Financial and Economic Risk in Developing Markets
Volume 3, Number 2, 2024

Digital Transformation and IoT in Industry 4.0: Opportunities and Security Challenge

Variandy Tiaraputra[1]

[1] Universitas Diponegoro, Semarang, Indonesia

Abstract

Article history:
Received: August 15, 2024
Revised: September 10, 2024
Accepted: October 19, 2024
Published: December 30, 2024

Keywords:
Cybersecurity,
Digital Transformation,
Efficiency,
Industry 4.0,
Internet of Things.

Identifier:
Zera Open
Page: 167-183
https://zeraopen.com/journal/ferdm

The rapid development of information and communication technology has driven a global digital revolution that fundamentally changes patterns of social interaction, business operations, and organizational management. Within the framework of the Industrial Revolution 4.0, the Internet of Things serves as the backbone of digitalization by connecting physical devices through sensors and intelligent systems capable of generating real-time data for decision-making. This concept enables higher operational efficiency, automation, more accurate predictions, and the creation of new data-driven business models. However, this transformation also brings significant challenges, particularly in terms of cybersecurity, data privacy, and the digital divide, which has the potential to widen inequalities in technology access. This study applies a literature review method to analyze IoT development, its contributions to digital transformation, as well as the risks and opportunities it generates. The findings indicate that IoT can enhance productivity and efficiency across sectors, yet requires robust security strategies and adaptive regulations to ensure sustainable implementation.

1. Introduction

The development of information and communication technology (ICT) over the last two decades has brought significant changes to various aspects of human life, both at the individual, organizational, and global societal levels. The presence of the internet, cloud computing, big data, Artificial Intelligence (AI), and the Internet of Things (IoT) has encouraged the creation of an increasingly complex and interconnected digital ecosystem. This digital revolution marks a paradigm shift towards the Industrial Revolution 4.0, characterized by the integration of the physical and digital worlds through the use of sensors, smart devices, and data-based automation systems (Wu et al., 2022). One of the key technologies in the Industrial Revolution 4.0 is the Internet of Things (IoT), a concept that connects physical devices to the internet to enable automatic data exchange without human intervention. IoT allows companies, governments, and individuals to obtain real-time data that can be used to improve operational efficiency, strengthen decision-making processes, and develop data-based business models (Bhadra et al., 2023).

In the context of the manufacturing industry, IoT even acts as the backbone of smart manufacturing, supporting automation, predictive machine maintenance, and product quality improvement (Wu et al., 2022). Apart from manufacturing, the use of IoT has also expanded to various other sectors, including health, education, agriculture, transportation, and retail business. In the health sector, for example, IoT devices are used to monitor patients' conditions in real-time, increase the efficiency of medical services, and support data-based clinical decision-making. In the field of agriculture, IoT technology helps monitor soil moisture and plant conditions, enabling

the application of more sustainable precision agriculture. However, the adoption of IoT is not without various challenges. One of the main issues is cybersecurity, which is becoming increasingly crucial as the number of interconnected devices increases. With billions of IoT devices operating worldwide, the potential for cyberattacks increases significantly.

Hacking, data manipulation, and digital identity theft are real threats that can disrupt company operations and cause major losses (Saeed et al. 2023). Therefore, the need for robust security strategies and adaptive regulations is becoming more urgent. In addition, there is also the challenge of the digital divide. Not all countries, organizations, or individuals have equal access to adequate digital infrastructure. This limitation has the potential to widen social and economic inequality, especially in developing countries that still face obstacles in the adoption of digital technology (Saeed et al., 2023). This imbalance has serious consequences, because digital transformation should be inclusive so that its benefits can be felt equally. On the other hand, the opportunities offered by IoT are very large. IoT not only increases efficiency and productivity but also encourages innovation in new business models. For example, with data obtained through IoT devices, companies can develop predictive maintenance-based services that not only extend the life of machines but also reduce maintenance costs.

At the macro level, digital transformation through IoT can contribute to the development of a more competitive digital economy, and accelerate the achievement of Sustainable Development Goals (SDGs) through innovation in the fields of energy, health, and education (Amalki et al., 2023). Thus, IoT is a key technology in the

Industrial Revolution 4.0 that offers great transformation opportunities for various sectors, but also poses significant challenges, especially in the aspects of cybersecurity and the digital divide. A literature review-based study is important to understand the extent to which the development of IoT has had a real impact, how these challenges are managed, and what strategies need to be implemented to ensure a safe, efficient, and sustainable implementation of IoT.

