International Journal of Service and Knowledge Management
International Institute of Applied Informatics
2021, Vol. 5, No. 2, 57 – 69

Multifaceted Risk Assessment and Risk Countermeasure Portfolio for Internet of Things

Sonam Wangyal [*], Tenzin Dechen [*], Shigeaki Tanimoto [*],
Hiroyuki Sato [†], Atsushi Kanai [‡]

Abstract

As global businesses now extensively depend on data, Internet of Things (IoT) sensors have become the primary source of real-time data that enable the digital transformation. According to Bain's Insight, the IoT market will grow to more than $520 billion by 2021. The technology has already been adopted for a wide array of use cases, but due to the ever-expanding threat landscape, many customers have indicated that security remains the primary barrier when it comes to their acceptance of IoT. The current security risk management methodologies focus mostly on the cyber view. In this work, we identify 28 risk factors extracted using the risk breakdown structure method and expand this traditional view to include others (physical, psychological) that are critical to business operations. Next, we proposed risk countermeasures for all the extracted risk factors using a risk matrix method. Further, from a practical point of view, a portfolio of the proposed risk countermeasures was clearly indicated to enable the gradual introduction of risk countermeasures. Finally, the effectiveness of the risk countermeasures was quantitatively evaluated on the basis of the risk values. Our findings help clarify IoT security and its relation to non-cyber risks for proper implementation of IoT systems.

Keywords: Internet of Things, risk breakdown structure, non-cyber aspect, psychological aspect

1 Introduction

As the current global business scene is now extensively data-driven, IoT systems have become a primary source of data that facilitate smarter systems and better decision analytics. IoT is now affecting almost every industry, from improving agricultural farm yields to providing predictive maintenance for aircraft engines. Particularly in Japan, IoT plays a key

[*] Faculty of Social System Science, Chiba Institute of Technology, Chiba, Japan
[†] Information Technology Center, The University of Tokyo, Tokyo, Japan
[‡] Faculty of Science and Engineering, Hosei University, Tokyo, Japan

role in achieving a super-smart society (Society 5.0) that makes people's lives more comfortable and sustainable [1].

According to Bain's Insight, the combined market for the Internet of Things will more than double by 2021, with a market size of $520 billion [2]. Although IoT technology has been adopted for a wide array of use cases such as smart grids, healthcare, smart homes, connected cars, and smart cities, among others, many customers still feel that security remains the primary barrier when it comes to their acceptance of IoT due to the ever-expanding threat landscape. Around 84% of IoT adopters have experienced a security breach [3]. These considerations highlight the importance of fully understanding the associated risks and determining how to enforce a security policy if we want to take full advantage of IoT systems.

In general, devices in IoT systems are both ubiquitous and inexpensive. This brings new risks that do not exist in the traditionally connected computer network. Indeed, devices in IoT systems are highly resource-constrained in terms of computing capacity, memory, and energy use. The sheer volume of devices and the complexity of the systems makes the existing risk assessment methodologies inapplicable. Existing risk assessment methodologies such as the National Institute of Standards and Technology (NIST) SP800-30 [4] and the Operational Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [5] mostly focus on the cyber view. We argue that IoT risk assessment should extend the view of traditional methods to include non-cyber views such as physical and psychological ones, which are critical to business operations. In short, we feel that the current assessment of non-cyber aspects is inadequate.

In this paper, using the risk breakdown structure [6], we extract both cyber and non-cyber risks and use them to clarify IoT security and its relation to non-cyber risks for proper implementation of IoT systems. As stated above, security risk management methodologies for IoT focus primarily on the cyber perspective. In contrast, this paper adds non-cyber aspects (physical and psychological) that are essential for real operations. In this study, we first comprehensively extracted the risk factors of IoT from the perspective of cyber and non-cyber aspects using the risk breakdown structure method. Next, we proposed risk measures for all the extracted risk factors using a risk matrix method. Further, from a practical point of view, a portfolio of the proposed risk measures was clearly indicated to enable the gradual introduction of risk measures. Finally, we quantitatively evaluated the effectiveness of the risk measures using a risk values method. Our findings help clarify IoT security and its relation to non-cyber risks for proper implementation of IoT systems.

2 Current Status and Issues

2.1 Explosion of IoT

IoT is one of several technologies that will change the course of people's lives. When the physical and cyber worlds are intertwined to produce a revolutionary change, it affects every part of our life and how we interact with physical systems. With the recent explosive growth of IoT systems, the IDC predicts there will be 41.6 billion connected devices generating 79.4 zettabytes (ZB) of data by 2025 [7].

These connected devices are used in various application domains ranging from the industrial field to consumer electronics. In terms of industrial applications, IoT is bringing about the Fourth Industrial Revolution, where industrial IoT is used to facilitate automation and predictive analytics. Many governments have also jumped on board and started implementing

Industrial IoT guidelines. Similarly, many businesses have made strategic alignments to exploit the rapid growth of IoT by transitioning from legacy systems to a complete IoT solution.

