAIA - Enabling Intelligence Data Pipelines for IoT-based Application Systems," *2020 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, Austin, TX, USA, 2020, pp. 1-9, doi: 10.1109/PerCom45495.2020.9127385.
2. Alkali, Yusuf and Routray, Indira and Whig, Pawan, Study of various methods for reliable, efficient and Secured IoT using Artificial Intelligence (January 28, 2022). Proceedings of the International Conference on Innovative Computing & Communication (ICICC) 2022, Available at SSRN: https://ssrn.com/abstract=4020364 or http://dx.doi.org/10.2139/ssrn.4020364.
3. A. Srivastava and U. Jain, "Securing the Future of IoT: A Comprehensive Framework for Real-Time Attack Detection and Mitigation in IoT Networks," *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Delhi, India, 2023, pp. 1-6, doi: 10.1109/ICCCNT56998.2023.10307306.
4. Choo, K.-K. R., Gai, K., Chiaraviglio, L., & Yang, Q. (2021). A multidisciplinary approach to Internet of Things (IoT) cybersecurity and risk management. *Computers & Security*, *102*, 102136. https://doi.org/10.1016/j.cose.2020.102136.
5. G. Gómez, E. Espina, J. Armas-Aguirre and J. M. M. Molina, "Cybersecurity architecture functional model for cyber risk reduction in IoT based wearable devices," *2021 Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI)*, Bogotá, Colombia, 2021, pp. 1-4, doi: 10.1109/CONIITI53815.2021.9619624.
6. Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*, *2020*(1). https://doi.org/10.1186/s13635-020-00111-0.
7. K. M. Edhrabooh and A. I. Al-Alawi, "AI and ML Applications in Supply Chain Management Field: A Systematic Literature Review," *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*, Manama, Bahrain, 2024, pp. 202-206, doi: 10.1109/ICETSIS61505.2024.10459449.
8. Kuzlu, M., Fair, C., & Guler, O. (2021). Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of Things*, *1*(1), https://doi.org/10.1007/s43926-020-00001-4.
9. L. Wang, "Application of Machine Learning in Risk Assessment of Big Data IOT Credit Financial Management of Operator," *2022 2nd International Conference on Networking Systems of AI (INSAI)*, Shanghai, China, 2022, pp. 228-232, doi: 10.1109/INSAI56792.2022.00050.
10. M. S. Z. Almahairah, S. Goswami, P. N. Karri, I. M. Krishna, M. Aarif and G. Manoharan, "Application of Internet of Things and Big Data in Improving Supply Chain Financial Risk Management System," *2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, Gautam Buddha Nagar, India, 2023, pp. 276-280, doi: 10.1109/UPCON59197.2023.10434460.
11. M. Waqdan, H. Louafi and M. Mouhoub, "An IoT Security Risk Assessment Framework for Healthcare Environment," *2023 International Symposium on Networks, Computers and Communications (ISNCC)*, Doha, Qatar, 2023, pp. 01-08, doi: 10.1109/ISNCC58260.2023.10324002.
12. NIST. (2018). Risk management framework for information systems and organizations: *Risk Management Framework for Information Systems and Organizations*, *2*(Revision 2). https://doi.org/10.6028/nist.sp.800-37r2.
13. 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," in *IEEE Access*, vol. 9, pp. 121975-121995, 2021, doi: 10.1109/ACCESS.2021.3109886.
14. P. G. Thirumagal, S. Vaddepalli, T. Das, S. Das, S. Madem and P. S. Immaculate, "AI-Enhanced IoT Data Analytics for Risk Management in Banking Operations," *2024 5th International Conference on Recent Trends in Computer Science and Technology (ICRTCST)*, Jamshedpur, India, 2024, pp. 177-181, doi: 10.1109/ICRTCST61793.2024.10578533.
15. S. Muammar, D. Shehada and W. Mansoor, "Digital Risk Assessment Framework for Individuals: Analysis and Recommendations," in *IEEE Access*, vol. 11, pp. 85561-85570, 2023, doi: 10.1109/ACCESS.2023.3293062.

 doi:10.20944/preprints202410.1083.v1

16. S. Surya, D. Bhuva, A. Bhuva, S. S. Chavan, D. K. Basha and S. Chattopadhyay, "Implementation of Internet of Things (IoT) framework for Governing Modern Cyber Attacks in Computer Network," *2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG)*, Indore, India, 2023, pp. 1-5, doi: 10.1109/ICTBIG59752.2023.10456364.