IoT in Banking: The trends, threats, and solution

Mardiana Abu Hassan, Nur Azaliah Abu Bakar, Noor Hafizah Hassan

Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia
mardiana.ah@graduate.utm.my; azaliah@utm.my; noorhafizah.kl@utm.my

Article history

Received:
10 May 2021

Received in revised form:
15 May 2021

Accepted:
25 May 2021

Published online:
26 Jun2 2021

*Corresponding author
azaliah @utm.my

Abstract

The Internet of Things is the next step of the digital revolution that will change consumers' lives. The Internet of Things promises to be a worthy representative of an open course in technology, economics, and culture. IoT, without a doubt, has a promising future. The modern consumer actions and uses represent inescapable digital transformations for banking institutions. Emerging digital world developments guide all banking services' digital transformation. However, the security threats of using IoT in banking are increasing. Cybercriminals such as hacking, corruption, and financial violence, data breaches, and financial expenditure risks will continue to trouble the use of IoT in banking. Therefore, this research aims to study the banking industry's existing IoT uses, issues, and challenges adopting the IoT in the banking industry. IoT threats are highlighted in this paper. This article sets out a model dimension of the process monitoring framework for IoT security risk management. Other than that, this paper also studies the existing security risk management model of IoT in banking. Moreover, preventive IoT protection initiatives and approaches to enhance IoT protection by implementing blockchain technology and Control Model Information Structure are addressed in this article

Keywords: *banking, digital trends, internet of things, risk assessment, security threats*

1. Introduction

Interconnected devices, also known as the internet of things (IoT), encompass the networked interconnection of everyday objects. They are all equipped with ubiquitous intelligence [1]. There are many and substantial consequences from such a corpus of technologies; indeed, the IoT increases the internet's ubiquity by integrating objects with interaction capability [2]. The Internet of Things promises to be a worthy representative of a forthcoming revolution in technology, economics, and culture. IoT, without a doubt, has a promising future[2, 3].

The modern consumer actions and uses represent inescapable digital transformations for banking institutions. Thus, emerging digital world developments guide all banking services' digital transformation. These two changes will probably upgrade the old paradigm of banking services that we know, leading to a new type of related banking system, the first brick to transform digital banking. However, the security threats of using IoT in banking are increasing. Cybercriminals such as hacking, corruption, and financial violence, data breaches,

* *Corresponding author. azaliah @utm.my*

and financial expenditure risks will continue to trouble the use of IoT in banking[4, 5].

This paper presents a methodology to encourage an IoT system's safety analysis using nearly fully automated threat modelling and risk evaluation processes. The proposed method relies on a modelling approach to architectural aspects of the IoT system components and their safety features. It enables identifying threats, risk assessment, and selecting appropriate countermeasures to mitigate existing risks. Therefore, our primary research goal is to study the banking industry's existing IoT uses, issues, and challenges adopting the IoT in the banking industry. IoT threats are also highlighted in this paper. Other than that, this paper also studies the existing security risk management model of IoT in banking. Moreover, preventive IoT protection initiatives and approaches to enhance IoT protection by implementing blockchain technology and Control Model Information Structure are addressed in this article.

2. Related Works

Visualise a world where all digital objects can share information and interact. Connected objects can also communicate through the internet and other communication networks with their user. The diversity of IoT interrelation globally will strike 25 billion by 2025. Kevin Ashton at the Massachusetts Institute of Technology (MIT) first came up with the term "Internet of Things" in 1998 and interpreted it as "allowing people and things to be interconnected with any time, anyplace, anything and anyone, typically using any path or network and any services" [6].

IoT has developed in five phases. The first phase is creating the World Wide Web by connecting two computers. The third phase is related to the mobile internet, which connects mobile devices and the internet. The fourth phase is people-internet explaining about the connection enabled by social networks. They advanced to the IoT for globally linked objects [7]. Figure 1 depicts the evolution of IoT Evolution of the Internet in five phases.