2.2 Security of IoT

As IoT moves towards the core business strategy, integrating new security solutions is imperative. Businesses also need to consider the potential risks of IoT-based business models, such as disruption to information flow, theft of sensitive information, damage to critical information, and even loss of life. Considering the array of use cases and the resource-constrained nature of IoT devices, the security of these devices is critical for the success of the intended use case. Bain's customer survey [2] shows that security is still the primary barrier to the adoption of IoT for analytic solutions. Therefore, identifying potential risks and vulnerabilities should be prioritized as a critical business objective.

2.3 Current Risk Assessment

Current risk assessment methods have huge limitations when it comes to applying them to ever-changing IoT systems [8]. Most of the existing risk assessments cannot adapt to the scalability requirements of IoT. Moreover, they are usually confined to a specific boundary perimeter, whereas the boundary perimeter of an IoT system's network is constantly changing depending on the situation. Nurse et al. [9] raised a strong argument about the need for new risk assessment methods that address the complexity of the new security landscape. They also showed where the current risk assessment methods fail when applied to IoT systems, as most of those methodologies were established prior to the widespread use of dynamic IoT systems. In this paper, on the basis of the present situation, we analyze the risks of IoT from multiple viewpoints.

3 Risk Assessment of IoT

Risk assessment is one of the most crucial steps in any risk management plan. The long-term success of a project inherently depends upon how well risk is managed by anticipating risks and taking measures to avoid them ahead of time. In general, risk assessment in project management is conducted in three steps: (1) risk specification, (2) risk analysis, and (3) risk evaluation [6].

3.1 Risk Specifications of IoT

3.1.1 Extraction Results of IoT Risk Factors

We systematically extracted the risk factors of IoT through a literature survey from multiple viewpoints with the Risk Breakdown Structure (RBS) method [10], [11]. Since IoT sensors and actuators closely interact with the physical environment, the risk factors are divided into Cyber, Physical, and Psychological categories as the first hierarchy of RBS. Next, Cyber Risk factors are classified into Communication, Hardware, and Software, where the hardware risk factors refer to intrinsic risks associated with the IoT device itself. Physical factors refer to the actual physical location of IoT devices and are classified into Location of Things and Location of Data. Psychological factors are usually overlooked by most industries, but in IoT systems, it is crucial that as many of the systems as possible be highly interconnected with people and their personal data, so Psychological factors are also considered as the first hierarchy. From these, we extracted 28 risk factors, as shown in Table 1.

Table 1: Extraction results.

No	First Level	Second Level	Risk Factors	Contents
1	1. Cyber	1.1 Communication	1.1.1 Lack of fog security policy	Lack of standard practices for fog computing compared to cloud security
2			1.1.2 Quality of services constraint	Latency and throughput constraint from IoT device to cloud
3			1.1.3 Heterogeneity of communication protocol	Lack of standard protocol and agreement on best practices
4			1.1.4 Lack of efficient encryption algorithm	Most of the standard secure encryption algorithms are resource-intensive
5			1.1.5 Lack of efficient network management	Lack of standard practices for managing and configurating IoT scale network
6		1.2 Hardware	1.2.1 Low capacity and memory	Ubiquitous devices with Low memory and capacity
7			1.2.2 Low energy constraint	Need to use energy efficiently without constant power supply
8			1.2.3 Lack of standard practices	Lack of standard practices for manufacturing of the products
9			1.2.4 Compromise gateway	Attack on gateway will cripple the whole IoT system
10		1.3 Software	1.3.1 Vulnerability in middleware	A vulnerable legacy system that is connected to IoT via middleware
11			1.3.2 Vulnerability in API	Poorly secured application program interface (API)
12			1.3.3 Remote updates and patches	Inability to easily update and send security patches
13			1.3.4 Malicious code injection	Malicious code injection leads to compromised device part of botnet
14	2. Physical	2.1 Things Location	2.1.1 Sensor data manipulation	Physical manipulation of sensor data
15			2.1.2 Theft and sabotage	Theft of IoT devices or intentionally sabotaging the function of IoT system
16			2.1.3 Sensitivity of location	Location and use of IoT in life critical environment
17			2.1.4 Breakage and out-of-services	Identifying and serving malfunctioning IoT devices
18			2.1.5 Management of things	Physical management and securing of IoT devices
19			2.1.6 Mobility	Constant of movement of IoT devices as in vehicular IoT system
20			2.1.7 Safety in industries	Risk of safety in industries by using IoT in a safety-critical environment
21		2.2 Data Location	2.2.1 Natural disaster	Risk of cloud data center under natural disaster
22			2.2.2 Theft, sabotage, and manipulation	Theft, sabotage and manipulation of data by services provider
23			2.2.3 Cloud and fog data center location	European Union's GDPR, and other laws that restrict data's location
24	3. Psychological	3.1 Privacy violation		Lack of standard practices for managing individual privacy
25		3.2 Security fatigue		Risk of being overwhelmed by constantly changing security practices
26		3.3 Lack of education		Lack of education regarding the security of IoT system
27		3.4 Unauthorized redistribution of confidential information		Redistribution of confidential information to an intruder
28		3.5 Social engineering		Intruder exploiting the psychology of people working within IoT system

