International Summit on Science Technology and Humanity
ISETH 2023
ISSN: 2807-7245 (online)

Toward A Comprehensive Framework for The Regulation of IoT Devices in Indonesia: A Taxonomic Analysis

Isman[1,*], Novita[2]

[1, 2] Universitas Muhammadiyah Surakarta

Abstract

This study aims to devise a regulatory framework for IoT devices in Indonesia via taxonomic analysis. Taxonomic analysis is the methodological approach to discern pivotal dimensions imperative for comprehensive IoT regulations. The outcomes underscore the imperative for regulatory inclusivity across boundaries to address the intricate nexus of technology, security, and device heterogeneity. The investigation underscores the importance of accessibility, anonymity, and interactivity in safeguarding user access and data within IoT networks. Furthermore, it accentuates the urgency for swift responses to security vulnerabilities. This research posits that Indonesia's IoT regulations must adeptly navigate the intricacies and dynamism inherent in the IoT landscape while addressing the evolving security challenges within this technological milieu.

Introduction Section

The exponential growth of Internet of Things (IoT) technology in Indonesia underscores the pressing need for a comprehensive scrutiny of regulatory frameworks to uphold the security and reliability of IoT devices.[1] With the escalating number of IoT deployments, there is a corresponding elevation in the significance of instituting comprehensive certification standards to safeguard user privacy, ensure data integrity, and bolster overall system security.[2] This paper undertakes a pivotal exploration to advance regulatory discourse by focusing on developing a robust IoT device certification framework specifically tailored to the Indonesian context.[1,3]

To address this imperative, our research adopts a taxonomic approach, delving into the intricate details of existing IoT device certification practices and proposing a comprehensive framework aligned with Indonesia's regulatory landscape. We commence this investigation by conducting an extensive literature review, synthesizing insights from diverse sources that categorize and classify IoT devices and certification processes.[4] By drawing upon existing taxonomies related to IoT security and certification, we establish the foundation for our analytical framework.[5,6]

The primary objective of this paper is to present a taxonomy that comprehensively encapsulates the multifaceted aspects of IoT device certification, considering not only technical specifications but also the legal and regulatory dimensions specific to Indonesia.[7] As we navigate through a taxonomic analysis, we meticulously scrutinize international best practices, identifying gaps and nuances essential for tailoring a framework that aligns with Indonesia's unique sociotechnical landscape.[8]

Beyond the theoretical foundation, our study considers the practical implications of implementing such a certification framework.[9–12] We explore the potential stakeholders involved—from government bodies and regulatory agencies to industry players—and underscore the collaborative efforts required to establish and enforce certification standards effectively. Additionally, the research highlights the role of this certification framework in promoting consumer trust, fostering industry growth, and contributing to the overall advancement of IoT technology in Indonesia.

In conclusion, this paper catalyzes discussions surrounding the establishment of a comprehensive IoT device certification framework in Indonesia. By employing a taxonomic analysis, we aspire to offer a structured and nuanced perspective that identifies challenges and outlines actionable steps toward fortifying the regulatory ecosystem for IoT devices.[13] Through this endeavor, we contribute to the ongoing discourse on IoT governance, positioning Indonesia at the forefront of secure and resilient IoT deployments.[12,14]

* Corresponding author: ism190@ums.ac.id

Method

This research employs a systematic approach to develop a comprehensive IoT device certification framework tailored for Indonesia.[12] Taxonomic analysis is adapted to scrutinize and categorize the various components and dimensions involved in IoT device certification from both a software and hardware perspective.[15] The study begins by establishing an overarching taxonomy that defines the core components integral to IoT device certification in Indonesia.[16] Three primary device categories are identified: the Certification Authority, the Certification Process, and the Certified Devices. These categories encapsulate the core elements of the certification ecosystem. [17]

Certification Authorities are depicted as gateways, processing certification requests, while Certified Devices encompass various hardware elements that contribute to the overall IoT ecosystem.[18] Our research aims to provide a structured understanding of the intricate facets of crafting a comprehensive IoT device certification framework in Indonesia.[19] The systematic approach ensures that various dimensions, encompassing both software and hardware aspects, are thoroughly explored to contribute to the advancement of regulatory practices in the evolving IoT landscape of Indonesia.[20]

