International Journal of Service and Knowledge Management
International Institute of Applied Informatics
2022, Vol. 6, No. 2, IJSKM703

Risk Management and Risk Countermeasure Portfolio of Fog Computing for Improving IoT Security

Shigeaki Tanimoto [*], Mari Matsumoto [*], Teruo Endo [†], Hiroyuki Sato [‡], Atsushi Kanai [§]

Abstract

In the era of Digital Transformation (DX), as the Internet continues to become more and more widespread, various devices are now connected to it and the number of IoT devices is increasing. Data generated by IoT devices has traditionally been aggregated in the cloud and processed over time. However, there are two issues with using the cloud. The first is the response delay caused by the long distance between the IoT device and the cloud, and the second is the difficulty of implementing sufficient security measures on the IoT device side due to the limited resources of the IoT device. To address these issues, fog computing, which is positioned in the middle between IoT devices and the cloud, has been attracting attention as a new network component. However, the risks associated with the introduction of fog computing have not yet been fully investigated. In this study, we conducted a risk assessment of fog computing, which is newly established to promote the use of IoT devices, and identified 24 risk factors. The main countermeasures include the gradual introduction of connected IoT connection protocols and security policy matching. We also demonstrated the effectiveness of the proposed risk countermeasures by evaluating the risk values. Furthermore, from a practical viewpoint, the portfolio for the proposed risk countermeasures is mentioned to ensure a more practical risk assessment result. As a result, the proposed risk countermeasures for fog computing will contribute to the safe and secure use of IoT devices.

Keywords: Fog Computing, IoT Devices, Risk Breakdown Structure, Risk Matrix

1 Introduction

The Internet is rapidly expanding with the development of Digital Transformation (DX) and Industry 4.0, and the number of IoT devices is increasing at an explosive rate, as not only conventional devices such as PCs and smartphones but also home appliances, automobiles, and industrial devices are now connected to the Internet. The number of IoT devices was estimated to be 27.4 billion as of 2017 and increased to 40.3 billion by 2020 [1]. As IoT progresses, the previously closed network environment is shifting to an open network environment. As a result, the

[*] Chiba Institute of Technology, Chiba, Japan
[†] Osaka Shoin Women's University, Osaka, Japan
[‡] The University of Tokyo, Tokyo, Japan
[§] Hosei University, Tokyo, Japan

IoT devices are exposed to a variety of cyber threats such as Dos attacks. The data generated by the large amount of IoT devices has conventionally been aggregated in the cloud and processed in a time-consuming manner. However, when using the cloud, there are two issues: (1) the response delay caused by the long distance between the IoT device and the cloud, and (2) the limited resources (CPU, memory, disk, etc.) of the end IoT device, which makes it difficult for the IoT device to take sufficient security measures [2]. To address these issues, fog computing, which is positioned between IoT devices and the cloud, is attracting attention as a new network component [3]. Fog computing shows promise because it can be used instead of IoT devices at the network edge to solve the aforementioned issues. However, research on fog computing is still in its infancy, and in particular, the risks associated with its introduction have not yet been fully investigated.

This paper deals with the risk management of fog computing, which is positioned between IoT devices and cloud computing. Specifically, we identify, analyze, and evaluate the risk factors in fog computing with the objective of contributing to secure IoT networking. The features of IoT networking and fog computing are discussed in Section 2, and Section 3 details the risk management to improve IoT security based on these features. Section 4 presents the risk countermeasure portfolio we developed from the practical viewpoint. We conclude in Section 5 with a brief summary and mention of future work.

2 IoT Networking and Fog Computing

2.1 IoT Networking

In general, there are two types of architecture related to IoT: a two-layer structure in which the "edge layer," which includes IoT devices and gateways, is directly connected to the "cloud layer," as shown in Fig. 1(a), and a three-layer structure in which a "fog layer" is added in between the edge layer and cloud layer, as shown in Fig. 1(b) [4], [5]. As the number of IoT devices (things) continues to increase, the two-layer structure is facing problems such as increased communica-tion charges, increased network load, difficulty in ensuring security, and high latency. Therefore, the three-layer structure is now attracting attention.

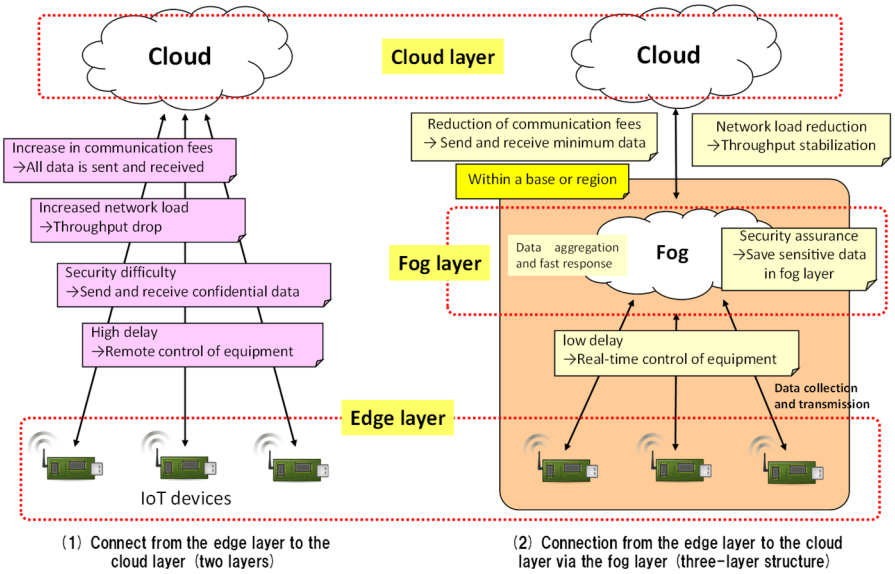

Figure 1: Overview of IoT network architecture [4].

