ISSN 2579-7298

Evaluation of IoT Regulatory Readiness in Indonesia and Policy Recommendations to Support Safe and Effective Implementation

Rizqon Robie [a,1,*], Rendy Munadi a[,1], Helni Mutiarsih Jumhur a[,3]

[a]Program of Master of Electrical-Telecommunication Engineering School of Electrical Engineering, Telkom University
rizqon.robie@gmail.com *
* corresponding author

ARTICLE INFO

Article history
Received
Revised
Accepted

Keywords
IoT Policy Readiness, Deep Deterministic Policy Gradient (DDPG), Regulatory Framework, Cybersecurity and Data Protection, Digital Infrastructure and Economic Impact

ABSTRACT

The rapid development of Internet of Things (IoT) technology in Indonesia presents significant opportunities as well as regulatory challenges. Although IoT adoption continues to increase across various sectors, national policies remain fragmented and lack an integrated framework to support safe and effective implementation. This study assesses Indonesia's readiness for IoT regulation and formulates policy recommendations using a mixed-methods approach. The dataset used in this study comprises both secondary and primary data. Secondary data includes Indonesia's Cybersecurity data, Digital Infrastructure Status, IoT Regulations and Laws, Bappenas Studies, Data from Bappenas, and several policies in other countries, such as America, China, Japan, Korea, and Europe. Meanwhile, primary data was collected through questionnaires distributed to several elements, including 61.5% respondents from IoT users, 19.3% respondents from IoT business actors/IoT Startups, 15.8% academics, and 3.7% Government as regulators. The results of this data were then processed to determine government policy readiness by implementing DDPG, where the state space consists of 6 dimensions of leading regulatory readiness indicators (infrastructure, security, data protection, interoperability, institutional maturity, and economy). The action space is a 6-dimensional vector with continuous values in the range of [-1, 1], representing policy interventions in each dimension. The implementation applies reward functions, actor networks, and critic networks. Training data was applied for several episodes at 400 and 1000 episodes. The comparison results show that IoT regulations and policies in Indonesia should be designed with an adaptive approach based on Reinforcement learning, where the balance between data security, technology readiness, and market penetration can be dynamically adjusted to national and global conditions.

1. Introduction

Current technological developments are very rapid. In the Industry 4.0 era, digital, physical, and biological technologies have been integrated into various aspects of life. Core components of

Industry 4.0 include autonomous robots, big data and analytics, Cyber-Physical Systems (CPS), simulations, IoT and services, cybersecurity, horizontal and vertical system integration, cloud computing, additive manufacturing, and machine learning cc.

The Internet of Things (IoT) is a technology that connects various electronic devices through the internet, enabling data exchange and interaction without human intervention. IoT applications have expanded into multiple sectors, including healthcare, transportation, agriculture, and manufacturing, with the potential to improve operational efficiency and service quality. (Soori et al., 2023)(Mar'ah Nailul Faroh, S.Pd.I, M.Pd., Safar Dwi kurniawan et al., 2023). IoT has revolutionized the way humans, machines, and systems connect, where this great potential strongly supports efficiency, productivity, and innovation across various sectors. IoT has become the backbone of national digital transformation.

In Indonesia, the adoption of IoT technology shows a positive trend. The Indonesia IoT Forum estimates that Indonesia's IoT market potential will reach approximately 35 billion dollars by 2020 (Kusumawati et al., 2017a). However, this development has not been matched by adequate regulations. To date, Indonesia does not yet have specific rules governing IoT, which can pose risks to security, data privacy, and uncertainty for industry players. (Salwa, 2024). The technological revolution in the Industry 4.0 era, particularly IoT, has brought great benefits to daily life. However, it also presents new challenges in terms of privacy and data security, as IoT network security is a crucial factor in maintaining confidentiality and mitigating risks of data breaches. (Sembiring et al., n.d.).

However, safe and effective IoT implementation requires a clear, adaptive, and comprehensive regulatory framework. In Indonesia, various digital policies have been introduced, including the National Digital Transformation Strategy. However, they are generally still macro in nature and have not specifically regulated technical aspects, data/cyber security, and IoT implementation ethics. Therefore, evaluating IoT regulation readiness is crucial for providing a foundation to formulate policies that can sustainably support the IoT ecosystem.

Several countries have taken advanced steps in regulating IoT. For example, the United States, through the Federal Trade Commission (FTC), emphasizes the importance of security in IoT devices and has issued guidelines related to this issue. The relationship between cybersecurity standards and trade secret law is crucial due to the prevalence of data breach incidents, including ransomware attacks, and the increasing value of confidential information across various industries in the information age. The United States has adopted a sectoral approach to cybersecurity and, over time, has mandated increasingly stringent cybersecurity standards for businesses. (Mireles, 2023).

The European Union has also implemented the General Data Protection Regulation (GDPR), which covers aspects related to security and privacy in IoT use based on Regulation 2016/679 (Bastos et al., 2018)(Pratama et al., 2019). Personal data protection and privacy in the European Union have been recognized as fundamental rights in the Charter of Fundamental Rights of the European Union. As a derivative of the Charter, the European Union introduced new personal data protection legislation in 2016, designed to protect personal data in the digital era. (Pratama et al., 2019).

An Asian country that has successfully improved Information and Communication Technology (ICT) iteration and IoT adoption is South Korea, where the government has driven innovation and digital economic growth. It not only provides new employment opportunities but also attracts significant foreign investment. South Korea's steps in addressing the impact of ICT iteration and IoT adoption include strengthening cybersecurity and developing appropriate regulations to protect personal data. (Mth, 2024).

The lack of specific regulations in Indonesia can hinder the development of IoT and pose risks to consumers. Privacy and personal data are essential because users in networks will not conduct digital transactions if they feel their privacy and personal data security are threatened. One protection for privacy and personal data relates to how that personal data will be processed, including sensitive user data that, if disseminated to irresponsible parties, could potentially cause financial losses or threaten the security and safety of the owner. (Pratama et al., 2019). Therefore, evaluating IoT regulatory readiness in Indonesia is crucial to ensure the safe and effective implementation of IoT. Technological developments have driven a shift from the traditional

economic era, also known as the "pre-digital" era, to the Digital Economy era. Thus, legal protection for privacy and personal data also needs to adapt. (Pratama et al., 2019).

The urgency of this research lies in three main dimensions. First, from a technological perspective, the distributed and connected characteristics of IoT require reliable digital infrastructure readiness and clear interoperability standards. Second, from a legal perspective, IoT devices can potentially violate user privacy and become targets of cyberattacks, necessitating specific legal protections and rigorous enforcement of rules. Third, from the policy perspective, the absence of explicit national regulations regarding IoT creates disparities across sectors, weak coordination among institutions, and minimal implementation guidance for industry players.

Although the Indonesian government has initiated various strategic documents, such as the National Digital Transformation Strategy and RPJMN (National Medium-Term Development Plan) 2020-2024, no single policy comprehensively and specifically regulates national IoT governance and development. This creates a gap between strategic vision and technical implementation in the field, hindering efforts to realize a safe, effective, and sustainable IoT ecosystem.

Research Motivation IoT technology holds great potential for enhancing efficiency, productivity, and service quality in both public and private sectors. However, if not properly regulated, this technology can also become a source of vulnerability and risk, including privacy violations, data security breaches, and social impacts. Weak or irrelevant regulations can hinder the adoption of technology, erode public trust, and lead to economic or reputational losses. Therefore, this research is motivated by the urgent need for integrated, adaptive, and risk-based national policies to ensure that the development of IoT in Indonesia can proceed safely and inclusively.

In ICT iteration and IoT adoption, higher cybersecurity standards are expected to result in better trade secret protection; however, some unprepared businesses may find that claimed trade secrets may not be legally protected due to non-compliance with these standards. (Pratama et al., 2019). Problem Formulation Based on the background above, it is evident that Indonesia lacks a comprehensive and adaptive national policy regulating IoT governance, security, and technology development, resulting in implementation disparities across sectors and inadequate protection for users and service providers. Therefore, the problem formulation in this research is: How is the implementation of the National Transformation Strategy regulations related to current IoT implementation in Indonesia and readiness to face the challenges of digitalization impacts? What challenges and opportunities emerge from existing policies? How can the experiences of other countries in regulating IoT be used as a reference for Indonesia? How can ideal IoT policy formulation support the safe, effective, and sustainable implementation of IoT?

Literature Review

Internet of Things Concept

The Industrial Revolution represents a significant shift in how humans extract and utilize resources to produce goods across various business sectors, ultimately affecting people's lives, economic well-being, politics, and even socio-cultural aspects. The development of the industrial revolution continues to evolve, and in its history, technology has undergone a revolution from 1.0 to the current 4.0. Industrial Revolution 4.0 enters the era of intelligent production, where all objects become smart with the help of technology interconnected through internet networks.