3.1.2 Tendency of risk specifications

A few of the 28 extracted risk factors in Table 1 have a high tendency to result in a catastrophic domino effect. Therefore, identifying the major risk factors will help in terms of prioritizing the risks and formulating countermeasures for each. Below are the results of identifying the major risk factors for each of the categories shown in Table 1.

(1) Cyber category

The cyber risk specification is sub divided in Communication, Hardware, and Software. Many of the extracted risks resemble the risks of traditional computer systems but with a few critical differences. Consider the risk "1.1.3 Heterogeneity" of the communication protocol. While traditional computer systems have only a few communication protocols, which are typically limited, IoT differs in that there are various competing communication protocols with very limited governance and standardization. Consequently, managing the communication links between various protocols is a cumbersome task that can also disrupt the business continuity.

Other notable risks are "1.2.1 Low capacity and memory" and "1.2.4 Compromised gateway". IoT devices are ubiquitous while also featuring limited computation and memory capacity. With a limited configuration like this, there is certain constraint when using traditional security mechanisms, where performance is proportional to computational capacity. This is problematic in businesses that use IoT because they require a more energy-efficient security mechanism, the level of which depends on the use case. In addition, the IoT gateway plays an important role in the Cloud-Fog-Edge architecture. Since it's a central component in building robust IoT systems and for delivering computational power in edge-computing scenarios, problems with the compromise gateway may cripple the whole IoT system.

(2) Physical category

The physical category corresponds to the physical location of IoT devices and its data. IoT devices are the prime source of real-time data, which are the foundation for many emerging technologies. In the physical category, there are three main risks. The first, "2.1.6 Mobility", corresponds to risks associated with IoT in the changing physical context. Unlike traditional computer systems, IoT devices are used heavily in mobile environments where the security context changes from one hop to the next. Without the appropriate countermeasure in place, this changing physical context will lead to other risks. "2.1.3 Sensitivity of location" corresponds to risks associated with the use of IoT devices in daily life and in mission critical environments. Lastly, we have "2.1.1 Sensor data manipulation", which corresponds to the manipulation of the physical environment to induce unintended actuation. The severity of each of these risks depends on the use case and the business objective.

(3) Psychological category

Many studies have suggested that users are the weak link in information security, but psychological factors are typically overlooked by most risk assessment methods. It's crucial to consider this aspect because IoT devices interact closely with both physical and social structures. In the psychological category, there are three main risks. The first is "3.1 Privacy violation", which is important because IoT devices emit and collect a lot of sensitive private data, the leakage and exploitation of which may have everlasting psychological consequences. Moreover, with the global movement toward stricter privacy regulation, IoT devices need to be manufactured by implementing a privacy-by-design approach. The next is "3.2 Security fatigue", which relates to the exponential changes in security and the threat landscape that may overwhelm users what with the constantly evolving security policies and guidelines. Security fatigue reduces the overall security of an IoT system because users are reluctant to take the proper steps for ensuring computer security. The final risk is "3.3 Lack of education and awareness", which is important because being aware of surrounding threats and keeping informed is a fundamental step to mitigating risks.

3.2 Risk Analysis

The analysis of risk can be broadly divided into two categories: qualitative analysis and quantitative analysis. Qualitative risk analysis is essentially an industry standard to prioritize risks and identify which ones require further quantitative analysis. In this paper, we use the Risk Matrix method based on the qualitative point of view. The Risk Matrix method classifies risk into four categories: (1) Risk Avoidance, (2) Risk Mitigation, (3) Risk Transference, and (4) Risk Acceptance. On the basis of the likelihood of the risk occurrence and corresponding risk impact, extracted risks are classified into one of these four categories. Each category acts as a guideline to draw up the corresponding countermeasures [6]. We analyzed the extracted risks listed in Table 1 in detail using the template shown in Fig. 1. The analysis results are shown in Table 2.