2.2 Fog Computing

As shown in Fig. 1(b), fog computing is a distributed processing environment with middleware located close to the edge layer before data from the edge layer is sent to the cloud computing. It is derived from a concept proposed by Cisco Systems to deal with IoT, and the term "fog" is used because of its position in relation to the "cloud" [6]. The aim is to avoid concentrating the burden on the upper system and the cloud computing by processing a large amount of data from the edge layer before sending it to cloud computing. In addition, fog computing is located close to the edge layer and communicates with higher-level systems for processing, so it can respond speedily to changes in usage and environment [6].

2.3 Related Work

This subsection presents the main studies related to the security of fog computing. A survey paper by S. Khan et al. focused on the technical aspects of security in fog computing with reference to a number of prior works. Specifically, the paper describes techniques such as Advance Persistent Threat (APT), Denial of Service (DoS), and Data Breaches (DB). However, these techniques refer only to cyber threats [7]. I. Stojmenovic et al. investigated the main security problem of fog computing, which is that fog nodes require different levels of authentication. While they state that Public Key Infrastructure (PKI)-based technology can solve this problem, they do not mention issues related to the operational side of fog [8].

P. Zhang et al. investigated the security architecture of fog by conducted a survey of related security and trust research results. In particular, to improve the reliability of fog computing, they pointed out that interoperability is crucial because the nature of fog assumes the connection of a variety of devices. For this reason, the implementation of new interfaces and protocols for fog is considered to be important. [9]. S. Yi, Z. Qin, et al. focus on privacy issues such as data privacy, usage privacy, and location privacy, which is interesting because fog computing has a data-centric architecture. However, they mainly discuss theoretical considerations and do not spend much time on concrete countermeasures [10].

Yokota et al. identified six requirements in IoT security, all of which are prominent issues with regard to the connectivity from the edge layer to fog computing and cloud computing [11]. Among them, the following two are of particular importance in terms of security measures in fog computing.

1) Security measures should be possible even with devices that use a network (NW) connection system without security functions.
2) Measures should presuppose illegal equipment connections and malfunctions.

These issues are not limited to IoT devices, but it is important to consider the related issues from edge fog to cloud [5], [12], [13].

As mentioned above, research on fog computing is still in its early stages. Most of the studies have focused mainly on the architecture, and there has not been a sufficient examination of the operational side.

3 Risk Management in Fog Computing

Risk assessment is one of the most important steps in any risk management approach. 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 is conducted in three steps: (1) risk identification, (2) risk analysis, and (3) risk evaluation [6].

3.1 Risk Identifications of Risk Factors

In general, the most important and difficult part of risk management is the identification of risk factors. To identify these risk factors, we utilized the Risk Breakdown Structure (RBS) method, which is a typical method of risk management in project management [14].

As shown in Table 1, the first level is divided into private fog and public fog. Then, in the second layer, the risk factors are classified into the user side and the provider side, and in the third and subsequent layers, the user side is divided into the edge side (IoT device) and the cloud computing side, while the provider side is divided into system, operation, and others. In this way, we extracted 24 risk factors in detail from an exhaustive perspective [15].

Table 1: Risk specification of mobile workers.

No.	Level 1	Level 2	Level 3	Level 4/Risk Factor	Risk Details
1	1. Private fog computing	1.1 User side of fog computing	1.1.1 Edge side (IoT device)	1.1.1.1 Protocols that can be connected to fog computing	In a private environment, each device in the factory has its own protocol. Therefore, the fog computing side also needs to implement protocols corresponding to these protocols. This means there are cases where the fog computing side cannot be connected to the fog depending on the protocol support status of the fog computing side.
2				1.1.1.2 Cyber risk	The edge layer (IoT devices) has traditionally been used in a closed environment, and in many cases, security functions have not been sufficiently considered.
3				1.1.1.3 Fog computing failure	When the fog fails, communication with cloud computing becomes impossible.
4				1.1.1.4 Reliability of fog computing	If the security function of fog computing is weak, risks such as information leakage can be assumed.
5			1.1.2 Cloud computing side	1.1.2.1 Connecting to fog computing having different security policies	Fog computing connection requests at a lower level than the security policy of public cloud computing are also expected.
6				1.1.2.2 Fog computing failure	It is assumed that there is a risk that communication with the edge side (IoT devices) below the fog computing will not be possible in the case of fog computing failure.
7		1.2 Fog computing side	1.2.1 System side	1.2.1.1 Edge-side (IoT device) reliability	When the edge side (IoT device) with weak security is connected, the risk of virus infection or cyber attack from the edge side (IoT device) is assumed.
8				1.2.1.2 Reliability of cloud computing	Virus infections and cyber attacks from cloud computing with weak security are expected.
9				1.2.1.3 Implementation of multiple protocols	In general, the edge side of the private side (IoT device side) has many kinds of protocols (e.g., for factory equipment). Therefore, it is a risk that the fog computing side must also implement these protocols to be able to connect.
10			1.2.2 Operation side	1.2.2.1 Matching security policies	When connected to cloud computing with low security policies, it is expected to be subject to virus infection and cyber attacks.
11				1.2.2.2 Troubleshooting failures	The addition of fog computing to the three-layer structure makes troubleshooting failure more complex than with the conventional two-layer structure.
12	1. Public fog computing	2.1 User side of fog computing	2.1.1 Edge side (IoT device)	2.1.1.1 Limitations of fog computing connection protocols	Because of the public environment, there are many different protocols on the edge side (IoT devices). Fog computing may not be able to support these protocols.
13				2.1.1.2 Cyber risk	Since the system is connected to fog computing in the public environment, cyber risks such as information leakage and malware infection are assumed.
14				2.1.1.3 Fog computing failure	When fog computing fails, communication is not possible.
15				2.1.1.4 Reliability of fog computing	If the security function of fog computing is weak, risks such as information leakage from the fog can be assumed.
16			2.1.2 Cloud computing side	2.1.2.1 Connecting to fog computing with different security policies	Connection requests from fog computing at levels lower than the security policy of cloud computing are also expected.
17				2.1.2.2 Reliability of fog computing	It is assumed that when fog computing fails, communication to the edge side (IoT devices) may not be possible.
18		2.2 Fog computing side	2.2.1 System side	2.2.1.1 Edge-side (IoT device) reliability	If an edge (IoT device) with weak security is connected, the risk of virus infection or cyber attacks from the edge (IoT device) can be assumed.
19				2.2.1.2 Cyber risk	Risks such as virus infection from cloud computing and cyber attacks are expected.
20				2.2.1.3 Implementation of many protocols	If a connection request is received from the edge side (IoT device) using a protocol that is not implemented by fog computing, the connection will not be possible and serviceability will be degraded.
21			2.2.2 Operation side	2.2.2.1 Matching security policies	There is a possibility of virus infection and cyber attacks when connecting to cloud computing with a low security policy level.
22				2.2.2.2 Isolation in case of failure	Compared to the conventional two-layer configuration, the three-layer configuration makes it more complicated to isolate failures.
23			2.2.3 Miscellaneous	2.2.3.1 Billing	The billing model will become more complex due to the change from the traditional two-tier structure to a three-tier structure.
24				2.2.3.2 Installation site	Risk of installing fog computing in locations with low traffic on the edge side (IoT devices).