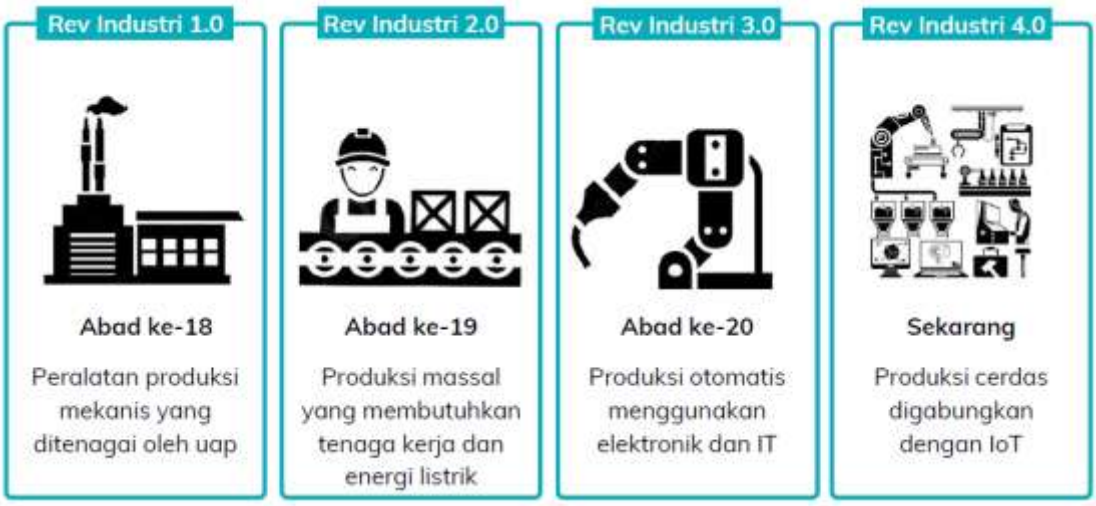

Figure 1. Stages of Industrial Revolution

(source: digital talent scholarship, Indobot Academy materials)

IoT consists of two terms: "internet" and "things." IoT enables objects, or non-computer devices, to perceive, process, and act by allowing them to communicate and coordinate with each other in decision-making. In other words, it enables objects to act intelligently and make consensus decisions beneficial for many applications. They transform objects or sensors into active computing, enabling them to communicate, collaborate, and make important decisions (Salman & Jain, 2017)**.** With the convenience of IoT, it has been implemented in several fields, including smart agriculture, smart homes, healthcare, and transportation (Mar'ah Nailul Faroh, S.Pd.I, M.Pd., Safar Dwi Kurniawan et al., 2023). One example of the currently available IoT ecosystem is the smart home, which utilizes sensors to remotely control temperature, heating, and air conditioning in our homes. Future expansion of such systems can prepare coffee, control TV, track health statistics, and drive vehicles. These applications will provide further challenges and the need for standards to handle the diversity of application requirements (Salman & Jain, 2017)(Amalia Yunia Rahmawati, Ida Afriliana, Safar Dwi Kurniawan, 2020)**.**

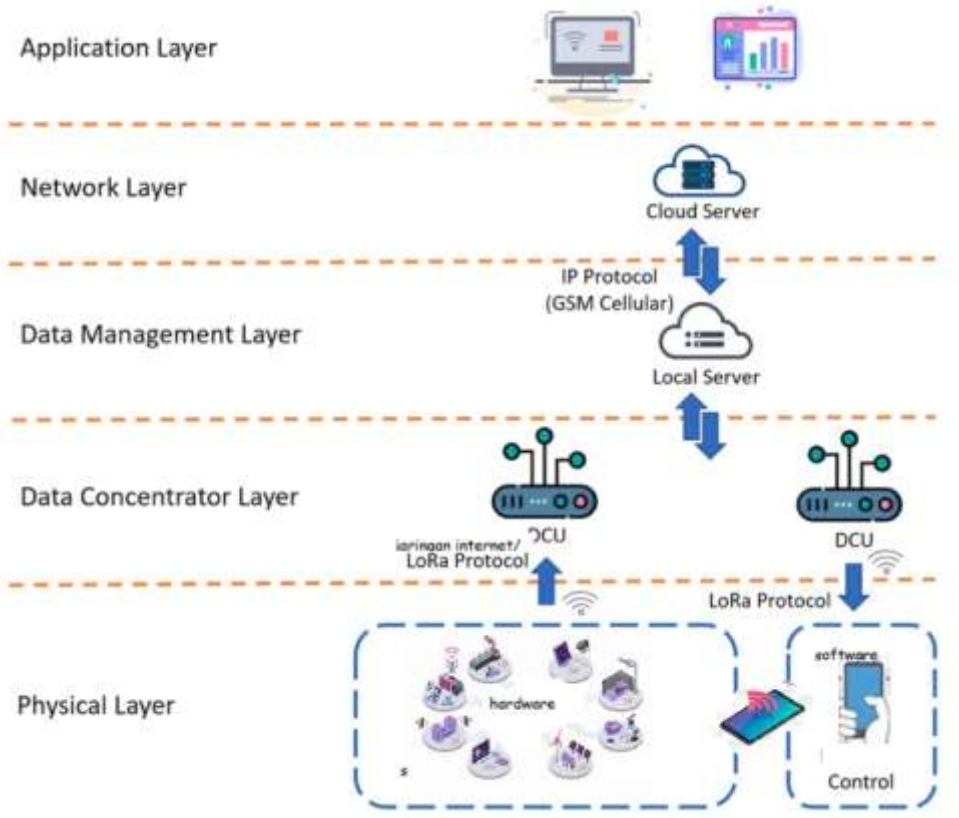

Figure 2. IoT Concept Divided into Several Layers

Information and Communication Technology Policy Framework

Information and Communication Technology (ICT) Policy refers to a set of principles, regulations, and strategies designed to regulate, promote, and develop the use of information and communication technology in a country. The primary objective of ICT policy is to establish an inclusive, secure, and sustainable digital ecosystem that fosters economic growth, enhances quality of life, and enhances government governance. The main components of a practical ICT policy framework should include several main dimensions (according to the World Bank, 2019), (Kelola et al., 2020).

Global and National IoT Regulations and Standards

The rapid development of the Internet of Things (IoT) has prompted many countries and international organizations to develop regulatory frameworks and standards that ensure security, interoperability, and data protection. These regulations and standards form a crucial foundation for a safe and sustainable IoT ecosystem. Global Regulations and Standards Globally, various institutions have formulated principles and standards related to IoT. Some of these include the International Telecommunication Union (ITU), which defines IoT architecture and technical requirements through Recommendation ITU-T Y.2060. ITU also publishes IoT security guidelines that encourage the implementation of security-by-design principles and proactive cyber risk management (Y.2060, 2012). European Union (EU): The European Union implements the General Data Protection Regulation (GDPR), which provides comprehensive protection for personal data, including data collected by IoT devices. (Bastos et al., 2018). GDPR mandates transparency, explicit consent, and user rights.

Internet of Things Ecosystem

IoT ecosystem theory is a conceptual approach that describes the interconnection and interdependence of various components in the IoT system, both from technological, actor, and governance aspects. This ecosystem comprises not only interconnected devices but also platforms, users, data, services, regulations, and infrastructure providers. Elements in IoT, such as sensors,

devices, and connectivity to multiple devices or users, are integral to the complex IoT ecosystem. (Amalia Yunia Rahmawati, Ida Afriliana, Safar Dwi Kurniawan, 2020).

Related Research Review

A study by OECD (2023) formulates a global IoT policy framework, exploring current conditions of IoT adoption and use in OECD countries among businesses, households, and individuals. According to some estimates, the number of IoT connections surpassed non-IoT connections in 2020. Semiconductor components of IoT devices have grown consistently in recent years and are estimated to account for between 5% and 7% of the worldwide semiconductor market. IoT-related patent applications increased by almost 20% per year from 2010 to 2018, accounting for more than 11% of all patent activity worldwide at the end of that period. Venture capital investment in IoT companies also increased dramatically during the last decade, reaching USD 8 billion in 2020. Despite this supportive environment, IoT spreads unevenly among companies, industries, and countries (Bastos et al., 2018; Lim et al., 2023; Mayfield, 2015; Measuring the Internet of Things.Pdf.Crdownload, n.d.)

