A Review of IoT Security Risk Management for The Transportation Industry

Muhammad Syahreen Zulkifli[1], Nur Azaliah Abu Bakar[2]

[1,2,3,4,5,6]Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia,54100 Kuala Lumpur

[1]muhammadsyahreen@graduate.utm.my,[2]azaliah@utm.my

Article history

Received:
10 Sept 2022

Received in revised form:
29 Nov 2022

Accepted:
1 Dec 2022

Published online:
15 Dec 2022

*Corresponding author
muhammadsyahreen
@garduate.utm.my

Abstract

Adapting a new technology such as the Internet of Things (IoT) has played a crucial role in managing facilities and transportation to improve the business process with a highly efficient system. The IoT is a commonly implemented ecosystem that interconnects numerous computing devices with an unprecedented identifier and the capability to systematically transfer data over the network without human intervention. However, IoT devices are vulnerable to security breaches alongside rapid development. In addition, the business is prone to becoming a cybercrime target without appropriate security practices. This paper aims to review IoT security risks, discloses gaps in security risk management, and present NIST Special Publication (S.P.) 800 as the proposed framework for security risk management in the transportation industry. The framework yields a systematic methodology for managing cybersecurity risk within the industry; therefore, it mitigates IoT security risk in the industry.

Keywords: *cybercrime, IoT risk management, IoT devices, risk management, transportation risk.*

1. Introduction

A new paradigm known as the Internet of Things (IoT) links computing devices together by automatically exchanging data via a wireless network without the need for human interaction. IoT ecosystems are made up of embedded intelligent devices that gather, send, and respond to the dataset that they have collected from their surroundings. The devices needed a special interaction application, network connectivity, and a communication protocol [1]. IoT is crucial to business, particularly for industry 4.0 and its potential to boost annual revenue, reduce operating costs, and increase operational efficiency [2]. Figure 1 below shows an illustration of the IoT ecosystem.

* *Corresponding author. muhammadsyahreen@graduate.utm.my*

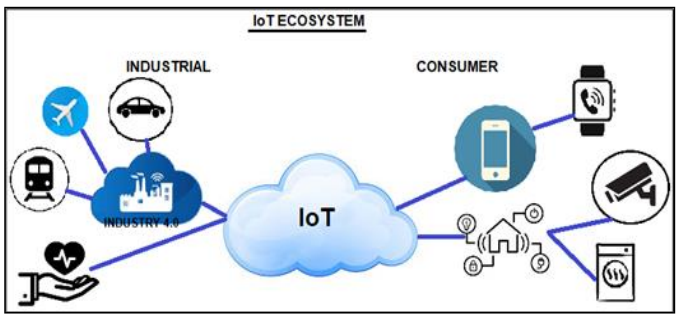

Figure 1. Simple LBS Architecture

All businesses have seen exponential development in the IoT environment, but not all industry players are prepared for significant changes and difficulties [3]. Machine learning models in several businesses must deal with massive data produced by IoT devices [4]. Industrial digitalization must be enabled by digital transformation in order to increase profitability and return on investment. Malware attacks are the primary threats in IoT as the traditional protection mechanisms such as firewalls and Intrusion Detection Systems (IDS) are insufficient as the countermeasure for cybersecurity attacks [5].

This paper discusses the gap in IoT ISRM among the practitioners and organizations that did not apply adequate security protection technologies [6]. The significant security challenges in the IoT ecosystem that threaten the consumer and the security infrastructure are also discussed in the following section. In addition, implementing security risk management based on the NIST framework is the determinant of success and achieving an optimal profit for the transportation industry [7].

Hence, this paper reviews the controls in Information Security Risk Management (ISRM) that handles potential risks in the IoT for the transportation industry and presents the Risk Management Framework (RMF) strategy. Therefore, the significant purpose of establishing adequate risk management is to fill in the security gaps by:

a. Implementation of significant controls efficaciously and consistently in the security risk management process.

b. Adopting the changes in the business workflow and process.

c. Ameliorate the ability to respond to threats, vulnerabilities, and cyberattacks.

d. Operate protective security performance and improvements.

The expected results indicate that the NIST SP800 framework reduces security threats by accessing vulnerability identification, and security risk management aids in prioritizing business decisions in the transportation industry.