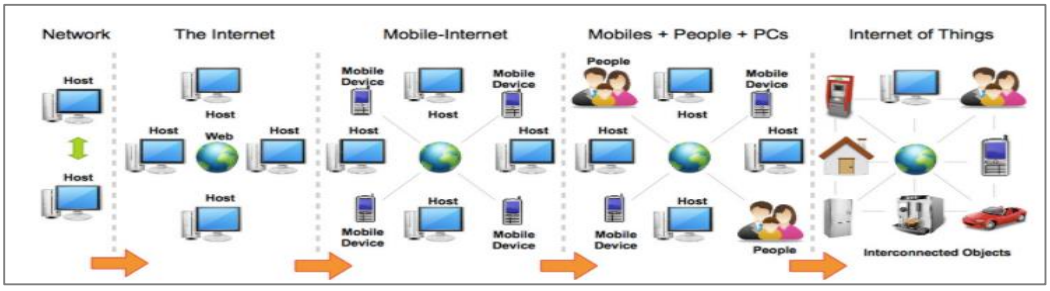

Figure 1. Evolution of Internet of Things [7]

Internet evolution starts with the connection of two computers and then moves towards creating the World Wide Web by connecting many computers. The mobile internet came into being through mobile devices' link to the internet. Then, through social networks, people's identities have joined the internet. Finally, it moves towards the Internet of Things that connects objects to the internet every day.

The IoT overgrowing and it influenced daily life. Interconnected devices are unquestionably a step towards new applications in many sectors of the economy. Service industries such as banking, insurance, transportation would primarily benefit from the rapid, automated processing and sharing of huge data quantities. Consequently, it will promote new business models of sophisticated networking for connected devices.

2.1 IoT in Financial Services

Interconnected devices are unquestionably a chance for banks to remain competitive. Consumers today expect from the Bank and, in particular, the new digital one a great deal of innovation that will provide them with adequate service in their new connected lifestyle[4]. Below we describe six digital developments using IoT, directly affecting financial services.

i. Mobile Banking

Consumers are now demanding fast, easy and instant access to all banking services in this digital age. IoT allows users to use digital devices to access their bank account anytime and anywhere. Presently, most of all digital devices are design with biometric characteristics. Biometrics recognise people's unique physical, behavioural characteristics. It enables access to mobile banking services from any digital device. Currently, E-Wallet is steadily growing, and e-wallet may help users reduce fraud as the data stored in the e-wallet is encrypted [4, 5].

ii. Virtual Money

Blockchain is an advanced technology that will track in the coming years. Many economic sectors could be revolutionised, beginning with banking and insurance. Customer can use securely and without central control to store and communicate information. It appears to be some data repository containing all user exchanges since its inception. The blockchain can be used in three respects: to transfer assets such as currency, securities, improved asset traceability, and automatic contract execution of "smart contracts." It also can be used on IoT platforms to face digital challenges as an analytical model tracking that records the data generated during IoT, ensuring protection through sharp identification rules and finally instant payments among devices and network members[8-10].

iii. Personal Financial Management (PFM)

The PFM solutions kit offers the customer a summary of all the flows from his accounts. Using IoT-generated data, PFM tools can help banks deliver personalised and more targeted services to their customers[11]. Hence, IoT is required to produce notifications to monitor customer usage.

iv. Know Your Customer (KYC)

KYC is using by financial institutions for identification and customer knowledge. Banks apply KYC procedures because it prevents fraud and money laundering. These statistical data can be linked to marketing uses[11, 12]. The IoT integrated with the digitalisation of identity will change customers' financial behaviour to provide related services and products.

v. Cyber Criminality

Financial institutions offer innovative solutions to secure banking transactions. One of the examples of this solution is Multi-Factor Authentication (MFA). MFA is one of the best methods to increase authentication assurance for consumers' confidential web, servers, machines, and mobile applications. Connected devices usually employ multi-factor authentication with a password used in conjunction with a time-boxed token that the staff possesses, push notification to a mobile app, or biometrics[5, 11].

