Modelling IoT Security Risk Management in Banking Environment

Ermina Syahirah bt Mohamad Nordin, Hafiza Abas, Azizul Azizan

Razak Faculty of Technology and Informatics

Universiti Teknologi Malaysia
erminasrc@gmail.com

Article history

Received:
08 June 2020

Received in revised form:
15 June 2020

Accepted:
20 June 2020

Published online:
20 July 2020

*Corresponding author
erminasrc@gmail.com

Abstract

This paper discusses the issue in the banking context, where the equilibrium between banking protection risk management and the IoT security threats that any bank will face today must be decided. The recommended solution involves an IoT risk assessment mechanism that quantifies risks based on real threats and combines them with financial regulation that any financial must comply with. The risk reduction approach is focused on values such as operation regulation, the preservation of information, and the accomplishment of security goals. Preventive IoT protection initiatives and approaches to enhance IoT protection in the banking setting are addressed in this article.

Keywords: *Banking environment, IoT, risk management model*

1. Introduction

The Internet of Things is a collection of interrelated electronic systems, mechanical and automated appliances, artifacts, animals, or individuals with specific identifiers and the capacity to transmit data across a network without the requirement for human-to-human or human-to-computer contact [1].

A bank is a position that means a rather unnecessary degree of security because any consumer is affected by day-to-day banking transactions [2]. Banks have also been eager to adopt emerging technology and have recognized the ability of IoT banking to offer unprecedented rates of data and consumer knowledge [3]. Banks also spent significantly on IoT technologies, with banks holding an estimated IoT banking expenditure of $117.4 million, or around 0.4 percent of sales [4]. IoT banking aims to provide consumers with tailor-made programs, to give feedback and new deals daily of their purchase patterns.

The usage of IoT in banking would continue to be troubled by problems such as rising hacking, corruption and financial abuse, loss of consumer details and frustration, higher running costs, and elevated financial expenditure threats. It poses a significant burden for banking to meet with the criteria of Bank Negara Malaysia (BNM) Consumer Knowledge Management and Certified Disclosure

* *Corresponding author*. erminasrc@gmail.com

Management [5]. Breaches of customer's information will be compounded under the Financial Services Act 2013 (FSA) [6].

Breaches happen every day, and James Comey, the director of the FBI, claims, "There are two kinds of American companies: those that have been compromised and those who don't realize it yet." Once hackers get unwelcome exposure to the Customer Information File (CIF), profits, liabilities/debts, and intellectual property, the consequences can be disastrous [7]. The adoption of a robust IoT risk model for banking is therefore very important today.

That is where IoT's risk model will help. The IoT risk assessment process will not only be carried out by technology experts, but also by the Chief Executive Officer. CEO's concerns will be around control:

1) *What are the expectations of the clients? What are their standards?*
2) *What IoT devices/wearables are ready to use?*
3) *How will clients be informed of their privacy and protection concerns?*
4) *What should be done to increase consistency through the usage of company data?*
5) *How will privacy policies be made transparent and accessible to clients?*

2. IoT in Banking

In the last 20 years, modern banks had to reconsider their way of working and their offering to adapt to these developments. IoT is one of the most significant resources for a bank to carry out a digital transformation [8]. Nowadays, consumers anticipate a lot of creativity from their bank and, in particular, from the latest digital one that will provide them with the correct services in their way [9].

Millions of computers are linked to each other, rendering them smart networks [10]. As these digital devices and systems exchange cloud data and begin to evaluate, they will change industry, life, and the environment in countless ways.

Figure 1 explains how IoT can be applied in banking by utilizing the Cloud Computing Network.

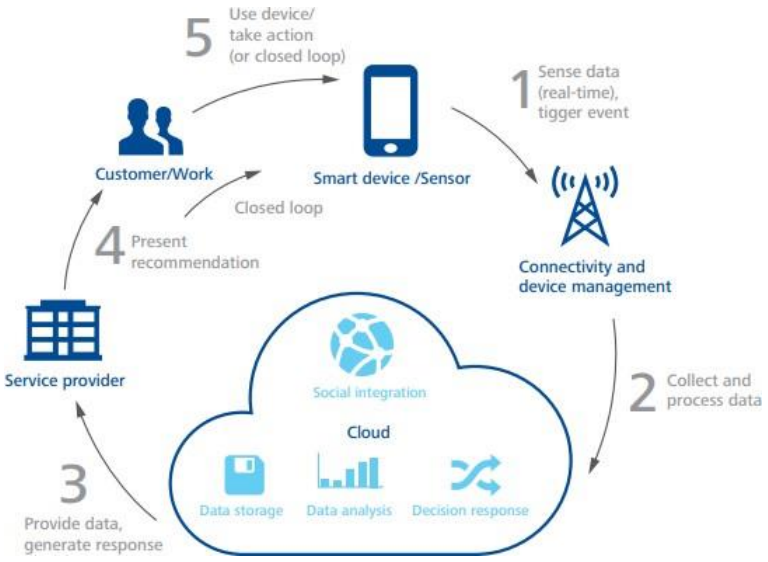

Figure 1: Cloud computing with IoT connected banking platform [11]