We then took the results of the extraction of risk factors, divided them into private fog and public fog, and clarified the characteristics of these two types of fog computing. First, the private fog side is characterized by the need to prepare new protocols and interfaces to connect existing

facilities to fog computing, assuming they are used in existing facilities such as factories. This is a risk factor from an economic point of view because the protocols of the existing facilities are diverse and not general-purpose; therefore, new protocols and interfaces must be prepared. In contrast, the public fog side is connected to the mobile edge, so there are risk factors related to the connection with a wide variety of protocols as well as billing and installation locations.

A common risk factor for both of these is the need to consider the existing cyber risks, as well as the need to isolate failures and match security policies due to the increasing number of components from the edge layer to fog computing to cloud computing.

3.2 Risk Analysis and Proposal of Countermeasures

In this section, we present the results of our risk analysis for the risk factors in fog computing shown in Table 1. The most common risk analysis methods are the decision tree method and the risk matrix method, where the former is based on a quantitative perspective and the latter on a qualitative perspective [16].

We opted to use the risk matrix method because we are dealing with security issues in fog computing when connecting to the edge and the cloud. As shown in Fig. 2, the risk matrix method classifies risks into four categories: Risk Avoidance, Risk Mitigation, Risk Acceptance, and Risk Transference, depending on the frequency of occurrence and the degree of impact, and then for-mulates countermeasures.

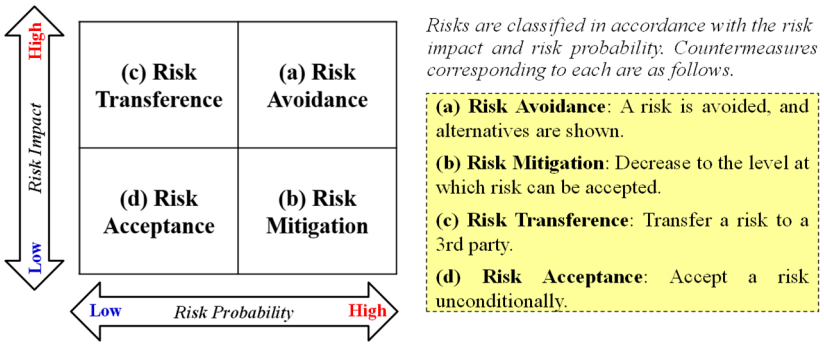

Figure 2: Risk matrix method.

The results of our analysis using the risk matrix method for the 24 risk factors shown in Table 1 are presented below.

3.2.1 Risk Transference

Table 2 shows the results where the corresponding measure is “Risk Transference”. The main tendency of these risk factors is the issue of isolation in the case of failure and the problem of matching the security policy during connection, since fog computing relays the network during edge and cloud computing.

As the main countermeasure to the first issue, it is necessary to implement new management functions such as mutual monitoring between elements for isolation in the case of failure. In this case, it is often difficult to provide network management functions at the edge of the IoT due to a lack of resources. Therefore, a centralized management by the fog computing side on the upper side of the network or a management by a third party is necessary.

Next is the problem of matching security policies at the time of connection, i.e., the problem of connecting between network elements with different security policies. For this, we establish a

security policy for fog computing beforehand, and publish the policy in the case of public fog. Furthermore, we implement a new security policy matching function between network elements. Thus, the idea of delegating to the security policy matching function is effective.

Table 2: Countermeasure characteristics of Risk Transference (16 risk factors).

