Challenges in promoting the Internet of Things Ecosystem for a government

Wasinee Noonpakdee
Collage of Innovation
Thammasat University
Bangkok, Thailand
wasinee@citu.tu.ac.th

***Abstract*—** The Internet of Things (IoT) has been receiving significant attention from academia, industry, and society due to its diverse range of applications. The IoT ecosystem is composed of different actors, each with a unique role and position. In Thailand, IoT ecosystem could help drive Thailand 4.0 policy that aims to unlock the country from several economic challenges. This paper presents challenges of promoting IoT Ecosystem in Thailand, and propose recommendations for addressing these challenges. The focus group interviews were conducted in five different regions of Thailand: North, East, Northeast, South, and Center. According to the analysis, challenges are addressed in the aspects of Strategy, Stakeholders, Human Resource, R&D and Innovation, Security & Privacy, Infrastructure & Platform, and Government Support. Based on the findings, recommendations for promoting IoT ecosystem in Thailand were proposed, which can be used as a guideline to support the country's Thailand 4.0 policy for economic development in a rapidly changing environment.

Keywords—The Internet of Things; IoT; Challenges; Ecosystem

I. INTRODUCTION

The Internet of Things (IoT) has gained attention on a large number of people from several industries through various applications such as smart cities, smart factories, and smart farms [1-4]. The IoT refers to a connection of consumer devices, industrial machines, equipment, appliances, sensors, and other things. The objective of the IoT is to connect anything, anytime, anywhere, with anybody [2]. The IoT also can be considered a network that connects between humans to humans and things to things through identification of each object [5].

IoT can connect all intelligent objects embedded with sensors to collect and exchange data over the internet with advanced technologies without human interactions [5] [6]. The IoT has brought about a new paradigm driving digital innovation by enabling organizations to provide value-added services for developing their business models, and increasing their sustainability [7]. The IoT ecosystem enables several activities of society to be more automated and efficiently implemented by software applications [8].

In Thailand, the IoT on the manufacturing factory sector in Thailand was estimated to be approximately 2.37 billion Thai baht in 2022, and the total IoT expenditure was also estimated to amount to around 7.69 billion Thai baht [9]. The implementation of IoT would help support Thailand 4.0 policy which focuses on a "value-based economy," as the country has to deal efficiently with disparities and the imbalance development. Therefore, it is significant for Thai Government to promote IoT implementation. This paper aims to study the challenges for promoting IoT ecosystem in Thailand in order to support Thailand 4.0, which focuses on achieving economic prosperity, social well-being, elevating human values, and protecting the environment.

The rest of this paper is organized as follows. Section 2 presents literature review of Thailand 4.0, IoT Ecosystem, Architecture, and challenges. Section 3 provides research methodology. The results are shown in Section 4. Finally, Section 5 concludes the paper.

II. LITERATURE REVIEWS

In literature reviews, the challenges of promoting IoT ecosystems in governments are presented. The first section presents Thailand 4.0, an economic model aimed at addressing the country's economic challenges. The second section provides an overview of IoT, including its architecture, framework, and challenges.

A. Thailand 4.0

Thailand 4.0 is an economic model that aims to unlock the country from several economic challenges include "a middle-income trap", "an inequality trap", and "an imbalanced trap". Four Objectives of Thailand 4.0 are Economic Prosperity, Social Well-being, Raising Human Values, and Environmental Protection [10].

According to [11], Thailand 1.0 was employed on the agricultural sector. Thailand 2.0 concentrated on light industries, which helped upgrade the country's economy from the low-income to middle-income status with low wages. Thailand 3.0 focuses on heavy industries for continued economic growth. During this period, Thailand has become stuck in the middle-income trap. Thailand 4.0 focuses on a "value-based economy," as the country needs to deal effectively with disparities and the imbalance between the environment and society.