2. Cloud Computing Implementation in SMEs

IoT incorporates multiple domains and devices connected to exchange data and information extensively. Therefore, the IoT immediately become a prime target for data breaches and information security incidents [8]. Even though the reported data

breaching incident contributed to increased IoT risk awareness, insecure devices are still being sold and distributed to the market leading to privacy violations, financial losses, and even fatalities [9]. In this section, this paper will focus on the IoT security challenges in the transportation industry. In order to establish a secure and well-connected device in the IoT network, the IoT devices face countless security and privacy challenges due to heterogeneity, and multiple interconnected objects, which are categorized below subsections.

2.1 Authentication and Authorization

Authentication is a process of regulating the validity of a connected user, and authorization is a process of determining user access level. Although a public key cryptosystem is introduced and widely used in most cases for producing authentication or authorization systems, the vulnerable aspect lacks the global root certificate authority.

Implementing an Identity Access Management (IAM) system in IoT ensures the security, authenticity, and integrity of data on connected devices and resources on the server [10]. IAM is generally referred to as the set of regulations and technological tools that guarantee only individuals with the proper authorization can access network resources within a specific organization. Identity management systems control the authentication access to resources within the organization and monitor the activities.

2.2 User Privacy and Data Protection

The IoT ecosystem's nature interconnects and exchanges data over the Internet, which is vulnerable to user data and privacy [11]. The noticeable vulnerabilities in IoT include security breaches, privacy and data protection concerns among the industry player. Hence, the effectiveness of the IoT infrastructure is measured by the ability to protect the user's data and privacy [12]. Therefore, user privacy and data protection awareness are vital in IoT and are classified as:

a. self-control and awareness of personal information from unauthorized use.

b. awareness of potential privacy risks obtruded by connected services and devices in the environment.

c. user control over the information passed through the connected systems and devices.

2.3 Ransomware Attack

Ransomware is classified as malware that sabotages documents by applying encryption to the file documents while the infected computer is still accessible. The attackers then blackmailed their victims into paying the ransom through undetectable Bitcoin currency before the victim could access their encrypted document files or data [13]. Unfortunately, no tools on the market can reverse engineer the document file's encryption.

By far, preventing infection is the best outcome; the organization should be aware of the new generation of self-propagating ransomware that spreads across networks utilizing stolen credentials and exploiting vulnerabilities [14]. Additionally, the

organization must monitor and minimize access level and permission to the IoT devices and secure all network endpoints.

2.4 End-to-End Devices

Multiple devices interconnecting in the IoT networks required a security solution to prevent internal and external attackers from manipulating the connected devices. Any device compromised with security threatens the network and the infrastructure. Furthermore, the attacker took advantage of the vulnerabilities in the IoT devices and launched sophisticated encryption of the victim's data. Hence, securing IoT devices from the end-to-end connection is crucial to ensure data security and privacy. Therefore, implementing security protocols and encryption methods is vital to handle this challenge.

2.5 Security Planning and Risk Management

The security risk is described together with its likelihood and consequences [15]. Potential security risks are typically caused by poor systems, people—such as hackers or human error—inefficient company processes or procedures, criminality, assaults, or unforeseen natural occurrences.

Therefore, planning for security comprises a scalable control for potential installation and assessment in response to a changing danger. Table 1 shows the business impact level.

Table 1. The Business Impact Level

No.	Business Impact Level	Consequence of Threat
1	Low Impact	Insignificant damage to the transportation industry
2	Low to Medium Impact	Limited damage to the transportation industry
3	High Impact	Significant damage to the transportation industry
4	Extreme Impact	Severe damage to the transportation industry
5	Catastrophic Impact	Exceptionally grave damage to the transportation industry

Risk management requires full-scale involvement from the business owner and third parties. Fundamentally, risk management is a process integrated into the business process and not as a separate entity [15]. This paper reviews the controls in Information Security Risk Management (ISRM) that handles potential risks in information technology.

The main objective of ISRM processes is to treat risk in the transportation industry after examining the risk assessment. Therefore, developing an ISRM Strategy for the transportation industry should involve five stages [16], shown in table 2 below.

