Vol. 2, Iss. 4 (2025) 151-158, DOI: 10.61552/JMES.2025.04.001

Journal of Management and Engineering Sciences

www.jmes.aspur.rs

Global VS Philippines: A Comparative Analysis of Data Privacy and Security Standards for Internet of Things Infrastructure

Elaine Aldous I. Samizo[a], Joseph T. Mindaña[a], Romeo Jousef A. Laxamana[a,*]

[a] *Batangas State University – The National Engineering University, College of Engineering Technology, Alangilan, Batangas City, Batangas, Philippines.*

Keywords:

Internet
Data Privacy
Cybercrime
Data Security
Internet of Things

* Corresponding author:

Romeo Jousef A. Laxamana
E-mail:
romeojousef.laxamana@g.batstate-u.edu.ph

Received: 21.10.2024.
Revised: 23.01.2025.
Accepted: 28.01.2025.

A B S T R A C T

The global surge in Internet of Things (IoT) devices has intensified concerns about data privacy and security. This study examines IoT data privacy and security standards in the Philippines, Japan, and the United States, emphasizing regulatory frameworks, enforcement strategies, and practical applications. As information technology advances, the importance of protecting IoT privacy has garnered significant attention. This paper explores privacy and security challenges across different IoT levels and proposes a comprehensive framework for addressing these concerns. The findings highlight notable differences in regulatory development, resource distribution, and adherence to global best practices. The study concludes by identifying pathways for the Philippines to strengthen its IoT security landscape through targeted legislation, international partnerships, and capacity-building measures, leveraging Japan's collaborative approach and the technical precision of U.S. standards.

1. INTRODUCTION

Internet of Things (IoT) is an integral part of modern life, connecting devices and enabling real-time data exchange across various industries. In the Philippines, IoT adoption is accelerating in sectors like healthcare, agriculture, and smart cities, driving innovation and efficiency. IoT devices collect and transmit vast amounts of sensitive data, making them highly susceptible to cyberattacks and breaches. Globally, frameworks like the European Union's General Data Protection Regulation (GDPR) and the United States' NIST Cybersecurity Framework provide comprehensive standards for addressing these issues. Cybercrime has become an escalating concern in the Philippines, driven by rapid technological advancements and

increasing digital interconnectivity across industries. This paper explores the dynamics of the cybercrime landscape in the Philippines, contextualizing its growth within the nation's technological and socio-economic framework. The interplay between limited cybersecurity infrastructure, inadequate public awareness, and the digital divide has compounded the vulnerability of individuals and organizations to cyber threats. Additionally, the Philippines' role as a regional hub for IT services and its strategic geographical position have made it a target for financially, politically, and ideologically motivated cyber-attacks. By benchmarking the Philippines' cybersecurity practices against global standards and those of other countries, this study seeks to identify gaps and opportunities to bolster the nation's defenses against the evolving cyber threat landscape.

2. LITERATURE REVIEW

2.1 Data privacy and Data Security in the United States

The United States Laws regarding Data Privacy Protection included the; Privacy Act of 1974 where it prohibits agencies to share data or information without a written consent or permission; the Health Insurance Portability and Accountability Act (HIPAA) which enacted two key sections: the Security and Privacy rule. This gives the health information providers and processors the ability in how they protect their client's data; the Gramm-Leach-Bliley Act that requires financial institutions to explain their information-sharing practices to their clients and to safeguard their data; Children Online Privacy Protection Act (COPPA) that aims to protect users under the age of 13 who utilize online services; and to California, the only state to have implemented its own state level Data Privacy Law. The California Consumer Privacy Act (CCPA) known as the strictest data privacy law in the U.S. This act is applied to businesses that collect personal information about consumers and outlines specific rights consumers have. The act allows consumers the right to know how their data is shared, and the right to freely delete their personal information collected by the business [1].