The importance of communication infrastructure in smart city development, economic growth, and quality of life [12] has been emphasized as a key factor in driving Thailand 4.0. The utilization of IoT can facilitate the transformation of digital government into data-driven smart government, enabling the delivery of policies and public value [13]. This transition towards smart government development is strongly connected to the application of intelligent technologies, which rely on large amounts of data that can be obtained through IoT [14]. In accordance with Thailand 4.0 policy, the implementation of IoT has also been a major driving force behind the development of Smart Thailand, including Smart City, Smart Industry, and Smart Life.

B. The Internet of things (IoT)

The Internet of Things (IoT) is a concept that has gained increasing importance among practitioners and researchers in recent years. Most definitions of IoT refer to the Internet-based connection of a variety of factors in a network [15].

The IoT is a connection of people and things at any time, in any place, with anyone and anything, using any network and any service [16]. IoT comprises several intelligent connected 'things' that can always be connected anywhere and anytime. 'Things' refer to any object that can transmit and receive data over a network which can be industrial and utility components, machines and other ordinary objects [6, 13]. IoT employs sensors to collect data from the environment. Data is sent to the devices and then forwarded and stored in the cloud that provides services and functions for specific applications [6].

1) IoT Ecosystem Architecture

IoT is a complicated system, and the elements must be placed together systematically. The Five-Layered Architecture is a basic model and conveys the main concept of IoT. Five-Layered Architecture includes Perception Layer, Network Layer, Middleware Layer, Application Layer, and Business Layer. For IoT Cloud Systems Architecture, the layers are IoT Things Layer, Edge Layer, Fog Layer, and Cloud Layer [6].

Regarding a model of the basic ecosystem architecture, the different IoT platforms give access to various kinds of things. The platforms can operate on the cloud level (for example, a server or datacenter), fog level (for example, a gateway or cellular-communication base station), or device level (for example, a Raspberry Pi computer, wearable, or smartphone) [17].

IoT business ecosystem comprises interacting IoT-related companies and individuals along with their socioeconomic environment. The ecosystem consists of software platform providers, hardware platform providers, and the standards. [7].

In a generic Blockchain IoT ecosystem, the four hierarchical layers comprises 1) Application layer with numerous applications of service domains in nowadays society, e.g., transport and mobility, logistics, environment, smart cities, surveillance, and Industry 4.0, 2) Processing layer which processes and stores data coming from the network layer with techniques often include, e.g., Big Data, intelligent processing, edge computing, and fog computing, 3) Network which can be wired, wireless, mobile, vehicular, and mesh with Communication technologies include, e.g., 4G/5G, Wi-Fi, Bluetooth, and ZigBee, and 4) Perception layer that covers a variety of smart devices using sensors to acquire some properties such as temperature, light, time, and location [8].

For IoT governance ecosystem, there are many players with very different statuses that operate on different layers, driven by technical innovation, user needs, market opportunities, and political interests [18].

2) Challenges

IoT complex architecture raises various security issues and challenges [5]. IoT environment makes it vulnerable to security and privacy threats. IoT devices interact with each other by sharing information over the public networks. If security measures are not deployed properly, it can cause severe consequences like stealing, blackmailing, loss of credentials, message modification attack, replay attack, impersonation attack, man-in-the-middle attack, and DoS/DDoS attacks [4]. The increased applications of IoT introduces major security, ethical, privacy, and legal challenges [3, 6]. Some challenges of using higher education in using IoT are studied, including cloud computing, instructional technologies, mobility applications, and privacy and security issues [5].

The ubiquitous nature of IoT data causes a number of privacy threats. These have become more crucial in IoT applications where different systems share and integrate data. A technical and legal framework should be enable to ensure stakeholders awareness and protection of subjects about privacy breaches due to information linkage [19].

There is no doubt that the development of IoT cannot go without regulation of governments [20]. A persistent issue is how governments and public organizations can adapt their traditional structures and processes to the innovative field of the IoT to create public value [15].

III. RESEARCH METHODOLOGY

This research is a qualitative research. The research process is composed of 3 stages: 1) Literature study, 2) Empirical study, and 3) Analysis and conclusion.

