Agile Governance and Innovation Measurement Journal

Agile Governance and Innovation Measurement Journal

ISSN: xxxx-xxxx (print), xxxx-xxxx (Online)

Vol 2, No 1 (2025): Page no: 15-25

Bibliometric Analysis of Research Trends in Data Security and Privacy for E-Government Implementation in Indonesia

Bagaskoro Nur Abu Yogar [1], Muhammad Akbar Nugraha Sabarna[2]

[1,2] International Program of Government Affairs and Administration, Universitas Muhammadiyah Yogyakarta, Indonesia

Corresponding Author: bagaskoro.nur.isip21@mail.umy.ac.id

Article Info

Check for updates

Article History;
Received:
2025-02-25
Revised:
2025-03-25
Accepted:
2025-03-26
Published:
2025-03-26

Abstract: This research analyses privacy and data security issues in the e-government sector in Indonesia through a qualitative approach with a bibliometric analysis method. As a developing country, Indonesia has shown progress in the implementation of e-government, which is reflected in the increasing rankings in the E-Government Development Index (EGDI) released by the United Nations. However, behind these developments, there are significant challenges related to personal data protection and cybersecurity. The novelty of this research lies in its bibliometric approach, which provides a comprehensive and systematic analysis of existing studies on data security and privacy in Indonesia's e-government sector. Unlike previous studies that focus on case studies or policy evaluations, this research maps research trends, key contributors, and gaps in the literature, offering a broader perspective on the issue. Additionally, this study contributes by highlighting the urgent need for interdisciplinary collaboration between policymakers, cybersecurity experts, and the public to develop sustainable security strategies. The results of this study emphasise the need for a comprehensive strategy to improve data security in e-government, including strengthening regulations, investment in cybersecurity infrastructure, and promoting public digital literacy. In the absence of concrete measures to address these challenges, the risk of data leakage is likely to persist, jeopardising the sustainability of digital transformation in Indonesia.

Keywords: *E-Government; Security; Privacy; EGDI; Bibliometric*

INTRODUCTION

In the context of public services, the development of technology and information has driven changes in the way the government provides services to the public through the process of digitalisation, which encourages the transformation of governance to be more efficient, transparent and accountable (Dewi & Suardana, 2023). In this modernisation effort, e-government and agile government are two complementary concepts. E-government focuses on the use of information technology to improve the accessibility and effectiveness of public services, while agile government emphasises flexibility and responsiveness in project management and decision-making. By integrating these two approaches, the government can not only provide technology-based services but also ensure that these services remain adaptive to the changing needs of society and the dynamics of the evolving environment (Gonin, 2024).

In such cases, e-government becomes a strategy to improve the accessibility of public services and strengthen the interaction between government and society. The

implementation process of e-government allows for flexible and responsive communication, which can engender an open government in the decision-making process. In addition to altering communication patterns, digitalization can enhance public participation in government processes (Akimov & Kadysheva, 2023). Furthermore, the digitalization process in public services can potentially reduce reliance on conventional bureaucracy, which is often considered inefficient. The digital system enables individuals to access various government services easily (Zichová, 2023).

Figure 1. E-Government Dev Index Rank (UN, 2024)

In order to illustrate the implementation of e-government in Indonesia, this country has succeeded in getting the Very High E-Government Development Index (VHEGDI). The United Nations assign this category to countries that have achieved a score above 0.75 on the E-Government Development Index (EDGI). This categorisation is based on the 2024 survey results, which indicate that Indonesia attained a score of 0.7991, positioning it at 64th out of 193 countries. This outcome signifies a substantial enhancement in Indonesia's endeavours concerning the implementation of e-government.

Despite the considerable progress achieved by Indonesia in the implementation of e-government, significant challenges remain. Nevertheless, technical and structural barriers continue to represent a considerable impediment to the propagation of e-government digitalisation. The disparity in the infrastructure sector is a salient factor impeding access and equity in the implementation of e-government in Indonesia (Novita, 2014; Samuel, 2021). Technological limitations and the heterogeneity of internet networks further compound this issue. Moreover, the government's delayed response to digital transformations negatively impacts the pace of e-government implementation. (Zhang & Kaur, 2024) explains that the lack of infrastructure is frequently encountered in developing countries as they seek to implement e-government, with significant repercussions for areas not yet fully covered by government services.