Results and Discussion

This paper analyses Indonesia's IoT device certification framework, commencing with exploring the broader IoT landscape.[21] The IoT is often likened to a complex territory defined by its inherent boundaries. These boundaries encapsulate the expansive and intricate nature of the IoT, marked by a myriad of interconnected devices with diverse functionalities and behaviors.[22] Our discussion will explore the facets of accessibility beyond these borderlines.[23] The ubiquitous nature of IoT devices provides an unprecedented level of accessibility but also raises concerns about security and privacy.[19] Anonymity, a crucial aspect of IoT interactions, presents challenges and considerations regarding the identification and privacy of users and devices within the network.[24] The discussion covers interactivity, which refers to the exchanges between devices and users. It is important to balance seamless connectivity with potential vulnerabilities. The discussion also acknowledges the rapid evolution of IoT technologies, which require regulatory frameworks that can adapt quickly to ensure the security and efficiency of IoT ecosystems.[25] This exploration sets the stage for examining Indonesia's IoT device certification framework. The taxonomic analysis of IoT devices will be based on the multifaceted approach presented here.[26]

Navigating the IoT Landscape

The Internet of Things (IoT) has rapidly evolved, witnessing a surge in interconnected smart objects. This proliferation, however, has brought forth an escalating threat landscape, marked by a sharp increase in attacks targeting IoT networks.[27] The sheer volume and diversity of devices in IoT networks make them susceptible to many security challenges.[28] This includes vulnerabilities stemming from the diverse behaviours exhibited by the vast array of connected devices, creating a complex and dynamic environment. Consequently, the IoT is often referred to as a "borderline" due to the intricate and expansive boundaries it occupies at the intersection of technology, security, and the sheer diversity of interconnected devices.[29]

In response to the growing security concerns within the IoT, researchers have been actively developing intrusion detection systems (IDSs) to improve the security posture of these networks.[30] The rapid expansion of IoT networks necessitates the development of advanced IDSs capable of adapting to attacks of a diverse and dynamic nature.[31] The novel IDS presented in this work embraces a multifaceted approach, integrating principal component analysis (PCA) and mayfly optimization (MAO) for dimensionality reduction, the borderline synthetic minority oversampling technique (BSMOTE) for handling imbalanced data, and long short-term memory (LSTM) for classification.[32] This combination signifies a comprehensive strategy aimed at addressing the unique challenges posed by the IoT's expansive and borderless characteristics.[33]

To evaluate the effectiveness of the proposed IDS, a diverse dataset combining the IoTID20, CIC-ToN-IoT, and USB-IDS-1 datasets was curated, providing a robust testing ground. The results of the performance assessment underscore the effectiveness of the hybrid PCA-MAO-based LSTM model, which achieved an impressive accuracy of 99.51%. Notably, the proposed IDS shows superior intrusion detection capabilities, particularly in high dimensionality, complexity, and data imbalance scenarios. This highlights the significance of adopting advanced methodologies, such as the one proposed, to navigate the borderlines of IoT security effectively. As the IoT landscape continues to expand, the need for robust and adaptable security measures becomes increasingly evident, and the proposed IDS represents a commendable stride in this direction.[34]

Taxonomic Analysis

Taxonomic analysis of IoT devices represents a multifaceted approach foundational for exploring and establishing standard regulatory designs for comprehensive certification in Indonesia.[11] The language is clear, objective, and value-neutral, with consistent technical terms and common sentence structure. The text is free from grammatical, spelling, and punctuation errors.[35] No changes in content were made as per the instructions. This approach delves into intricate aspects such as borderlines, accessibility, anonymity, interactivity, and rapidity within IoT networks. As the taxonomy navigates the complex landscape of the IoT, it is clear that a robust regulatory framework is essential for addressing the diverse behaviours exhibited by interconnected devices. The upcoming analysis aims to outline the important considerations for crafting comprehensive IoT certification regulations that align with the nuanced characteristics of the evolving IoT environment.[36]