Table 2. Stages in ISRM

Stage	ISRM Control	Description
1	Business Awareness	To understand and measure the current business status and business strategy in the market space.
2	Strategy Definition	To identify the point of arrival based on business requirements and guidance to meet security compliance.
3	Strategy Development	To define the governance model in modular format and inventory of available services and the industry's capabilities.
4	Metrics and Benchmarking	To ensure industry-standard alignment with KPIs' guidelines to measure the ISRM strategy's effectiveness.
5	Implementation and Operation	To apply the controls, capabilities, guidelines, and standards should follow local enforcement rules and regulations.

The strategic plan's ability to offer an information infrastructure protection roadmap will determine how effective the ISRM framework is. ISRM has traditionally been viewed as a component of an I.T. function and a strategic business plan.

However, because ISRM is so essential, it necessitates the development of a different strategy to guarantee that business objectives can be supported. Therefore, after the business accomplishes measuring the strategy plan above, the following steps are implementing the ISRM framework based on categorizing, selecting controls, implementation controls, authorization, and monitoring controls.

3. Methodology

In the previous section, this paper presented that IoT device security vulnerabilities could generate spillover risks to individual safety, privacy, and data protection and can be exploited en masse to attack part of the Internet's critical infrastructure. Next, this paper discusses the research methodology through the NIST RMF process. This paper methodology comprises three steps which are i) Investigation of the current risk management framework by conducting literature analysis, ii) Review of the vital process in risk management framework, and iii) Propose the steps to assist the company in adopting the framework.

Risk management in the IoT ecosystem addresses the process of managing security risks. A large and significant literature addresses IoT security risk management issues. Given the pervasive impact of digital computerized information systems on every conceivable discipline, discussions on the topic of security risk management have varied widely. Indeed, these discussions have focused on issues such as the definition of IoT security risk [17] and information security policy [18]. Certainly, a comprehensive approach to cybersecurity risk management requires understanding all the above topics. Thus, it is unsurprising that many of the aforementioned references address several underlying cybersecurity risk management issues.

This paper uses a traditional literature review search to identify security risk management in the transportation industry using a public database such as Google Scholar. The information was derived from previous studies that focused on the cybersecurity framework of the IoT ecosystem.

Numerous risk management frameworks coexist and compete. This paper focuses on the National Institute of Standards and Technology (NIST) Cybersecurity Framework, one of the most well-known cybersecurity frameworks [19]. Cybersecurity under the NIST framework is appropriate for embedding IoT technology, even though several frameworks are available to aid the transportation industry build an ISRM framework. Version 1.1 of the NIST, released in April 2018, improves and clarifies version 1.0, released in February 2014.

The updated NIST framework was developed due to its adaptability and is advised for new and experienced users. Six components comprise the risk management process, and the necessary supporting documentation is based on the NIST SP800 framework. Initially, a more comprehensive range of sectors and diverse types and sizes utilized NIST's approach to protect critical infrastructure [20]. In addition, this paper believes that the framework gave companies direction and customization options to achieve their particular business and mission goals.

4.0 Results

The result section comprises two subsections: the literary analysis of the existing IoT Risk Management Framework and the Final Review section that presents the Input and Output of the proposed NIST RMF Processes.

4.1 Review of Existing IoT Risk Management Framework

The transportation industry potentially improves IoT security and minimizes security risk by performing risk assessments based on the NIST SP800 framework [21]. The NIST cybersecurity framework focuses on IoT infrastructure treatment with an enterprise risk management mechanism, which is most suitable for adoption in the transportation industry.

The NIST framework, for instance, is appropriate for businesses in the transportation sector or those whose operations depend on the mobility of vehicles. The NIST introduced RMF for large-scale architecture consists of the seven processes based on NIST 800-37, Revision 2 (2018), listed in figure 2 below.