No.	Risk Factor	Risk Probability	Risk Impact	Risk Classification	Risk Countermeasure
2	1.1.1.2 Cyber risk	L	H	Risk Transference	Install anti-virus software on the edge side (IoT devices). If it cannot be installed on the edge side, monitor the edge side (IoT device) by fog computing.
3	1.1.1.3 Fog computing failure	L	H	Risk Transference	If a fog computing fails, connect to a nearby fog computing. Important fog computing should be redundant.
4	1.1.1.4 Reliability of fog computing	L	H	Risk Transference	Publish a security policy for fog computing.
6	1.1.2.2 Fog computing failure	L	H	Risk Transference	If a fog computing fails, connect to a nearby fog computing. Important fog computing should be redundant.
7	1.2.1.1 Edge-side (IoT device) reliability	L	H	Risk Transference	Implementing anti-virus and other security software for fog computing.
8	1.2.1.2 Reliability of cloud computing	L	H	Risk Transference	Check the security policy of cloud computing. Implement anti-virus and other security software for fog computing as well.
10	1.2.2.1 Matching security policies	L	H	Risk Transference	Establish a security policy for fog computing. Connect to cloud computing that has the same or higher policy level.
11	1.2.2.2 Troubleshooting failures	L	H	Risk Transference	Establish a monitoring function that originates from fog computing.
12	2.1.1.1 Limitations of fog computing connection protocols	L	H	Risk Transference	Confirm the security policy of fog computing installed in a public environment.
14	2.1.1.3 Fog computing failure	L	H	Risk Transference	When fog computing in the public environment is not connected, it tries to connect with nearby fog computing.
15	2.1.1.4 Reliability of fog computing	L	H	Risk Transference	In the case of a public environment, implement a security policy matching function to connect to fog computing with the same security policy.
17	2.1.2.2 Reliability of fog computing	L	H	Risk Transference	In the case of a public environment, implement a security policy matching function to connect to fog computing with the same security policy.
19	2.2.1.2 Cyber risk	L	H	Risk Transference	Install anti-virus and other security software. Also, update the software periodically.
21	2.2.2.1 Matching security policies	L	H	Risk Transference	Establish a security policy for fog computing. Connect to cloud computing that has the same or higher policy level.
22	2.2.2.2 Isolation in case of failure	L	H	Risk Transference	Establish a monitoring function that originates from fog computing.
24	2.2.3.2 Installation site	L	H	Risk Transference	Plan in advance to predict the traffic on the edge side (IoT devices) that will be connected to the fog computing.

3.2.2 Risk Acceptance

Table 3 shows the results of the “Risk Acceptance” of the countermeasures. The main trend is that the edge side has a variety of protocols, including proprietary protocols. Therefore, when a connection request is made from the edge, if the protocol is not implemented by fog computing, the connection is not possible and the serviceability is degraded. To solve this problem, we set the priority of the edge protocols to be connected and introduce them in stages.

Table 3: Countermeasure characteristics of Risk Acceptance (4 risk factors).

No.	Risk Factor	Risk Probability	Risk Impact	Risk Classification	Risk Countermeasure
1	1.1.1.1 Protocols that can be connected to fog computing	L	L	Risk Acceptance	For use in private environments, connect with fog computing that supports edge-side (IoT device) protocols.
9	1.2.1.3 Implementation of multiple protocols	L	L	Risk Acceptance	Define the priority of the edge side (IoT devices) to be connected and introduce them in a step-by-step approach.
20	2.2.1.3 Implementation of multiple protocols	L	L	Risk Acceptance	Define the priority of the edge side (IoT devices) to be connected and introduce them in a step-by-step approach.
23	2.2.3.1 Billing	L	L	Risk Acceptance	Simplify the system by using a subscription-based billing system.

3.2.3 Risk Avoidance

Table 4 shows the results where the countermeasure is “Risk Avoidance”. Here, the risks are the reliability of the edge side of the connection and the cyber attacks from the cloud computing.

Regarding these, it is important to introduce security software (e.g., anti-virus software) in fog computing.

Table 4: Countermeasure characteristics of Risk Avoidance (2 risk factors).

No.	Risk Factor	Risk Probability	Risk Impact	Risk Classification	Risk Countermeasure
13	2.1.1.2 Cyber risk	H	H	Risk Avoidance	Install anti-virus software on the edge (IoT devices). Publish the security policy of fog computing.
18	2.2.1.1 Edge-side (IoT device) reliability	H	H	Risk Avoidance	Implement anti-virus and other security software for fog computing.

3.2.4 Risk Mitigation

Table 5 shows the results of the "Risk Mitigation" of the response measures. The issue here is the connection between network elements with different security policies. In response to this, net-work elements with different security policies should not be connected by installing a security policy matching function in fog computing.

Table 5: Countermeasure characteristics of Risk Mitigation (2 risk factors).

No.	Risk Factor	Risk Probability	Risk Impact	Risk Classification	Risk Countermeasure
5	1.1.2.1 Connecting to fog computing having different security policies	H	L	Risk Mitigation	Implement a security policy matching function and do not connect fog computing with low security level.
16	2.1.2.1 Connecting to fog computing with different security policies	H	L	Risk Mitigation	Implement a security policy matching function and do not connect fog computing with low security level.

3.2.5 Summary

As shown in Fig. 3, the main risk countermeasures in fog computing are as follows.

1) First, gradually introduce protocols from an economic point of view for the IoT's various protocols.
2) Second, implement a security policy matching function between the network elements connected to fog computing.

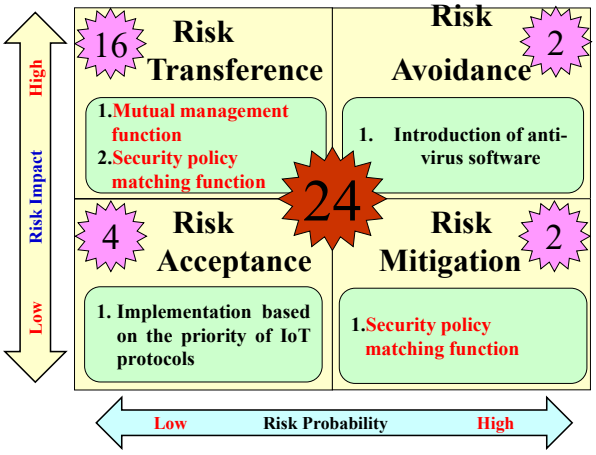

Figure 3: Summary: Main risk countermeasures for each category.