Borderlines

The term "borderlines" in the context of the IoT refers to its intricate and expansive boundary, emphasizing the intersection of technology, security, and the diverse range of interconnected devices. To address the borderless nature of the IoT, regulations should focus on defining clear boundaries and standards for secure IoT interactions.[37] This involves establishing protocols for device communication, ensuring secure gateways, and defining the permissible scope of IoT networks.[38] The taxonomy suggests that regulations must account for connected devices' diverse behaviour, reflecting the IoT environment's complexity and dynamism. The provided passage emphasizes the necessity for regulations to establish protocols for device communication, ensure secure gateways, and define the permissible scope of IoT networks.[39]

The analysis of this statement in the context of the presented research on IoT security sheds light on several key contributions:

1. **Establishing Protocols for Device Communication:** This research acknowledges the escalating threat landscape in IoT networks due to the increasing number of connected smart objects. To address this, regulations should mandate the establishment of clear and secure protocols for device communication. The taxonomy analysis suggested that these protocols should encompass standards for data exchange, authentication mechanisms, and encryption protocols. By doing so, the regulations can ensure that communication between devices is efficient and secure, mitigating the risk of unauthorized access or malicious attacks.[32]
2. **Ensuring Secure Gateways:** This passage underlines the rapid growth of attacks against IoT networks, indicating the critical need for secure gateways. Regulatory frameworks should include provisions that mandate the implementation of secure gateways in IoT ecosystems. These gateways act as entry points to the network and are often susceptible to attacks. The taxonomy analysis emphasizes that regulations must outline specific security measures for gateways, including intrusion prevention systems, secure bootstrapping, and continuous monitoring, to detect and thwart potential threats at network entry points.[40]
3. **Defining the Permissible Scope of IoT Networks:** Considering the exponential growth in connected devices, regulations must define the permissible scope of IoT networks to manage their complexity effectively. The taxonomy analysis suggested that regulatory frameworks should provide clear guidelines on the types of devices, their functionalities, and their interactions within the IoT ecosystem. This involves categorizing devices based on their behaviours and functionalities to establish a framework that ensures compatibility, interoperability, and security. By defining the permissible scope, regulations can contribute to creating a structured and secure IoT environment.[41]
4. **Accounting for Diverse Behaviours of Connected Devices:** The taxonomy analysis highlights the importance of regulations accounting for the diverse behaviours exhibited by connected devices. IoT networks encompass a wide array of devices with varying functionalities and behaviours. Regulatory frameworks need to consider this diversity and establish guidelines that address the specific security challenges posed by different types of devices. This involves categorizing devices based on their behaviours, potential vulnerabilities, and communication patterns. Regulations should encourage the development of security measures tailored to the unique characteristics of each device category, ensuring a comprehensive and adaptive security approach.[30]

The passage contributes to the analysis by emphasizing the crucial role of regulations in establishing secure communication protocols, ensuring gateway security, and defining the permissible scope of IoT networks. The taxonomy analysis further underscores the need for regulations to be dynamic and adaptive, considering the diverse behaviours many connected devices exhibit in the IoT environment.

Accessibility

In the context of IoT regulation in Indonesia, regulations mandate an integrated access management strategy involving sophisticated authentication policies and mechanisms to address security challenges related to accessibility. This ensures users, administrators, and authorized entities have seamless and secure access to IoT networks and devices. Additionally, it is important to address security in cloud computing. As the IoT expands, integration with cloud computing technology

becomes increasingly important. Regulations should prioritize high-level security in cloud computing, ensuring that cloud service providers have the capacity and strategies to safeguard data from unauthorized access and potential attacks.[13]

Specifically, protection against attacks should be a key focus. To protect IoT devices from potential accessibility attacks, regulations should establish strict security standards that guard against threats such as exploiting security vulnerabilities and denial-of-service attacks.[42] Additionally, regulations should recognize the role of automation and artificial intelligence in enhancing accessibility security. This includes implementing technology to monitor, detect, and automatically respond to suspicious activities or security threats.[43]

