GOVERNANCE: Jurnal Ilmiah Kajian Politik Lokal dan Pembangunan
ISSN: 2406-8721 (Media Cetak) dan ISSN: 2406-8985 (Media Online)
Volume 12 Nomor 1 September 2025

SECURING THE DIGITAL NATION: A RESEARCH EXPLORATION OF CYBERSECURITY IN E-GOVERNMENT

Dyah Rahayuning Perwitasari[1*], Gusti Naufal Rizky Perdana[2], Lara Ayu Lestari[3], Iqbal Saputra Zana[4], Bulan Erika Bato[5]
[1*,2,3,4,5]Department of Public Administration, Universitas Mulawarman, Samarinda, East Kalimantan, Indonesia
Email Korespondensi: dyahrahayuningperwitasari@fisip.unmul.ac.id

ABSTRACT
This study examines the development and trends in cybersecurity research within the context of e-government from 2012 to 2024 using a bibliometric analysis method. Through bibliometric analysis, this research analyzes publications indexed in the Scopus database to identify trends, author contributions, institutions, and countries involved in cybersecurity research in the digital government sector. The analysis results indicate that cybersecurity topics in e-government have gained increasing attention in line with the growing adoption of digital technologies in government. Dominant themes such as cybersecurity, security, system, technologies, digital, and e-government reflect efforts to enhance government efficiency and transparency while addressing cybersecurity challenges. Furthermore, the study identifies the growing importance of implementing technical solutions such as blockchain and artificial intelligence (AI) to strengthen the security of digital government systems. The research also highlights significant contributions from specific authors, institutions, and countries in enriching this body of literature. Nonetheless, this study is limited by the scope of data used and proposes future research directions that incorporate socio-political factors and emerging technologies to reinforce the secure implementation of e-government.

ABSTRAK
Studi ini mengkaji perkembangan dan tren penelitian dalam bidang keamanan siber dalam konteks *e-government* dari tahun 2012 hingga 2024 dengan menggunakan metode analisis bibliometrik. Melalui analisis bibliometrik, penelitian ini menganalisis publikasi yang terindeks dalam basis data Scopus untuk mengidentifikasi tren, kontribusi penulis, institusi, dan negara yang terlibat dalam penelitian keamanan siber di sektor pemerintahan digital. Hasil analisis menunjukkan bahwa topik keamanan siber dalam *e-government* semakin mendapatkan perhatian seiring dengan meningkatnya adopsi teknologi digital dalam pemerintahan. Tema-tema dominan seperti keamanan siber, keamanan, sistem, teknologi, digital, dan *e-government* mencerminkan upaya untuk meningkatkan efisiensi dan transparansi pemerintahan sambil mengatasi tantangan keamanan siber. Selain itu, studi ini mengidentifikasi pentingnya penerapan solusi teknis seperti *blockchain* dan kecerdasan buatan (AI) untuk memperkuat keamanan sistem pemerintahan digital. Penelitian ini juga menyoroti kontribusi signifikan dari penulis, institusi, dan negara tertentu dalam memperkaya literatur ini. Meskipun demikian, studi ini terbatas oleh ruang lingkup data yang digunakan dan mengusulkan arah penelitian masa depan yang mengintegrasikan faktor sosial politik serta teknologi yang sedang berkembang untuk memperkuat implementasi *e-government* yang aman.
Keywords: Cybersecurity; E-Government; System Security; Bibliometric Analysis

INTRODUCTION
The development of government digitalization includes improving the efficiency of public services, reducing direct interactions, and leveraging digital technologies to enhance service delivery (Trubetskaya, 2020). The digitalization of government, enabled by the use of Information and Communication

ISSN: 2406-8721 (Media Cetak) dan ISSN: 2406-8985 (Media Online)
Volume 12 Nomor 1 September 2025

Technology (ICT), has significantly improved the performance and effectiveness of public administration (Wandaogo, 2022). The digitalization of government replaces conventional approaches with more efficient digital systems, improves the quality of public services, and strengthens interactions among government institutions, citizens, and the business sector (Zioło et al., 2022). Indeed, the successful implementation of this technology has heightened public expectations for public services to be delivered more efficiently and effectively through digital platforms (Sadar, 2023).

Janowski (2015) It is observed that digital government evolves through four distinct phases: Digitalization, Transformation, Engagement, and Contextualization. However, the adoption of these technologies also introduces vulnerabilities to cybersecurity threats—an increasingly pressing issue in parallel with the advancement of digitalization. V. Weerakkody, et al. (2011) emphasize that public transformation through e-government must be accompanied by a comprehensive overhaul of internal processes and sufficient preparedness in establishing cybersecurity infrastructure. Inadequate readiness in developing a secure and resilient cybersecurity framework within e-government systems can significantly increase the risk of digital threats, ranging from personal data breaches to the disruption or suspension of public services. Such incidents may undermine public trust and hinder the comprehensive digital transformation of the public sector (Wirtz & Muller, 2019). Without a strong security foundation, e-government systems become vulnerable to cyberattacks and data misuse, potentially undermining the credibility of public institutions and endangering national stability. Cybersecurity in electronic governance highlights the critical need for stringent regulations to safeguard data, the implementation of security technologies to prevent misuse, and the establishment of robust infrastructure to defend against cyber threats and foster public trust in digital governance (Bisoyi et al., 2020).