The Literature Review in this study covers various aspects related to Thailand 4.0, IoT Ecosystem, Architecture, Framework, and challenges of IoT. The review provides an overview of the current state of research in these areas.

To gain a deeper understanding of the challenges facing the promotion of IoT ecosystem in Thailand, an empirical study was conducted. The study involved the use of focus group interviews as a research method to gain an in-depth understanding of the challenges facing the promotion of IoT ecosystem in Thailand. The focus groups were conducted in five different regions of Thailand: North, East, Northeast, South, and Center. Each region had 3 focus groups, and each group had 10 participants for a total sample size of 30 participants per region. This brings the total sample size to 150 participants across all five regions. The participants were selected from a diverse range of backgrounds, including residents of the regions, university students, telecommunication operators, and government officials.

After conducting the focus groups, the data was analyzed, and the results of the study were then applied to draw conclusions and develop recommendations for addressing the challenges facing the promotion of IoT ecosystem in Thailand.

IV. CHALLENGES FOR PROMOTING IOT ECOSYSTEM

Based on the literature review and focus group findings, the components for promoting IoT ecosystems are described in Table 1, which comprises Strategy, Stakeholders, Human Resource, R&D and Innovation, Security & Privacy, Infrastructure & Platform, and Government Support.

A. Strategy

The strategy includes policy, regulation, roadmap and plan and the standard for IoT. The implementation of a comprehensive strategy for promoting IoT ecosystem in Thailand is crucial in order to support the Thailand 4.0 vision. This strategy should include a policy framework that outlines the government's vision and objectives for IoT implementation, as well as clear and specific regulations that ensure compliance and consistency in the implementation of IoT initiatives.

A lack of clear strategy can lead to issues such as undirected development of IoT networks, duplicate investments, a shortage of frequencies, interference, and a lack of compatibility among systems. Additionally, a detailed roadmap and action plan should be developed to guide the implementation of IoT initiatives and ensure that they are aligned with the overall strategy.

According to the discussions in the focus group, the government has issued guidelines to properly supervise developers and test innovations, and there are clear standards in place for network technology. However, measures and should be further adjusted to be more beneficial for entrepreneurs to support the growth of IoT ecosystem in Thailand. Moreover, the strategy should be flexible and adaptive to the rapidly changing technological landscape of IoT.

B. Stakeholders

Stakeholders of IoT ecosystem are customers, developers, manufacturers, system integrators, researchers and network providers. According to the focus group, there is a lack of clear cooperation and coordination among stakeholders. Entrepreneurs have not yet fully realized the potential benefits of investing in IoT resources.

The government should play a key role in supporting and driving demand for IoT to further facilitate innovation. Furthermore, private sectors should be invited to participate in meetings and discussions about the IoT roadmap to drive a comprehensive plan. Collaboration among stakeholders such as researchers, private sectors, and experts from various related industries is crucial in order to obtain empirical results and address any challenges facing the IoT ecosystem in Thailand. Through this collaboration, stakeholders can work together to develop new business models and opportunities, as well as identify and mitigate any potential risks to the implementation of IoT.

TABLE I. CHALLENGES FOR PROMOTING IOT ECOSYSTEM

Challenges	Details
Strategy	- Policy - Regulation - Roadmap and Plan
Stakeholders	- Customers - Developers - Manufacturers - Systems integrators - Researchers - Network providers
Human Resource	- Knowledge & Skill - Mindset
R&D and innovation	- R&D investment - Innovation developmemt
Security & Privacy	- Message modification attack - Replay attack - Impersonation attack - Man-in-the-middle attack - DoS/DDoS attacks - Information Leakage
Infrastructure & Platform	- Network - IoT platform and Application - Devices - Standard
Government support	- Funding - Test base & Sandbox - Awareness

C. Human resource (HR)

Human resource (HR) is one of the major challenges for promoting IoT. HR includes both knowledge & skills, as well as the necessary mindset to fully utilize IoT technology. Through the focus group interviews, it was observed that many participants had an insufficiency of knowledge and understanding of IoT, and raised concerns about the increasing cost burden associated with IoT technology adoption. Furthermore, many participants also conveyed a perception of limited usefulness of IoT, indicating that there is a need for more education and awareness-raising efforts to better inform the public on the benefits and potential applications of IoT technology.