2.2 IoT Challenges and Issues in Banking

Even though IoT would greatly benefit the banking and financial institutions, there are still significant challenges that need to be considered and resolved before adoption in those environments.

i. Data Breach

Data breaches, especially data that contain sensitive intelligence information, can pose a threat. Bank holds valuable information and top confidential data. If this information is breached and made available, it can exploit to initiate multiple social engineering attacks. Data tempering can also be a way to illegally obtain data that contribute to data leakage or data breach[13, 14].

ii. Complex Infrastructure

Above mentioned, IoT is an interconnected device through a network. Many people find it difficult to understand what IoT technologies are all about because they are quite complex to use. When connected through a network, all of the previously mentioned technologies make it possible for them to interact and influence one another. However, when the interaction is broken and a single device removed, the formed system may ultimately break down and lead to huge losses[15]. The main reason that financial and banking institutions shun the use of IoT technology is that many are unwilling to use hardware led by companies they are unaware of and then use programming companies they have never heard of before[11].

iii. No Standard Operating Procedure for Maintainance

There are different types of IoT hardware equipment, including home devices and industrial equipment[13, 16]. They are created by different kinds of manufacturers and require other maintenance requirements. There would be problems caused by a universal standard that can hinder how these devices function and can only be solved if there is only one seller or distributor of these IoT devices. Even then, monopolisation will severely negatively impact the worldwide economy.

2.3 IoT Threats to Banking

The effects of a cyberattack on a banking institution can be horrendous. This threat can also have explosive consequences. Without implementing strong security measures, banking institutions would continue to face the threat of cybercrimes. That estimate is likely inaccurate, as IoT expenditures were expected to increase once vendors gain a clearer understanding of security and privacy risks associated with the IoT[17, 18]. More IoT decision-making will include security spending in the future because of people's awareness of smart devices' vulnerability to hacks.

Some risks are associated with the increase in IoT in the banking industry, such as data capacities always pose a threat to cyber criminals[13]. The sophistication

of IoT infrastructure has allowed tremendous information to be collected. For example, intelligent sensors have been used in machine learning to collect data to increase organisations' value[19]. Furthermore, confidentiality in the IoT setting is always questioned. Regardless of whether insurance is used to validate details, digital aggressors' success is critical[12]. Banking institutions have been the target of device theft from various groups such as hackers, cybercriminals.

These devices, such as laptops and mobile phones, are easy to target because they are small, handy, and easy to remove quickly. The price of stolen laptops, mobile phones, and other handheld electronic devices is not just on the replacement cost. The cost of equipment and accessories, the software installed, the cost of configuring replacement software, and the cost of lost time for the owner while the device replaced[20]. But the more significant cost that a bank has to bear is the potential data leakage and liability resulting from lost confidential valuable, and top-secret intelligence information[18].

Many IoT in financial services devices will be targets for cybercriminals because of the personal information collected and payment capabilities created by the objects[21]. Since financial companies do not control this information, it's vulnerable to threats. Customers must know what data gathered and how they will use it. Top innovations in the banking industry include the following but not limited to:

i. Banking on wearables

Wearable gadgets have been the most influential banks until now, owing to a developing biological system of devices and a generally simple beginning. Many banks now allow credit card credit to watch Apple Watch and Fit Pay applications. Numerous banks are utilising their very own wristbands to offer some contact-free instalments[22].

ii. Proactive service

IoT will substantially enhance monetary and financial administrations' ability to change a financial product or administration choices effortlessly. Suppose there is any uncertainty or concerns about an item. In that case, it can be spotted easily, and the issues resolved as fast as possible. Advisors are also pleased to get past examples to clients, and they manage them accordingly. This development of modern accounting tools can help improve companies' operations [21].

iii. Banking at home

Capital One in the United States currently makes it possible for customers to pay their bills through Amazon's Alexa, yet this is by no means the only retail managing account association to do so, nor will it be the last. Take UK challenger bank Starling, for example, trying different things with Google Home, coordinating its API with a smart speaker to empower clients to bring equalisation issues and instalments through voice directions[23].