State of The Art of IoT Research

Global research on IoT and policy has developed significantly in recent years, as shown in Table 1 In 2022, the OECD presented an IoT policy framework focusing on consumer protection and data management. In 2015, the United States Federal Trade Commission (FTC) emphasized the importance of securing IoT device design from the outset of the development process. The European Union, through GDPR in 2018, has expanded the scope of personal data protection for IoT devices, marking one of the most comprehensive regulations. South Korea also demonstrates progress through the development of 5G infrastructure and collaborative regulation between the government and industry. In Indonesia, studies and policies remain fragmented, so this research aims to systematically review this readiness and contribute to the national policy direction**.**

Table 1. State of The Art

No	Country /Institution	Year	Research	Main Approach/ Policy	Contribution to IoT Development
1	OECD	2022	Global IoT policy framework	Comprehensive approach to consumer protection, data security, interoperability	Provides multilateral policy guidance and general principles for OECD member countries
2	FTC (United States)	2015	IoT device security	"Security by design", routine testing, access control, and encryption as part of early design	Became an early reference for the importance of security in IoT development from the design stage
3	Uni Eropa (GDPR)	2018	Personal data protection in IoT	Strict regulation on personal data, including data generated from IoT devices	Forms the basis for the most comprehensive global IoT data protection regulation
4	South Korea	2021	5G infrastructure and collaborative IoT regulation	Government-industry collaboration, development incentives, IoT-based smart city trials	Encourages acceleration of IoT adoption through an ecosystem and digital infrastructure approach
5	Indonesia	-	IoT studies and policies are still fragmented.	No integrated national framework yet; still in the sectoral policy development stage	Requires a comprehensive and systematic study for the development of national policy direction development

DDPG and Its Implications for IoT Decision Making

Previous research to determine the extent to which IoT policies have been widely conducted has focused on the complexity of compliance with regulations and certification related to firmware and communication modules in IoT devices in various regions. (Ghag, n.d.). Regulatory authorities play a crucial role in protecting customers, promoting innovation, and fostering growth. Outdated or non-existent regulatory frameworks for IoT can be one of the barriers to IoT's long-term growth, and avoiding side effects will be difficult to achieve (Hadzovic, 2021).

Economic and Technical Regulation Dimensions in IoT

This research not only focuses on technical regulations, such as security, frequency, and certification, but also examines economic regulations, including fiscal incentives, spectrum tariffs,

and support policies for the IoT industry. This research not only examines technical regulation readiness, including device security, frequency, and IoT certification, but also expands its scope to include economic regulation. The economic dimension encompasses spectrum tariff policies, IoT infrastructure development subsidies, fiscal incentives for the IoT industry, and fiscal/monetary policies that affect digital technology sector investment. This evaluation aims to assess whether the regulatory framework in Indonesia can provide sufficient economic stimulus for the IoT ecosystem to grow inclusively and sustainably. (Anwar & Sanmorino, 2024; Kusumawati et al., 2017b).

2. Method

This section outlines the research methodology employed to assess the readiness of Internet of Things (IoT) regulations in Indonesia and formulate national policy recommendations that are safe, effective, and adaptable to technological advancements. The methodology is systematically designed to address research problems through a data-driven approach, supported by empirical validation obtained from qualitative analysis. Thus, the results of this research are expected not only to provide conceptual contributions but also practical implications in the context of public policy and national IoT ecosystem development.

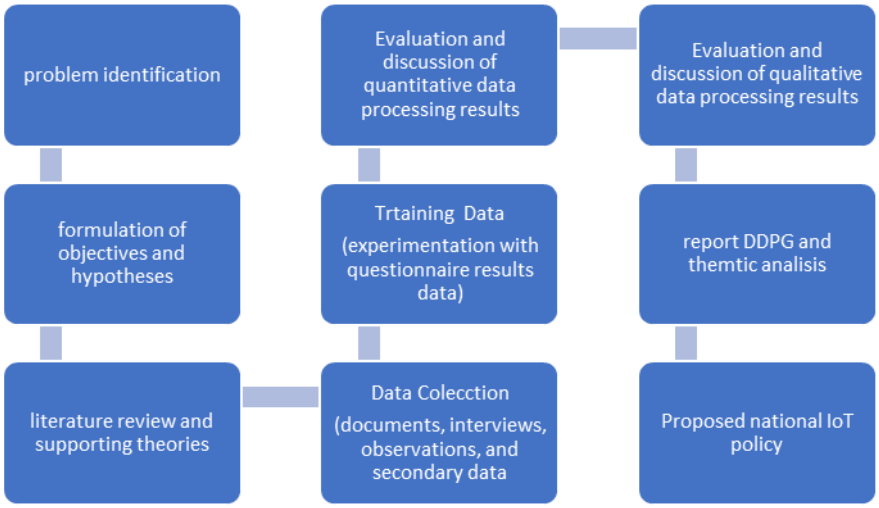

Figure 3. Research Block Diagram

The research methodology block diagram in Figure 3.1 illustrates the systematic research stages designed to evaluate Indonesia's readiness for IoT regulation and formulate adaptive, data-driven national policy recommendations. Each stage in this diagram is logically connected, spanning from problem identification to the formulation of policy recommendations. Overall, the research framework demonstrates a structured and integrated process, combining data-driven approaches and public policy analysis to produce IoT policy recommendations that are applicable, measurable, and aligned with Indonesia's national digital transformation direction.

Table 2. Dataset Used in the Research

Data Type	Time Range	Source
Indonesian Cyber Security Index	(2018).–2024	BSSN, Global Cybersecurity Index (ITU)
Digital Infrastructure Status (IoT readiness, 4G/5G penetration)	2018–2024	Ministry of Communication and Informatics, APJII, GSMA
Regulations and Laws Related to IoT	2018–2024	PDP Law, Postal Government Regulation, BSSN Regulations, SNI
Readiness of Government Institutions & Industry	2020–2024	BAPPENAS Study, Ministry of Communication and Informatics, PwC Report
Security Risks & Interoperability	2019–2024	BSSN Incident Reports, Cyber Attack Reports
Policy Effectiveness from Developed Countries	2018–2024	OECD, South Korea (PIPA), European Union (GDPR), US (FTC, Cyber Labeling Program)

The dataset for DDPG utilizes global indices (GCI, GSMA, EGDI) to enhance dataset validity, normalize values, and validate weights through expert input.

Hypotheses IoT regulations that are more integrated and risk-based will enhance readiness and trust in the implementation of IoT technology. This research presents three hypotheses, as outlined in Table 3.2.

Table 3. Research Hypotheses

No.	Hypothesis	Main Indicators	Implications
1	IoT regulation in Indonesia is not fully ready	Limited regulation on frequency & data, without certification & security standards	Government needs to formulate new regulations that are more specific and technical
2	Developed countries have more comprehensive IoT regulations	US (FCC Labeling), EU (GDPR & CRA), Korea (IoT Certification, PIPA Act)	Indonesia lags behind in device regulation & network readiness
3	Adoption of international best practices can increase security & effectiveness of IoT implementation	Policy evaluation and simulation and Model Training	Global-based policy models can accelerate digital transformation and increase public trust

Research Framework

This research is based on a framework that connects public policy theory, regulation readiness, and DDPG machine learning approach. Conceptually, the relationship among variables is shown in Figure 4.

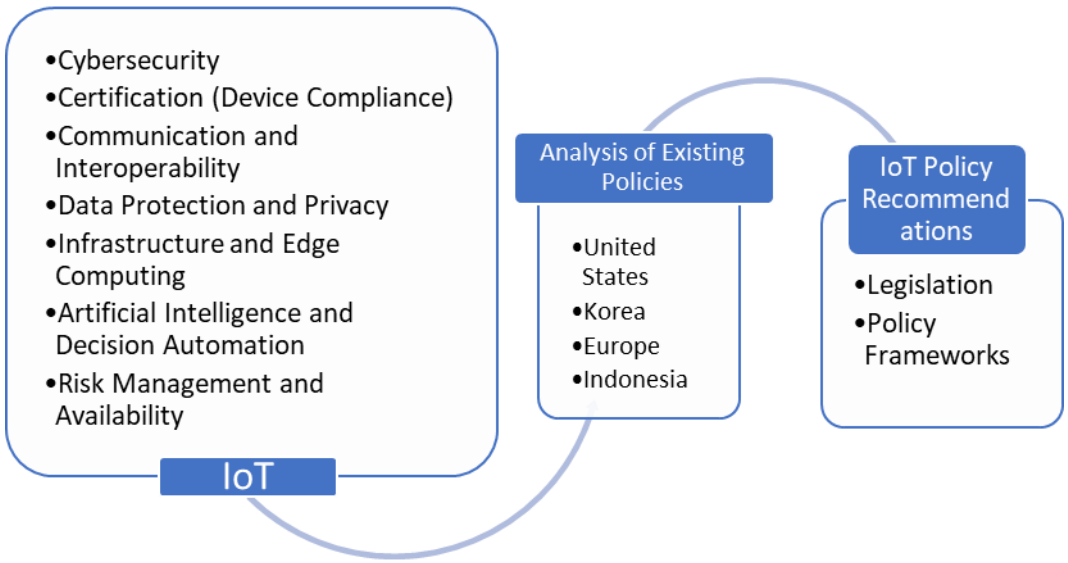

Figure 4. IoT Policy in Various Countries

This research will be conducted in several stages, as shown in Figure 4, divided into nine stages, and the research framework is shown in Figure 5

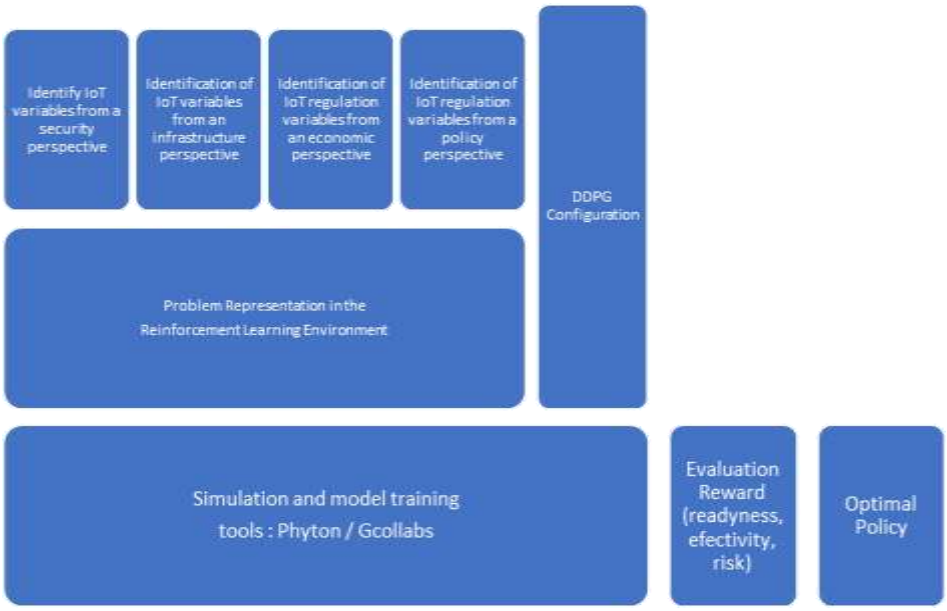

Figure 5. IoT Policy Research Framework

These stages are conducted for three variables: security, infrastructure, and Internet of Things (IoT) policy.