2. Literature Review

2.1. The Role of IoT in the Industrial Revolution 4.0

The Internet of Things (IoT) is one of the main pillars of the Industrial Revolution 4.0, which basically allows the creation of more sophisticated automation and digitalization-based industrial systems. By connecting physical devices through sensors, communication networks, and internet connectivity, IoT is able to facilitate the process of collecting and analyzing data in real-time that was previously difficult to do. This ultimately allows for the realization of the concepts of smart manufacturing, more accurate predictive machine maintenance systems, and a significant increase in product quality (Wu et al., 2022).

In the manufacturing sector, the implementation of IoT makes a real contribution to generating higher operational efficiency, supporting the optimization of the supply chain, and creating a production system integration that is increasingly adaptive to changes and market demand dynamics. Not only limited to the manufacturing industry, IoT has also expanded the reach of digital transformation to various other important fields, including health, education, transportation, and even

agriculture. As a concrete example, today's IoT-based medical devices allow remote patient monitoring with a better level of accuracy, thereby increasing the quality of health services.

Meanwhile, in the field of modern agriculture, IoT-based agricultural sensors help farmers in the application of precision agriculture which is more sustainable and environmentally friendly, with the aim of increasing productivity as well as the efficiency of resource use (Kim et al., 2019).Thus, IoT ultimately does not only play a role in supporting industrial growth, but also encourages the birth of various forms of cross-sector innovation that can create new added value for society and the global economy.

2.2. Challenges of Cybersecurity and the Digital Divide

Even though it offers great opportunities in various sectors of modern life, the implementation of the Internet of Things (IoT) also presents a number of significant challenges, especially related to the issue of cybersecurity. The number of devices connected through the internet network continues to increase exponentially, which ultimately expands the attack surface that can be exploited by irresponsible parties. Cyberattacks targeting IoT-based systems can have very serious impacts, ranging from theft and misuse of personal data, leakage of sensitive information, to causing disruption to crucial industrial operations. Therefore, a truly robust, multi-layered cybersecurity strategy and supporting regulations are absolutely necessary to protect the sustainability of an increasingly complex digital infrastructure.

Apart from the security problems, the adoption of IoT still faces another obstacle in the form of a fairly real digital divide. Not all regions, especially in

developing countries, have adequate internet and technological infrastructure to support the optimal use of IoT. This infrastructure inequality has the potential to widen the social and economic gap between developed and developing countries (Feng et al., 2023). The next no less important challenge is the high cost of IoT implementation, both from the side of hardware, software, and the need for truly competent human resources. A number of studies emphasize that even though IoT has great potential to increase efficiency and productivity, the success of its implementation still depends heavily on the readiness of infrastructure, security guarantees, and government policies that support digital innovation. In other words, for IoT to be truly able to provide a positive and inclusive impact, a comprehensive, integrated, and sustainable strategy is needed.

3. Methods

This This research uses a literature review method to analyze the development of the Internet of Things (IoT) in the context of the Industrial Revolution 4.0, and to examine the opportunities and challenges that arise, especially related to aspects of cybersecurity and the digital divide. The literature review method was chosen because it is able to provide a comprehensive understanding of the phenomenon being studied through a systematic review of the results of previous research. The research stages begin with the identification of relevant literature using a reputable scientific database from Google Scholar. The inclusion criteria used are scientific publications in the form of journal articles, conference proceedings, and academic books that were published. The search keywords used include "Internet of Things (IoT)", "Industry 4.0", "digital

transformation", "cybersecurity", and "efficiency". After the literature is collected, a selection process is carried out by reviewing the title, abstract, and content of the article to ensure its suitability with the research focus.

Articles that specifically discuss the application of IoT in various industrial sectors, its contribution to digital transformation, and the issues of security and the digital divide are prioritized for further analysis. From the search results, a number of relevant literatures were obtained. The next stage is content analysis. The selected literature is studied in depth to identify the main themes, namely: the contribution of IoT to digital transformation and the improvement of operational efficiency; the application of IoT in various industrial sectors; the challenges of cybersecurity in IoT implementation; and adoption barriers related to the digital divide and costs. The results of the analysis are then synthesized to find patterns, research gaps, and recommendations that can be given for the future development of IoT.