This is further worsened by the lack of adequately skilled human resources in e-government management, which can increase the risk of cyber-attacks (Setyawan, 2024).

The security aspect of data privacy is a primary concern in the e-government system, as the implementation of e-government often exposes public data to the risk of cyberattacks and theft by irresponsible groups. The repercussions of such occurrences are manifold; community members suffer data leakage and theft, and public confidence in government performance is diminished. Consequently, the necessity for an effective strategy has been identified, encompassing the equitable development of infrastructure, the enhancement of human resources, and the promotion of equitable e-government (Dhandar, 2024).

Therefore, this research will focus on analysing the development of e-government in Indonesia that emphasises privacy and security issues that illustrate the urgency in managing risks inherent to e-government systems, such as security and protection of personal data, ease of access, and public trust in government. Utilising a bibliometric analysis approach, this research endeavour will furnish a comprehensive overview of prevailing research trends, patterns, and themes that have emerged in publications pertinent to the subject of e-government, with a particular focus on privacy and security issues (İri & Ünal, 2024; Obeidat et al., 2024).

METHOD

This research was conducted using a qualitative method with bibliometric analysis. Bibliometric analysis can be defined as a research method that is both quantitative and qualitative in its approach to scientifically analyze literature through the use of metadata. The process aims to identify the number of publications, author collaboration patterns, research trends, and the development of research themes (Fajry & Barra, 2024; Lazarides et al., 2023). The analysis is frequently supported by data sources such as the Scopus Database or Web of Science, and the subsequent processing of the data is conducted using the Vos Viewer software to visualise the results in charts or figures for further analysis (Ersen et al., 2024). This research adopts the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) method to ensure a systematic and transparent selection of relevant studies. PRISMA provides a structured approach to identifying, screening, and selecting studies by following a clear set of inclusion and exclusion criteria. By using this method, the research ensures that only high-quality and relevant publications are analyzed, reducing bias and improving the reliability of bibliometric findings (Peixoto Rodriguez & Espina-Romero, 2024). The data utilised in this research is obtained from the Scopus Database, with a particular focus on the issues of data security and privacy in the context of e-government implementation in Indonesia.

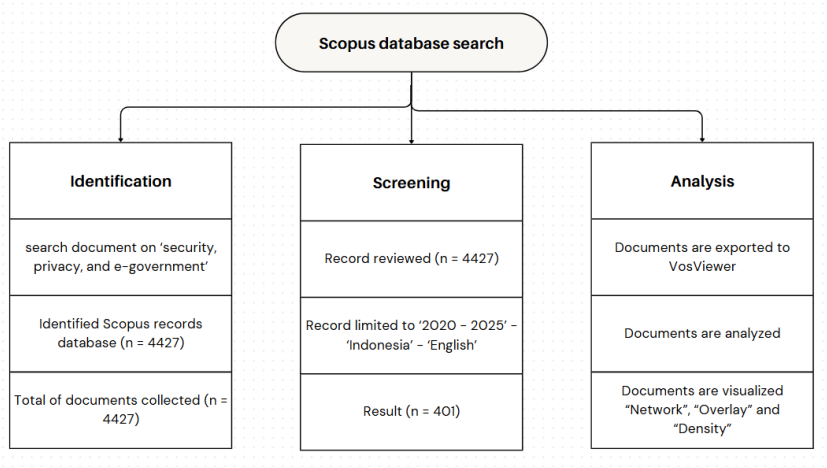

Figure 2. Research Method by using PRISMA Method

Therefore, the data retrieval process in this study goes through several stages, namely the searching for publication articles with the theme Security and Privacy in E-Government, until a total of 4,427 is obtained. The subsequent stage involves the filtration of the aforementioned total number of documents (4,427) through the subsequent steps (TITLE-ABS-KEY (Security AND Privacy AND E-Government) AND PUB YEAR TO 2020 AND PUB YEAR TO 2025 AND (LIMIT TO (AFFIL COUNTRY 'Indonesia') AND (LIMIT TO (LANGUAGE 'English')), until a total of 401 documents is obtained, which will then be analysed through Vos Viewer.