California being the first state to have its own state-level Data Privacy Law. The California Consumer Privacy Act (CCPA) that was implemented on the 1st of January, year 2020. Specifies that the consumers might ask businesses to disclose the type of information they collect, the purpose of collecting the data and its source. On the other hand, the California Privacy Rights Act that took effect on January 1, 2023. It enhances and modifies the CCPA by granting citizens the power to stop firms from sharing their personal information, to request the correction of inaccurate personal information, and to stop businesses from using sensitive PII, such as sexual orientation and race [2].

2.2 Blockchain in the IoT in United States

Seventy-five percent of IoT technology adopters in the United States have already adopted blockchain or are planning to adopt it by the end of 2020. Among the blockchain adopters, 86% are implementing the two technologies together in various projects, according to survey results from Gartner. The integration of IoT and blockchain networks is a sweet spot for digital transformation and innovation. It is actually moving ahead at a much faster pace than expected, according to the survey [3].

2.3 Data Privacy and Security Data in Japan

Koji Nakao stated that" but, as you may know, the automatic translation systems have not been so advanced in the case of translation into Japanese. So, when I read such emails containing some malicious URL, the Japanese seems to be extremely badly written, and we can easily identify that there is something wrong here and that this is malicious". This indicates that in order to identify if the emails sent to you have some malicious intent behind it, you should note its fluency in Japanese. By this, the Japanese are thought to be wary of such emails containing such poor Japanese translations. He also stated that we have two kinds of basic regulations in Japan. One is the Communications Secrecy Law. For example, in the case where an Internet Service Provider (ISP) gets information about the user – the source user, the destination user, the communication time, the amount of data, and the content – in order to route and deliver the information, this set of information should not be disclosed outside, because the ISP needs to protect this kind of communication data to comply with this law. This is a very basic regulation for

telecommunications carriers in Japan, and Germany has a similar law.

On the other hand, the Unauthorized Access Law is another regulation in this context". Wherein he briefly explained Japan's two kinds of Data Privacy and Security Data; the Communications Secrecy Law and the Unauthorized Access Law [4].

Japan's Data Privacy and Cybersecurity Handbook stated that the Act on Protection of Personal Information (APPI), Japan's data protection law, was modified. The 2023 modifications increased the security procedures and data breach notification requirements that businesses must follow, even though they had less of an impact than the 2020 amendments. The Personal Information Protection Commission has started its 3-year review process to assess and identify potential amendments to the APPI [5].

2.4 Blockchain in the IoT in Japan

Japan is making waves by adopting blockchain technology and non-fungible tokens (NFTs) to boost its local economies. Prime Minister Shigeru Ishiba sees these digital innovations as vital for rejuvenating areas hit hard by economic downturns, especially in sectors like agriculture, culture, and tourism [6].

2.5 Data Privacy and Security Data in the Philippines

The Department of Information and Communications Technology (DICT) has emphasized the necessity of developing security standards and frameworks, particularly in the context of 5G technology as this is the main concern with regards to Data Privacy in the Philippines. Vulnerabilities in 5G architecture, such as the radio access network (RAN) and core network, along with the proliferation of Internet of Things (IoT) devices, are exacerbating security risks. One important step that the DICT initiated is the implementation of the Network Equipment Security Assurance Scheme (NESAS) for the Global System for Mobile Communications (GSMA). A thorough framework for assessing the security of mobile network equipment is offered by NESAS, which covers topics including vendor development procedures, product lifecycle management, and security testing. By following NESAS guidelines, suppliers can show that they are dedicated to protecting the security and integrity of their goods. In order to improve the security and dependability of its mobile network infrastructure, the Philippines plans to use internationally accepted cybersecurity standards like NESAS in the future. By following these guidelines, the nation hopes to uphold the robustness of its telecommunications networks, foster competition, encourage innovation, and foster trust in the digital age. In an increasingly digital world, the Philippines is well-positioned to fortify its cybersecurity posture and safeguard the interests of its citizens thanks to the momentum created by the adoption of NESAS in other regions [7].