3.3 Risk Evaluation of Proposed Countermeasures

Next, we evaluated the effectiveness of our proposed countermeasures through a quantification of the risk factors shown in Table 1. We utilized a risk formula commonly used in the ISMS field and then calculated the risk value on the basis of our previous qualitative results. Finally, the risk value was deduced by using the formula and approximation [17].

3.3.1 Ordinary Risk Value Formula

Each risk value is quantified as

$$\text{Risk value} = \text{value of asset} * \text{value of threat} * \text{value of vulnerability}. \quad (1)$$

Generally, all elements on the right-hand side of Eq. (1) are very difficult to calculate. We use the following approximation to simplify these elements [18]–[20].

3.3.2 Approximate Risk Value Formula

(Step 1) Approximation of Asset Value: The asset value is approximated in terms of the risk impact in the risk matrix, as shown in Fig. 4. In other words, the asset value is considered to be the risk impact. The degree of risk impact is defined as anywhere from 1 (low) to 5 (high) [18]. As a further approximation, these values are mapped as risk impact in a risk matrix. As shown in Fig. 4, the risk impact of the risk matrix is divided into two. For simplicity, the maximum degree of risk impact (5) is approximated to the higher of the two divisions. Similarly, the minimum risk impact (1) is approximated to the lower of the two.

(Step 2) Approximation of Threat Value: The threat value of Eq. (1) is approximated in terms of the risk probability in the risk matrix. On the basis of references, the risk probability is defined to range from 1 (low) to 3 (high) [18]. These values are mapped to the risk probability of the risk matrix in Fig. 2, as well as the above-mentioned degree-of-seriousness approximation. That is, the maximum risk probability (3) is approximated to the higher of the two divisions, and the minimum (1) is approximated to the lower of the two.

(Step 3) Approximation of Value of Vulnerability: The vulnerability evaluation is defined on a three-level scale: 3 (high), 2 (medium), and 1 (low) [18]. These levels are approximated in accordance with the classification of the risk matrix in Fig. 2. Here, the four domains of the figure are classified into three categories in accordance with the risk probability and risk impact: Risk Avoidance cases are approximated to 3 (high), Risk Transference and Risk Mitigation cases to 2 (medium), and Risk Acceptance cases to 1 (low).

As stated above, Eq. (1) is approximated as Eq. (2). In addition, the approximate value of each parameter of Eq. (2) is shown in Table 6.

$$\text{Risk value} \fallingdotseq \text{value of risk impact} * \text{value of risk probability} * \text{value of vulnerability} \quad (2)$$

Table 6: Approximate values of Eq. (2).

	Risk Impact	Risk probability	Vulnerability	
High	5	3	Risk Avoidance	3
Low	1	1	Risk Transference and Risk Mitigation	2
			Risk Acceptance	1

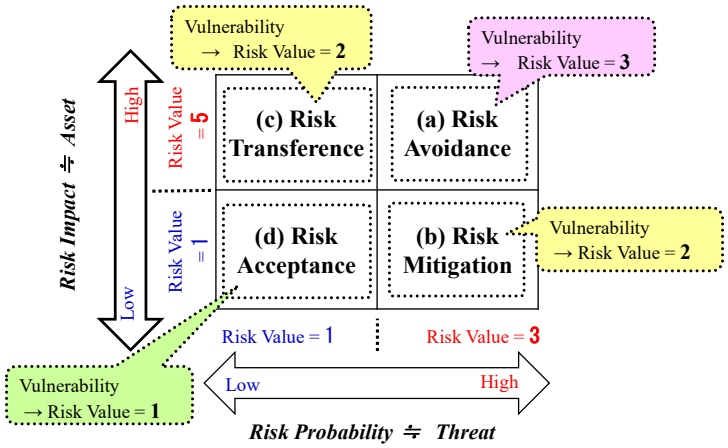

Figure 4: Risk value approximation of risk matrix.

3.3.3 Calculation of Risk Value Based on Eq. (2)

We calculated the risk values for all risk factors shown in Table 7 by using Eq. (2). Next, the risk values after carrying out the proposed countermeasures in Tables 2–5 were calculated by using Eq. (2).

Table 8 shows the reduction rate of the risk values after the implementation of risk countermeasures. As we can see, the overall risk reduction rate after the countermeasures was about 55% compared to before the countermeasures. This demonstrates that the effectiveness of the proposed countermeasures can be clarified even though the risk value is a relative index.

Table 7: Risk values before and after countermeasures.