3. Results and Discussion

This research employs a mixed-methods approach, combining quantitative and qualitative data to provide a comprehensive understanding of Indonesia's readiness for IoT regulation.

Table 4. Secondary Dataset

Jenis Data	Rentang Waktu	Sumber & Keterangan (link/laporan)
Indonesia Cyber Security Index	(2018).–2024	BSSN — Cybersecurity Landscape/Report Indonesia (annual reports/monitoring) — BSSN annual reports (Cybersecurity Landscape, Monitoring) include incidents, APT trends, ransomware, phishing, and annual data summaries. (alika.pesisirbaratkab.go.id)
ITU — The Global Cybersecurity Index (GCI) provides comparative scores between countries (2018, 2020, 2024 editions, etc.). GCI Package/PDF available for download. (ITU)		
Digital Infrastructure Status (IoT readiness, 4G/5G penetration)	2018–2024	Ministry of Communication & Informatics/Digital Ministry — Performance reports & digital transformation (containing broadband penetration data, 4G/5G coverage, IoT initiatives). (eppid.komdigi.go.id)
APJII — Indonesian Internet User Penetration Survey (annual survey; 2018–2024 penetration data). APJII reports can be downloaded (PDF). (apjii.or.id)		
The GSMA Mobile Connectivity Index (MCI) provides an Excel dataset (scores/indicators, 2014–2023) relevant to mobile penetration and connectivity readiness. (.xlsx file available). (mobileconnectivityindex.com)		
Regulations and Laws Related to IoT	2018–2024	Personal Data Protection Law (Law No.27/2022) — official legal text (JDih). (Peraturan BPK)
BSSN regulations/Directorate General of SDPPI (Ministry of Communication and Informatics) related to security and frequency/SDPPI; and SNI/BSN (adoption of SNI related to IoT — example SNI adoption ISO/IEC TR 30148 and SNI ISO/IEC 30179 related to IoT). (Postel)		
Government & Industry Institution Readiness	2020–2024	Bappenas/RPJMN & Digital Industry Development Master Plan (2020–2024/2023–2045 policy documents) — readiness analysis, policy framework, institutional capability references. (Perpustakaan Bappenas)
Industry/consultant reports (example: PwC Indonesia, TMT/digital readiness reports) — insights on private sector readiness and industry collaboration for IoT/digital transformation. (PwC TMT 2023 report & digital publications). (PwC)		
Security & Interoperability Risks (incidents, attack reports)	2019–	BSSN — Monitoring & landscape reports

Third-party incident reports/journal analysis summarizing major attacks and interoperability issues (e.g., research publications, whitepapers). (PhilArchive)	2024	(annual incidents; attack statistics, traffic anomalies, ransomware, phishing). (alika.pesisirbaratkab.go.id)
Policy Effectiveness from Developed Countries (comparative study)	2018–2024	OECD — whitepapers/ policy reviews on cyber policy & digital regulation (policy evaluation reports). (Open Knowledge)
European Union — GDPR (text & effectiveness evaluation), implementation studies; South Korea — PIPA (Personal Information Protection Act); United States — FTC guidance & cyber labeling program (official sources and comparative studies available on official sites/regulators). (These sources are useful for comparative policy studies). (UNESCO Digital Library)		

For data obtained from mobileconnectivityindex.com, for Indonesia (year 2021) based on GSMA Mobile Connectivity Index (MCI) as shown in Table 4

Table 5. MCI Table for Indonesia

Main Dimension	Value	Interpretation
Overall Index	69,04	Upper-middle position globally. Indonesia is categorized as Advanced for East Asia & Pacific region, but still lags behind developed countries (OECD average >80).
Infrastructure	64,63	Digital infrastructure is quite good but not yet equitable. 4G is 96% and 5G is still low (4.6%) — this shows limitations in IoT readiness based on low latency.
Affordability	64,98	Data tariffs are relatively affordable, but device prices are still high (handset price score 38.29). This impacts IoT adoption gaps in lower society.
Consumer Readiness	67,99	Digital literacy is quite high (96%), but school life expectancy and mean years of schooling are still low — indicating long-term digital competency gaps.
Content & Services	79,60	High score — shows local application ecosystem, e-Government (68.24), and cybersecurity (94.59) are improving. Shows great potential for sustainable local IoT.

When compared with several countries in Asia, America and Europe, from the Mobile Connectivity Index (MCI), as seen in Table 6.

Table 6. MCI Comparison with Other Countries

Country	Index	Infrastructure	Affordability	Cybersecurity	5G Coverage
Indonesia	69,0	64,6	65,0	94,6	4,6%
South Korea	89,5	90,2	85,7	96,0	99%
Japan	88,3	89,1	84,5	95,2	98%
China	85,0	87,3	80,1	94,8	98%
Europe (average)	82,0	84,0	81,0	95,0	97%
US	87,5	88,0	79,5	96,5	97%

Indonesia's position in the global digital ecosystem shows significant strengths especially in cybersecurity and local content development aspects. The Cybersecurity Index value reaching 94.6 confirms that the national digital security policy framework, including the role of the National Cyber and Crypto Agency (BSSN) and implementation of the Personal Data Protection Law (PDP Law), has been at a level parallel with developed countries such as Japan, South Korea, and the United States. In addition, the high score on the Content and Services dimension (79.5) reflects the maturity of the local digital ecosystem, from improving e-Government, social media penetration, to developing national applications that are inclusive and relevant to community needs.

However, these strengths have not been fully supported by advanced digital infrastructure. Indonesia still faces major challenges in terms of 5G network coverage, which has only reached 4.61%, as well as limitations in Internet Exchange Points (IXPs) and international bandwidth per user. This condition limits the country's ability to support high-speed connectivity that becomes the backbone for industrial-scale Internet of Things (IoT) implementation. In addition, device affordability also becomes a significant obstacle, with relatively low device price scores (38.29), indicating that public access to IoT technology is still limited by high hardware prices and dependence on imports. Overall, although Indonesia demonstrates strong regulatory and innovative readiness, accelerating infrastructure development and technological independence remains key to strengthening national competitiveness in the IoT-based digital transformation era.

DDPG Architecture

Basic DDPG Concept

Deep Deterministic Policy Gradient (DDPG) is a reinforcement learning algorithm designed to handle decision-making problems in continuous action spaces. In the context of this research, DDPG is used to simulate optimal IoT policy decision-making processes based on current regulation readiness conditions.

DDPG combines the advantages of Deterministic Policy Gradient (DPG) and DQN) by utilizing deep neural networks to estimate policy and value functions. This algorithm is very suitable for dynamic and complex IoT systems, where policy decisions must be adaptive to changing environmental conditions.

DDPG Model Components

The DDPG model implemented consists of the following components:

1. Environment (IoTPolicyEnv)
   a. State Space: 6-dimensional vector representing Indonesia's IoT regulation readiness conditions based on six main indicators (security_index, incident_rate, penetration, infrastructure_readiness, compliance, economic_index). These variables are used in DDPG experiments.
   b. Action Space: 4-dimensional vector namely surveillance, incentive, investment, certification.
   c. Reward Function: The reward function is designed to maximize regulation readiness by considering:

$$\text{Reward} = 6.0 \times \Delta(\text{readiness}) - P(\text{incident}) \times \text{cost\_incident} - \text{cost\_action}$$

Where Δ(readiness) is the average readiness change from 5 main components, P(incident) is the probability of security incidents = max (0.01, 1.0 - security_score), cost_incident is the cost of security incidents (constant 0.5), and cost_action is the policy implementation cost (0.25 × Σ action).

2. Neural Networks
   a. Actor Network: Neural network that generates deterministic actions. With input: state (6 dimensions) and output: action (4 dim) with tanh activation → scaled to [-1,1].
   b. Critic Network: Neural network that evaluates state-action pair quality. With input: concatenated state + action (10 dim) and output: Q-value (scalar).
3. Training Loop
   a. Critic update: minimize TD-error between Q(s,a) and target Q(s',a')
   b. Actor update: maximize expected Q-value with policy gradient.
   c. Done every 2 steps for efficiency.