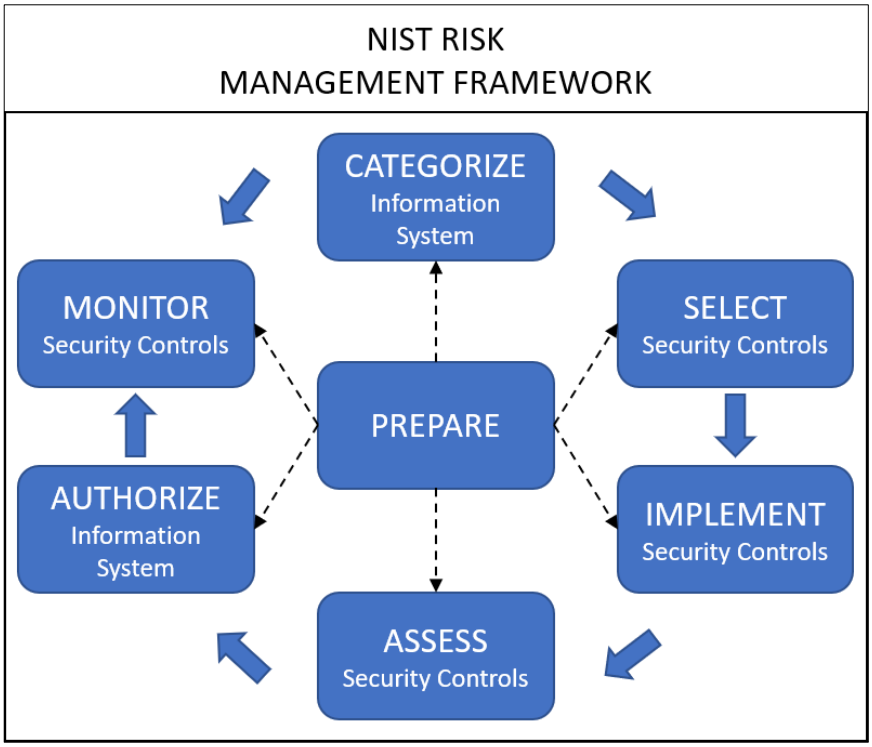

Figure 2. NIST RMF Strategy Revision 2

Hence, implementing the framework would aid the company in facilitating the agreement between stakeholders and leadership on risk tolerance and other strategic risk management issues. These understandings, in turn, can guide the organization in security project prioritization and funding. Therefore, one of the essential pilot outcomes was proving the value of establishing cybersecurity protection in IoT architecture through internal dialogue based on the threats, vulnerabilities, and impacts the business faces [23].

In addition, this paper proposed the steps to assist the company as the countermeasures in the transportation industry based on NIST RMF revision 2 published in the year 2018, listed in table 3.

Table 3. NIST RMF Strategy Revision 2

No	Process	Input	Output
1	Prepare	• Organizational security and privacy policies and procedures; organizational charts.	• Documented Risk Management Framework role assignments.
2	Categorize	• System design and requirements documentation; authorization boundary information; • list of security and privacy requirements allocated to the system,	• A security categorization of the system, including the information processed by the system represented by the organization-identified information types, is completed.

		system elements, and the environment of operation;	• Documented system description.
3	Select Security Controls	• Security categorization; organization- and system-level risk assessment results; system element information; system component inventory; list of security and privacy requirements	• An organizational risk management strategy is developed. • Controls selected for the system and the environment of operation.
4	Implement Security Controls	• Approved security and privacy plans; system design documents; organizational security and privacy policies and procedures; business impact or criticality analyses; enterprise, security, and privacy architecture information;	• Controls specified in the security and privacy plans are implemented. • The security and privacy plans are updated based on information obtained during the implementation of the controls.
5	Assess Security Controls	• The assessment team is selected to conduct the control assessments. • Security, privacy, and SCRM plans; program management control information; common control documentation; organizational security and privacy program plans;	• Security and privacy assessment report on findings and recommendations. • Developed a plan of action and milestones on unacceptable risks identified in security and privacy assessment reports.
6	Authorize	• Security and privacy plans; security and privacy assessment reports; plan of action and milestones; supporting assessment evidence or other documentation, as required.	• Authorization package with an executive summary, which generated from a security or privacy management tool
7	Monitor	• Organizational continuous monitoring strategy; organizational configuration management policy and procedures; organizational policy and procedures for handling unauthorized system changes;	• Updated security and privacy plans; updated plans of action and milestones; updated security and privacy assessment reports.

4.2 Final Review

This paper discusses the security challenges and gaps in IoT among the practitioners and organizations that did not apply adequate security protection technologies. The significant security challenges in the IoT ecosystem that threaten the consumer and the security infrastructure are also discussed. This paper then reviewed the security challenges in the IoT environment.