RESULTS

Research Trends on E-Government

Following the various stages of the data retrieval process on the Scopus Database, researchers finally obtained the results of publications focusing on the issue of 'Privacy and Security' in 2020 - 2025. The total number of documents obtained was 401, as illustrated in Figure 2 below.

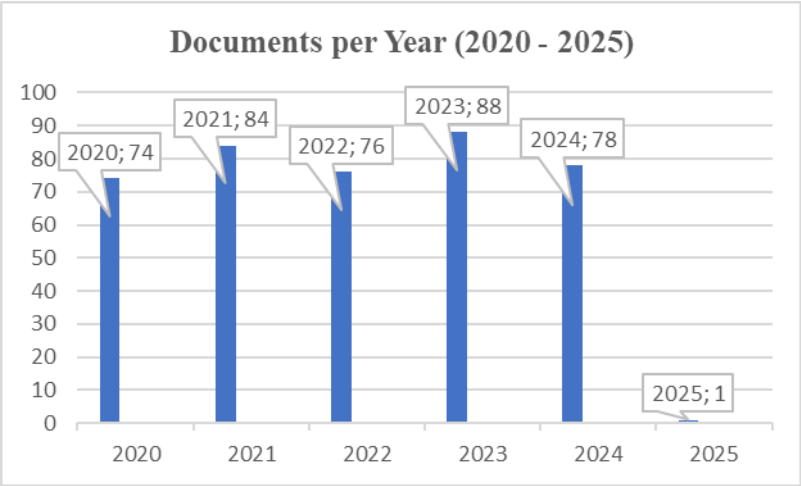

Figure 3. Document per year (Scopus, 2025)

Based on Figure 3 above, which shows the frequency of publications related to privacy and security issues in e-government implementation in Indonesia during the period 2020 to early 2025, the publication trend tends to be stable with a relatively small number from year to year, as many as 74 documents in 2020, then 84 documents in 2021, 76 documents in 2022, 88 documents in 2023, and 78 documents in 2024, and 1 document in January 2025. The stability in the number of publications indicates that the privacy and security issues in e-government persist as a substantial academic concern. Furthermore, the increase in publications in 2021 and 2023 indicates the existence of policies that encourage an increased research interest in the e-government sector, particularly about privacy and security in Indonesia.

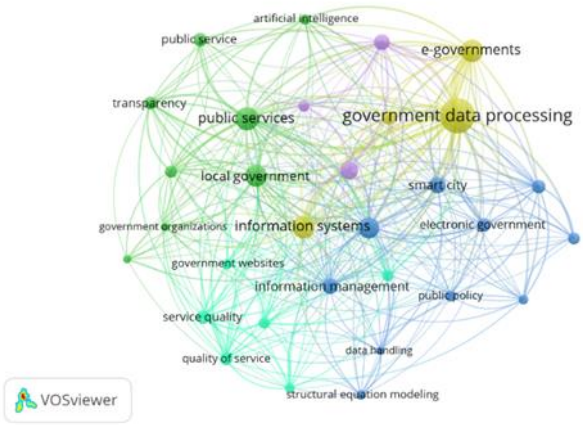

Figure 4. Network analysis (Vos viewer, 2025)

Table1. Cluster Analysis (Scopus, 2025)

Keywords	Cluster	Quantity
Data Handling, Electronic Government, Government Institution, Information and Communication Technologies, Information Management, Information Services, Information Technology, Public Policy, Smart City, Structural Equation Modelling	1	10
Artificial Intelligence, Economic and Social Effects, Government Organization, Local Government, Public Services, Transparency	2	8
Government Agencies, Government Websites, Information Quality, Quality Control, Service Quality	3	6
Decision Making, E-Government, Government Data Processing, Information Systems	4	4
Developing Countries, E-Government Implementation	5	2

As demonstrated in Figure 4 and Table 1 above, which illustrate bibliometric clusters based on the search results of the research theme 'Data Security and Privacy in E-Government' through the Scopus database, five clusters are identified, each with a unique set of keywords. There are a total of five clusters that have different keywords, which will be explained at the points below;

1. Cluster 1
   The first cluster focuses on data management and the use of technology in government, as evidenced by the keywords 'data handling', 'information management', and 'information technology'. These keywords underscore the significance of leveraging technology to support the development of targeted public policies for the broader community.