4.2.1 Training Parameters

Hyperparameters used in DDPG model training are as follows:

Table 7. Training Parameters

Parameter	Value	Description
Episodes	400 , 1000	Number of training episodes
Max steps per episode	8	Maximum steps per episode
Learning rate (Actor)	1×10^{-4}	Learning speed of actor network
Learning rate (Critic)	1×10^{-3}	Learning speed of critic network
Discount factor (γ)	0.97	Discount factor for future rewards
Soft update rate (τ)	5×10^{-3}	Rate for updating target networks
Replay buffer size	10,000	Size of replay buffer memory
Batch size	16	Batch size for training
Exploration noise	σ = 0.12	Standard deviation of exploration noise

DDPG Implementation

DDPG implementation is performed using Python programming language with PyTorch library for deep learning framework on the Google Colaboratory platform. Experiments were conducted with comparison of 400 and 1000 iterations.

Environment Simulation

IoTPolicyEnv environment is designed to simulate IoT policy system dynamics in Indonesia. Environment implementation uses class-based design patterns compatible with PyTorch and can run efficiently on Google Colab with GPU acceleration. This environment has characteristics of state representation which is the condition of regulation readiness in 6 dimensions, then there is action effect where each action changes state with factor alpha (0.06) plus Gaussian noise, and reward calculation to calculate reward based on readiness improvement, incident risk reduction, and cost efficiency.

Neural Network Architecture

Neural network architecture uses fully connected layers with non-linear activation to capture complex patterns in policy data. The actor network utilizes the Tanh activation function on the output layer to limit actions to the range [-1, 1], whereas the critic network employs a linear output for Q-value estimation.

Training Loop

The training process is conducted iteratively through several steps, starting with episode initialization, which resets the environment to initial conditions taken randomly from the dataset. Next, in the action selection stage, the actor network generates actions by adding exploration noise to maintain a balance between exploration and exploitation. The environment step is conducted, which executes that action and observes the next state, reward, and done signal. Each transition ((s, a, r, s', done)) is then stored in the replay buffer at the experience storage stage. After the replay buffer contains enough data, a network update is conducted, which includes taking a random batch from the buffer, updating the critic network using temporal difference error, updating actor network with policy gradient, and soft update on target networks to maintain learning stability.

Simulation Results and Evaluation

DDPG simulation results run on Google Colab with GPU acceleration produce four main metrics visualized in the figures below.

1. Training 400 Episodes

Figure 4. 1 Training Reward Graph for 400 Episodes

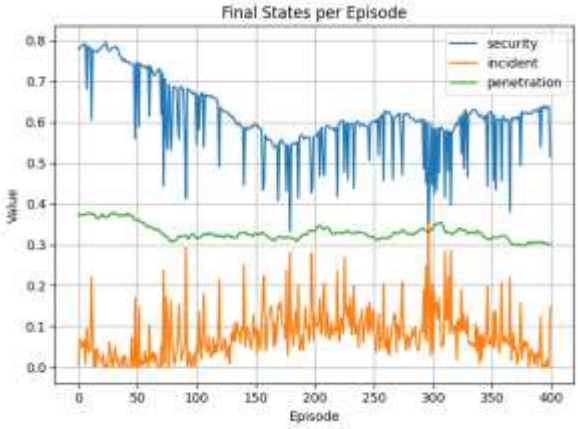

Figure 4. 2 Final States Graph for 400 Episodes

a. Early Phase: Aggressive Exploration and Security Spike

In the first 50 episodes, the agent shows very aggressive exploration behavior. The final states graph displays dramatic spikes in security index reaching peaks at 0.78-0.80. This phenomenon indicates that the agent quickly discovers that massive investment in surveillance, investment, and certification produces significant security improvements. However, this behavior is also accompanied by extreme volatility, visible from sharp fluctuations reaching as low as 0.62 in the same episode range. Interestingly, incident rate in this phase also shows quite high spikes, ranging between 0.20-0.25. This reflects conditions where the system is still vulnerable to attacks despite high security index, possibly because penetration rate is still low (~0.37) and infrastructure readiness is not yet optimal. The agent is still in the trial-and-error stage, has not found an optimal balance among various policy components.

b. Consolidation Phase: Gradual Degradation and Stabilization

Entering episodes 50 to 200, there is a gradual degradation trend in security index declining from peak 0.80 to stabilize at around 0.55-0.65. This decline is not a learning failure, but rather a reflection of more mature reward function optimization. The agent begins to understand that maintaining maximum security requires very high cost (especially from investment with weight 0.4), so it's not efficient in the long term. Incident rate shows significant improvement in this phase, consistently declining to range 0.05-0.15. This decline indicates that the agent successfully finds effective surveillance and investment combinations to suppress security incidents without having to maximize security index. However, penetration rate remains stagnant at 0.30-0.38, showing that agent strategy tends to be defensive and less focused on increasing IoT adoption.

c. Final Phase: Plateau with Decline

Episodes 200 to 400 show a concerning pattern. Training reward graph shows that after reaching peak performance around episode 200 with reward -15, there is a gradual decline until returning to level -10 to -6 in final episodes. This phenomenon indicates possible overfitting or instability in learning. The agent may be trapped in suboptimal local optimum or experiencing catastrophic forgetting where learned policy degrades due to continued exploration. Security index in this phase maintains high volatility with large fluctuations between 0.45-0.65, showing that learned policy is not yet fully robust to variations in environmental conditions. Incident rate remains at low level of 0.05-0.15, which is a positive achievement. However, the penetration rate remaining flat at 0.30-0.38 confirms that the agent fails to develop strategies to increase IoT adoption significantly.

2. Training 1000 Episodes

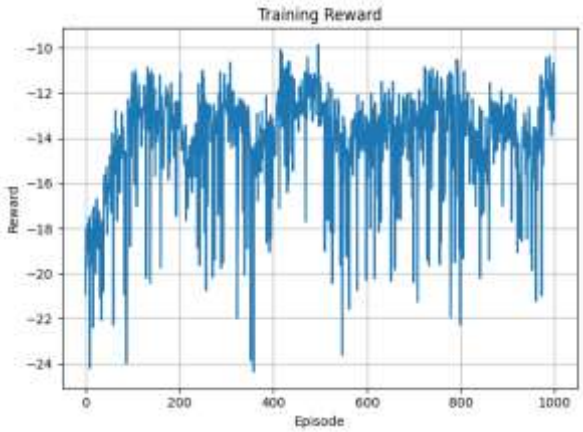

Figure 4. 3 Training Reward Graph for 1000 Episodes

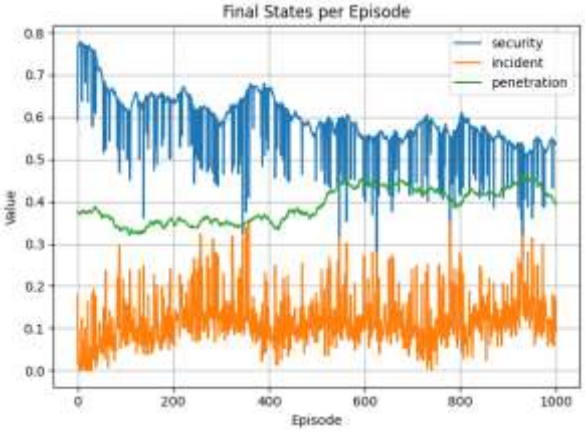

Figure 4. 4 Final States Graph for 1000 Episodes

a. Early Exploration Phase: Extreme Volatility

Unlike 400 episode training, early phase of 1000 episode training shows more extreme and prolonged volatility. Security index indeed also experiences early spike to 0.75-0.80, but its fluctuations are much more dramatic with sharp declines to 0.45 and rebounds forming very wild oscillating patterns until episode 200. This pattern reflects more intensive exploration and higher persistence in trying various policy combinations. Training reward in this phase shows very different characteristics. Instead of experiencing rapid improvement, reward fluctuates extremely between -14 to -24 throughout the first 400 episodes. This very wide fluctuation range indicates that the agent is exploring much wider policy space, not rushing to converge to "good enough" solutions. Incident rate also shows high variability, ranging between 0.05-0.35, reflecting experimentation with various surveillance and security investment levels.

b. Transition Phase: Emergence of Balanced Strategy

Episodes 400 to 600 mark an important turning point in learning. In this range, final states graph begins to show interesting patterns: security index experiences more consistent decline toward level 0.50-0.60, but more significantly penetration rate begins to show upward trend from 0.33-0.37 toward 0.38-0.42. This change is not coincidental, but indication that the agent begins to find strategies that are fundamentally different from 400 episode training. The agent apparently begins to understand more complex trade-offs: by slightly sacrificing security (from 0.65 to 0.55), the agent can allocate more resources to incentive and investment that increase penetration. Reward function giving weight 4.0 for penetration changes begins to give more significant influence in agent decision-making. Incident rate in this phase begins to stabilize at range 0.10-0.20, slightly higher than 400 episode training, but still at acceptable level.

c. Convergence Phase: Stabilization with Balanced Strategy

Episodes 600 to 1000 display stabilization with very different character than 400 episode training. Security index consolidates at level 0.50-0.60 with much lower variance, forming more smooth and predictable patterns. Most strikingly penetration rate successfully reaches and maintains level 0.40-0.45, marking approximately 25-35% increase compared to initial value and consistently higher than 400 episode training results. Training reward although at numerically lower level (-12 to -18), shows much better consistency. There is no significant decline as occurred in 400 episode training. Fluctuations remain but are within more controlled range, indicating more robust and stable policy. The incident rate is maintained at a level of 0.10-0.20, indicating that although security is not maximized, the system remains capable of handling threats adequately.