Regulations should encourage comprehensive and integrated system management for IoT security. It is important to understand various technologies, such as blockchain, that can enhance data integrity and security in the IoT context. By incorporating these aspects into the regulatory framework, Indonesia can establish a strong legal foundation to ensure accessibility and security in an increasingly complex and dynamic IoT environment.[44]

Anonymity

When formulating regulations for IoT security in Indonesia, it is recommended to use a taxonomy based on anonymity concerns. This taxonomy suggests several key aspects, including guidelines and standards for implementing voice anonymization techniques in voice-based IoT interactions. Solutions such as VoicePM, which optimize the trade off between privacy and utility, can serve as a reference for achieving effective voice anonymization.[48]

Additionally, it is important to consider the use of quantum-safe cryptosystems. Given the constantly changing cybersecurity landscape, regulations should encourage the implementation of quantum-safe cryptographic systems. One such system is anonymous hierarchical identity-based encryption with traceability identities, which provides anonymity for communication networks while allowing for traceability in specific situations. This aligns with the unique security needs of distributed IoT data.[49]

The use of blockchain for anonymity is also worth considering. Regulations should acknowledge the role of blockchain in ensuring anonymity in IoT applications. A review of blockchain technology in smart applications highlights its advantages, including anonymity and trustlessness. Integrating blockchain solutions into IoT systems can enhance data privacy and security. By incorporating these aspects into IoT regulations, Indonesia can establish a comprehensive framework that addresses anonymity concerns, fostering user trust and data confidentiality within the IoT environment.[50]

Interactivity

In the context of interactivity in IoT security, the taxonomy recommends several key aspects to consider when designing comprehensive regulations for the IoT in Indonesia. One crucial aspect is real-time communication security. Regulations must address the real-time interactions between IoT devices to prevent unauthorized access and protect the integrity of data exchanges between devices.[51]

Another pivotal facet of IoT security pertains to using secure protocols for device interactions. It is imperative to delineate and enforce secure protocols for interactions among IoT devices. This encompasses the specification of standardized communication protocols that precede security, encryption, and authentication, laying a secure groundwork for device interactions within the IoT ecosystem. Regulatory frameworks should prioritize upholding the integrity of the entire IoT ecosystem. Safeguarding the security of the overarching IoT environment necessitates thwarting malicious activities that could jeopardize interconnected devices. Hence, it is imperative to underscore the necessity of security measures that transcend individual devices. By incorporating these facets into IoT regulations, Indonesia can proactively anticipate and mitigate security challenges associated with interconnectivity.[52] The study's findings offer valuable insights into the technological landscape and potential threats linked to interconnectivity within the IoT. The technical report presents a comprehensive framework that underscores the pivotal role of security across various dimensions, notably interactivity, thereby underscoring its significance in developing IoT software systems. With the evolution of the Internet of Things (IoT) landscape, regulatory frameworks must adapt concomitantly to uphold the security and resilience of ongoing, dynamic interactions among devices, safeguarding against emerging threats.[53]

Rapidity

In the context of IoT security, the taxonomy suggests several aspects that should be considered when designing comprehensive regulations for the IoT in Indonesia. One of the most important aspects of this field is swift threat detection. Regulations should mandate mechanisms for the rapid detection of security threats. This involves setting up protocols and systems to quickly identify potential security breaches, minimizing the time window for malicious activities, and enhancing overall system security.[54]

Another crucial aspect is the implementation of effective response mechanisms. Regulations should prioritize effective responses to security threats by defining procedures and technologies that enable prompt and decisive actions to mitigate and neutralize security incidents, preventing escalation and potential harm. Additionally, regulations should encourage the integration of advanced technologies to enhance the rapidity of threat detection and response. Sophisticated models and

frameworks, such as the hybrid PCA-MAO-based LSTM model presented in the study, are recommended for their effectiveness in handling complex security scenarios. The research studies highlight various technological advancements, including ATP hygiene detection technology, wearable IoT devices in healthcare, trust management in wireless sensor networks, and efficient autoscaling schemes. Incorporating these advancements into regulations can enhance the speed of security measures. [55]