Customers use smart data access devices that allow banks to have a full view of consumer finances in real-time. Banks can predict consumer desires through data collection and provide strategies and guidance that can help consumers make reasonable and informed financial choices. In this sense, a bank will become a very effective facilitator to improve consumer satisfaction and, in effect, to attract more customers to the banks.

Throughout the interrelated environment, banks connect with customers and provide advice through their mobile phones. A common strategy should be adopted for consumer purchasing habits. There are many opportunities for banks to communicate with their customers by providing guidance and benefits in certain aspects of their life, not just financial ones. This will, in effect, increasing consumer satisfaction.

Here are the most IoT threats for the banking sector categorized by services:

A. Wearables Banking

Bank will give promotional alerts regarding new products and account balances while a customer is approaching a branch / ATM from wearable devices for instant updates [12]. Banks may also incorporate incentives offered by various merchants, based on the quality of the balance of the customer's account and locality.

Although the use of IoT has many advantages for the banking sector, IoT wearable banking equipment is of various types; it is manufactured by different manufacturers and needs different maintenance approaches. It is this lack of a popular standard that can lead to a flaw in the functionality of IoT; even though all manufacturers decide to use one basic standard, the question of technical problems will still have to be addressed.

B. Wealth management personalization

Use data mining techniques to produce insights into asset management is a standard procedure. The Internet of Things in banks can only increase the quality and pace of knowledge collection and expand the spectrum of accessible insights [13]. IoT-enabled wealth management applications can often warn consumers if their financial security is under attack.

On the other hand, IoT may produce large quantities of data, generating additional costs associated with the storing and securing of all those data. Organizations also don't have the systems available to test IoT data for errors and omissions, so data quality isn't always accurate. That is a project that needs to be planned separately.

C. Transaction automation

The usage of IoT in banking allows any payment process to be technically regulated. The technology would ultimately allow the 'Internet of Value'—a safe and regulated foreign trade ecosystem where all payments are managed by a smart sensor network and connected devices [14]. IoT should be a primary protection regulator here.

As a result, IoT has increases the unemployment rate. IoT technology reduces the dependency on human efforts as this technology automates work processes that require the human brain. As time goes on, banks, as well as other financial institutions, may cut the workforce as a result of this technology leading to a high increase in the unemployment rate which can harm so many countries ' economies.

D. Chatbots

According to a survey by LivePerson, the production of Chatbot is gaining global prominence. Of the 5,000 people participating in the study, 38 percent ranked their overall view of Chatbot as favorable globally, and just 11 percent registered negative views of Chatbots, while 51 percent registered neutral attitudes [15]. The creation of Chatbot is also bursting the banking industry. This has the potential to simplify processes and therefore meet more consumers to have more friction-free banking experience [16]. For both of these apps, the creation of the chatbot is streaming and integrating with all of the bank's digital services.

The security risks to chatbot fall into two categories – threats and vulnerabilities. Threats a chatbot may pose include spoofing / impersonating someone else, data manipulation, and data theft [17].

E. Capacity management

One way to harness the potential of the Internet of Things is by improving capacity utilization in bank branches. Through gathering, storing, and exchanging customer data in real-time, branch managers may be able to monitor the number of customers entering the bank regularly, how much personnel is required to reach optimum performance, and how to automate the counters [18].

In 2018, multiple data breaches made headlines for compromising millions of people's data. These data breaches have stolen confidential information such as personal details, credit and debit card credentials, and email addresses. Hackers can now attack IoT devices like smartwatches, smart meters, and smart home devices to gain additional user and organizational data

F. Transparency on customer data

The prospect of IoT in banking ensures that payment providers should be presented with accurate consumer data: loan debt and history, asset specifics and valuation, as well as product yields generated by the company (a critical consideration for agricultural companies dependent on financial services banks) [19].

Although the use of IoT technologies has so many benefits on banking, IoT however, is prone to hacking. There is a high risk of data and personal information regarding the customer's privacy and security of funds being compromised through wearable "hacking.