D. R&D and innovation

The focus group participants noted that the level of R&D investment among organizations is relatively low. They suggested that the government should offer more tax incentives for R&D to encourage greater investment. R&D is considered crucial for driving innovation and progress, even though it may take a long time to see results. The government should therefore take a more active role in promoting R&D, as the benefits of successful R&D efforts can be considerable.

E. Security & Privacy

IoT ecosystem is vulnerable to a variety of security threats, including message modification attacks, replay attacks, impersonation attacks, man-in-the-middle attacks, and denial of service/distributed denial of service (DoS/DDoS) attacks. The scale and diversity of devices, communication networks, and

protocols involved in IoT environments can also lead to privacy breaches due to the linkage of information.

To mitigate these threats, a robust infrastructure and platform must be in place, including secure networks, IoT platforms, applications, and devices. Additionally, government support in the form of funding and test and sandbox environments for experimenting with IoT implementations is crucial for promoting IoT. Furthermore, raising awareness among the general public about the security of IoT is essential for the overall success and sustainability of the IoT ecosystem.

According to the focus group, some participants have raised concerns about the potential security and privacy risks associated with the use of IoT technology. These concerns include issues such as unauthorized access to personal data, data breaches, and the risk of cyber-attacks. Additionally, there is a need for increased transparency and control over how data is collected, stored, and used by IoT devices and systems.

F. Infrastructure & Platform

Infrastructure and platform are fundamental components in promoting IoT ecosystems. The availability and quality of broadband internet service play a significant role in the adoption and implementation of IoT technology. However, it has been noted through the focus group findings that the broadband coverage is not consistent and may not be accessible in certain areas such as rural or remote locations. Additionally, there are concerns among participants regarding the cost of broadband internet, with some considering it too high while others find it reasonable. To ensure the smooth functioning and integration of IoT technology, it is necessary to establish and adhere to industry standards for IoT devices and systems to ensure interoperability and compatibility among them.

G. Government support

Government support is also crucial in promoting the development and growth of IoT in Thailand. This includes support for various components including Strategy, Stakeholders, Human Resource, R&D and Innovation, Security & Privacy, and Infrastructure & Platform, as outlined in Figure 1. It is important for the government to provide support in all of these areas in order to ensure the successful implementation and growth of IoT in the country.

Government should allocate resources towards R&D and innovation, including funding for test bases and sandboxes. A regulatory sandbox can be implemented to facilitate testing and R&D activities for telecommunication innovation, allowing for temporary use of the devices until they are ready for mass production or commercial deployment.

The focus group participants highlighted that while government support for IoT test bases has been provided, there is a lack of real-world applications currently in place. To increase the utilization of IoT technology, it was suggested that test bases be established in various sectors such as agriculture, industry, and tourism. Furthermore, the government should take measures to raise public awareness and understanding of IoT through various forms of media.

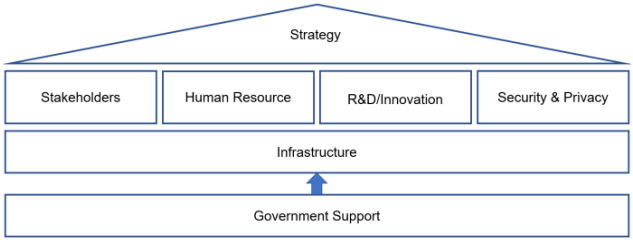

Fig. 1. Compoments for promoting IoT ecosystem

Additionally, some participants suggested the use of IoT for smart city management, including smart traffic, intelligent electric poles, and intelligent security management. The government should also support the implementation of IoT in multiple industries such as agriculture, medicine, and tourism to increase production efficiency and have a positive impact on the economy.

Participants also pointed out that the implementation of IoT in industrial automation can help reduce issues of quality in product production. Many people still lack experience in using IoT, and thus, participants want to apply technology and information to make processes as efficient as possible.