No.	Risk Factor	Risk Probability	Risk Impact	Before risk countermeasures		After risk countermeasures	
				Vulnerability (Risk Classification)	Risk value	Vulnerability (Risk Classification)	Risk value
1	1.1.1.1 Protocols that can be connected to fog computing	1	1	1	1	1	1
2	1.1.1.2 Cyber risk	1	5	2	10	1	5
3	1.1.1.3 Fog computing failure	1	5	2	10	1	5
4	1.1.1.4 Reliability of fog computing	1	5	2	10	1	5
5	1.1.2.1 Connecting to fog computing having different security policies	3	1	2	6	1	3
6	1.1.2.2 Fog computing failure	1	5	2	10	1	5
7	1.2.1.1 Edge-side (IoT device) reliability	1	5	2	10	1	5
8	1.2.1.2 Reliability of cloud computing	1	5	2	10	1	5
9	1.2.1.3 Implementation of multiple protocols	1	1	1	1	1	1
10	1.2.2.1 Matching security policies	1	5	2	10	1	5
11	1.2.2.2 Troubleshooting failures	1	5	2	10	1	5
12	2.1.1.1 Limitations of fog computing connection protocols	1	5	2	10	1	5
13	2.1.1.2 Cyber risk	3	5	3	45	1	15
14	2.1.1.3 Fog computing failure	1	5	2	10	1	5
15	2.1.1.4 Reliability of fog computing	1	5	2	10	1	5
16	2.1.2.1 Connecting to fog computing with different security policies	3	1	2	6	1	3
17	2.1.2.2 Reliability of fog computing	1	5	2	10	1	5
18	2.2.1.1 Edge-side (IoT device) reliability	3	5	3	45	1	15
19	2.2.1.2 Cyber risk	1	5	2	10	1	5
20	2.2.1.3 Implementation of many protocols	1	1	1	1	1	1
21	2.2.2.1 Matching security policies	1	5	2	10	1	5
22	2.2.2.2 Isolation in case of failure	1	5	2	10	1	5
23	2.2.3.1 Billing	1	1	1	1	1	1
24	2.2.3.2 Installation site	1	5	2	10	1	5
Risk value (total)					266	Risk value (total)	120

Table 8: Reduction rate of risk values.

	Before risk countermeasures (1)	After risk countermeasures (2)
Risk value (total)	266	120
Risk value reduction rate = ((1)-(2))/ (1)		0.55

4 Portfolio of Risk Countermeasures for Fog Computing

Here, we evaluate the risk measures for fog computing shown in Section 3 (Tables 2–5) from a practical perspective. In general, from a practical point of view, it is necessary to consider the priority of risk countermeasures in terms of cost constraints. In this paper, we apply the portfolio approach to prioritization. In other words, from a practical point of view, a portfolio of risk countermeasures for fog computing enables step-by-step risk countermeasures.

4.1 Application of Portfolio Management

In general, it makes sense to implement risk countermeasures in stages in view of their cost-effectiveness. In this subsection, we propose a portfolio (priority) of risk countermeasures based on prior literature on portfolios [21]-[25], in particular, the Computer Security Incident Response Team (CSIRT) risk countermeasure classification [21]–[22]. The CSIRT classifies risk countermeasures into three categories: Proactive Service, Reactive Service, and Security Quality Management Services. 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. As the proposed portfolio of risk countermeasures clearly identifies Proactive Service, Security Quality Management Service, and Reactive Service for each countermeasure, the measures can be introduced step-by-step.

The following subsections show the results of the portfolio for the private fog user side (edge side, cloud side) and the provider side (fog side), as well as for the public fog user side (edge side, cloud side) and the provider side (fog side).

4.2 Risk Countermeasure Portfolio of Private Fog

4.2.1 Private Fog User Side (Edge side, Cloud side)

In a private environment, the main countermeasures to mitigate risk include, on the edge side, installing anti-virus software and connecting to fog that supports the edge protocol. On the cloud side, this includes implementing security policy matching with fog.

The portfolio results of these countermeasures are shown in Table 9. Because of the private environment, the results show that there are few precautionary countermeasures that need to be taken, and that security quality functions such as post-measures and matching functions should be satisfied after the fog and other environments are in place.

Table 9: Portfolio results of private fog user side (Edge side, Cloud side).

No.	Risk Factor	Risk Classification	Risk Countermeasure	Pre	Post	Quality
1	1.1.1.1 Protocols that can be connected to fog computing	Risk Acceptance	For use in private environments, connect with fog computing that supports edge-side (IoT device) protocols.		○	
2	1.1.1.2 Cyber risk	Risk Transference	Install anti-virus software on the edge side (IoT devices). If it cannot be installed on the edge side, monitor the edge side (IoT device) by fog computing.	○		
3	1.1.1.3 Fog computing failure	Risk Transference	If a fog computing fails, connect to a nearby fog computing. Important fog computing should be redundant.		○	
4	1.1.1.4 Reliability of fog computing	Risk Transference	Publish a security policy for fog computing.			○
5	1.1.2.1 Connecting to fog computing having different security policies	Risk Mitigation	Implement a security policy matching function and do not connect fog computing with low security level.			○
6	1.1.2.2 Fog computing failure	Risk Transference	If a fog computing fails, connect to a nearby fog computing. Important fog computing should be redundant.		○	

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

○: High Priority, Blank: Low Priority

4.2.2 Private Fog Provider Side (Fog side)

The main countermeasures to mitigate risk on the fog side of the private environment include anti-virus functions, the establishment of security policies, and monitoring functions such as edge.

The portfolio results of these countermeasures are shown in Table 10. For the fog itself on the private side, most of them should be equipped as preliminary measures, and the results show that the protocol implementation on the edge side should be satisfied step by step as a security quality function.

Table 10: Portfolio results of private fog provider side (Fog side).