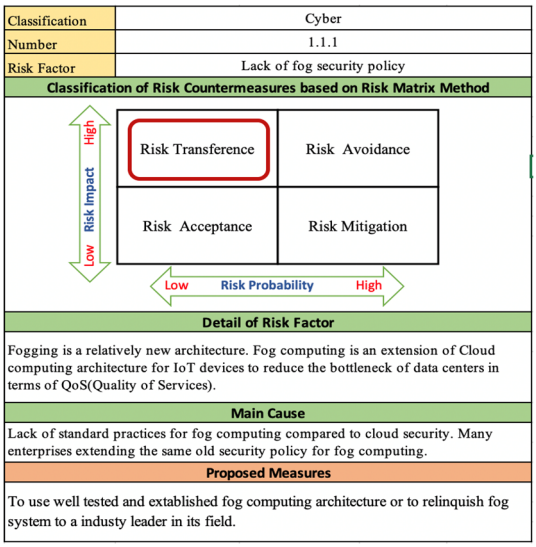

Figure 1: Example of risk analysis result based on template.

Table 2: Risk analysis results.

No	Risk Factors	Contents	Risk Probability	Risk Impact	Risk Classification
1	1.1.1 Lack of fog security policy	Lack of standard practices for fog computing compared to cloud security	Low	High	Risk Transfer
2	1.1.2 Quality of services constraint	Latency and throughput constraint from IoT device to cloud	High	High	Risk Avoidance
3	1.1.3 Heterogeneity of communication protocol	Lack of standard protocol and agreement on best practices	High	Low	Risk Mitigation
4	1.1.4 Lack of efficient encryption algorithm	Most of the standard secure encryption algorithms are resource-intensive	High	High	Risk Avoidance
5	1.1.5 Lack of efficient network management	Lack of standard practices for managing and configurating IoT scale network	Low	High	Risk Avoidance
6	1.2.1 Low capacity and memory	Ubiquitous devices with Low memory and capacity	High	Low	Risk Mitigation
7	1.2.2 Low energy constraint	Need to use energy efficiently without constant power supply	High	Low	Risk Mitigation
8	1.2.3 Lack of standard practices	Lack of standard practices for manufacturing of the products	High	Low	Risk Mitigation
9	1.2.4 Compromise gateway	Attack on gateway will cripple the whole IoT system	Low	High	Risk Transfer
10	1.3.1 Vulnerability in middleware	A vulnerable legacy system that is connected to IoT via middleware	Low	High	Risk Transfer
11	1.3.2 Vulnerability in API	Poorly secured application program interface (API)	Low	High	Risk Transfer
12	1.3.3 Remote updates and patches	Inability to easily update and send security patches	Low	High	Risk Transfer
13	1.3.4 Malicious code injection	Malicious code injection leads to compromised device part of botnet	Low	High	Risk Transfer
14	2.1.1 Sensor data manipulation	Physical manipulation of sensor data	Low	High	Risk Transfer
15	2.1.2 Theft and sabotage	Theft of IoT devices or intentionally sabotaging the function of IoT system	High	High	Risk Avoidance
16	2.1.3 Sensitivity of location	Location and use of IoT in life critical environment	Low	High	Risk Transfer
17	2.1.4 Breakage and out-of-services	Identifying and serving malfunctioning IoT devices	Low	Low	Risk Acceptance
18	2.1.5 Management of things	Physical management and securing of IoT devices	High	Low	Risk Mitigation
19	2.1.6 Mobility	Constant of movement of IoT devices as in vehicular IoT system	High	High	Risk Avoidance
20	2.1.7 Safety in industries	Risk of safety in industries by using IoT in a safety-critical environment	Low	High	Risk Transfer
21	2.2.1 Natural disaster	Risk of cloud data center under natural disaster	Low	Low	Risk Acceptance
22	2.2.2 Theft, sabotage, and manipulation	Theft, sabotage and manipulation of data by services provider	Low	High	Risk Transfer
23	2.2.3 Cloud and fog data center location	European Union's GDPR, and other laws that restrict data's location	Low	High	Risk Transfer
24	3.1 Privacy violation	Lack of standard practices for managing individual privacy	High	High	Risk Avoidance
25	3.2 Security fatigue	Risk of being overwhelmed by constantly changing security practices	Low	High	Risk Transfer
26	3.3 Lack of education	Lack of education regarding the security of IoT system	High	High	Risk Avoidance
27	3.4 Unauthorized redistribution of confidential information	Redistribution of confidential information to an intruder	Low	High	Risk Transfer
28	3.5 Social engineering	Intruder exploiting the psychology of people working within IoT system	High	High	Risk Avoidance

The risk categories and countermeasures depend highly on the type of use case and the overall objective of the company. In this section, we detail the risk management proposals for each classification using the template shown in Fig. 1. In general, it makes sense to implement risk countermeasures in stages in view of their cost-effectiveness. We therefore propose a portfolio (priority) of risk countermeasures based on the Computer Security Incident Response Team (CSIRT) risk countermeasure classification [12]–[13]. The CSIRT classifies risk countermeasures into three categories: Proactive Service, Reactive Service, and Security Quality Management Service. Proactive Service and Security Quality Management Service are classified as pre-countermeasures and are given a higher priority in the introduction of countermeasures than Reactive Service. Our proposed portfolio of risk countermeasures clearly identifies Proactive Service, Security Quality Management Service, and Reactive Service for each countermeasure, which allows for a step-by-step introduction of the measures.