In order for the review results to be objective, the analysis process is carried out with a comparative approach, which is comparing findings from various sources. For example, literature that highlights the benefits of IoT in manufacturing efficiency is compared with research that places more emphasis on security risks in the health sector. Thus, the results obtained can provide a more balanced picture of the benefits and challenges faced. This literature review method aims to present a clear conceptual mapping of the development of IoT in the Industrial Revolution 4.0. This approach allows researchers to present a critical synthesis of the contributions, opportunities, and risks of IoT so that it can be used as a reference for further research and decision-making in the implementation of technology in the real world.

4. Results

The results of the literature review show that the Internet of Things (IoT) is one of the most significant components in driving digital transformation in the Industrial Revolution 4.0 era. IoT not only connects physical devices through sensors and networks, but also enables the formation of intelligent systems that are able to communicate, analyze data in real-time, and support more accurate decision-making. IoT has developed into an important foundation in the application of the concepts of smart manufacturing, smart healthcare, smart agriculture, and smart cities. With its data-oriented characteristics, IoT allows various sectors to optimize performance, reduce operational costs, improve service quality, and create new data-based business models (Wu et al., 2022).

In the context of the manufacturing industry, IoT is the backbone for the integrated application of smart manufacturing. Currently, the manufacturing industry aims to increase competitiveness through innovative technologies, called enabling technologies with the aim of encouraging new growth in the industrial sector. Competitiveness, innovation, and sustainability represent strategic levers for global economic development (Nugrowibowo & Muslimin, 2023). Through a network of sensors and automatic control systems, companies are able to monitor machine conditions in real-time, predict potential damage, and perform predictive maintenance. With this approach, machine downtime can be minimized, machine life can be extended, and maintenance costs become more efficient. The integration of IoT with other technologies such as Artificial Intelligence (AI) and machine learning also supports more precise decision-making, because the data produced can be

processed into strategic information that guides companies in determining production, distribution, and supply chain management policies (Bhadra et al., 2023).

In the health sector, IoT plays an important role in creating a more effective and efficient medical service system. IoT-based medical devices, such as wearable devices and biometric sensors, allow continuous monitoring of patients' conditions, both in hospitals and at home. Health data collected in real-time can be sent to medical personnel, so that diagnosis can be done faster and clinical decision-making becomes more accurate. In addition, IoT also helps in drug management, tracking the logistics of health equipment, and the integration of electronic medical record systems. However, the literature shows that the implementation of IoT in the health sector also poses major risks related to data privacy and cybersecurity. Medical information is sensitive data that is very valuable, so the potential for data theft or manipulation by irresponsible parties is a serious threat that must be anticipated with a strong security strategy (Kim et al., 2019).

Meanwhile, in the field of agriculture, IoT supports the application of precision agriculture which allows farmers to monitor soil conditions, moisture, and weather more accurately. The data obtained from field sensors can be used to determine the needs of irrigation, fertilization, and pest control. As a result, agricultural productivity can be increased, while the use of natural resources becomes more efficient and environmentally friendly. The literature emphasizes that this technology is very potential to support global food security, especially in the midst of the challenges of climate change and rapid population growth. However, the adoption of IoT in the

agricultural sector is still limited in developing countries due to the limited digital infrastructure and high initial investment costs (Saeed et al., 2023).

Apart from the manufacturing, health, and agriculture sectors, IoT also plays a role in the transformation of transportation systems. The implementation of smart transportation based on IoT allows for more efficient traffic management, real-time monitoring of vehicle conditions, and the development of autonomous vehicles that can operate with a higher level of safety. At the urban level, IoT also supports the development of smart cities with environmental monitoring systems, energy management, and digital-based public services. This creates a more effective, efficient, and environmentally friendly city governance (Almalki et al., 2023).

However, the results of the literature review also show that the implementation of IoT brings a number of major challenges, especially related to cybersecurity. With the increasing number of connected devices, the potential for cyberattacks increases significantly. IoT-based systems are very vulnerable to hacking, malware attacks, and data theft. On an industrial scale, cyberattacks can cause major losses, ranging from operational disruption to damage to the company's reputation. Therefore, the literature emphasizes the importance of developing a comprehensive cybersecurity strategy, including data encryption, multi-layered authentication, and AI-based monitoring to detect anomalies (Saeed et al., 2023).