In specific regions of Thailand, such as the southern areas, IoT can be applied for quick tsunami warning which would enhance the fisheries industry. In the northern regions, IoT can be utilized for mountain landslide prevention and agriculture. In the Eastern Economic Corridor (EEC) region, which is an area-based development initiative with the goal of revitalizing the well-known Eastern Seaboard, the implementation of IoT technology in smart factories has the potential to bring significant benefits.

The focus group participants discussed the importance of government support in developing and implementing IoT partnerships with large factories, specifically through Memorandums of Understanding (MOUs) to establish guidelines for sharing information. They also noted the potential for creating real prototypes and testing them in designated facilities. However, they acknowledged that government funding for such projects can be hindered by changes in government leadership and lack of clear follow-up plans. The group emphasized the need for government support in driving the use of IoT in real-world industries, such as industrial factories, and also highlighted the potential of the virtualization industry, particularly in the use of Mixed Reality (MR) across various industries for improving user experience with the use of IoT sensors.

The recommendations for handling the challenges of IoT are proposed as follows:

A clear and effective strategy and plan must be developed to fully realize the potential of IoT. This can be achieved by involving various stakeholders, including industry leaders and researchers, in the planning process. The government should play a key role in facilitating cooperation among these stakeholders to ensure that the plan is inclusive and effective. To support the development of new and innovative technologies using IoT, the government should provide funding

for research and development. Additionally, efforts should be made to broaden knowledge and skills related to IoT, and to promote the many benefits that IoT can bring to different sectors.

Security and privacy issues are a major concern with the implementation of IoT. To address these issues, proper measures must be implemented to protect sensitive data against cyber-attacks and breaches. This includes raising awareness about cybersecurity and privacy among all stakeholders, as well as developing a robust infrastructure and platform to support the growth of IoT. Furthermore, to ensure that the benefits of IoT are accessible to all, the government should invest in expanding broadband infrastructure to cover the most remote and marginal areas.

V. Conclusion

This paper presents the challenges facing the promotion of an IoT ecosystem in Thailand and offers recommendations for addressing them. The challenges are grouped into several categories: strategy, stakeholders, human resources, R&D and innovation, security and privacy, infrastructure and platform, and government support.

The recommendations for addressing these challenges include creating a clear and effective strategy, fostering cooperation among stakeholders, expanding knowledge and skills related to IoT, promoting R&D and innovation, raising awareness about security and privacy concerns, and improving broadband infrastructure coverage. The future work could involve the implementation and evaluation of the recommendations proposed in this study. Furthermore, to identify unique challenges and opportunities in different sectors, specific applications of IoT in sectors such as agriculture, healthcare, and manufacturing could be explored. The results of this research would help create an effective ecosystem suitable for the development and growth of IoT-related technologies in order to drive Thailand 4.0 efficiently.

References

[1] A. AlEnezi, Z. AlMeraj, and P. Manuel, "Challenges of IoT Based Smart-Government Development," in 2018 IEEE Green Technologies Conference (GreenTech), 4-6 April 2018 2018, pp. 155-160, doi: 10.1109/GreenTech.2018.00036.

[2] S. R. F. M. Borhan, N. Maarop, N. H. Hassan, R. C. M. Yusoff, G. N. Samy, and N. Kamaruddin, "Feasibility of IoT Acceptance Among Malaysian Government Agencies Considering Security Factors," in 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS), 2-3 Dec. 2019 2019, pp. 1-6, doi: 10.1109/ICRIIS48246.2019.9073633.

[3] A. Koohang, C. S. Sargent, J. H. Nord, and J. Paliszkiewicz, "Internet of Things (IoT): From awareness to continued use," International Journal of Information Management, vol. 62, p. 102442, 2022/02/01/ 2022, doi: https://doi.org/10.1016/j.ijinfomgt.2021.102442.