3.2.1 Risk Transference

As shown in Table 3, many risks in this category pertain to the lack of security policies and standards. IoT is an evolving technology with an ever-expanding security landscape, and enterprises need to be ahead of these changes.

Table 3: Countermeasures for Risk Transference (13 risk factors)

No	Risk Factor	Countermeasure	Pre	Post	Quality
1	1.1.1 Lack of fog security policy	To use well tested and established fog computing architecture or to relinquish fog system to an industry leader in its field.			○
9	1.2.4 Compromise gateway	Choosing the right gateway device for your business need and always change the default security configuration.	○		
10	1.3.1 Vulnerability in middleware	Use of industry-standard middleware which can efficiently interface between two systems.			○
11	1.3.2 Vulnerability in API	Rigorous testing of API with proper authentication level. Even after the launch, continuous monitoring and improvement of API. Initiating a bug bounty program will also secure your API.			○
12	1.3.3 Remote updates and patches	Enabling remote updates and patches via a secure channel with a strong authentication mechanism. updates and patches using context-aware communication can be also achieved in vehicular IoT systems.		○	
13	1.3.4 Malicious code injection	Utilizing secure input and output handling and rigorous testing for user input. Initiating a bug bounty program will also secure your application.	○		
14	2.1.1 Sensor data manipulation	Detection of inconsistency sensor data using historical data. Deployment of physical intruder detection and monitoring system at the site.		○	
16	2.1.3 Sensitivity of location	Elevation of security compliance with respect to the sensitivity of the location. Test for leakage information to reduce side-channel attacks.			○
20	2.1.7 Safety in industries	Enforcement of strict security policy in a critical environment. Also, create a redundant or backup provision if they is IoT device failure.		○	
22	2.2.2 Theft, sabotage, and manipulation	The company should get a third party to review its compliance criteria satisfied before the contract and compliance auditing cloud or fog service providers after it.	○		
23	2.2.3 Cloud and fog data center location	Edge computing with customer private data is encrypted and stored locally on the device. Creation of data portfolio on private data and regular data.			○
25	3.2 Security fatigue	Limit the number of security decisions users need to make. Make it simple for users to choose the right security action. if possible, use of passwordless authentication mechanism.	○		
27	3.4 Unauthorized redistribution of confidential information	Use of multi-factor authentication to protect from intruder. For better use of passwordless authentication mechanism. Ex. FIDO Alliance	○		

Pre: Proactive Service. Post: Reactive Service. Quality: Security Quality Management Service.

One way to address this challenge is to adopt a well-tested security policy or insurance

with the help of a third party. In addition, reviewing and auditing the enterprise security should be done in a timely fashion. The countermeasure against Risk Transference is to adopt an industry standard security policy.

Next, we present the Risk Transference portfolio. As shown in Table 3, out of the 13 risk factors, Proactive Service and Security Quality Management Service, which are pre-emptive measures, accounted for ten, whereas Reactive Service, which refers to post-measurements, totaled three. From the above, we can see that about 80% of the total measures should be prioritized.

3.2.2 Risk Mitigation

Countermeasures for the risks classified as Risk Mitigation are shown in Table 4. These risks involve aligning the IoT system and protocol to business needs. Many enterprises face a dilemma due to the number of competing protocols in IoT systems and the wide array of device choices. Therefore, it is imperative to adopt the right protocol that has widespread acceptance for better support in the future and the right IoT device for a particular security level.

Next, we present the Risk Mitigation portfolio. As shown in Table 4, out of the five risk factors, Proactive Service and Security Quality Management Service, which are precautionary measures, totaled four, while Reactive Service, which refers to post-cautionary measures, totaled 1. From the above, we can see that 80% of the total measures should be prioritized.

Table 4: Countermeasures for Risk Mitigation (5 risk factors)

Pre: Proactive Service. Post: Reactive Service. Quality: Security Quality Management Service.