The security for Internet of Things (IoT) in the Philippines. That the cyber defenses of corporations are being strengthened. 94% of respondents increased the pace of their digital transformation projects. With identity and access management at the top of the list (57%), local firms are also putting cybersecurity plans into practice [8].

2.6 Blockchain in the IoT in the Philippines

Blockchain technology in the Philippines has been evolving, showing promise in addressing various issues, including those in the Internet of Things (IoT) ecosystem. The country has been exploring blockchain to improve data transparency and security across sectors, with an increasing number of startups and government-backed initiatives leveraging this technology. In particular, the integration of blockchain and IoT has been highlighted in projects like the rehabilitation of the Pasig River, where IoT devices and blockchain are used to monitor environmental data in real time, ensuring transparency and accountability in the cleanup efforts [9].

A research into the status and trends of blockchain adoption in the Philippines indicates that there is a growing interest in using blockchain for digital assets and public services. The intersection of blockchain with IoT presents opportunities for secure data exchanges, enhancing trust in automated systems and ensuring the integrity of information shared across connected devices. However, challenges such as regulatory frameworks, scalability, and

public awareness remain, limiting the broader adoption of these technologies [10].

3. METHODOLOGY

3.1 Strategies of United States in Data Privacy and Security Standards

The country known as one of the countries with a high level of Cybersecurity, the United States (US) proves to handle one's data safely, ensuring safe possession of your sensitive information. To handle data privacy, the US uses a mix of federal and state legislation, industry standards, and regulatory actions. In contrast to certain other countries, like the European Union, the United States lacks a single, all-encompassing data privacy regulation. Rather, it employs a sectoral strategy that incorporates a number of frameworks and techniques to safeguard data privacy. They've also established Self-Regulation and Industry Standards which are; the Payment Card Industry Data Security Standard (PCIDSS) which applies to companies handling credit card transactions that sets security standards and the Digital Advertising Alliance (DAA) Principles that provides necessary guidelines for online behavioural advertising and data collection.

In terms of IT Infrastructure, the US is supported by a variety of methods and frameworks to ensure scalability, security, and efficiency. This includes; the use of On-premise and Cloud Computing Infrastructure which is the set of software and hardware components required to make cloud computing possible. It has networking, storage, and processing capacity in addition to an interface that lets users access their virtualized resources. It offers the same capabilities as physical infrastructure but can provide additional benefits like a lower cost of ownership, greater flexibility, and scalability; Hybrid Infrastructure which is a mix of both [11].

3.2 Strategies of Japan in Data Privacy and Security Standards

Japan has a well-established framework for data privacy, primarily governed by the Act on the Protection of Personal Information (APPI), which was first enacted in 2005 and has since undergone significant amendments to address evolving digital privacy concerns. Japan's APPI is a federal personal information protection law to regulate the handling of personal information by individuals and organizations, including government agencies, businesses, and nonprofits. It mandates that companies that wish to gather personal data must get people's consent before collecting, using, or sharing it—but only under specific circumstances, including when the data is sensitive or needs to be forwarded to a third party or outside of Japan. In many situations, the APPI does not require consent for the collection or use of personal information that is not sensitive or that satisfies other requirements, which is more in accordance with US law. It was applied to business operators before, but due to the recent amendment, it now takes effect to all business operators that process personal information for commercial purposes regardless of how many individuals' personal information they process. [5]

With regards to the IT Infrastructure methods that Japan uses, Japan utilizes Advanced Network Infrastructure offering Broadband Penetration, 5G Deployment, and IPv6 Adoption. They also use Data Centers, and Cloud Computing. Together with establishing a Cybersecurity Framework, this makes up Japan's IT Infrastructure that keeps one's personal and sensitive data or information.

3.3 Strategies of Philippines in Data Privacy and Security Standards

The Philippines, already a developing country, have already established some ways for data to be private in terms of the utilization of Internet of Things (IoT) Devices in the growing world. With the help of the Data Privacy Act established in 2012, privacy of data could be achieved as it enables limited access to such sensitive information to only a most fundamental component for protecting personal data used in the whole world. Encryption converts sensitive information into a coded form which can only be decoded by authorized individuals [12].