No.	Risk Factor	Risk Classification	Risk Countermeasure	Pre	Post	Quality
7	1.2.1.1 Edge-side (IoT device) reliability	Risk Transference	Implementing anti-virus and other security software for fog computing.	○		
8	1.2.1.2 Reliability of cloud computing	Risk Transference	Check the security policy of cloud computing. Implement anti-virus and other security software for fog computing as well.	○		
9	1.2.1.3 Implementation of multiple protocols	Risk Acceptance	Define the priority of the edge side (IoT devices) to be connected and introduce them in a step-by-step approach.			○
10	1.2.2.1 Matching security policies	Risk Transference	Establish a security policy for fog computing. Connect to cloud computing that has the same or higher policy level.	○		
11	1.2.2.2 Troubleshooting failures	Risk Transference	Establish a monitoring function that originates from fog computing.	○		

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

○: High Priority, Blank: Low Priority

4.3 Public Fog User Side (Edge side, Cloud side)

4.3.1 Public Fog User Side (Edge side, Cloud side)

In the public environment, as with the private side, the main measures to mitigate risk are to install anti-virus software on the edge side and connect to fog that supports the edge protocol. Similarly, on the cloud side, the implementation of security policy matching with fog is also a good example.

The portfolio results from these countermeasures are shown in Table 11. As it is the use side of fog, the results show that as in the private environment, there are few precautionary countermeasures, and after the fog and other environments are in place, the security quality functions such as post-countermeasures and matching functions can be satisfied.

Table 11: Portfolio results of public fog user side (Edge side, Cloud side).

No.	Risk Factor	Risk Classification	Risk Countermeasure	Pre	Post	Quality
12	2.1.1.1 Limitations of fog computing connection protocols	Risk Transference	Confirm the security policy of fog computing installed in a public environment.		○	
13	2.1.1.2 Cyber risk	Risk Avoidance	Install anti-virus software on the edge (IoT devices). Publish the security policy of fog computing.	○		
14	2.1.1.3 Fog computing failure	Risk Transference	When fog computing in the public environment is not connected, it tries to connect with nearby fog computing.		○	
15	2.1.1.4 Reliability of fog computing	Risk Transference	In the case of a public environment, implement a security policy matching function to connect to fog computing with the same security policy.			○
16	2.1.2.1 Connecting to fog computing with different security policies	Risk Mitigation	Implement a security policy matching function and do not connect fog computing with low security level.			○
17	2.1.2.2 Reliability of fog computing	Risk Transference	In the case of a public environment, implement a security policy matching function to connect to fog computing with the same security policy.		○	

Pre: Proactive Service. Post: Reactive Service. Quality: Security Quality Management Service.
○: High Priority, Blank: Low Priority

4.3.2 Public Fog Provider Side (Fog side)

The main risk countermeasures on the fog side of the public environment include the implemen-tation of anti-virus functions, security policy formulation and monitoring functions such as edge, and the implementation of various protocols that the edge has.

The portfolio results of these countermeasures are shown in Table 12. As with the fog on the private side, most of these countermeasures should be taken in advance. In addition, edge-side protocol implementation and billing functions, as well as public fog deployment plans, should be supported gradually as security quality functions.

Table 12: Portfolio results of public fog user side (Fog side).

No.	Risk Factor	Risk Classification	Risk Countermeasure	Pre	Post	Quality
18	2.2.1.1 Edge-side (IoT device) reliability	Risk Avoidance	Implement anti-virus and other security software for fog computing.	○		
19	2.2.1.2 Cyber risk	Risk Transference	Install anti-virus and other security software. Also, update the software periodically.	○		
20	2.2.1.3 Implementation of multiple protocols	Risk Acceptance	Define the priority of the edge side (IoT devices) to be connected and introduce them in a step-by-step approach.			○
21	2.2.2.1 Matching security policies	Risk Transference	Establish a security policy for fog computing. Connect to cloud computing that has the same or higher policy level.	○		
22	2.2.2.2 Isolation in case of failure	Risk Transference	Establish a monitoring function that originates from fog computing.	○		
23	2.2.3.1 Billing	Risk Acceptance	Simplify the system by using a subscription-based billing system.			○
24	2.2.3.2 Installation site	Risk Transference	Plan in advance to predict the traffic on the edge side (IoT devices) that will be connected to the fog computing.			○

Pre: Proactive Service. Post: Reactive Service. Quality: Security Quality Management Service.
○: High Priority, Blank: Low Priority

4.4 Discussion

The fog computing risk countermeasure portfolio was divided into four forms: fog computing provision form (private, public) and component (user side, provider side). As we can see from the results of the portfolio, there was not much difference in the form of provision, but there was a difference in the components, as shown below.

(1) User Side (Edge side, Cloud side): As shown in Tables 9 and 11, on the risk countermeasures on the fog user side, that is, the cloud side and the edge side, as a result of the portfolio, about half of the items can be classified as post-measures.

(2) Provider Side (Fog side): As shown in Tables 10 and 12, as a result of the portfolio, we found that proactive risk countermeasures are important for the risk countermeasures of the fog provider, that is, fog computing itself.

(3) Summary: As these results demonstrate, it is important for the fog side, which is the provider of fog computing, to focus on proactive measures and invest in risk countermeasures for fog computing. On the other hand, on the user side of fog computing, it is possible to invest with a slight time lag, so it was clarified that it is possible to proceed with the risk countermeasures of fog computing step by step as a whole.
(4) Validity of the portfolio assessment: As mentioned above, the portfolio-based evaluation was developed based on the authors' discussions. The authors have many years of experience working for IT companies and also have experience in software implementation and education at universities. The portfolio was created based on these experiences and knowledge, as well as previous studies [21]-[25]. Thus, although it is a qualitative assessment, the portfolio of countermeasures against the extracted risk factors of fog computing is derived from a deductive point of view, which is appropriate.