Implementation of identity access management ensures authentication and authorization protection. In order to secure user privacy and data protection, this paper highlights the importance of user awareness and access control privileges. A ransomware attack can be prevented by securing all endpoints, monitoring and minimizing access and user permission to the IoT devices. In addition, securing end-to-end devices through encryption methods is vital to ensure overall security [24].

This paper reviewed IoT security risks and disclosed gaps in security risk management by proposing an RMF based on NIST SP 800 revision 2, and steps description to assist the organization. This paper believes that implementing the NIST RMF and efficiently addressing each determinant will reduce the existing and future security risks in IoT [25].

The proposed NIST RMF Strategy focusing on IoT for the transportation industry comprises preparation, categorization, selection, implementation, assessment, authorization, and monitoring. In this framework, each determinant is designed to safeguard information on the IoT devices in the new technology wave. In addition, this framework is believed to assist security officers in enhancing and improving the current IoT architecture and mitigating technology risks such as cyber-attacks, data breaches, and ransomware attacks in the industry. This paper finalized the proposed framework in Figure 3 below shows the NISK RMF, including input, process, and output.

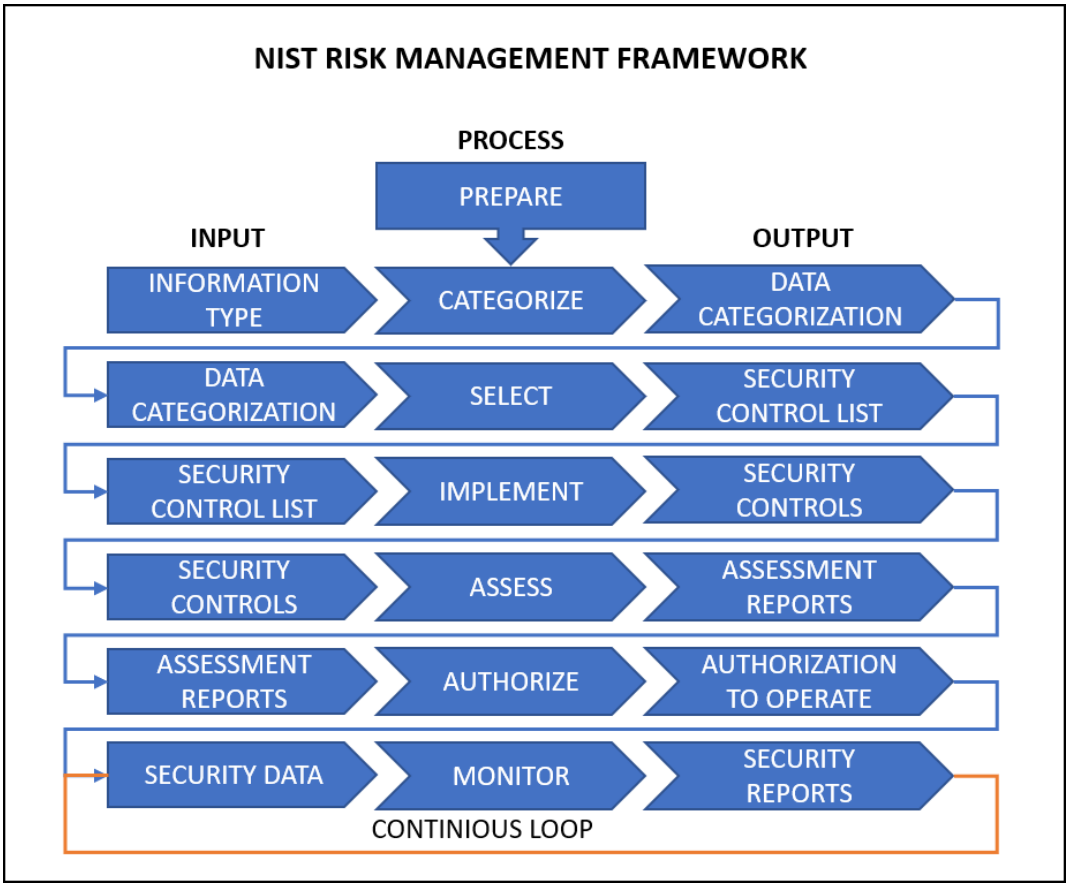

Figure 3. Input and Output of the Proposed NIST RMF Processes

The risk management approach described above is concerned with choosing the right level of security as needed by information security. With the help of this alternative RMF depiction, the transportation sector may better grasp the security life cycle from a different angle. The result of one process is the input of the

following process, with the exception of the initial and last phases. This process flow implies that the accomplishment of the preceding stage is necessary for the success of subsequent steps.