[4] S. U. Rehman, P. Singh, S. Manickam, and S. Praptodiyono, "Towards Sustainable IoT Ecosystem," in 2020 2nd International Conference on Industrial Electrical and Electronics (ICIEE), 20-21 Oct. 2020 2020, pp. 135-138, doi: 10.1109/ICIEE49813.2020.9277090.

[5] N. Sultana and M. Tamanna, "Evaluating the Potential and Challenges of IoT in Education and Other Sectors during the COVID-19 Pandemic: The Case of Bangladesh," Technology in Society, vol. 68, p. 101857, 2022/02/01/ 2022, doi: https://doi.org/10.1016/j.techsoc.2021.101857.

[6] A. Karale, "The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws," Internet of Things, vol. 15, p. 100420, 2021/09/01/ 2021, doi: https://doi.org/10.1016/j.iot.2021.100420.

[7] I. Lee, "The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model," Internet of Things, vol. 7, p. 100078, 2019/09/01/ 2019, doi: ttps://doi.org/10.1016/j.iot.2019.100078.

[8] C. K. da Silva Rodrigues, "Analyzing Blockchain integrated architectures for effective handling of IoT-ecosystem transactions," Computer Networks, vol. 201, p. 108610, 2021/12/24/ 2021, doi: https://doi.org/10.1016/j.comnet.2021.108610.

[9] Statista. "Forecasted value of IoT expenditure Thailand 2022, by sector." https://www.statista.com/statistics/1131812/thailand-forecasted-spending-on-iot-by-sector/

[10] W. D. C. Royal Thai Embassy. "Thailand 4.0." https://thaiembdc.org/thailand-4-0-2

[11] O. Languepin. "Thailand 4.0, what do you need to know ?" ThailandBusinessNews. https://www.thailand-business-news.com/featured/54286-thailand-4-0-need-know

[12] Narendra Mangra and A. Ghasempour, "Smart Cities: Connected Ecosystem of Ecosystems," IEEE Perspectives on 5G Applications and Services, 2018.

[13] A. T. Chatfield and C. G. Reddick, "A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government," Government Information Quarterly, vol. 36, no. 2, pp. 346-357, 2019/04/01/ 2019, doi: https://doi.org/10.1016/j.giq.2018.09.007.

[14] A. Kankanhalli, Y. Charalabidis, and S. Mellouli, "IoT and AI for Smart Government: A Research Agenda," Government Information Quarterly, vol. 36, no. 2, pp. 304-309, 2019/04/01/ 2019, doi: https://doi.org/10.1016/j.giq.2019.02.003.

[15] B. W. Wirtz, J. C. Weyerer, and F. T. Schichtel, "An integrative public IoT framework for smart government," Government Information Quarterly, vol. 36, no. 2, pp. 333-345, 2019/04/01/ 2019, doi: https://doi.org/10.1016/j.giq.2018.07.001.

[16] A. Ghasempour, "Internet of Things in Smart Grid: Architecture, Applications, Services, Key Technologies, and Challenges," Inventions, vol. 4, no. 1, p. 22, 2019. [Online]. Available: https://www.mdpi.com/2411-5134/4/1/22.

[17] A. Bröring et al., "Enabling IoT Ecosystems through Platform Interoperability," IEEE Software, vol. 34, no. 1, pp. 54-61, 2017, doi: 10.1109/MS.2017.2.

[18] V. A. F. Almeida, B. Goh, and D. Doneda, "A Principles-Based Approach to Govern the IoT Ecosystem," IEEE Internet Computing, vol. 21, no. 4, pp. 78-81, 2017, doi: 10.1109/MIC.2017.2911433.

[19] N. Madaan, M. A. Ahad, and S. M. Sastry, "Data integration in IoT ecosystem: Information linkage as a privacy threat," Computer Law & Security Review, vol. 34, no. 1, pp. 125-133, 2018/02/01/ 2018, doi: https://doi.org/10.1016/j.clsr.2017.06.007.

[20] M. Kai, "The game analysis of regulation of the government in the Internet of Things," in 2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), 8-10 Aug. 2011 2011, pp. 1672-1675, doi: 10.1109/AIMSEC.2011.6010641.