As a result, banking institutions should have an enhanced decision-making mechanism for the issuance of loans. IoT-induced openness should offer some protection to banks as it reduces the possibility of dealing with poor debtors in the future. The data provided by IoT will provide, among other things, flexibility for banks that are usually struggling to provide.

3. Existing IoT Security Risk Management Model

Building on the interpretation of the dimensional concept of related technology and the vulnerability and life-cycle characteristics of information systems, this paper includes a dimension model of the process monitoring framework for IoT security risk management, as shown in Figure 2

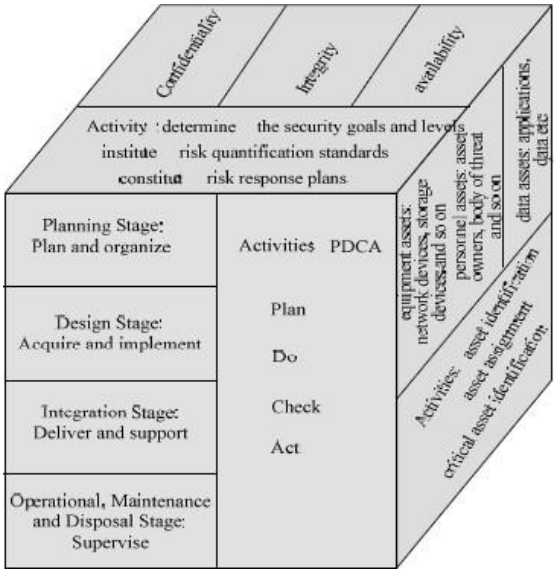

Figure 2: Digital protection risk assessment and control system three-dimensional model [20]

A. S-dimension

This aspect that controls objectives for the stabilization of the IS and its activities. The basic aim of S-dimension is to protect the secrecy, reliability, transparency of information systems, and activities. The tasks associated with S-dimension management goals include the following:

1) *Define the security priorities and stages of the IoT program.*
2) *Establish risk quantification criteria.*
3) *Represent preparations for risk management.*

B. R-dimension

The R-dimension is the properties that support the dimension, including infrastructure and interrelated events. Data management tools are as follows:

1) *Network properties, such as network and storage units.*
2) *Private properties, such as wealth owners, and offending organs.*
3) *Computer properties, such as documents and software. Events relevant to the resource security aspect include identification, designation and recognition of essential assets.*

C. P-dimension

P-dimension is a mechanism that governs the dimension. Threat risk assessment and monitoring is carried out through processes such as preparation and start-up, architecture, growth and deployment, operation, maintenance, and disposal of the IS life cycle.

4. Methodology

To order to resolve the above-listed problems, IoT risk management should be used to select the right approach to maintain the IoT banking ecosystem at a reduced rate. There are many IoT risk assessment methodologies, but they all aim to answer the following questions:

1) *What needs to be covered by this?*

2) *Who / What are the risks and vulnerabilities?*

3) *What are the consequences if they have been harmed or lost?*

4) *What is the worth of the bank?*

5) *What can be done to mitigate the chance of failure or damage?*

The solution suggested is to make IoT protection based decisions using the vulnerability approach seen in Figure 3.

Figure 3: Risk management decision-making process.[21]

Nearly every bank has informed users of the previous successful link to the Internet system. This dynamically analyzes the IP addresses of each active login and decides the country of origin of the IP address. If the user has signed in from various countries for the last 24 hours – the details on the last active international and local login IP addresses and counter is provided to him or her in the database [22]. Information that the customer will change his or her password immediately if he or she does not accept the login as their own. The trial lasted 30 days, as seen below:

Table 1: Pattern of password change

A complete number of users	Users signed in from various countries during the trial period	Users who changed their passwords following notification
100	61	39

5. IoT Security Risk Management Model Proposed

Based on the Control Model Information Structure in IoT Control, this paper provides an enhanced IoT security risk management framework, as seen in Figure 4.