4. Conclusion

IoT is a growing technology that significantly improves the transportation industry [26]. The IoT is recognized for delivering better externalities, but it also needs a regulatory framework that can keep up with emerging, challenging-to-manage negative externalities that are frequently globally networked. In addition, it is crucial to be aware of the difficulties brought on by such revolutionary communication and computing capabilities, particularly those pertaining to security, privacy, and data protection. Therefore, adopting an information security framework is crucial to protect the transportation industry from possible malicious attacks in the IoT ecosystem. This paper reviews the significant threats and appropriate solutions by identifying the industry's gaps in security risk management. Furthermore, the study evaluates the NIST framework to address the security and privacy challenges across the transportation industry boundaries because the controls are flexible and customizable based on the industry requirements and risk management.

As future work, the study shall focus on the extended NIST framework's characteristics and align with the company's assets, business requirements, and goals.

Acknowledgements

This paper describes work undertaken in the context of Risk Management for the organization in the transportation industry based on the NIST SP800 framework in the context of IoT. We sincerely thank the Universiti Teknologi Malaysia (UTM) for organizing Razak Annual Technology, Informatics and Policy Seminar (RATIPS) 2022 by providing a platform for conducting research and education in the field of informatics.

References

5.1. Journal Article

[1] I. Lee, "The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model," *Internet of Things*, vol. 7, p. 100078, 2019, doi: https://doi.org/10.1016/j.iot.2019.100078.

[2] E. Manavalan and K. Jayakrishna, "A review of Internet of Things (IoT) embedded sustainable supply chain for industry 4.0 requirements," *Comput Ind Eng*, vol. 127, pp. 925–953, Jan. 2019, doi: 10.1016/j.cie.2018.11.030.

[3] T. Saarikko, U. H. Westergren, and T. Blomquist, "The Internet of Things: Are you ready for what's coming?," *Bus Horiz*, vol. 60, no. 5, pp. 667–676, Sep. 2017, doi: 10.1016/j.bushor.2017.05.010.

[4] M. S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, and A. P. Sheth, "Machine learning for internet of things data analysis: a survey," *Digital Communications and Networks*, vol. 4, no. 3. Chongqing University of Posts and Telecommunications, pp. 161–175, Aug. 01, 2018. doi: 10.1016/j.dcan.2017.10.002.

[5] I. Lee, "Internet of Things (IoT) cybersecurity: Literature review and iot cyber risk management," *Future Internet*, vol. 12, no. 9. MDPI AG, Sep. 01, 2020. doi: 10.3390/FI12090157.

[6] I. Brass and J. H. Sowell, "Adaptive governance for the Internet of Things: Coping with emerging security risks," *Regul Gov*, vol. 15, no. 4, pp. 1092–1110, Oct. 2021, doi: 10.1111/rego.12343.