Indonesia can develop a comprehensive legal framework that anticipates and addresses security threats swiftly and effectively by including these aspects in IoT regulations. The research findings offer valuable insights into technological solutions that can contribute to developing rapid and responsive IoT security measures.[17]

Conclusion

The research concludes by advocating for a comprehensive regulatory framework tailored to IoT devices in Indonesia, achieved through taxonomic analysis. This framework prioritizes key dimensions such as boundaries, accessibility, anonymity, interactivity, and rapidity, thereby establishing a legal infrastructure adaptable to the intricate dynamics of the IoT landscape. Emphasizing the necessity of a holistic regulatory approach to tackle IoT security challenges, the study underscores the utility of taxonomic analysis in crafting regulations attuned to the unique characteristics of the Indonesian IoT ecosystem. Moreover, it furnishes practical guidance for policymakers and stakeholders in crafting regulations safeguarding the dimensions mentioned above.

However, it is essential to acknowledge the limitations of taxonomic analysis in grappling with the evolving complexity of IoT dynamics, alongside the contextual confinement of the research to Indonesia. Consequently, the proposed regulations necessitate adaptation to global advancements. Recommendations for future research entail delineating implementation strategies for the proposed IoT regulations, broadening stakeholder involvement, assessing global ramifications, and aligning regulations with forthcoming IoT technological progressions.

References

[1] H. Rajput, and K. Saxena, in *2023 1st International Conference on Circuits, Power, and Intelligent Systems, CCPIS 2023* (2023).

[2] C. Metallidou, K.E. Psannis, and E. Alexandropoulou-Egyptiadou, in *2020 3rd World Symposium on Communication Engineering, WSCE 2020* (2020), pp. 79–83.

[3] S. Crompton, and J. Jensen, in *Proceedings - 11th IEEE/ACM International Conference on Utility and Cloud Computing Companion, UCC Companion 2018* (2018), pp. 296–301.

[4] J. Fernquist, T. Fängström, and L. Kaati, in *Proceedings - 2017 European Intelligence and Security Informatics Conference, EISIC 2017* (2017), pp. 61–67.

[5] C. Bistolfi, and L. Scudiero, in *Proceedings - IEEE 30th International Conference on Advanced Information Networking and Applications Workshops, WAINA 2016* (2016), pp. 607–610.

[6] R.H. Weber, "Internet of things - Need for a new legal environment?," Computer Law and Security Review **25**(6), 522–527 (2009).

[7] V. Morel, M. Cunche, and D. Le Metayer, in *Proceedings - 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering, TrustCom/BigDataSE 2019* (2019), pp. 366–373.

[8] J. Tapsell, R.N. Akram, and K. Markantonakis, in *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018* (2018), pp. 1380–1385.

[9] S.K. Misra, S. Das, S. Gupta, and S.K. Sharma, in *IFIP Adv Inf Commun Technol* (2020), pp. 100–111.

[10] K. Lambok Siregar, and M. Asvial, in *MECnIT 2020 - International Conference on Mechanical, Electronics, Computer, and Industrial Technology* (2020), pp. 19–23.

[11] S.P. Venkatesan, M. Sanjay, R. V Gopinath, and M.S. Natarajan, in *Proceedings - 2023 3rd International Conference on Pervasive Computing and Social Networking, ICPCSN 2023* (2023), pp. 1360–1365.

[12] D. Pal, X. Zhang, and S. Siyal, "Prohibitive factors to the acceptance of Internet of Things (IoT) technology in society: A smart-home context using a resistive modeling approach," Technol Soc **66**, (2021).

[13] M. Li, Y. Ma, Z. Yin, C. Wang, and A. Chai, in *Proceedings of the 34th Chinese Control and Decision Conference, CCDC 2022* (2022), pp. 4387–4393.

[14] S.G. Tzafestas, "Ethics and law in the internet of things world," Smart Cities **1**(1), 98–120 (2018).