Table 8. Training Results Comparison between 400 and 1000 Episodes

Metric	Episode 400	Episode 1000	Change
Security (final)	0.55-0.65	0.50-0.60	Slightly lower, but more stable
Incident (final)	0.05-0.15	0.10-0.20	Slightly higher
Penetration (final)	0.30-0.38	0.40-0.45	Significantly increased (+25%)
Peak reward	~-7 (ep. 200)	~-10 (ep. 400-600)	Lower peak
Final reward	-10 to -12	-12 to -18	Worse at 1000 ep
Reward stability	Decline after ep. 200	More stable after ep. 500	More consistent at 1000 ep
Security variance	High (large fluctuations)	Medium (smoother)	More stable at 1000 ep
Learning speed	Fast (peak at ep. 200)	Slow (peak at ep. 400+)	400 ep converges faster
Trade-off learned	Security increases, Penetration stagnant	Security decreases, Penetration increases	Different strategies

The analysis results of IoT policy based on the Deep Deterministic Policy Gradient (DDPG) model show that the success of Internet of Things (IoT) technology implementation in Indonesia is strongly determined by three strategic elements, namely strengthening digital infrastructure, improving regulation reliability, and supporting incentives for industry and academics.

1. Strengthening Digital Infrastructure and Adaptive Cybersecurity

The government needs to prioritize the construction and expansion of digital infrastructure, especially 4G and 5G networks, national data centers, and local Internet Exchange Points (IXPs) to strengthen connectivity and reduce data latency between regions. In the context of cybersecurity, an adaptive security approach is needed that can transform dynamically to new threats through integration of artificial intelligence (AI) and machine learning for attack detection and mitigation systems. This step will ensure that every growth in IoT adoption is accompanied by adequate protection of national digital data and infrastructure. In addition, the formation of a Cybersecurity Framework for IoT Ecosystem adapted to the characteristics of public and private sectors needs to be a priority agenda in the national cybersecurity plan.

2. Improving Regulation Reliability and Consistency

Cross-sectoral regulation harmonization is needed between the Ministry of Communication and Informatics, BSSN, and other technical institutions so that IoT policies in Indonesia have legal clarity and uniformity of standards. Existing regulations—such as the Personal Data Protection Law (PDP Law), spectrum frequency policies, and SNI technical standards for IoT devices—need to be strengthened through responsive and risk-based regulation mechanisms. Thus, every technological change can be immediately accommodated without hindering innovation. The establishment of a national framework "IoT Readiness and Compliance Index" can also be a monitoring tool for how far industry, public institutions, and society meet security, interoperability, and legal compliance aspects.

3. Incentive Support for Industry and Academics

The government needs to expand fiscal and non-fiscal incentive support for industry players and higher education institutions to accelerate innovation and IoT technology adoption. Incentives can take the form of collaborative research subsidies, tax reductions for technology investments, and matching fund programs between industry and universities. On the academic side, strengthening research capacity and development of IoT-based curriculum, artificial intelligence, and cyber-physical systems needs to be facilitated to create superior human resources ready to support the national industry. Triple helix collaboration (government–industry–academics) can be the main catalyst in building a highly competitive and sustainable IoT ecosystem.

Qualitative Data Collection

Qualitative data collection in this research uses questionnaires, interviews and observations. For observations conducted through national IoT seminars in the year (2023-2024), organized by strategic forums held by the Ministry of Communication and Informatics, several notes include the dynamics of dialogue among cross-sectoral stakeholders in formulating comprehensive regulations. These observation results are then followed up by tracing document analysis, one of which is strategic documents, such as several policies related to IoT, although not specific and not focused, but there are already several policies related to this, such as the ITE Law or the use of IoT in the industrial world. Questionnaire results obtained as explained below:

1. Types of questions given:
   a. Prolog, request for respondent's willingness to fill out the questionnaire,
   b. Respondent identity, by providing choices from government elements, IoT business actors/startups, IoT Technology users or academics, and interaction time with that technology,
   c. Perception and experience, where these questions are given using a scale between 1 – 5, using a Likert scale (strongly disagree to very strongly agree),
   d. Policy recommendations, where these questions are given using open questions, so respondent answers will provide an overview of suggestions and improvements,
   e. IoT Regulation Readiness in Indonesia, questions are given with scale 1-5 questions, with Likert scale,
   f. IoT Challenges and Opportunities in Indonesia, where some questions use closed questions and some use Likert scale.
2. From respondents totaling 104, classified respondents 3.8% are respondents from government, 15.4% from academic respondents, 20.2% respondents from business actors in startups and the like, and 60.6% respondents from IoT users.
3. Respondent involvement in IoT varies from those who have never been involved, less than one year, and more than 3 years, or ordinary IoT users. From questionnaire results, 35.6% agree that current IoT regulations in Indonesia are only sufficiently clear, 25% strongly agree with this.
4. Regarding IoT security in Indonesia, 33.7% of respondents stated they strongly agree with current IoT security conditions. Similarly with government support, there are 32.8% of respondents who agree with the support that has been provided by the government toward IoT use in Indonesia.
5. Some input from respondents includes assessing the need for technical certification for IoT devices that are available and easily accessible, recorded 36.5% of respondents strongly agree with this.
6. Similarly for personal data protection that supports trust in IoT devices, about 30.8 respondents stated they agree.

7. According to respondents, these IoT devices have significant contribution to digital economic growth, recorded 54.8% stated strongly agree with this.
8. A number of respondents strongly agree with the statement that the absence of specific regulations is the main obstacle in IoT development, recorded 39.4%.

In this research, Likert scale is ordinal but assumed to be interval, so the approach used is Pearson correlation (r). Pearson correlation formula generally:

$$r = \frac{\sum (Xi - \bar{X})(Yi - \bar{Y})}{\sqrt{\sum ((Xi - \bar{X})^2 \sum (Yi - \bar{Y})^2}}$$

The value of r is between -1 and +1 where +1 = perfect positive relationship, -1 = perfect negative relationship and 0 = no linear relationship. To test the relationship among respondent perception variables toward the main aspects of IoT in Indonesia using variables and coding as in Table 10

Table 10. Variables and Coding

Aspect	Variable	Scale	Description
IoT Regulation Clarity	X1	Likert (1–5)	Level of perception of IoT rule clarity
Government Support	X2	Likert (1–5)	Perception toward government support
IoT Significant Contribution	X3	Likert (1–5)	Perception toward IoT contribution
Cybersecurity	X4	Likert (1–5)	Perception toward IoT system security
Personal Data Protection	X5	Likert (1–5)	Perception of IoT data protection
Contribution to Digital Economy	Y	Likert (1–5)	Perception of IoT impact toward digital economy

The results of that relationship calculation as in Table 11.

Table 11. Pearson Correlation Calculation Results

Correlations						
		X1	X2	X3	X4	X5
X1	Pearson Correlation	1	.589**	.161	.463**	.461**
	Sig. (2-tailed)		.000	.105	.000	.000
	N	103	103	103	103	103
X2	Pearson Correlation	.589**	1	.079	.577**	.565**
	Sig. (2-tailed)	.000		.429	.000	.000
	N	103	103	103	103	103

X 3	Pearson Correlation	.161	.079	1	.084	.153
	Sig. (2-tailed)	.105	.429		.398	.123
	N	103	103	103	103	103
X 4	Pearson Correlation	.463**	.577**	.084	1	.716**
	Sig. (2-tailed)	.000	.000	.398		.000
	N	103	103	103	103	103
X 5	Pearson Correlation	.461**	.565**	.153	.716**	1
	Sig. (2-tailed)	.000	.000	.123	.000	
	N	103	103	103	103	103
**. Correlation is significant at the 0.01 level (2-tailed).						