2. Cluster 2
   The second cluster indicates the utilisation of Artificial Intelligence (AI) by governmental entities within the context of public services. This term refers to the specific keywords 'artificial intelligence' and 'public services', which delineate the implementation of technological advancements, such as artificial intelligence, within governmental agencies or organisations to enhance public services.

3. Cluster 3
   The third cluster of keywords is focused on the quality of services and information in e-government, with several keywords such as 'information quality' and 'quality control' being used to emphasise efforts to ensure that the quality of services and information provided to the public can be accounted for and trusted.

4. Cluster 4
   Meanwhile, the fourth cluster focuses on the decision-making process based on electronic government systems. The keywords 'e-government decision making' demonstrate that the cluster focuses on the use of e-government information systems in making data-based decisions made by the government.

5. Cluster 5
   The final cluster focuses on the process of e-government implementation in developing countries, which is exemplified by the keywords 'developing countries' and 'e-government implementation'. This cluster refers to the challenges and opportunities that developing countries will face in realising e-government. This process requires various qualified supporting sectors, such as the availability of experts, infrastructure, and targeted government policies.

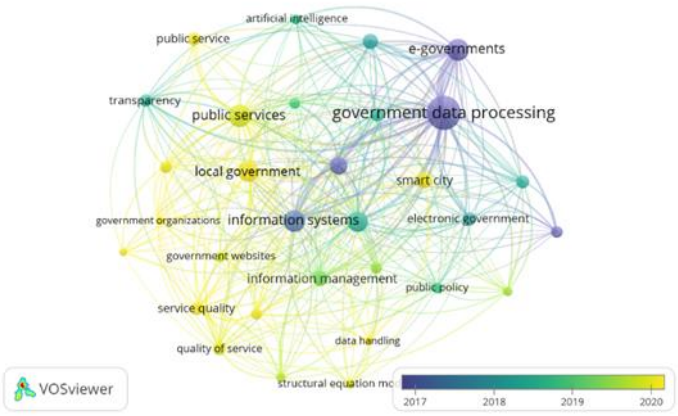

Figure 5. Overlay analysis (Vosviewer, 2025)

The overlay analysis in Figure 5 illustrates the evolution of the research timeline from 2017 to 2020, showcasing many interconnected themes. In 2017, research concentrated on keywords such as government data processing, information systems, and e-government, as indicated by the purple marking. However, from 2018 to 2019, the green labels indicated a notable shift towards more contemporary topics, such as electronic government, artificial intelligence, transparency, public policy, and information management. The year 2020 marked a significant progression in the field, with the emergence of keywords related to public services, service quality, government websites, service quality, data handling, smart cities, government organisations, and local government.

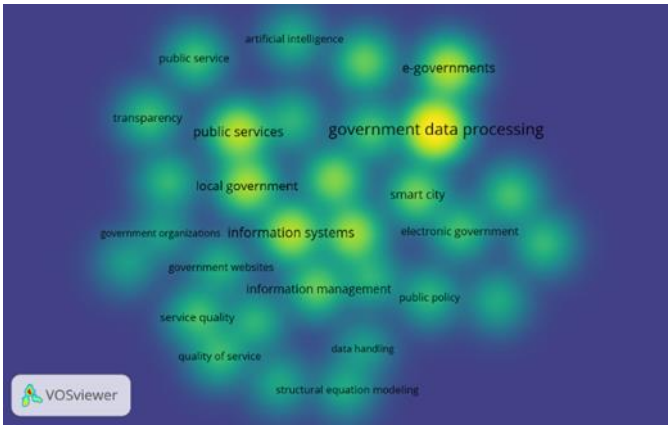

Figure 6. Density analysis (Vosviewer, 2025)

The density analysis results through Vos viewer in figure 6 above demonstrate that several keywords are represented by yellow, indicating that these keywords are most often studied in a literature review. The first keywords are 'government data processing', 'public services', 'e-government', 'information systems', and 'local government'. In contrast, keywords represented by a faded colour can be categorised as those reviewed with less frequency, such as 'data handling', 'transparency', and 'artificial intelligence'.