Another challenge that arises is the digital divide, which reflects the inequality in access to and use of technology. Developed countries are relatively faster in adopting IoT because they have more adequate digital infrastructure, while developing countries still face major obstacles, such as limited internet access, high device costs,

and a lack of competent workforce in the field of digital technology (Saeed et al., 2023). This inequality not only slows down digital transformation but also has the potential to widen the social and economic gap between regions. It is said that improvements in transportation access do not only have an impact on the economic sector through increased trade, but also on social dimensions such as participation in education and access to health services. Therefore, the development of transportation infrastructure is often used as a main indicator in measuring the level of regional development. In development theory, adequate access is considered a catalyst for inclusive economic growth. Good access allows for a faster flow of goods, services, and information (Chang et al., 2020).

In addition, several studies also highlight ethical and privacy issues in the implementation of IoT. Data collected through IoT devices often includes sensitive personal information, which raises concerns about data misuse. The lack of clear regulations regarding the protection of personal data adds to the complexity of this challenge. Therefore, a regulatory framework is needed that is able to balance the use of data for innovation with the protection of individual privacy rights (Mijwil et al., 2023). Although facing challenges, the literature shows that IoT still has a bright prospect in driving digital economic growth. With the right implementation strategy, IoT can increase global competitiveness, strengthen industrial resilience, and support the achievement of sustainable development. The integration of IoT with other technologies such as blockchain, AI, and cloud computing will further expand its potential use. Blockchain, for example, can be used to improve the security of IoT data by creating a transparent and difficult-to-manipulate transaction recording

system. AI can strengthen IoT's predictive analysis capabilities, while cloud computing provides flexibility in storing and processing large-scale data (Trung et al., 2021).

The results of the literature review confirm that IoT is a transformational technology with a wide impact on various sectors. Its implementation provides great opportunities for increasing efficiency, productivity, and innovation. However, without proper management, the risks it poses, especially in the aspects of cybersecurity, the digital divide, and privacy, can hinder the benefits that should be obtained. Therefore, the success of IoT implementation in the Industrial Revolution 4.0 era is highly dependent on a combination of technological readiness, supportive regulations, and sustainable security and inclusiveness strategies.

5. Discussion

The results of the literature review show that the Internet of Things (IoT) plays a role as one of the main pillars in the Industrial Revolution 4.0 with a widespread impact on various sectors. However, further discussion is needed to understand the strategic implications of these findings, especially related to the potential, risks, and future direction of IoT development. First, from an opportunity perspective, IoT offers a major transformation in how organizations operate. In the manufacturing sector, the implementation of IoT is proven to be able to increase productivity through predictive maintenance, process automation, and supply chain optimization. This efficiency not only reduces operational costs but also strengthens the company's competitiveness in the global market (Wu et al., 2022). In the health sector, IoT presents opportunities in creating a more personal and responsive service system

through real-time patient monitoring, which can ultimately save lives (Kim et al., 2019).

In the transportation and urban planning sectors, the concept of smart cities based on IoT allows for the management of energy, mobility, and public services that are more efficient and sustainable (Almalki et al., 2023). Thus, the potential of IoT in accelerating digital transformation seems very large and cross-sectoral. Second, from the side of challenges, the literature emphasizes that cybersecurity is the most urgent issue. IoT systems that connect billions of devices worldwide create a large attack surface, making it vulnerable to hacking, data manipulation, and malware attacks. Some studies show that without an adequate security strategy, cyberattacks can paralyze company operations and even a country's critical infrastructure (Saeed et al., 2023). Another challenge is the issue of data privacy, especially in the health and transportation sectors, where personal information can be easily exploited if not protected properly.

Apart from security, the digital divide also emerges as a major obstacle in the adoption of IoT. Developed countries with mature digital infrastructure are able to adopt IoT faster, while developing countries still face major obstacles, such as limited internet access, high implementation costs, and a lack of competent human resources in the field of digital technology (Costan et al., 2021). This has the potential to widen the global inequality in digital transformation. Therefore, an inclusive strategy is needed so that the benefits of IoT can be felt equally, including government policy support, public-private collaboration, and investment in increasing digital capacity. Third, the results of the literature confirm that the success of IoT implementation is

highly dependent on integration with other technologies. The use of AI in analyzing IoT data allows for more accurate predictions, while blockchain can improve security through a distributed recording system that is difficult to manipulate. Cloud computing also plays an important role in providing the flexibility of large-scale data storage and processing (Trung et al., 2021).