2.4 McCumber Cube Security Management Model

John McCumber created a model framework for establishing and evaluating information security (information assurance) programs, known as The McCumber Cube. This security model is depicted as a three-dimensional Rubik's Cube-like grid, as shown in Figure 2.

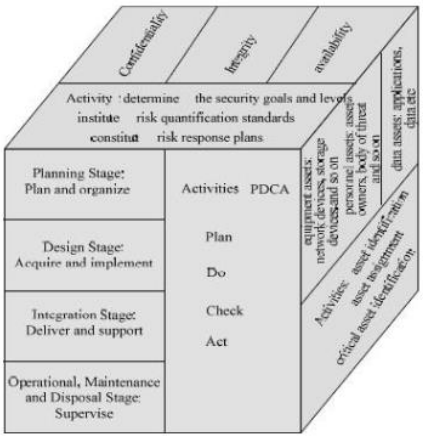

Figure 2. McCumber Cube Security Management Model[24]

i. S-dimension

S-dimension governs the stability and operation of the information system. The S-Dimension aims to protect information systems and activities' reliability, privacy, and accountability. The tasks about management priorities of the S-Dimension include:

1) Risk-taker will define the IoT software and security policies.
2) To initiate risk qualification criteria.
3) Reinforce risk management preparedness.

ii. R-dimension

The R-dimension features support the scale, including infrastructure and associated events. Data management tools include network and storage units, network properties, wealthy owners, and offending organs for private properties and documents and software for computer properties.

iii. P-dimension

P-dimension is an approach that regulates the dimension. The process of preparation, start-up, the architecture of the information system life cycle is carried from the threat risk assessment and monitoring process.

This study adopts this model to design the IoT Security Risk Management Process for the banking industry.

3. Methodology

The lack of an integrated threat model to IoT systems that can consider the specific characteristics of all possible components of a complex IoT infrastructure is also a problem. This shortage makes it very difficult for actual IoT deployments to perform an efficient security evaluation. Although the literature is quite generous about threats to specific alternatives and technologies, a complete and consistent list of threats applicable to a system to be deployed on production is difficult to find. Finally, the key players involved in the setup and implementation of an IoT device must be considered. It is worth noting that these tasks are mostly assigned to technicians without particular experience because it is often not economically feasible to include highly trained and costly security experts. For instance,

implementing a smart home device is linked to the provider's home network and provides total control over the building. While this opens up a great deal of danger, a trained security professional is not involved in configuring such a device at implementation.

We propose a modelling approach based on the ISO standards guidelines to address such issues. This model allows us to build a threat model for a particular IoT system deployment in a semi-automated way and support safe design activities by establishing a range of security measures to mitigate existing ones. In particular, security countermeasures are indicated in security controls defined in the NIST Security Control System. It is quickly and easily accessible to map other existing structures, making our method versatile and easy to reuse in various contexts. The methodology introduced in this study makes almost completely automatic threat modelling and risk evaluation of IoT systems following the standard IoT features. The suggested methodology illustrated in Figure 3

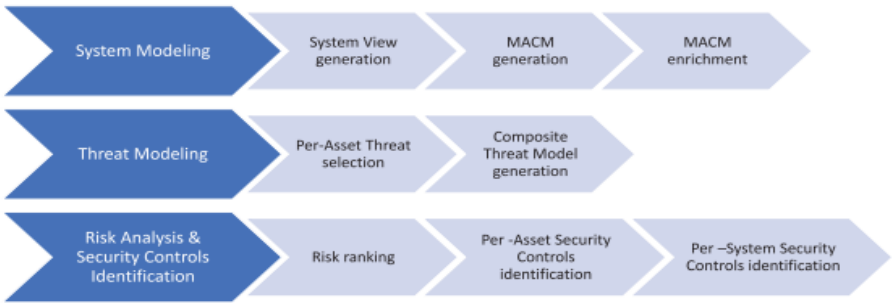

Figure 3. IoT automated risk analysis methodology

Figure 3 comprises three key steps:

1) System modelling is intended to evaluate the IoT system to define the key assets to secure and model them properly.
2) Threat modelling focuses on the detection of device threats.
3) Risk analysis and security control are intended to estimate each perceived hazard and identify countermeasures to mitigate current safety control risks.