DISCUSSION

Data Privacy and Security in the Implementation of E-Government in Indonesia

Data security and privacy issues in the contemporary digital era in Indonesia have become paramount. This is due to the increasing use of technology in government services, public administration, and the private sector. The rapid advancement of technology brings both opportunities and challenges, especially in protecting personal data and the integrity of information systems. This article discusses the current state of data security and privacy in Indonesia, highlighting key challenges, legal frameworks, and initiatives aimed at addressing these issues (Witjaksono & Kriswibowo, 2023).

The utilization of the internet within governmental environments is undergoing a marked increase. This concomitant development has given rise to challenges, chiefly in confidentiality, integrity, and service availability. In response, the Indonesian government has initiated several policies and systems to enhance data security, including the SRIKANDI e-government policy and the 'Satu Data Indonesia' policy, which prioritises information security, citizen engagement, and human resource management (Maulidya & Rozikin, 2022; Zakaria et al., 2025). However, challenges persist, particularly in regions with a paucity of technical expertise and adequate workforce numbers. The implementation of blockchain technology and a stable microservices architecture has been proposed as a solution to enhance system reliability and data integrity.

However, cyberattacks on e-government in Indonesia have become a significant concern, especially as the country digitalizes its public services and infrastructure. These attacks not only threaten the integrity of government operations but also jeopardise citizens' privacy and data security. Recent incidents, including the hacking of the National Data Centre (PDN) in 2024, have exposed vulnerabilities in Indonesia's cybersecurity framework, resulting in data leaks and potential breaches of sensitive information (Ramadhani et al., 2025; Sakdiah et al., 2024). Indonesia's legal and regulatory framework has been criticized for its inadequacy in addressing cybersecurity threats. Despite the adoption of the Personal Data Protection Law (PDPL) in 2022, the implementation of this legislation continues to encounter challenges due to the absence of comprehensive regulations and robust enforcement mechanisms (Hendra Wicaksana et al., 2020). Moreover, the fragmented nature of cybersecurity regulations in Indonesia has impeded effective responses to cyber threats, underscoring the necessity for a more integrated approach to data protection and cybersecurity (Asyari, 2023; Juaningsih & Hidayat, 2022).

Furthermore, human factors play a significant role in the high rate of cyberattacks in Indonesia. A study on cyber threats in Indonesia revealed that 64% of respondents had limited knowledge of cybersecurity threats and regulations, indicating a lack of awareness among the general public (Judijanto et al., 2023). This lack of awareness also occurs among government officials and agencies, where inadequate training and lack of preparedness have contributed to the vulnerability of e-government systems. This human factor is further exacerbated by the limited capacity of law enforcement officials to effectively investigate and prosecute cybercrime, emphasizing the need for increased

human resource development in the cybersecurity sector. In order to address the challenges previously mentioned, several recommendations have been proposed. These include the development of a comprehensive cybersecurity policy, the establishment of a special task force for cybersecurity, and the implementation of advanced security technologies such as real-time threat monitoring systems (Judijanto et al., 2023). Furthermore, it is necessary to increase public awareness and education on cybersecurity issues and promote closer international cooperation in combating cybercrime (Ramayanti & Lubis, 2023). The integration of legal, technological, and human factors approaches will be pivotal in establishing a robust cybersecurity framework for Indonesia's e-government sector.