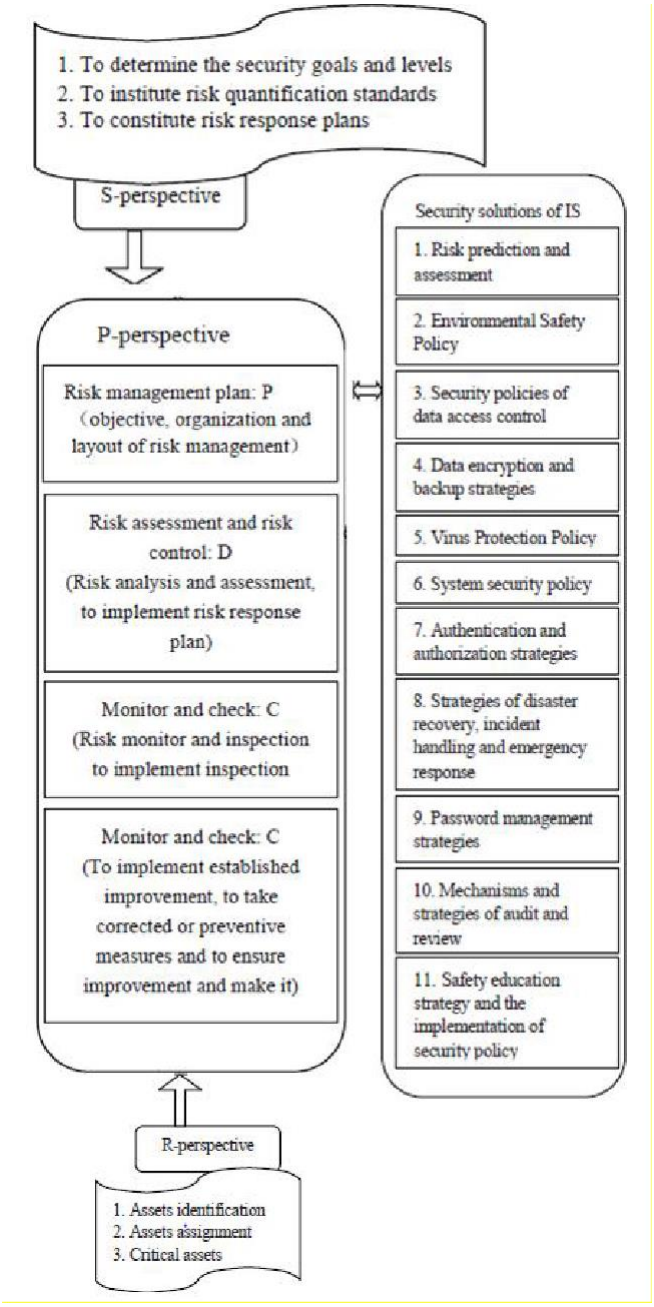

Figure 4: Proposed risk management of IoT security [23]

The risk-takers should be in a position to better appreciate the emerging security conditions that banking is facing by assessing and defining vulnerability and drawing on IoT Security Risk Management Dimensional Model. There will be appropriate security solutions developed to ensure that the risk of security is within an admissible range when it is outside the IoT threshold.

Building on an improved cyber technology risk management framework:

1) Protecting the view of capital (R viewpoint)

All knowledge and its related structures, applications, and networks are essential tools in IT governance. This is important to identify, enforce, sustain, and improve the security of information assets to retain a competitive edge in the market, cash flow, competitiveness, enforcement, and commercial identity. The objective of the process for managing information security risk shall protect intelligence properties due to damages.

Maximizing asset identification is key to connecting dots across a variety of tools to detect and respond to threats. SOC analysts need to be able to break through the alert clutter and empower the security team to detect known and unknown threats with a security platform that provides visibility across all environments.

2) Analysis of the application of the goals of the organization of the information technology (S analysis)

Four types of IS security risk assessment priorities are strategic objective, market purpose, IS security purpose, and enforcement objective. The market goal is to be met by managerial oversight, corporate development, human resources administration, and organizational culture.

Before it happens, the Bank must prepare for an IoT attack by developing policies and procedures based on established risk tolerance, document workflows to centrally manage investigations and remediation, and coordinate mission response. This provides a repeatable process to triage the incident cross-functionally with coordinated, well-defined plans that reduce effort and complexity.

3) IS life-cycle method

Specific security concerns will emerge at each stage in the life-cycle of the communication network and would entail assistance for risk control. Risk control is a comprehensive process that is being introduced in the various stages of the lifecycle of the information system which can be achieved through risk control mechanisms such as risk management strategy and risk assessment.

Centralize IoT management of incidents across functional silos inside and outside the bank's "glass walls" to ensure consistent, coordinated, and automated responses. This centralization allows stakeholders to have a unique view of "what the risk is," "how bad it is," "what is affected" and "what is done to address it," enabling department leadership to make better mission decisions to minimize the impact on them.

6. Conclusion

There are many different IoT Security Risk Management Frameworks and best practices that are very useful and necessary to make the IoT environment healthier, so if IoT needs to be combined with protection, it's very important to use the most efficient IoT protection handling method. Based on the suggested strategy, IoT consumption, strict budgeting, and IoT protection issues can be addressed.