With regards to IT Infrastructure, the Philippines has also established some methods as to how they keep your data secure and private. On-premise Infrastructure is one of the Philippines methods to keep your data safe, it is when companies establish their own Information Technology (IT) and physical resources, such as computer systems, applications, servers, and data storage, within their own facilities. It offers

significant advantages, such as customization capabilities and total control over the infrastructure, allowing adjustments according to specific needs at any given time. However, it presents challenges such as the need to invest capital and intensively manage the infrastructure. Here are some of the companies that offer on-premise infrastructure services in the Philippines; NTT DATA Philippines, Archive One, and Oracle Philippines [13].

4. RESULTS AND DISCUSSIONS

4.1 IT Infrastracture

The United States, Japan, and the Philippines demonstrate varying levels of technological development across several dimensions. The US leads globally with an average internet speed of 161.97 Mbps, supported by robust broadband infrastructure and widespread fiber optic networks, while Japan follows closely at 139.53 Mbps, reflecting its commitment to high-speed fiber deployment. The Philippines, at 52.07 Mbps, has made progress but requires further investment in broadband expansion. In 5G penetration, the US and Japan boast urban coverage rates of 85–90%, showcasing advanced mobile networks, whereas the Philippines lags at ~30%, with deployment still in its early stages but expanding to 105 cities as of April 2023. In terms of data centers, the US dominates with 2,700 facilities, accounting for 40% of global capacity, while Japan's 200 centers emphasize disaster resilience, and the Philippines, with ~22 centers, shows growth potential. E-government rankings reveal Japan (13th, 0.93) and the US (19th, 0.91) as leaders in digital governance, whereas the Philippines (76th, 0.76) indicates progress but needs further digitization and infrastructure development. Finally, in cybersecurity, the US and Japan are Tier 1 nations with strong frameworks like NIST and robust anti-cyber threat measures, while the Philippines, a Tier 2 nation, continues to face challenges despite ongoing initiatives to enhance its cybersecurity infrastructure.

Table 1. Infrastructure of Information Technology of Philippines, Japan and United States.

	Philippines	Japan	United States
Internet Speed	52.07	139.53	161.97
5G Coverage	~30%	~90%	~85%
Data Centers	~22	~200	~2700
E-Government Development Index (EGDI)	0.76	0.93	0.91
Cybersecurity Ranking	Tier 2	Tier 1	Tier 1

4.2 IoT Infrastracture

The Philippines, United States, and Japan exhibit different levels of progress in 5G deployment, IoT adoption, and smart technology integration. The Philippines is in the early stages of 5G rollout, with about 10% urban coverage and 105 cities connected as of April 2023, still relying on 4G LTE for IoT connectivity. In contrast, the US leads with 80% 5G coverage, enabling advanced IoT applications in smart cities and autonomous vehicles. Japan, with 50% 5G coverage concentrated in major metropolitan areas, focuses on integrating 5G into smart city and autonomous systems initiatives.

In smart city development, the Philippines has pilot efforts in Makati and Davao, while the US has over 30 communities implementing diverse initiatives, such as environmental monitoring and smart traffic. Japan is progressing with 5–10 cities like Tokyo and Kobe leveraging IoT for transportation, disaster resilience, and energy efficiency. IoT adoption in the Philippines is concentrated in agriculture and healthcare, with a 50% adoption rate, while the US (80%) and Japan (85%) lead in areas like smart manufacturing, healthcare, and agriculture.

Smart grid technologies show varying levels of adoption: the Philippines lags with 10% integration, while the US incorporates IoT energy solutions in 40% of its systems. Japan excels with 50% integration, focusing on renewable energy and efficiency. Environmental monitoring via IoT highlights similar disparities, with 20% of

Philippine metropolitan areas using sensors compared to 60% in the US and 70% in Japan, where advanced systems manage air quality and disaster resilience.