[7] O. M. Araz *et al.*, "Role of Analytics for Operational Risk Management in the Era of Big Data," 2020.
[8] S. Bhattarai and Y. Wang, "End-to-end trust and security for Internet of Things applications," 2018. Accessed: Oct. 12, 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8352081/
[9] IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), "IoTSM: an end-to-end security model for IoT ecosystems," IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)., 2019.
[10] P. R. Carnley and H. Kettani, "Identity and Access Management for the Internet of Things," *International Journal of Future Computer and Communication*, vol. 8, no. 4, pp. 129–133, Dec. 2019, doi: 10.18178/ijfcc.2019.8.4.554.
[11] M. M. Ogonji, G. Okeyo, and J. M. Wafula, "A survey on privacy and security of Internet of Things," *Computer Science Review*, vol. 38. Elsevier Ireland Ltd, Nov. 01, 2020. doi: 10.1016/j.cosrev.2020.100312.
[12] C. Chong, K. Lee, and G. Ahmed, "Improving Internet Privacy, Data Protection and Security Concerns," *International Journal of Technology, Innovation and Management (IJTIM)*, vol. 1, no. 1, 2021, [Online]. Available: https://journals.gaftim.com/index.php/ijtim/issue/view/1PublishedbyGAF-TIM,gaftim.com
[13] M. Humayun, N. Z. Jhanjhi, A. Alsayat, and V. Ponnusamy, "Internet of things and ransomware: Evolution, mitigation and prevention," *Egyptian Informatics Journal*, vol. 22, no. 1. Elsevier B.V., pp. 105–117, Mar. 01, 2021. doi: 10.1016/j.eij.2020.05.003.
[14] S. R. Zahra and C. M. Ahsan, "RansomWare and Internet of Things: A New Security Nightmare," *IEEE 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, pp. 551–555, 2019, doi: 10.1109/CONFLUENCE.2019.8776926.
[15] J. Oehmen, A. Guenther, J. W. Herrmann, J. Schulte, and P. Willumsen, "RISK MANAGEMENT in PRODUCT DEVELOPMENT: RISK IDENTIFICATION, ASSESSMENT, and MITIGATION - A LITERATURE REVIEW," in *Proceedings of the Design Society: DESIGN Conference*, 2020, vol. 1, pp. 657–666. doi: 10.1017/dsd.2020.27.
[16] S. Mohammed, H. R. Arabnia, X. Qu, D. Zhang, T. H. Kim, and J. Zhao, "IEEE ACCESS SPECIAL SECTION EDITORIAL: BIG DATA TECHNOLOGY and APPLICATIONS in INTELLIGENT TRANSPORTATION," *IEEE Access*, vol. 8. Institute of Electrical and Electronics Engineers Inc., pp. 201331–201344, 2020. doi: 10.1109/ACCESS.2020.3035440.
[17] C. Vorakulpipat, E. Rattanalerdnusorn, P. Thaenkaew, and H. D. Hai, "Recent Challenges, Trends, and Concerns Related to IoT Security: An Evolutionary Study," in *International Conference on Advanced Communications Technology (ICACT)*, 2018.
[18] F. Zantalis, G. Koulouras, S. Karabetsos, and D. Kandris, "A review of machine learning and IoT in smart transportation," *Smart Transportation Future Internet*, vol. 11, no. 4. MDPI AG, 2019. doi: 10.3390/FI11040094.
[19] "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," Gaithersburg, MD, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.
[20] P. R. Prameet, "A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard," in *IEEE 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)*, Sep. 2020. doi: 10.2307/j.ctvndv9kx.11.
[21] K. N. Megas, M. Fagan, B. Cuthill, B. Hoehn, D. Lemire, and R. Herold, "Workshop Summary Report for Building on the NIST Foundations: Next Steps in IoT Cybersecurity," Sep. 2022. doi: 10.6028/NIST.IR.8431.
[22] E. Takamura, C. Gomez-Rosa, K. Mangum, and F. Wasiak, "MAVEN information security governance, risk management, and compliance (GRC): Lessons learned," in *IEEE Aerospace Conference Proceedings*, 2014. doi: 10.1109/AERO.2014.6836516.
[23] I. Lee, "Internet of Things (IoT) cybersecurity: Literature review and iot cyber risk management," *Future Internet*, vol. 12, no. 9, Sep. 2020, doi: 10.3390/FI12090157.
[24] S. K. Mousavi, A. Ghaffari, S. Besharat, and H. Afshari, "Security of internet of things based on cryptographic algorithms: a survey," *Wireless Networks*, vol. 27, no. 2, pp. 1515–1555, Feb. 2021, doi: 10.1007/s11276-020-02535-5.
[25] M. al Fikri, F. A. Putra, Y. Suryanto, and K. Ramli, "Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in profit-based organization: Case study of ZZZ information system application in ABC agency," in *Procedia Computer Science*, 2019, vol. 161, pp. 1206–1215. doi: 10.1016/j.procs.2019.11.234.
[26] F. Zantalis, G. Koulouras, S. Karabetsos, and D. Kandris, "A review of machine learning and IoT in smart transportation," *Future Internet*, vol. 11, no. 4. MDPI AG, 2019. doi: 10.3390/FI11040094.