Acknowledgments

Indebted gratitude goes to my lecturer, Dr. Hafiza Abas, who gave me her unwavering encouragement and expertise during the study. On top of that, she encouraged me to work in my way while at the same time giving her brilliant positive feedback to ensure the success of this study.

References

[1] Chen Jian-Hua, Research on Information Security Risk Management, Evaluation and Control, Jilin University, 2008.
[2] James J.Jiang, Gray Klein.Software, Development Risk to Project Effectiveness, The Journal of Systems and Software.2000 (8):3�10.
[3] Gu Yong-hao, Research on Theory and Key Technologies of Information System Risk Management [D], Beijing University of Posts and telecommunications, 2007.
[4] Josep Domingo-Ferrer, Vicen Torra.Disclosure risk assessment in statistical data protection, Journal of Computational and Applied Mathematics, 2004, pp. 285�293.
[5] Chen Guang, Research on Method of Information System Information Security Risk Management [D], National University of Defense Technology, 2006.
[6] Yulin. Research on IT Control Based on COBIT and SOX Compliance
[7] Tianjin University of Finance and Economics, 2006.
[8] Randall C.Reid, Stephen A. Floyd. Extending the Risk Analysis Model to Include Market-Insurance.Computers&Security, 2001(4), pp. 331�339.
[9] Song Ru-shun, Comprehensive analysis of the security risk of an information system [J], Computer Engineering, 2000.26.12, pp. 33-34. U.S. Department of homeland security "Cyber Risk Management Primer for CEOs" 1-2.p. https://www.dhs.gov/sites/default/files/publication /C3%20Voluntary% 20Program%20-%20Cyber%20Risk%20Management%20Primer%20for%20CEOs%20_5.pdf
[10] Nbcnews report "Cyberattack 101: Why Hackers Are Going After Banking" https://www.nbcnews.com/tech/security -targets-hackers-n429821
[11] THE INDEPENDENT news on 6 October 2014 "FBI's James Comey accuses China of hacking into every major American company"
[12] http://www.independent.co.uk/news/business/news/fbis-james-comeyaccuses-china-of-hacking-into-every-major-american-company- 9777587.html
[13] Howard Anderson, News Editor, ISMG "What's Wrong With Relying on HIPAA Compliance?" https://www.careersinfosecurity.com/whatswrong-Relying-on-HIPAA-compliance-a-10013
[14] Wayne State University "IT Security Best Practices" TOP 10 RECOMMENDED INFORMATION SECURITY PRACTICES https://internalaudit.wayne.edu/security-practices
2017 a Breach Investigations Report 10th Edition by Verizon. WP16943 04/17
[15] EU General Data Protection Regulation http://eur-lex.europa.eu/legalcontent/ EN/TXT/?uri=CELEX:32016R0679
Ian Cooke, "Doing more with less" in ISACA Journal 2017, vol. V, 6-9. p.
[16] P. Dorogovs, A. Romanovs. Overview of government e-service security challenges. Information, Electronic and Electrical Engineering (AIEEE), 2015 IEEE 3rd Workshop on Advances in, Issue Date: 13-14 Nov. 2015. 1-5.p.
[17] SANS Institute InfoSec Reading Room" An Overview of Threat and Risk Assessment"https://www.sans.org/readingroom/ whitepapers/auditing/overview-threat-risk-assessment-76
[18] Emerging Threats.net open rulesets. https://rules.emergingthreats.net/blockrules/compromised-ips.txt
[19] GeoIP location provider MaxMind https://www.maxmind.com/en/home
[20] Quinnell, R. (2015) "Low power wide-area networking alternatives for the IoT", EDN Network [Online] Available: http://www.edn.com/design/systems-design/4440343/Low-power-wide-areanetworking-alternatives-for-the-IoT [Accessed: 04 February 2016].
[21] Shang, X., Zhang, R., Hu, X. and Zhou, Q. (2015) "Design theory, modeling and the application for the Internet of Things service", Enterprise Information Systems, Vol. 10, No. 3, pp. 249-267. ISSN 1751-7575. DOI: 10.1080/17517575.2015.1075592.
[22] Vermesan, O. and Friess, P. (2013) "Internet of things: converging technologies for smart environments and integrated ecosystems", Aalborg Denmark: River Publishers. ISBN 978-87-92982-96-4.

[23] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M. (2015) "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", IEEE Communications Surveys & Tutorials, Vol. 17 No. 4, pp. 2347-2376. ISSN 1553-877x. DOI: 10.1109/COMST.2015.2444095.