Table 12. Correlation Elaboration

Variable Relationship	R Value	Sig. (2-tailed)	Correlation Interpretation	Significance Note
X1 ↔ X2	0.589	0.000	Medium-strong positive correlation	Significant
X1 ↔ X3	0.161	0.105	Weak positive correlation	Not significant
X1 ↔ X4	0.463	0.000	Medium positive correlation	Significant
X1 ↔ X5	0.461	0.000	Medium positive correlation	Significant
X2 ↔ X3	0.079	0.429	Very weak positive correlation	Not significant
X2 ↔ X4	0.577	0.000	Medium-strong positive correlation	Significant
X2 ↔ X5	0.565	0.000	Medium-strong positive correlation	Significant
X3 ↔ X4	0.084	0.398	Very weak positive correlation	Not significant
X3 ↔ X5	0.153	0.123	Weak positive	Not significant

Variable Relationship	R Value	Sig. (2-tailed)	Correlation Interpretation	Significance Note
			correlation	
X4 ↔ X5	0.716	0.000	Strong positive correlation	Significant

The strongest relationship is between IoT Security (X4) and Data Protection (X5) with r value = 0.716 (p = 0.000). This means, the higher the perception of IoT security, the higher the perception of personal data protection. This shows that these two aspects mutually support and are viewed as one unit by respondents.

IoT Regulation (X1) has significant relationships with Government Support (X2) → r = 0.589, IoT Security (X4) → r = 0.463 and Data Protection (X5) → r = 0.461, which means, perception about regulation clarity is closely related to how respondents assess government support and guarantees of security and data protection.

Government Support (X2) strongly relates to IoT Security (X4) → r = 0.577, Data Protection (X5) → r = 0.565, where this shows that respondents see the government's role directly influences security aspects and data protection policies in the IoT ecosystem. IoT contribution to digital economy (X3) shows weak and non-significant correlation to all other variables (p > 0.05), this shows perception about IoT economic benefits is relatively independent from regulation, government support, security, or data protection factors.

Various proposals were also raised by respondents, while questionnaire results are in the appendix, and excel results from respondent assessments become datasets, which will then be processed for Deep Deterministic Policy Gradient (DDPG).

Interview results with 15 resource persons provide some overview of IoT implementation for various Industry and manufacturing sectors. One interview resource person was conducted with Tony Wijaya, a technology industry practitioner who currently serves as CEO of SmartFrance/XL Smart, a company engaged in Internet of Things (IoT) solution development in Indonesia. The resource person has experience in IoT implementation across various industry sectors, from manufacturing, mining, to smart city. With this position, his views are considered relevant and credible to assess IoT regulation readiness in Indonesia from industry player perspective. The list of interview resource persons is shown in Table 13.

Table 13 Resource Person Profile

No	Resource Person Name	Description
1	Tony Wijaya	CEO SmartFrance/XL Smart (IoT field Practitioner)
2	Ida Afriliana	IoT field Practitioner
3	Tuada Rahadatul .A	IoT field Practitioner
4	Rudi	IoT field Practitioner
5	Isyfa Khoinunisa	IoT field Practitioner
6	Reynaldi.G	IoT field Practitioner

No	Resource Person Name	Description
7	Andika R.	IoT field Practitioner
8	Arif Rakhman	IoT field Practitioner
9	Roni Darpono	IoT field Practitioner
10	Amanah Nurauliya	IoT User
11	Rosyid Mustofa	IT Civil Registry Office
12	Ayoeng	CEO Molca (IoT field Practitioner)
13	Drs. Mayang Herbimo	Former Head of Civil Registry Office
14	Ahmad Maulana	IoT User
15	Ahmad Firdaus	IoT User

This interview was conducted as part of field validation to answer research problem formulation, namely assessing the extent of IoT regulation readiness in Indonesia and how national policy direction should be formed. By exploring perceptions from industry players, this interview is expected to provide:

a. Empirical confirmation of literature review findings regarding IoT regulation weaknesses in Indonesia.
b. Identification of policy gaps between existing regulations and industry needs.
c. Concrete input in formulating more comprehensive national IoT policy proposals.

Based on interview results, there are several important and relevant matters that become focus in IoT policy, as shown in table 14. below:

Table 14. Main Findings Based on Resource Person Quotes

Analysis Theme	**Resource Person Quote**	**Interpretation**
Regulation Fragmentation	"The government actually already has several rules like ITE Law and PDP Law, but they are all still separate. There is not yet one legal umbrella that truly unifies." (Wijaya, Personal Interview, October 2, 2024)	IoT regulations in Indonesia are not yet integrated and still sectoral.
Legal Uncertainty	"Many companies ask: if we use sensors and collect public data, is that legal or not? Because there are no clear rules, they become afraid to move."	Industry players face regulatory uncertainty that hinders IoT adoption.
Absence of Security Standards	"IoT has many security gaps, but in Indonesia there is not yet mandatory security certification for devices"	There are not yet IoT device security standardization like SNI.
Low Public Sector	"The public sector and MSMEs are still lagging. Many smart cities only	IoT implementation in government is still

Analysis Theme	Resource Person Quote	Interpretation
Readiness	install CCTV but haven't used AI or analytics."	cosmetic and not yet effective.

Thematic Analysis

Overall, these interview results indicate that Indonesia's readiness for IoT regulation can be categorized as "partial but not yet comprehensive." Although several regulations related to IoT already exist, such as the ITE Law and the Personal Data Protection Law (PDP Law), as well as frequency regulations from the Ministry of Communication and Informatics, there is currently no comprehensive umbrella policy that provides legal certainty.

This finding aligns with the literature analysis results in Chapter 2, which explain that various developed countries, such as the European Union, South Korea, and the United States, already have specific IoT frameworks that cover security by design principles, interoperability standards, and privacy governance. Meanwhile, Indonesia has only adopted a small part of that digital regulation, not in the form of a complete system.

Based on the interview and observation results, it can be concluded that the current regulations in Indonesia are not yet structurally or functionally ready. There are still gaps between industry needs and available legal instruments.

Table 15. Conclusion of Interview and Observation Results

No	Economic Sector	IoT Implementation Example	Main Economic Impact	Estimated Impact (%)	Additional Notes/National Relevance
1	Industry & Manufacturing (Industrial IoT)	Production sensors, predictive maintenance, smart logistics	Increases production process efficiency and reduces machine downtime	25–40% operational cost efficiency	Supports Making Indonesia 4.0 program and manufacturing digital transformation
2	Agriculture & Plantations (Smart Farming)	Soil moisture sensors, automatic irrigation, weather monitoring	Increases harvest yields and efficiency of water/fertilizer use	10–20% productivity increase, 20–25% resource efficiency	Encourages food security and precision agriculture in rural areas
3	Health (IoT in Healthcare)	Wearable devices, telemedicine, remote patient monitoring devices	Reduces treatment costs and expands healthcare access	15–30% healthcare service cost savings	Great potential for 3T region services through e-health

No	Economic Sector	IoT Implementation Example	Main Economic Impact	Estimated Impact (%)	Additional Notes/National Relevance
4	Transportation & Smart City	Traffic sensors, smart parking systems, public transportation management	Reduces congestion, pollution, and travel time	20–30% transportation and energy efficiency	100 Smart City program and digital transportation system integration
5	Energy & Utilities (Smart Grid, Smart Meter)	Energy consumption monitoring, smart grid management	Distribution energy efficiency and consumption transparency	10–15% energy consumption efficiency	Supports national energy efficiency targets and carbon emission reduction
6	Retail & Logistics	Inventory tracking, RFID, temperature and goods position tracking	Supply chain optimization and on-time delivery	15–25% logistics cost savings	Relevant for e-commerce and national product distribution
7	Environment & Disaster Mitigation	Air quality sensors, flood or forest fire detection	Improved early detection and environmental risk mitigation	10–20% decrease in economic loss impact due to disasters	Can support sustainable resource and environmental management
8	Household & Lifestyle (Smart Home/Consumer IoT)	Smart TV, smart speaker, smart home security system	Household energy efficiency and user comfort	5–10% household energy savings	Increases digital adoption of society and digital consumption economy

4. Conclusion

Penelitian ini bertujuan untuk mengevaluasi tingkat kesiapan regulasi Internet of Things (IoT) di Indonesia serta merumuskan usulan kebijakan berbasis analisis data dan pendekatan kecerdasan buatan menggunakan metode **Deep Deterministic Policy Gradient**

(DDPG). Berdasarkan hasil survei terhadap 104 responden, analisis indeks kesiapan komposit, dan simulasi DDPG, tingkat kesiapan regulasi IoT Indonesia berada pada kategori **sedang**, dengan nilai indeks rata-rata sebesar 0,60 pada skala 0–1. Temuan ini menunjukkan bahwa meskipun arah kebijakan nasional telah menunjukkan perkembangan positif, kapasitas regulasi masih belum sepenuhnya mampu mengimbangi laju perkembangan teknologi IoT, khususnya dalam mengantisipasi risiko keamanan siber dan perlindungan data pribadi. Kondisi ini sejalan dengan temuan Prabowo et al. (2023) yang menyatakan bahwa kerangka kebijakan IoT di Indonesia masih bersifat parsial dan belum memiliki pengaturan spesifik yang komprehensif.