5 Conclusion and Future Work

In this paper, we conducted a risk assessment of fog computing, which is newly established to promote the utilization of IoT devices. Specifically, we comprehensively extracted 24 risk factors of fog computing by using the RBS method, analyzed them, and proposed countermeasures using the risk matrix method. Our analysis of the risk countermeasures showed that two related to "Risk Avoidance," 16 related to "Risk Transference," two related to "Risk Mitigation," and four related to "Risk Acceptance." In other words, most of the countermeasures were for "Risk Transference." We also clarified that the main risk countermeasures for fog computing included the gradual introduction of connected IoT connection protocols and the implementation of security policy matching functions.

Although the risks were extracted comprehensively, this was not exhaustive, and other views (e.g., the economic and operational views) will be examined in future work. We will also perform a more detailed assessment of the proposed countermeasures and examine new ones. We also clarified the effectiveness of the proposed risk measures by evaluating the risk values. The total reduction rate of the risk values after implementing the countermeasures was about 55% compared with before the countermeasures. This result can function as a reference when a risk countermeasure is applied, even though it is a relative index of the risk value. In addition, from the viewpoint of practical use, the results of the portfolio of risk countermeasures show that the gradual introduction of risk countermeasures for fog computing is feasible.

Overall, our findings on risk countermeasures for fog computing should help ensure the safe and secure use of IoT devices.

Future work will include quantitative evaluation of the proposed risk countermeasures based on their cost-effectiveness.

Acknowledgement

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

References

[1] Ministry of Internal Affairs and Communications, White Paper on Information and Commu- nications 2018, The rapid spread of IoT devices, 2018, (Japanese Edition), [Online]. Available from: http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd111200.html

[2] M. Niwa et al., Study on the IoT system using fog computing, CSEC-83, 1-7, ISPJ, 2018, (Japanese Edition)

[3] CISCO, Fog computing, (Japanese Edition), [Online]. Available from: https://www.cisco.com/c/m/ja_jp/solutions/internet-of-things/iot-system-fog-computing.html

[4] M. Saito, Alternative Blog, The three-layered structure of the IoT [Revised Edition], (Japanese Edition), [Online]. Available from: https://blogs.itmedia.co.jp/itsolutionjuku/2017/10/iot_iot.html

[5] S. Tanimoto, et al., Proposal of a perimeter line management method for fog and edge computing with SDP concept, Advances in Networked-Based Information Systems, AISC 1264, pp.290-302, Springer, 2020

[6] KEYENCE, glossary of terms, Fog Computing, (Japanese Edition), [Online]. Available from: https://www.keyence.co.jp/ss/general/iot-glossary/fog-computing.jsp

[7] S. Khan, S. Parkinson, and Y. Qin, Fog computing security: a review of current applications and security solutions, Journal of Cloud Computing: Advances, Systems and Applications. DOI 10.1186/s13677-017-0090-3, 6(19)(2017)

[8] I. Stojmenovic, S. Wen, X. Huang, and H. Luan, "An overview of Fog computing and its security issues," Concurrency Comput. Pract. Exp., vol. 28, no. 10, pp. 2991–3005, Jul. 2015

[9] P. Zhang, M. Zhou, and G. Fortino, "Security and trust issues in fog computing: A survey," Future Generation Computer Systems, vol. 88, pp. 16–27, 2018

[10] S. Yi, Z. Qin, Q. Li, Security and privacy issues of fog computing: A survey, in: Wireless Algorithms, Systems, and Applications the 10th International Conference on, 2015, pp. 1–10

[11] H. Yokota et al., Edge Computing Technologies to Connect the Missing Link of IoT, NEC Technical Journal, Vol.12, No.1, pp.24-28, 2017

[12] P. Chertchom, et al., Data Management Portfolio for Improvement of Privacy in Fog-to-cloud Computing Systems, 2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI), pp.884-889, 2019.

[13] P. Chertchom, et al., "Edge Computing Platform Management: Design for F2C and F2F for Small Businesses to Reduce Costs," 2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI), pp.890-895, 2019.

[14] Risk Breakdown Structure, [Online]. Available from: http://www.justgetpmp.com/2011/12/risk-breakdown-structure-rbs.html

[15] S. Tanimoto, et al., Risk Management of Fog Computing for Improving IoT Security, 2021 10th International Congress on Advanced Applied Informatics (IIAI-AAI), pp.703-709, 2021

[16] Cox's risk matrix theorem and its implications for project risk management, [Online]. Available from: http://eight2late.wordpress.com/2009/07/01/cox%E2%80%99s-risk-matrix-theorem-and-its-implications-for-project-risk-management/

[17] ISMS Risk Assessment Manual v1.4, [Online]. Available from: https://www.igt.hscic.gov.uk/KnowledgeBaseNew/ISMS%20Risk%20Assessment%20Manual%20v1.4.pdf, 2015.1.4

[18] H. Sato, et al., Information Security Infrastructure, Kyoritsu Shuppan Co., Ltd., 2010, (Japanese Edition)

[19] 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

[20] S. Tanimoto, et al., Risk Assessment Quantification of Ambient Service, ICDS 2015 : The Ninth International Conference on Digital Society, pp. 70-75, Lisbon, Feb. 2015

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

[22] 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

[23] C Mican, et al., A method for project portfolio risk assessment considering risk interdependencies–a network perspective, Elsevier, Procedia Computer Science, 196(2022) 948–955

[24] F.J. Joubert, et al., Using Monte Carlo simulation to quantify the cost impact of systemic risk factors in a project portfolio: a case study, South African Journal of Industrial Engineering, vol.32, n.4, pp.67-82, 2021

[25] S. C. Geuther, et al., BBN-Based Portfolio Risk Assessment for NASA Technology R&D Outcome, International Annual Conference of the American Society for Engineering Management "Energizing Engineering Management", [Online]. Available from: https://ntrs.nasa.gov/api/citations/20160013839/downloads/20160013839.pdf