CONCLUSION

This research uses a bibliometric approach to analyze data security and privacy issues in Indonesia's e-government system. As a developing country, Indonesia has shown progress in e-government implementation, as evidenced by its increasing ranking in the UN E-Government Development Index (EGDI). However, significant challenges arise regarding data security, especially data leakage and cyber-attacks that often occur. The study identifies several key contributing factors to these challenges, including a lack of robust cybersecurity infrastructure, government limitations in data management, and a general lack of public awareness regarding the protection of personal information. While this study provides a broad bibliometric analysis of data security and privacy concerns, it cannot offer an in-depth empirical assessment of the effectiveness of existing security policies and strategies. Future research should focus on conducting case studies or field investigations to evaluate the actual implementation of cybersecurity measures and their impact on mitigating risks. Additionally, comparative studies with other developing nations could provide valuable insights into best practices that may be applicable in the Indonesian context. To ensure the sustainability of e-government, a comprehensive strategy is recommended, encompassing the following measures: the strengthening of regulations, investment in cybersecurity, and the education of the public on the importance of data privacy. The absence of concrete steps to address these challenges will continue to perpetuate the data leakage risk, posing a significant threat to Indonesia's ongoing digital transformation process.

REFERENCE

Akimov, A., & Kadysheva, K. (2023). E-Government As a Tool for Communication With Young People: Legal Aspects. *Journal of Law and Sustainable Development*, *11*(1), 1–11. https://doi.org/10.37497/sdgs.v11i1.272

Asyari, H. Al. (2023). Between Freedom And Protection: A Critical Review Of Indonesia's Cyberspace Law. *Prophetic Law Review*, *5*(1), 79–103. https://doi.org/10.20885/plr.vol5.iss1.art5

Dewi, L. P. R. S., & Suardana, I. B. R. (2023). Reflections of agile governance in public services in the digital age. *Publisia: Jurnal Ilmu Administrasi Publik*, *8*(1), 84–90. https://doi.org/10.26905/pjiap.v8i1.9154

Dhandar, K. A. (2024). E-Government and Digital Transformation: Investigate the implementation and impact of e-government initiatives on public service delivery, citizen engagement, and administrative efficiency. *Gurukul International Multidisciplinary Research Journal*, *2394*, 3–13. https://doi.org/10.69758/gimrj/2408ii05v12p0001

Ersen, N., Akyüz, İ., & Akyüz, K. C. (2024). Bibliometric Analysis of the International Journal in Wood Science Using Visualization Mapping Method. *Eurasian Journal of Forest Science*, *12*(2), 47–65. https://doi.org/10.31195/ejejfs.1467759

Fajry, A., & Barra, A. (2024). Analisis Bibliometrik Model Regresi Spline untuk Pemetaan Tren dan Pengembangan Strategi Penelitian Menggunakan VOSviewer. *Nucleus*, 74–82.

Gonin, A. (2024). Stephens, Melodena, Awamleh, Raed, and Salem, Fadi (Eds.) (2022) Agile Government: Emerging Perspectives in Public Management, World Scientific Publishing Company. *Information Polity*, *29*(2), 253–255. https://doi.org/10.3233/ip-249005

Hendra Wicaksana, R., Imam Munandar, A., Samputra, P. L., Salemba, J., No, R., & Indonesia, J. (2020). Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic. *Jurnal Ilmu Pengetahuan Dan Teknologi Komunikasi*, *22*(2), 143–158. http://dx.doi.org/10.33164/iptekkom.22.2.2020.143-158

İri, R., & Ünal, E. (2024). Bibliometric Analysis Bibliometric Analysis of Research (1980-2023). *Ahi Evran Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *10*(2), 386–403. https://doi.org/10.31592/aeusbed.1446738

Juaningsih, I. N., & Hidayat, R. N. (2022). Legal Protection For The Community In Cyber Space Through Regulation Forming With The Omnibus Mehtod. *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, *2*(2), 143–156. https://doi.org/10.15294/ipmhi.v2i2.54684

Judijanto, L., Rahardian, R. L., Muthmainah, H. N., & Erkamim, M. (2023). Analysis of Threat Detection, Prevention Strategies, and Cyber Risk Management for Computer Network Security in Government Information Systems in Indonesia. *West Science Information System and Technology*, *1*(02), 90–98. https://doi.org/10.58812/wsist.v1i02.479

Lazarides, M. K., Lazaridou, I., & Papanas, N. (2023). Bibliometric Analysis: Bridging Informatics With Science. *The International Journal of Lower Extremity Wounds*, 15347346231153538. https://api.semanticscholar.org/CorpusID:256389006

Maulidya, R., & Rozikin, M. (2022). Analisis Retrospektif Kebijakan Satu Data Indonesia. *Dinamika : Jurnal Ilmiah Ilmu Administrasi Negara*, *9*(2), 273. https://doi.org/10.25157/dak.v9i2.7884

Novita, D. (2014). Faktor-Faktor Penghambat Pengembangan E-Government. *Eksplora Informatika*, *4*, 3–5.