Analisis per dimensi menunjukkan bahwa aspek keamanan dan perlindungan data merupakan area dengan tingkat kesiapan terendah, sementara infrastruktur digital dan interoperabilitas relatif lebih siap. Hasil simulasi DDPG memperkuat temuan ini, di mana kebijakan yang berfokus pada penguatan regulasi keamanan dan privasi memberikan dampak paling signifikan terhadap peningkatan indeks kesiapan. Selain itu, aspek kelembagaan juga menunjukkan tingkat kesiapan yang belum optimal akibat lemahnya koordinasi lintas institusi, seperti antara Kementerian Komunikasi dan Informatika, BSSN, dan Kementerian Perindustrian. Fragmentasi ini menyebabkan kebijakan IoT cenderung sektoral dan kurang berkelanjutan, sebagaimana juga ditekankan dalam berbagai literatur internasional (OECD, 2022; ITU, 2023) yang menegaskan pentingnya tata kelola lintas lembaga dalam membangun ekosistem IoT nasional yang resilien.

Dari sisi infrastruktur, meskipun capaian digitalisasi nasional meningkat pesat melalui perluasan jaringan 4G/5G dan pembangunan backbone serat optik, distribusi infrastruktur IoT masih belum merata antara wilayah perkotaan dan perdesaan. Simulasi DDPG dengan pelatihan jangka panjang (1000 episode) menunjukkan kemampuan model dalam mengoptimalkan kebijakan IoT secara lebih strategis dan realistis, dengan mempertimbangkan trade-off antara manfaat kebijakan dan biaya implementasi. Hasil ini mengindikasikan bahwa pendekatan kebijakan yang gradual dan proporsional lebih efektif dibandingkan intervensi ekstrem yang berbiaya tinggi. Secara keseluruhan, penelitian ini menegaskan bahwa penguatan perlindungan data pribadi, peningkatan keamanan perangkat, dan integrasi koordinasi kelembagaan merupakan arah kebijakan paling berdampak, serta memberikan dasar kuantitatif yang terukur untuk mempercepat transformasi digital dan meningkatkan kepercayaan publik terhadap implementasi IoT di Indonesia.

Recommendations

Based on research results and literature review, several policy recommendations that can be proposed are as follows: Strengthening Security and Data Privacy Regulations The government, through the Ministry of Communication and Informatics and BSSN, needs to establish an IoT regulatory framework that emphasizes security by design and privacy by default. Security standards must be applied mandatory for IoT device producers and service providers, equipped with device security certification and periodic audits. PDP Law (2022) provisions must be integrated with IoT technical policies to ensure that personal data protection encompasses the entire device life cycle.

Formulation of Integrated National Regulatory Framework Across Sectors Current IoT policies are still scattered across various sectoral regulations. A "National IoT Policy Framework" design is needed that serves as a legal umbrella for all sectors, encompassing aspects of security, interoperability, and device certification. BSN can lead the formulation of IoT-specific SNI as a national technical basis, while cross-ministerial coordination needs to be formalized through Presidential Regulation or a permanent coordination body.

Acceleration of Digital Infrastructure Development and Equalization The government needs to expand the broadband network, accelerate 5G implementation

outside the Greater Jakarta area, and optimize the allocation of NB-IoT and LoRa spectrum. The Universal Service Obligation (USO) program should be directed not only to provide basic internet access, but also to support the connectivity of IoT devices. In addition, fiscal incentives for operators and companies investing in 3T regions (frontier, outermost, and disadvantaged) will help reduce the digital divide.

Improving Institutional Capacity and Inter-Agency Coordination. The formation of the IoT Regulation Task Force, comprising the Ministry of Communication and Informatics, BSSN, the Ministry of Industry, BSN, and academics, is necessary to accelerate policy synchronization. This institution is responsible for determining priorities, harmonizing regulations, and monitoring industry compliance. Capacity-building activities for regulators and researchers in the IoT security field also need to be strengthened.

Economic Incentive Schemes and Support for Local Innovation. The government can provide tax relief, research subsidies, or ease certification requirements for the local IoT industry, ensuring compliance with security and interoperability standards. This approach has proven effective in countries such as South Korea and Singapore (OECD, 2021), where financial support can accelerate national IoT adoption without compromising security aspects.

Improving Digital Literacy and Public Awareness. Public education regarding device security and data privacy needs to be intensified through national campaigns, educational curriculum, and community-based training. User awareness is a crucial factor in mitigating data leak risks and fostering public trust in IoT technology.

Regular and Data-Based Policy Evaluation

The government needs to implement an evidence-based policy approach by utilizing simulation methods, such as DDPG or system dynamics, to assess policy impacts before implementation. An annual evaluation of the regulation readiness index will ensure that policies remain relevant and responsive to national digitalization dynamics.

Future Research Direction

Future researchers are advised to expand the data scope, both sectorally and temporally, and develop more realistic simulation models, such as agent-based modeling. Integration of socio-economic, cultural, and political factors in policy models is also important to understand field implementation obstacles

References

1. Amalia Yunia Rahmawati, Ida Afriliana, Safar Dwi Kurniawan, dkk (penamuda meida). (2020). *Intenet ofThings*. *July*, 1–23.
2. Anwar, Y. Z., & Sanmorino, A. (2024). Hukum dan Kebijakan Keamanan Siber: Tantangan Regulasi Perangkat IoT. *Jurnal Ilmiah Informatika Global*, *15*(3), 95–99.
3. Bastos, D., Giubilo, F., Shackleton, M., & El-moussa, F. (2018). *GDPR Privacy Implications for the Internet of Things GDPR Privacy Implications for the Internet of Things*. *December*.
4. Ghag, O. M. (n.d.). *Regulatory Compliance and Certification in IoT Development*. *1*(3), 1–3.
5. Hadzovic, S. (2021). Internet of Things from a regulatory point of view. *2021 20th International Symposium INFOTEH-JAHORINA (INFOTEH)*, 1–4.
6. Kelola, T., Sistem, P., Informasi, T., & Tik, D. A. N. K. (2020). *TATA KELOLA PERENCANAAN SISTEM TEKNOLOGI INFORMASI GOVERNANCE OF INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SYSTEM PLANNING*. *July 2015*. https://doi.org/10.20422/jpk.v18i1.20
7. Kusumawati, D., Winarko, B., Wahab, A., & Pradono, W. (2017a). *Analisis*

Kebutuhan Regulasi Terkait dengan Internet of Things Analisis Kebutuhan Regulasi Terkait dengan Internet of Things The Analysis of The Required Regulation of Internet of Things. *December*. https://doi.org/10.17933/bpostel.2017.150205

8. Kusumawati, D., Winarko, B., Wahab, R. A., & Pradono, W. (2017b). Analisis Kebutuhan Regulasi Terkait dengan Internet of Things [The Analysis of The Required Regulation of Internet of Things]. *Buletin Pos Dan Telekomunikasi*, *15*(2), 121–138.
9. Lim, Y., Edelenbos, J., Gianoli, A., & Lim, Y. (2023). *Dynamics in the governance of smart cities : insights from South Korean smart cities Dynamics in the governance of smart cities : insights from*. *5934*. https://doi.org/10.1080/12265934.2022.2063158
10. Mar'ah Nailul Faroh, S.Pd.I, M.Pd., Safar Dwi kurniawan, S. K., M.Kom., Dr. Dwi Prasetyo, Dipl.Inf, S.Kom, M.Si., Ida Afriliana, S., M.Kom., Qirom, S.Pd., M.T., Ajang Sopandi, S.Kom., M.Kom., N., Hendri Adi Nurohim, S.ST., M.Kom., Nurohim, S.ST., M.Kom., A., Irmansyah Lubis, Rometdo Muzawi, M.Kom., CEH., CCNA., Rais, S. P., & M.Kom., Anton Prafanto, Muhammad Panji Muslim, S.Pd., M. K. (2023). *Internet of Things*.
11. Mayfield, J. (2015). *FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privasy and Security Risks*.
12. *Measuring the Internet of Things.pdf.crdownload*. (n.d.).
13. Mireles, M. S. (2023). 36 Cybersecurity Standards and Trade Secrecy in the United States. *Developmensts and Directions in Intellectual Property Law*.
14. Mth, E. (2024). Menggali Kecanggihan Teknologi IoT Korea Selatan.pdf. *Universitas Ciber Asia*.
15. Pratama, G. G., Hukum, F., & Padjadjaran, U. (2019). *Urgnesi Perlindungan Data Privasi Dalam Era Ekonomi Digital dI Indonesia*. *June 2018*. https://doi.org/10.25123/vej.2916
16. Salman, T., & Jain, R. (2017). *Advanced Computing and Communications , Vol . 1 , No . 1 , March 2017 . 1*(1).
17. Salwa, N. D. K. (2024). Kebijakan IoT di Indonesia.pdf. *Cloud Computing Indonesia*.
18. Sembiring, T. B., Koynja, J. J., Maharaja, T., & Febryani, E. (n.d.). *REVOLUSI TEKNOLOGI DAN TANTANGAN HUKUM: PERSPEKTIF PRIVASI DAN KEAMANAN DATA DALAM ERA INTERNET OF THINGS (IOT) 1Tamaulina*. 1217–1222.
19. Soori, M., Arezoo, B., & Dastres, R. (2023). Internet of things for smart factories in industry 4.0, a review. *Internet of Things and Cyber-Physical Systems*, *3*(April), 192–204. https://doi.org/10.1016/j.iotcps.2023.04.006
20. Y.2060, R. I.-T. (2012). *GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXTGENERATION NETWORKS*.