No	Risk Factor	Countermeasure	Pre	Post	Quality
3	1.1.3 Heterogeneity of communication protocol	To mitigate, choose the right protocol for your business needs. Also choosing a protocol that has widespread acceptance for better support in the future.	○		
6	1.2.1 Low capacity and memory	The business need for computation and memory capacity differ vastly on the use case of IoT devices. Choosing the right IoT device for a particular security level is crucial.	○		
7	1.2.2 Low energy constraint	Efficient power management in IoT system is crucial for long-lasting IoT devices. Use of energy harvesting mechanism in IoT devices. Ex. EnOcean Easyfit			○
8	1.2.3 Lack of standard practices	Use of open source and industry-wide accepted IoT devices. Elevating the manufacture's security level to match your business need.	○		
18	2.1.5 Management of things	Recently many new device management proposed, which are independent of the status of the application provider. Ex. Open Mobile Alliance’s Device Management (OMA DM).		○	

3.2.3 Risk Avoidance

Countermeasures for the risks classified as Risk Avoidance are shown in Table 5. Since many of these risks are closely tied to business operations, it is crucial that the enterprises reduce the likelihood of these risks ever happening. This can be achieved by implementing a “security first” design when adopting any IoT technology. Moreover, as IoT devices are the primary source of data for many emerging technologies, following governmental laws and regulations (e.g., those of the GDPR) regarding private data is imperative.

Next, we present the Risk Avoidance portfolio. As shown in Table 5, out of the eight risk factors, there were a total of eight Proactive Service and Security Quality Management Service, which are pre-measures, and no Reactive Service, which refers to post-measures. Here, we can conclude that all measures are important.

Table 5: Countermeasures for Risk Avoidance (8 risk factors).

No	Risk Factor	Countermeasure	Pre	Post	Quality
2	1.1.2 Quality of services constraint	To bring analytics closer to IoT devices by using edge analytics from cloud service providers. Implementation of fog computing.			○
4	1.1.4 Lack of efficient encryption algorithm	Use of ECC(Elliptic-Curve Cryptography) based standard algorithm which provides similar security levels with shorter operand size and more efficient implementations. In the case of vehicular IoT, context-aware security implementation will increase the overall performance.			○
5	1.1.5 Lack of efficient network management	Overhauling an existing network management system. Network devices using software-Defined Networks(SDN) collect configures data from sensors, thus creating the context of managing a network.	○		
15	2.1.2 Theft and sabotage	Deployment of physical intruder detection and monitoring system at the site.	○		
19	2.1.6 Mobility	Context-awareness plays a very important role in a dynamic environment. Context-aware information will bring more values and enhance the decision process in IoT applications and services.	○		
24	3.1 Privacy violation	Enforcing GDPR(General Data Protection Regulation) regulation. Regulation of privacy and manufacturers to initiate the implementation of privacy by design.	○		
26	3.3 Lack of education	Educate the user regarding IoT security. Ease users by making security enforcement simpler and natural. Use of passwordless authentication mechanism. Ex. FIDO Alliance			○
28	3.5 Social engineering	Training-based defenses which train the user to defend himself. Use of passwordless authentication mechanism.			○

Pre: Proactive Service. Post: Reactive Service, Quality: Security Quality Management Service

3.2.4 Risk Acceptance

Countermeasures for the risks classified as Risk Acceptance are shown in Table 6. IoT devices are both ubiquitous and inexpensive, so the risks in this category tend to be based on external dynamics. Countermeasures include creating a contingency plan for when nodes go down and formulating a disaster recovery plan with the cloud service provider.

Next, we present the Risk Acceptance portfolio. As shown in Table 6, out of the two risk factors, there were a total of two Proactive Services and Security Quality Management Services, which are pre-measures, and no Reactive Service, which refers to post-measures. Here, we can conclude that all measures are important.

Table 6: Countermeasures for Risk Acceptance (2 risk factors).

No	Risk Factor	Countermeasure	Pre	Post	Quality
17	2.1.4 Breakage and out-of-services	Implementation of mesh IoT network can bring the capability of self-healing and self-configuration of IoT nodes. It removes the reliance on single node communication.	○		
21	2.2.1 Natural disaster	General many cloud service providers have their own Disaster Recovery Plan. Chose a personal cloud or fog service vendor compatible with your business need.	○		

Pre: Proactive Service. Post: Reactive Service. Quality: Security Quality Management Service.

3.3 Risk Evaluation

In this section, we evaluate the proposed countermeasures through a quantification of the extracted risks. We use the risk formula of the Information Security Management System (ISMS) to approximate the risk value on the basis of previous qualitative results [14]–[16].