5. Proposed Work

There are many advantages of using IoT in the banking sector. For example, there are numerous types of IoT wearable banking equipment produced by various manufacturers and need a different maintenance approach. A defect in IoT functionality can result from the lack of a standard. While every manufacturer agrees to use basic standards, it is always important to fix technical problems. Besides, IoT has allowed wealth management application, alarming consumers if their account is targeted[18].

However, IoT will produce vast data and additional costs to maintain and safeguard them. Organisations do not have IoT data testing systems available for errors and omissions. Therefore data quality is not always accurate. IoT allows the banking sector to makes any payment. As a result, technology allows for a stable

and controlled international trade environment in which all payments are handled via an intelligent sensor network and connected devices. IoT should also be the main protective regulator[18]. As IoT adoption continues to expand, researchers are also developing a range of reference architectures, structures, guidelines, mechanisms, and standards relevant to IoT.

With a rapidly growing number of IoT systems with an increased number of things and devices, a more significant number of interactions will take place. These new connected devices would use the internet as a communication resource. This will trigger several challenges, as most of the stored data on central servers in IoT systems are preserved. Only those devices which are connected to the centralised network can obtain the data from the servers. The majority of IoT systems are implemented using a centralised server approach. IoT systems collect information from the sensor devices, focusing the data such that it is appropriately transmitted to the server through a wired or wireless network or the internet.

Correspondingly, the existing internet infrastructure's processing capabilities may not be supported effectively for the large-scale IoT system. Expansion in the internet infrastructure must manage the vast data processed in large-scale IoT systems. The best solution to do this is to have decentralised or distributed networks where Peer-to-Peer Networking (PPN), Distributed File Sharing (DFS), and Autonomous Device Coordination (ADC) functions can be used[25].

This study will clarify the value of selecting a blockchain technology solution. Blockchain technology offers a better solution to improve the IoT security in IoT systems. Blockchain can perform these three functions, allowing IoT systems to track many connected and networked devices. BC allows IoT systems to process transactions between coordinated devices. BC will enhance IoT systems' privacy and reliability, making them more robust[26]. BC allows peer-to-peer messaging faster with the distributed ledger's help, as shown in Figure 5.

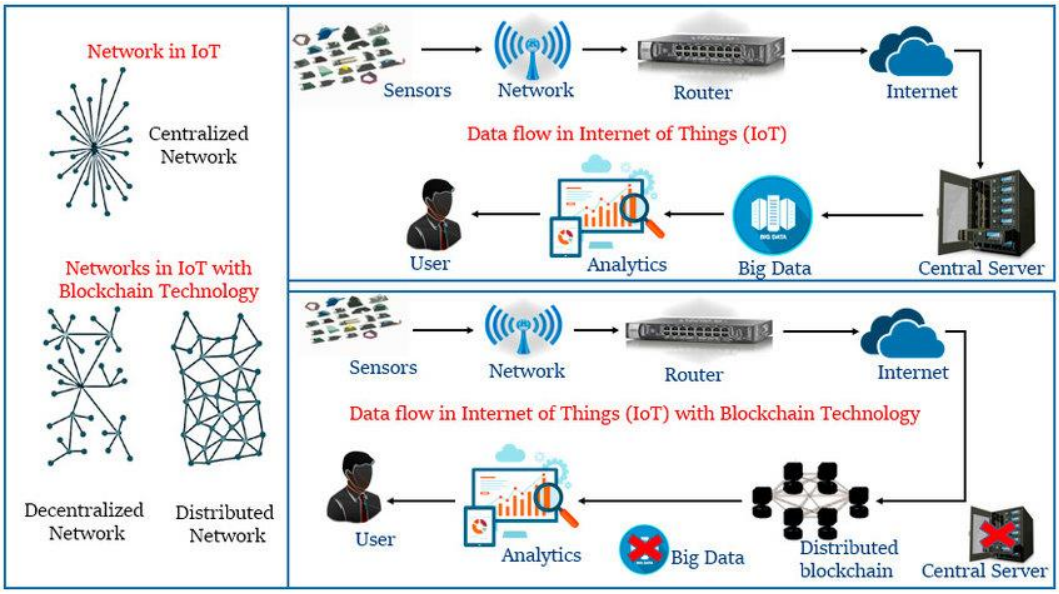

Figure 4. IoT with Blockchain Technology[26]