[15] P. Yadav, J. Moore, Q. Li, R. Mortier, Y. Amar, A.S. Shamsabadi, A. Brown, A. Crabtree, C. Greenhalgh, D. McAuley, and H. Haddadi, in *CitiFog 2018 - Proceedings of the 1st Workshop on Smart Cities and Fog Computing, Part of SenSys 2018* (2018), pp. 29–34.

[16] O.R. Sanchez, I. Torre, Y. He, and B.P. Knijnenburg, "A recommendation approach for user privacy preferences in the fitness domain," User Model User-Adapt Interact **30**(3), 513–565 (2020).

[17] C. Millard, W.K. Hon, and J. Singh, in *Proceedings - 2017 IEEE International Conference on Cloud Engineering, IC2E 2017* (2017), pp. 286–291.
[18] R. Pinto, "Industry 4.0 and the GDPR: Two sides of the same coin," Journal of Data Protection and Privacy **2**(3), 201–207 (2019).
[19] S. Nimkar, and M.M. Khanapurkar, in *2021 International Conference on Computational Intelligence and Computing Applications, ICCICA 2021* (2021).
[20] L.A. Remotti, "IoT innovation clusters in Europe and the case for public policy," Data Policy **3**(4), (2021).
[21] S. Dhyani, D. Bhaskar, H. Santhanam, and I.K. Murthy, "Postpandemic recovery through landscape restoration," Restor Ecol **30**(5), (2022).
[22] D.E. Morrison, "Some Notes Toward Theorg on Relative Deprivation, Social Movements, and Social Change," American Behavioral Scientist **14**(5), 675–690 (1971).
[23] E. Magrani, "Threats of the internet of things in a techno-regulated society: A new legal challenge of the information revolution," International Journal of Private Law **9**(1–2), 4–18 (2018).
[24] A. Ghandour, and B.J. Woodford, "Regulating Internet of Things: The Case of the United Arab Emirates," TEM Journal **10**(3), 1031–1038 (2021).
[25] P. Pandey, and R. Litoriya, in *Intelligent Systems Reference Library* (2020), pp. 367–388.
[26] T. Shaikh, S. Kadam, S. Sonawane, P. Narkar, P. Mhatre, and M. Muthu, in *Proceedings of the 8th International Conference on Communication and Electronics Systems, ICCES 2023* (2023), pp. 32–39.
[27] E. Del Re, in *2020 IEEE 3rd 5G World Forum, 5GWF 2020 - Conference Proceedings* (2020), pp. 235–238.
[28] S. Diwakaran, B.S. Kumar, K. Kumar, K. Sushmitha, and K.R. Chandra Siddhardha Reddy, in *2023 9th International Conference on Advanced Computing and Communication Systems, ICACCS 2023* (2023), pp. 1845–1850.
[29] Y.-C. Yang, and R.-S. Tsay, in *2023 International Conference on Consumer Electronics - Taiwan, ICCE-Taiwan 2023 - Proceedings* (2023), pp. 141–142.
[30] T. Quill, and R. Lennon, in *IEEE 5th World Forum on Internet of Things, WF-IoT 2019 - Conference Proceedings* (2019), pp. 408–412.
[31] C. Fu, G. Zhang, J. Yang, and X. Liu, "Study on the contract characteristics of Internet architecture," Enterp Inf Syst **5**(4), 495–513 (2011).
[32] O. Abdulkader, A.M. Bamhdi, V. Thayananthan, and F. Elbouraey, in *Proceedings of the 3rd World Conference on Smart Trends in Systems, Security and Sustainability, WorldS4 2019* (2019), pp. 363–367.
[33] M.E. Alim, S. Ahmad, M.N. Dorabati, and I. Hassoun, in *11th Annual IEEE Information Technology, Electronics and Mobile Communication Conference, IEMCON 2020* (2020), pp. 576–581.
[34] D. Sarris, K. Xynos, H. Read, and I. Sutherland, in *European Conference on Information Warfare and Security, ECCWS* (2020), pp. 342–350.
[35] K. Rabbani, A. Moore, and J. Rafferty, in *2022 IEEE 8th World Forum on Internet of Things, WF-IoT 2022* (2022).
[36] S. Chatterjee, and A.K. Kar, "Regulation and governance of the Internet of Things in India," Digital Policy, Regulation and Governance **20**(5), 399–412 (2018).
[37] V. Kavitha, and S. Mohanraj, "Green engineering principles for global water quality monitoring using IoT," International Journal of Environment and Sustainable Development **18**(1), 120–129 (2019).
[38] T. Burns, G. Fichthorn, S. Zehtabian, S.S. Bacanli, M. Razghandi, L. Boloni, and D. Turgut, in *2020 IEEE International Conference on Communications Workshops, ICC Workshops 2020 - Proceedings* (2020).
[39] A. Hefnawy, A. Bouras, and C. Cherifi, in *IFIP Adv Inf Commun Technol* (2018), pp. 442–452.
[40] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities," Comput Secur **88**, (2020).
[41] M. Stočes, J. Vaněk, J. Masner, and J. Pavlík, "Internet of things (IoT) in agriculture - Selected aspects," Agris On-Line Papers in Economics and Informatics **8**(1), 83–88 (2016).
[42] C. Freitag, M. Berners-Lee, K. Widdicks, B. Knowles, G.S. Blair, and A. Friday, "The real climate and transformative impact of ICT: A critique of estimates, trends, and regulations," Patterns **2**(9), (2021).
[43] M. Koutli, N. Theologou, A. Tryferidis, D. Tzovaras, A. Kagkini, D. Zandes, K. Karkaletsis, K. Kaggelides, J. Almela Miralles, V. Oravec, and S. Vanya, in *Proceedings - 15th Annual International Conference on Distributed Computing in Sensor Systems, DCOSS 2019* (2019), pp. 263–270.
[44] D.E.L. Majdoubi, H. El Bakkali, and S. Sadki, in *Proceedings of 2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications, CloudTech 2020* (2020).
[45] X. Feng, and Y. Zhao, in *Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, IThings-GreenCom-CPSCom-SmartData 2017* (2017), pp. 858–862.
[46] M. Weber, D. Lučić, and I. Lovrek, in *Proceedings of International Conference on Smart Systems and Technologies 2017, SST 2017* (2017), pp. 187–193.
[47] S. Chatterjee, "Influence of IoT policy on quality of life: From government and citizens' perspectives," International Journal of Electronic Government Research **15**(2), 19–38 (2019).