Obeidat, I., Alhayek, E., & Obeidat, A. (2024). A Model for Adaptive Bug Bounty Programs and Responsible Disclosure in E-Government Vulnerability Management. *2024 International Conference on Multimedia Computing, Networking and Applications (MCNA)*, 102–107. https://doi.org/10.1109/MCNA63144.2024.10703931

Peixoto Rodriguez, E., & Espina-Romero, L. C. (2024). Mapping digital marketing research in social networks: A short-term bibliometric analysis (2018–2023). *Revista de Ciencias Sociales*, *30*(2), 15–31. https://doi.org/10.31876/rcs.v30i2.41906

Ramadhani, E. H., Enriko, I. K. A., Lety, E., & Puspita, I. (2025). Kajian Strategik Manajemen Keamanan Siber terhadap Proyek Telematika di Indonesia: Studi Kasus Kebocoran Pusat Data Nasional Abstrak. *Jurnal Indonesia: Manajemen Informatika Dan Komunikasi*, *6*(1), 570–580. https://doi.org/10.35870/jimik.v6i1.1210

Ramayanti, H., & Lubis, A. F. (2023). Peran Hukum dalam Mengatasi Serangan Cyber yang

Mengancam Keamanan Nasional. *Jurnal Hukum Dan HAM Wara Sains*, *2*(09), 904–912. https://doi.org/10.58812/jhhws.v2i09.672

Sakdiah, H., Geby, N., Ginting, T., Gea, M., & Aisyah, N. (2024). Korelasi Hak & Kewajiban Warga Negara & Negara Dalam Perlindungan Data Pribadi (Menyoroti Kasus Peretasan Data Nasional). *Jurnal Multidisiplin Indonesia*, *3*(2), 1303–1308.

Samuel, C. A. (2021). Capaian, Peluang, dan Tantangan Implementasi E-Government di Indonesia. *Center For Digital Society*, 1–12. https://cfds.fisipol.ugm.ac.id/wp-content/uploads/sites/1423/2021/01/15-CfDS-Case-Study-Capaian-Peluang-dan-Tantangan-Implementasi-e-Government-di-Indonesia.pdf

Setyawan, A. C. (2024). Enhancing Public Service Delivery through Digital Transformation: A Study on the Role of E-Government in Modern Public Administration. Open Access. *Global International Journal of Innovative Research*.

Witjaksono, D. K., & Kriswibowo, A. (2023). Fondasi Kemananan Siber Untuk Layanan Pemerintah. *Al-Ijtima`i: International Journal of Government and Social Science*, *9*(1), 21–38. https://doi.org/10.22373/jai.v9i1.2057

Zakaria, T. Z., Deliarnoor, N. A., & Sukarno, D. (2025). SRIKANDI AND INDONESIA'S E-GOVERNMENT POLICY: SYSTEM RELIABILITY AND THE CRUCIAL ROLE OF POLITICAL COMMITMENT. *Jurnal Wacana Politik*, *10*(1), 81–93. https://doi.org/10.24198/jwp.v10i1.57854

Zhang, M., & Kaur, M. (2024). Toward a theory of e-government: Challenges and opportunities, a literature review. *Journal of Infrastructure, Policy and Development*, *8*(10), 1–27. https://doi.org/10.24294/jipd.v8i10.7707

Zichová, T. (2023). Towards the E-Society: Social Media As a Tool To Support E-Participation. *Proceedings of the International Conferences on E-Society 2023, ES 2023 and Mobile Learning 2023, ML 2023*, *2020*, 461–465. https://doi.org/10.33965/es_ml2023_202302s061