The IoT data flow process with BC technology is different from the IoT system alone. In IoT with BC, the data flow is from the sensor-network-router-internet-distributed blockchain-analytics-user. Here, the distributed ledger is tamper-proof that does not allow incorrect interpretation, incorrect authentication of the data. BC complexly eliminates single thread communication (STC) in IoT to make the system more trustless. With BC's adoption in IoT, the data flow will become more reliable and secure[5, 26].

The next suggestion to propose the Banking IoT Security Risk Management Model is by adopting the McCumber Cube Security Management Model. Organisations should identify the vulnerabilities and drawbacks of the risk management model, and they should always get ready to face the emerging security conditions. Several solutions have been designed to ensure the risk is still in the range outside the IoT environment. Figure 6 depicts an improved risk management model proposed by the abovementioned researchers. There is 3 phase involved in this proposed model.

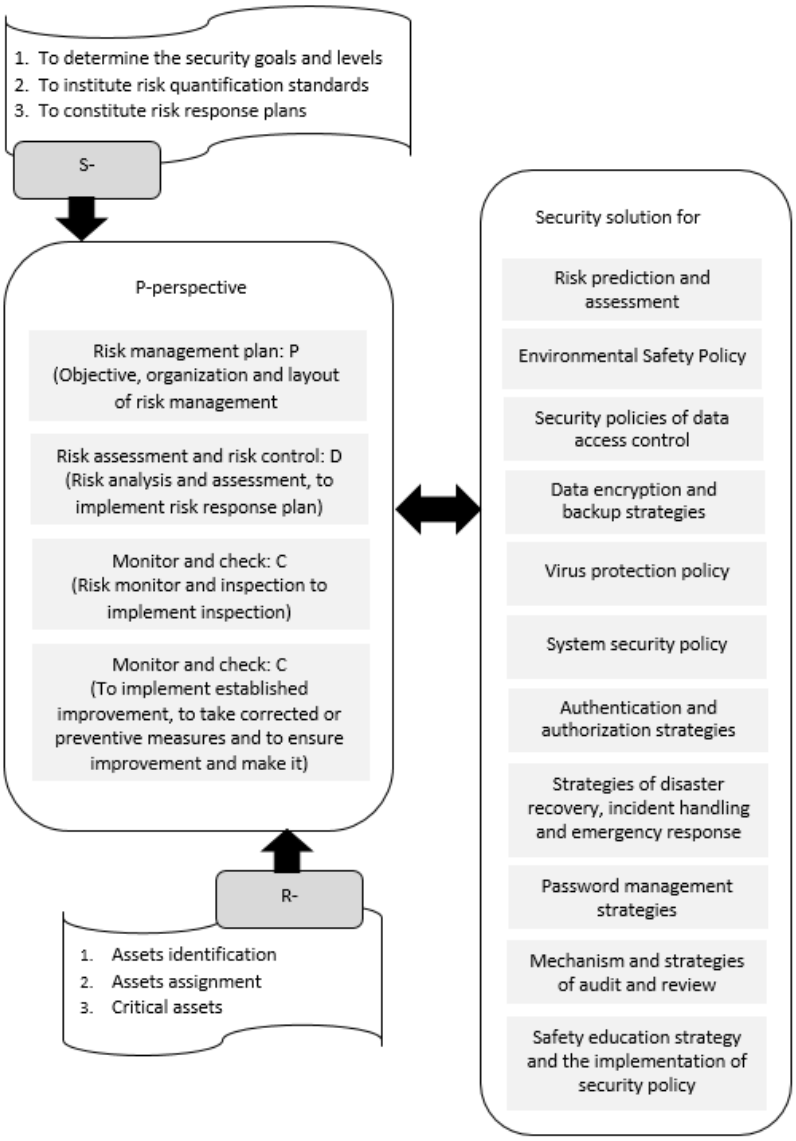

Figure 5. Proposed Risk Management for Banking

i. R-Viewpoint – Protecting Information Assets

R-Viewpoints focuses on protecting information assets as *"any software, hardware, data, administrative, physical, communications, or personnel resource within an information system."* This phase is vital to determine, implement, and enhance information assets' security in organisations to maintain their cash flow, competitive strategies, and identity.

ii. S-Analysis – Analyse application goals

While S-Analysis focuses on risk assessment for strategic objective, market purpose, security purposes, and enforcement objective, by designing policies and procedures based on internal risk tolerance and document workflows, banks should be ready for any form of cybercriminal attacks.

iii. P-Perspective -A lifecycle approach

P-Perspective look at the risk assessment at various life cycle stages. Centralise IoT control for events across functional silos both inside and outside the banks' glass walls to ensure simple, coordinated and automated responses. This centralisation allows stakeholders to have a single view on the "risk," the "bad thing," or "what is affected," which assists departmental leaders in making informed decisions about projects to minimise their effect on them. Hence the P-Perspective follow the Plan-Do-Check-Act (PDCA) steps to ensure its secured process is in place.