3.3.1 Risk Formula

Corresponding risk values are quantified using Eq. (1), which is commonly used in the field of ISMS.

$$\begin{aligned} \textit{Risk value} = {} & \textit{value of asset} \times \textit{value of threat} \\ & \times \textit{value of vulnerability} \end{aligned} \tag{1}$$

Generally, the value of elements on the right-hand side of the equation is very complex to derive. To simplify, we use an approximation method.

a) Approximation of Asset Value

The asset value of Eq. (1) is approximated in terms of the risk impact in the risk matrix, as shown in Fig. 2. We assume that the amount of risk impact approximately reflects the amount of damage to assets. The degree of risk is determined from 1 (Low) to 5 (High) [8]–[10]. For further simplicity, we map these values to the risk impact of the risk matrix and divide them into two. The higher of the two divisions is approximated to the maximum risk impact (risk value = 5) and the lower of the two to the minimum (risk value = 1).

b) Approximation of Threat Value

Similarly, the value of threat in Eq. (1) is approximated in terms of the risk probability in the risk matrix. The risk probability is defined to range from 1 (Low) to 3 (High). These values are mapped to the risk probability of the risk matrix in Fig. 2. The same as above, the higher of the two divisions is approximated to the maximum risk probability (risk value = 3), and the lower to the minimum (risk value = 1).

c) Approximation of Value of Vulnerability

The value of vulnerability is defined on a three-level scale: 3 (High), 2 (Medium), and 1 (Low). These levels are approximated in accordance with the classification of the risk matrix in Fig. 2. Here, the four domains of the risk matrix are classified into three levels on the basis of the risk probability and risk impact. Risk Avoidance corresponds to level 3, where both risk probability and risk impact are high. Risk Transference and Risk Mitigation correspond to level 2, where either the risk probability or risk impact is high. Lastly, Risk Acceptance corresponds to level 1, where both metrics are low.

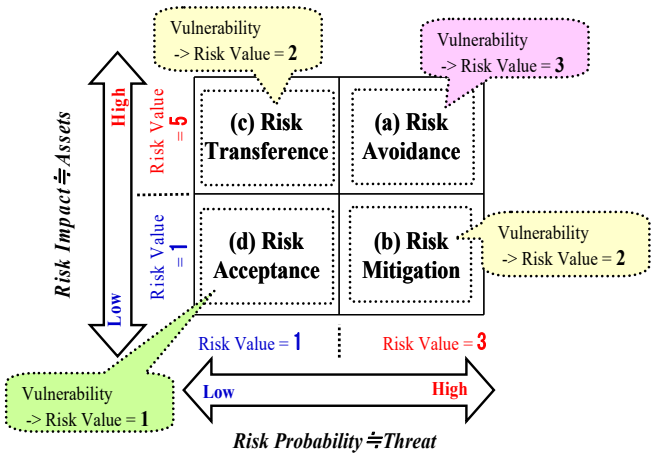

Figure 2: Risk value approximation of risk matrix [13].

3.3.2 Calculation of Risk Value

The risk values for all the extracted risks in Table 1 are calculated using Eq. (2). The risk values after performing the proposed countermeasures shown in Table 3, 4, 5, and 6 are also calculated with this equation.

$$Risk\ value = Risk\ impact \times Risk\ probability \times value\ of\ vulnerability \quad (2)$$

In general, implementing a countermeasure perfectly is not realistic. Thus, we assumed that all the vulnerabilities were decreased by one level after implementing the countermeasures. Tables 7 and 8 list the risk value results.

Table 7: Detailed evaluation results (before and after countermeasures).

No.	Risk Factors	Asset ≒ Risk Impact	Threat ≒ Risk Probability	Vulnerability ≒		Risk Value ≒	
				Before Countermeasure	After Countermeasure	Before Countermeasure	After Countermeasure
1	1.1.1 Lack of fog security policy	5	1	2	1	10	5
2	1.1.2 Quality of services constraint	5	3	3	2	45	30
3	1.1.3 Heterogeneity of communication protocol	1	3	2	1	6	3
4	1.1.4 Lack of efficient encryption algorithm	5	3	3	2	45	30
5	1.1.5 Lack of efficient network management	5	1	3	2	15	10
6	1.2.1 Low capacity and memory	1	3	2	1	6	3
7	1.2.2 Low energy constraint	1	3	2	1	6	3
8	1.2.3 Lack of standard practices	1	3	2	1	6	3
9	1.2.4 Compromise gateway	5	1	2	1	10	5
10	1.3.1 Vulnerability in middleware	5	1	2	1	10	5
11	1.3.2 Vulnerability in API	5	1	2	1	10	5
12	1.3.3 Remote updates and patches	5	1	2	1	10	5
13	1.3.4 Malicious code injection	5	1	2	1	10	5
14	2.1.1 Sensor data manipulation	5	1	2	1	10	5
15	2.1.2 Theft and sabotage	5	3	3	2	45	30
16	2.1.3 Sensitivity of location	5	1	2	1	10	5
17	2.1.4 Breakage and out-of-services	1	1	1	1	1	1
18	2.1.5 Management of things	1	3	2	1	6	3
19	2.1.6 Mobility	5	3	3	2	45	30
20	2.1.7 Safety in an industries	5	1	2	1	10	5
21	2.2.1 Natural disaster	1	1	1	1	1	1
22	2.2.2 Theft, sabotage, and manipulation	5	1	2	1	10	5
23	2.2.3 Cloud and fog data center location	5	1	2	1	10	5
24	3.1 Privacy violation	5	3	3	2	45	30
25	3.2 Security fatigue	5	1	2	1	10	5
26	3.3 Lack of education	5	3	3	2	45	30
27	3.4 Unauthorized redistribution of confidential information	5	1	2	1	10	5
28	3.5 Social engineering	5	3	3	2	45	30
Total						492	302

Table 8: Summary of evaluation results.