This cross-technology integration strengthens the usability of IoT and expands the scope of its application. Thus, this discussion confirms that IoT is a disruptive technology that brings opportunities and challenges at the same time. For IoT to be able to provide a positive impact in a sustainable way, a strategy that prioritizes security, inclusivity, and cross-technology integration is needed. Furthermore, the development of adaptive regulations and an increase in public awareness of digital privacy are important prerequisites for creating a safe and widely beneficial IoT ecosystem.

6. Conclusion

The results of the literature review show that the Internet of Things (IoT) is a key technology in the Industrial Revolution 4.0 that drives digital transformation across sectors, from manufacturing, health, agriculture, transportation, to urban governance. IoT contributes greatly to the improvement of operational efficiency, more accurate predictions, and the creation of data-based business models. The implementation of IoT in the manufacturing industry supports smart manufacturing, while in the health sector it helps manage real-time data-based medical services, and in the agricultural sector it facilitates more sustainable precision agriculture. However,

these great benefits are accompanied by significant challenges, especially in the aspects of cybersecurity, data privacy, and the digital divide. Many studies emphasize that the wider network of IoT devices increases vulnerability to cyberattacks, which can disrupt operations and even threaten critical infrastructure. In addition, the uneven distribution of access to technology in various countries has the potential to widen the social-economic gap.

For IoT to be able to provide an inclusive positive impact, a comprehensive strategy is needed, including strengthening digital security, data protection regulations, and government policies that support the even adoption of technology. The integration of IoT with other technologies such as artificial intelligence, blockchain, and cloud computing is also a key factor in expanding its use while strengthening its security. With the right approach, IoT is not only a main driver of efficiency and innovation but also an important catalyst in building a sustainable digital economy and a smarter society in the Industrial Revolution 4.0 era.

References.

Almalki, F. A., Alsamhi, S. H., Sahal, R., Hassan, J., Hawbani, A., Rajput, N. S., ... & Breslin, J. (2023). Green IoT for eco-friendly and sustainable smart cities: future directions and opportunities. *Mobile Networks and Applications*, *28*(1), 178-202.

Bhadra, P., Chakraborty, S., & Saha, S. (2023). Cognitive IoT meets robotic process automation: The unique convergence revolutionizing digital transformation in the Industry 4.0 era. In *Confluence of artificial intelligence and robotic process automation*. Singapore: Springer Nature Singapore,355-388.

Chang, Y., Iakovou, E., & Shi, W. (2020). Blockchain in global supply chains and cross border trade: a critical synthesis of the state-of-the-art, challenges and opportunities. *International Journal of Production Research*, *58*(7), 2082-2099.

Costan, E., Gonzales, G., Gonzales, R., Enriquez, L., Costan, F., Suladay, D., ... & Ocampo, L. (2021). Education 4.0 in developing economies: A systematic literature review of implementation barriers and future research agenda. *Sustainability*, *13*(22), 12763.

Feng, Y., Hu, J., Afshan, S., Irfan, M., Hu, M., & Abbas, S. (2023). Bridging resource disparities for sustainable development: A comparative analysis of resource-rich and resource-scarce countries. *Resources Policy*, *85*, 103981.

Kim, S. K., Cheon, S. P., & Eom, J. H. (2019). A leading cyber warfare strategy according to the evolution of cyber technology after the fourth industrial revolution. *International Journal of Advanced Computer Research*, *9*(40), 72-80.

Mijwil, M., Filali, Y., Aljanabi, M., Bounabi, M., & Al-Shahwani, H. (2023). The purpose of cybersecurity governance in the digital transformation of public services and protecting the digital environment. *Mesopotamian journal of cybersecurity*, *2023*, 1-6.

Nugrowibowo, S., & Muslimin, M. (2023). Smart Manufacturing: Latest Technologies And Applications In Industrial Engineering. *Jurnal Minfo Polgan*, *12*(1), 305-310.

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(1), 1-20.

Trung, N. D., Huy, D. T. N., & Le, T. H. (2021). IoTs, machine learning (ML), AI and digital transformation affects various industries-principles and cybersecurity risks solutions. *Management*, *18*,501-513.

Wu, Y., Dai, H. N., Wang, H., Xiong, Z., & Guo, S. (2022). A survey of intelligent network slicing management for industrial IoT: Integrated approaches for smart transportation, smart energy, and smart factory. *IEEE Communications Surveys & Tutorials*, *24*(2), 1175-1211.