6. Conclusion

Our goals are to safeguard the IoT by proposing a framework contrary to a collective solution. This paper presents a methodology to encourage an IoT system's safety analysis using nearly fully automated threat modelling and risk evaluation processes. Moreover, the proposed methodology relies on a modelling approach to architectural aspects of the IoT system components, and their safety features have been introduced. It enables identifying threats, risk assessment, and selecting appropriate countermeasures to mitigate existing risks.

The future work will focus on IoT-related compliance, including current compliance, best practices and the review of recent attempts to regulate IoT in general. As IoT adoption continues to expand, many reference architectures, structures, guidelines, mechanisms, and standards relevant to IoT are also developing to enhance IoT security. This study had clarified the value of selecting a blockchain technology solution as blockchain technology offers a better solution to improve the IoT security in IoT systems.

Acknowledgments

These should be brief and placed at the end of the text before the references.

References

[1] S. Akter, K. Michael, M. R. Uddin, G. McCarthy, and M. Rahman, "Transforming business using digital innovations: The application of AI, blockchain, cloud and data analytics," *Annals of Operations Research,* pp. 1-33, 2020.

[2] Y. Velayutham, N. A. A. Bakar, N. H. Hassan, and G. N. Samy, "IoT security for smart grid environment: Issues and solutions," *Jordanian Journal of Computers and Information Technology,* vol. 7, no. 1, pp. pp. 13-24, 2021.

[3] N. A. Bakar, W. M. W. Ramli, and N. H. Hassan, "The internet of things in healthcare: an overview, challenges and model plan for security risks management process," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS),* vol. 15, no. 1, pp. 414-420, 2019.

[4] A. Alti and A. Almuhirat, "An Advanced IoT-Based Tool for Effective Employee Performance Evaluation in the Banking Sector," *Journal homepage: http://iieta. org/journals/isi,* vol. 26, no. 1, pp. 103-108, 2021.