	(1) Before countermeasure	(1) After countermeasure
Total risk value	492	302
Risk reduction rate = (1) - (2) / (1)		≈ 0.39

3.3.3 Results of Evaluation

As shown in Table 8, the proposed countermeasures were able to reduce the risk rate by ≈ 39%. These results clearly demonstrate the quantitative effectiveness of the proposed countermeasures against the risks in an IoT system. Even though these were roughly estimated countermeasures for the extracted risks, a 39% reduction in the overall risk was achieved. Ideally, the proposed countermeasures should be able to reduce the risk level to close to 0. Investigation of such specific and effective countermeasures will be the focus of our future work.

4 Conclusion and Future Work

In this paper, we conducted a risk assessment of IoT to clarify the importance of cyber and non-cyber risks when it comes to proper implementation of IoT systems. A total of 28 risk factors were extracted with the RBS method and then analyzed and classified using the risk matrix method. Further, from a practical viewpoint, a portfolio of the proposed risk countermeasures was clearly indicated to enable the gradual introduction of risk countermeasures based on priority. Finally, risks were quantitatively evaluated before and after the implementation of countermeasures using the ISMS equation for a detailed risk assessment. The results clearly demonstrate the effectiveness of the proposed countermeasures with a roughly 39% reduction in risks related to IoT.

Although the risks were extracted from multiple viewpoints, this was still not exhaustive, and other views (e.g., the economic view, the operational view) will be examined in future work. We will also perform a more detailed assessment of the proposed countermeasures and examine new ones.

Acknowledgement

This work was supported by JSPS KAKENHI Grant Number JP 19H04098

References

[1] Government of Japan, The 5th Science and Technology Basic Plan, https://www8.cao.go.jp/cstp/english/society5_0/index.html

[2] Bain & Company, Unlocking Opportunities in the Internet of Things, https://www.bain.com/insights/unlocking-opportunities-in-the-internet-of-things/

[3] KPMG, Risk or reward: What lurks within your IoT?, https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/04/risk-or-reward-what-lurks-within-your-IoT.pdf

[4] NIST (National Institute of Standards and Technology) SP800-30 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[5] Operational critical threat, asset, and vulnerability evaluation (OCTAVE) https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_ 001_14885.pdf

[6] Projecet Management Institute, “A guide to the procjet management body of knowledge PMBOK Guide”, Sixth Edition, PMI, 2017

[7] International Data Corporation (IDC), “The Growth in Connected IoT Devices”, https://www.idc.com/getdoc.jsp?containerId=prUS45213219

[8] B. Ali, et al., “Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes”, Sensors 2018, 18, 817;
doi:10.3390/s18030817

[9] J. R.C Nurse, et al., "Security risk assessment in Internet of Things systems", IT professional (IT Pro), 2017, https://arxiv.org/ftp/arxiv/papers/1811/1811.03290.pdf

[10] D. E. Kouicem, et al., "Internet of Things Security: a top-down survey" Computer Networks, 2018, https://hal.archives-ouvertes.fr/hal-01780365/file/survey.pdf

[11] S. Wangyal, et al., A Study of Multi-viewpoint Risk Assessment of Internet of Things (IoT), 9th International Congress on Advanced Applied Informatics (AAI2020), pp.643-648, 2020

[12] J.Wiik, et al., Effectiveness of Proactive CSIRT Services, In 18th Annual FIRST Conference on Computer Security Incident Handling, 2006

[13] Y. Kenmoku, et al., A Study of Assurance Level in Information Security Management - LoA Introducing Method for CSIRT Deployment -, 6th International Conference on Project Management (ProMAC 2012), 2012

[14] ISMS Risk Assessment Manual v1.4, [Online]. Available from: https://www.igt.hscic.gov.uk/KnowledgeBaseNew/ISMS%20Risk%20Assessment%20Manual%20v1.4.pdf, 2020.7.19

[15] S. Tanimoto, et al., "A Study of Risk Assessment Quantification in Cloud Computing," 8th International Workshop on Advanced Distributed and Parallel Network Applications (ADPNA-2014), pp. 426-431, Sep., 2014

[16] JNSA, 2011 Investigation Report on Information Security Incidents , 2011, http://www.jnsa.org/result/incident/2011.html, (in Japanese)