[48] S. Rizou, E. Alexandropoulou-Egyptiadou, Y. Ishibashi, and K.E. Psannis, in *2021 IEEE 9th International Conference on Information, Communication and Networks, ICICN 2021* (2021), pp. 269–272.

[49] R. Alharbi, and H. Almagwashi, in *Proceedings - 2019 International Conference on Future Internet of Things and Cloud Workshops, FiCloudW 2019* (2019), pp. 18–25.

[50] X. Feng, E.S. Dawam, and S. Amin, in *Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, IThings-GreenCom-CPSCom-SmartData 2017* (2017), pp. 274–279.

[51] T.M. Kazenga, J.B. Tuyishimire, A.A. Garba, M. Saint, and L. Deen, in *International Conference on Information and Communication Technology Convergence: ICT Convergence Technologies Leading the Fourth Industrial Revolution, ICTC 2017* (2017), pp. 622–627.

[52] S. Debdas, S. Mishra, S. Saha, A. Bag, N. Shukla, and A. Kumar, in *2022 IEEE 2nd International Conference on Sustainable Energy and Future Electric Transportation, SeFeT 2022* (2022).

[53] S.R. Niya, J. Willems, and B. Stiller, in *IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2022* (2022).

[54] A. Sinha, A. Patel, and M. Jagdish, in *2022 1st International Conference on Artificial Intelligence Trends and Pattern Recognition, ICAITPR 2022* (2022).

[55] M. Shukla, S.D. Johnson, and P. Jones, in *2019 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2019* (2019).