Table 2. Infrastructure of Internet of Things in the Philippines, Japan and United States.

	Philippines	Japan	United States
5G Coverage	10%	80%	50%
Smart City Projects	3-5 cities	30+	5-10
IoT Adoption in Industry (Manufacturing, Healthcare, Agriculture)	50%	80%	85%
Smart Grid Deployment	10%	40%	50%
Environmental IoT Solutions	20%	60%	70%
Government IoT Investment	Moderate	High	High
Integration with 5G for IoT Applications	5%	70%	60%

In IoT cybersecurity, the Philippines achieves 60% compliance, while the US (90%) and Japan (85%) uphold strict security standards, bolstered by frameworks like NIST. The Philippines has moderate investments in IoT under its Department of Information and Communications Technology, whereas the US and Japan benefit from significant government support in smart city and energy initiatives. Integration of 5G with IoT applications is minimal in the Philippines (5%) but more advanced in the US (70%) and Japan (60%), particularly in healthcare, smart cities, and autonomous vehicles.

4.3 IoT Regulations

The cybersecurity and IoT landscape in the Philippines, Japan, and the United States shows significant differences in terms of measures, compliance, certification, connectivity, and standardization. Both Japan and the U.S. have robust cybersecurity frameworks, with 99% of cyber measures and 98% of compliance in place, while the Philippines also demonstrates strong measures but faces challenges in full compliance and policy implementation. IoT certification is more advanced in the U.S. (60% of manufacturers comply) and Japan (55% of devices certified), while the Philippines lags behind with only 40% of devices meeting security standards. Spectrum allocation reveals a disparity: Japan leads with 1100 MHz for 5G, followed by the U.S. with 450 MHz, and the Philippines with 3.4-3.7 GHz. In terms of interoperability and standardization, Japan excels, with 70% of IoT systems meeting international standards, while the U.S. follows closely with 65% compliance, and the Philippines is at 30%, reflecting the need for further infrastructure development. These figures indicate that Japan and the U.S. are more advanced in IoT integration and cybersecurity, while the Philippines faces room for improvement in infrastructure, certification, and standardization.

Table 3. Regulations of Internet of Things in the Philippines, Japan, and the United States.

	Philippines	Japan	United States
Cybersecurity Improvement Act	99% (cyber measures)	98% (cyber compliance)	95% (cyber policies)
Certification of IoT Security	40% (IoT Devices)	55% (IoT Devices)	60% (IoT manufacturers)
Spectrum Allocation and Connectivity	3.4–3.7 GHz	1100 MHz	450 MHz
Interoperability and Standardization	30% (technical infrastructure)	70% (IoT systems)	65% (IoT Devices)

4.4 Data Privacy in Internet of Things

The adoption of privacy-focused technologies and data protection measures in IoT varies across the Philippines, Japan, and the United States. In terms of privacy-focused IoT technologies, Japan leads with 70%, followed by the U.S. at 60%, and the Philippines at 40%, reflecting stronger regulations and technological infrastructure in Japan. Regarding cybersecurity and IoT data privacy, the U.S. stands out with 90% of IoT devices ensuring robust security, while Japan follows at 85% and the Philippines lags behind at 60%. Privacy attacks on IoT devices are most prevalent in the U.S. (32%) and Japan (30%), with the Philippines experiencing 20% of such attacks. Finally, in the collection, use, and disclosure of IoT data, the U.S. is again ahead at 70%, Japan at 60%, and the Philippines at 40%, highlighting the Philippines' ongoing challenges in IoT data privacy and security. These disparities underscore the need for continued development in regulatory frameworks, enforcement, and technology in the Philippines, while Japan and the U.S. continue to make strides in addressing IoT security and privacy concerns.

Table 4. Data Privacy in Internet of Things (IoT) in the Philippines, Japan and United States.