[5] B. Li, R.-s. Chen, and H. Wang, "Using intelligent prediction machine and dynamic workflow for banking customer satisfaction in IoT environment," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-10, 2021.
[6] TrendMicro. (2019, 15/05/2020). *Industrial Internet of Things (IIoT)*. Available: https://www.trendmicro.com/vinfo/us/security/definition/industrial-internet-of-things-iiot
[7] J. Wang, M. K. Lim, C. Wang, and M.-L. Tseng, "The evolution of the Internet of Things (IoT) over the past 20 years," *Computers & Industrial Engineering*, vol. 155, p. 107174, 2021.
[8] Y. Sharma, B. Balamurugan, N. Snegar, and A. Ilavendhan, "How IoT, AI, and Blockchain Will Revolutionize Business," *Blockchain, Internet of Things, and Artificial Intelligence*, p. 235, 2021.
[9] R. Garg, P. Gupta, and A. Kaur, "Secure IoT via Blockchain," in *IOP Conference Series: Materials Science and Engineering*, 2021, vol. 1022, no. 1, p. 012048: IOP Publishing.
[10] P. Garg, B. Gupta, A. K. Chauhan, U. Sivarajah, S. Gupta, and S. Modgil, "Measuring the perceived benefits of implementing blockchain technology in the banking sector," *Technological Forecasting and Social Change*, vol. 163, p. 120407, 2021.
[11] G. Suseendran, E. Chandrasekaran, D. Akila, and A. S. Kumar, "Banking and FinTech (Financial Technology) Embraced with IoT Device," in *Data Management, Analytics and Innovation*: Springer, 2020, pp. 197-211.
[12] L. Denis, D. T. K. Kumar, D. Karthikeyan, and D. S. Sasipriya, "Offline Mobile Based Otp Technology for Enterprise IoT Enabled Architecture in Banking Cash Logistics & ATM Operations," *International Journal of Advanced Research in Engineering and Technology (IJARET)*, vol. 11, no. 1, pp. 61-69, 2020.
[13] F. Khanboubi and A. Boulmakoul, "Risk-Driven Analytics for Banking IoT Strategy," in *Internet of Things, Smart Computing and Technology: A Roadmap Ahead*: Springer, 2020, pp. 189-215.
[14] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702-2733, 2019.
[15] S. Rizvi, R. Orr, A. Cox, P. Ashokkumar, and M. R. Rizvi, "Identifying the attack surface for IoT network," *Internet of Things*, vol. 9, p. 100162, 2020.
[16] J. Pacheco and S. Hariri, "IoT security framework for smart cyber infrastructures," in *2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS* W)*, 2016, pp. 242-247: IEEE.
[17] N. Scheidt and M. Adda, "Threats in industrial IoT," in *Internet of Things, Threats, Landscape, and Countermeasures*: CRC Press Inc, 2021, pp. 137-166.
[18] M. Bansal, N. Oberoi, and M. Sameer, "IoT in Online Banking," *Journal of Ubiquitous Computing and Communication Technologies (UCCT)*, vol. 2, no. 04, pp. 219-222, 2020.
[19] R. El-Aziz, S. El-Gamal, and M. Ismail, "Mediating and Moderating Factors Affecting Readiness to IoT Applications: The Banking Sector Context,"

International Journal of Managing Information Technology (IJMIT) Vol, vol. 12, 2020.

[20] B. Liao, Y. Ali, S. Nazir, L. He, and H. U. Khan, "Security analysis of IoT devices by using mobile computing: a systematic literature review," *IEEE Access*, vol. 8, pp. 120331-120350, 2020.

[21] S. Ammirato, F. Sofo, A. M. Felicetti, and C. Raso, "A methodology to support the adoption of IoT innovation and its application to the Italian bank branch security context," *European Journal of Innovation Management*, 2019.

[22] T. Alladi, V. Chamola, B. Sikdar, and K.-K. R. Choo, "Consumer IoT: Security vulnerability case studies and solutions," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 17-25, 2020.

[23] D. Daniel, N. Nicolas, C. Ozden, B. Rijkers, M. Viollaz, and H. Winkler, "Who on Earth Can Work from Home?," ed: The World Bank, 2020.

[24] C. Easttom and W. Butler, "A modified McCumber cube as a basis for a taxonomy of cyber attacks," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 2019, pp. 0943-0949: IEEE.

[25] K. Ali and S. Askar, "Security Issues and Vulnerability of IoT Devices," *International Journal of Science and Business*, vol. 5, no. 3, pp. 101-115, 2021.

[26] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," *Procedia Computer Science*, vol. 132, pp. 1815-1823, 2018.