	Philippines	Japan	United States
Privacy-Focused Technologies in IoT	40%	70%	60%
Cybersecurity and IoT Data Privacy	60%	85%	90%
Privacy attacks in IoT	20%	30%	32%
Collection, use, and disclosure of IoT Data	40%	60%	70%

5. CONCLUSION

The adoption of IoT in the Philippines presents immense opportunities for innovation and economic growth but also raises significant concerns about data privacy and security. While the Data Privacy Act of 2012 provides a foundational framework, it lacks the specificity and technical rigor required to address IoT-specific risks. By comparing the Philippine framework with international standards like GDPR and NIST, this study highlights critical gaps and offers recommendations to strengthen regulatory and technical measures. Addressing these challenges will be crucial for fostering a secure IoT ecosystem that balances innovation with the protection of user data and privacy.

Acknowledgement

We would like to acknowledge our family and friends by providing us moral and monetary support during the development of this study.

Lastly, we give thanks to the Lord, Jesus Christ by giving us wisdom and understanding before, during, and after the development of this research study.

REFERENCES

[1] C. Murray, (2023). "US Data Privacy Protection Laws: A Comprehensive Guide." https://www.forbes.com/sites/conormurray/2023/04/21/us-data-privacy-protection-laws-a-comprehensive-guide/ (accessed 2023).

[2] P. Kirvan. "U.S. Data Privacy Protection Laws: 2025 Guide." https://www.techtarget.com/searchsecurity/tip/State-of-data-privacy-laws#:~:text=U.S (accessed 2024).

[3] "Blockchain combined with IoT is booming in the U.S.," News Group. Institute for Operations Research and the Management Sciences (INFORMS), 2019. doi: 10.1287/lytx.2020.01.13n.

[4] K. Nakao, "Cyber Security & Data Protection in Japan." https://www.dotmagazine.online/issues/safe-xmas/why-it-security-is-like-shopping-for-christmas/cyber-security-data-protection-in-japan (accessed 2017).

[5] Usercentrics, "Japan Act on the Protection of Personal Information (APPI): An Overview." https://usercentrics.com/knowledge-hub/japan-act-on-protection-of-personal-privacy-appi/ (accessed 2023).

[6] Onesafe, "Japan's Blockchain Revolution: Boosting Local Economies." https://www.onesafe.io/blog/blockchain-

technology-japan-economic-growth#:~:text=Japan%20is%20making%20waves%20by,agriculture%2C%20culture%2C%20and%20tourism (accessed 2024).

[7] Telecom Review, "Data Privacy and Security Concerns in the Phillipines Telecom Sector." https://www.telecomreviewasia.com/news/featured-articles/4192-data-privacy-and-security-concerns-in-the-philippines-telecom-sector (accessed 2024)

[8] A.L. Monton, "Internet of Things in the Philippines." https://www.globalsign.com/en-sg/blog/iot-philippines (accessed 2022).

[9] C. Rivet, "Philippines to use blockchain and IoT devices to clean up Pasig River." https://coinrivet.com/philippines-to-use-blockchain-and-iot-devices-to-clean-up-pasig-river (accessed 2018).

[10] M. F. Bongo and A. B. Culaba, "Blockchain technology in the Philippines: Status, trends, and ways forward," 2019 IEEE 11th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM), pp. 1–8, Nov. 2019, doi: 10.1109/hnicem48295.2019.9073349.

[11] Cloud Zero, "What Is Cloud Infrastructure? Everything You Need To Know." https://www.cloudzero.com/blog/cloud-infrastructure/#:~:text=Cloud%20infrastructure%20is%20a%20set,specific%20workloads%20over%20the%20internet (2023).

[12] Titan File, "Top 5 Methods of Protecting Data." https://www.titanfile.com/blog/5-methods-of-protecting-data/#:~:text=Encryption,decode%20and20view%20the%20information (2024).

[13] Stark Cloud, "Infrastructure Decisions: Cloud vs On-Premise." https://www.starkcloud.com/en/starkcloud-blog/infrastructure-decisions-cloud-vs-on-premise#:~:text=On%2DPremise:%20Total%20Control%20and,and%20worry%20about%20local%20infrastructures (2024).