From a more strategic perspective, Cavelty (2015) asserts that cybersecurity in the public domain is not merely a technical issue, but an integral part of national security, as it involves citizens' data and critical infrastructures that support governance. Therefore, the state must develop security capacities that are not only reactive but also proactive, through systematic and sustainable cyber resilience policies. According to Yildiz (2007) a key factor in the success of e-government lies in the government's ability to manage and optimize the integration between digital systems and existing public policies. Without proper regulation, reliance on technology may in fact amplify potential vulnerabilities.

Cavelty (2015) notes that in developing countries, the implementation of effective cybersecurity policies is often hindered by structural factors, such as limited availability of trained human resources, inadequate infrastructure, and misalignment between governmental policies and existing technologies. This study highlights the importance of cross-sector collaboration—among government, private sector, and civil society—in building a sustainable cybersecurity ecosystem that does not rely solely on technological solutions, but also emphasizes institutional capacity and public awareness. The success and sustainability of implementing secure e-government systems are significantly influenced by the readiness of digital infrastructure, proactive policymaking, and effective cross-sector collaboration. Cybersecurity must be positioned as a top priority in every stage of digital transformation to ensure that public services are delivered efficiently, transparently, and securely, thereby fostering public trust and supporting national stability in an increasingly digital era.

METHOD

This study employs a bibliometric analysis approach to explore the development and research trends related to cybersecurity in the context of e-government. This approach was selected to identify the evolution of the literature, collaboration patterns among authors and institutions, and to map the key themes that have emerged in the academic discourse over the period from 2012 to 2024. The analysis aims to provide a comprehensive overview of how cybersecurity is understood and implemented in e-government, as well as how the issue has evolved over time.

The research data were obtained from the Scopus database, which is widely recognized for its

ISSN: 2406-8721 (Media Cetak) dan ISSN: 2406-8985 (Media Online)
Volume 12 Nomor 1 September 2025

reliability in providing comprehensive academic information. The search was conducted using the following query: TITLE-ABS-KEY ("Cybersecurity") AND TITLE-ABS-KEY ("E-Government") AND PUBYEAR > 2011 AND PUBYEAR < 2025 AND (LIMIT-TO (DOCTYPE, "ar") OR LIMIT-TO (DOCTYPE, "cp") OR LIMIT-TO (DOCTYPE, "ch")). This query ensured the inclusion of only those publications that were relevant to cybersecurity and e-government within the timeframe of 2012 to 2024. Furthermore, only English-language documents—comprising journal articles, conference proceedings, and book chapters—were considered. The search results yielded 99 relevant documents.

The data retrieved from Scopus were subsequently analyzed using the VOSviewer software to map author collaborations, institutional affiliations, and the co-occurrence relationships among frequently appearing keywords. This visualization provides insights into the dominant research themes and the shifting focus of cybersecurity research within the e-government domain. In addition, NVivo 12 Plus was utilized to conduct thematic analysis of the textual content, leveraging the Autocode feature to identify recurring keywords and core concepts across the selected body of literature.

DISCUSSION

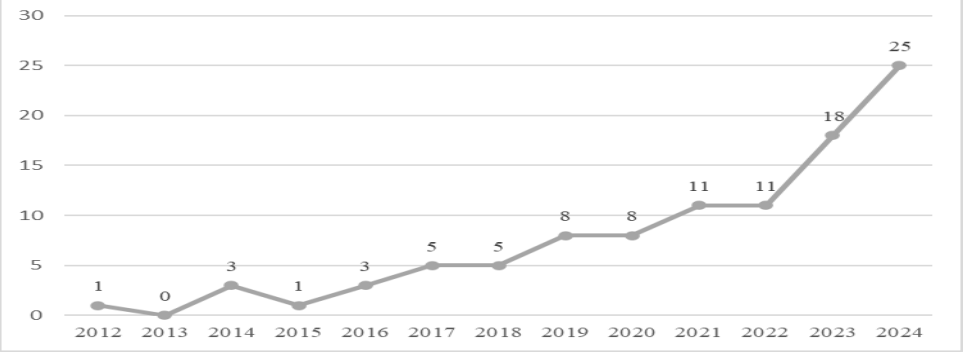
Trends in Cybersecurity Research within the E-Government Context

Research on cybersecurity within the context of e-government has demonstrated a significant upward trend over the years. In the initial stage, specifically in 2012, there was only a single publication addressing this topic, indicating that attention to cybersecurity in e-government was still highly limited. In the subsequent years—namely from 2013 to 2015—the number of publications remained notably low, with only one to three publications recorded annually. This pattern reflects that cybersecurity had not yet emerged as a central focus within the field of digital government research during that period.

However, starting in 2016, a moderate increase was observed, with three to five publications released annually. This upward trend continued more prominently in 2019 and 2020, with eight articles published in each of those years. This pattern indicates that, alongside the growing adoption of digital technologies in government, cybersecurity issues began to receive greater scholarly attention reflecting the rising need to safeguard governmental systems and data.

A more significant increase occurred in 2021 and 2022, with the number of publications reaching eleven articles in each of those years. In 2023, this figure surged to 18, and it is projected to reach 25 publications in 2024. This surge reflects the growing importance of cybersecurity as a research topic within the e-government domain, particularly in response to the increasing complexity of digital threats. The rising number of publications suggests that the academic community is becoming more focused on how to secure digital government systems in order to ensure their effectiveness and maintain public trust. This growing attention can be attributed to the rapid evolution of cybersecurity challenges, as advanced threats such as ransomware and phishing attacks have become more frequent and sophisticated (Mijwil et al., 2023).

Figure 1: Cybersecurity Research Trends in E-Government



Source: (Scopus Database)

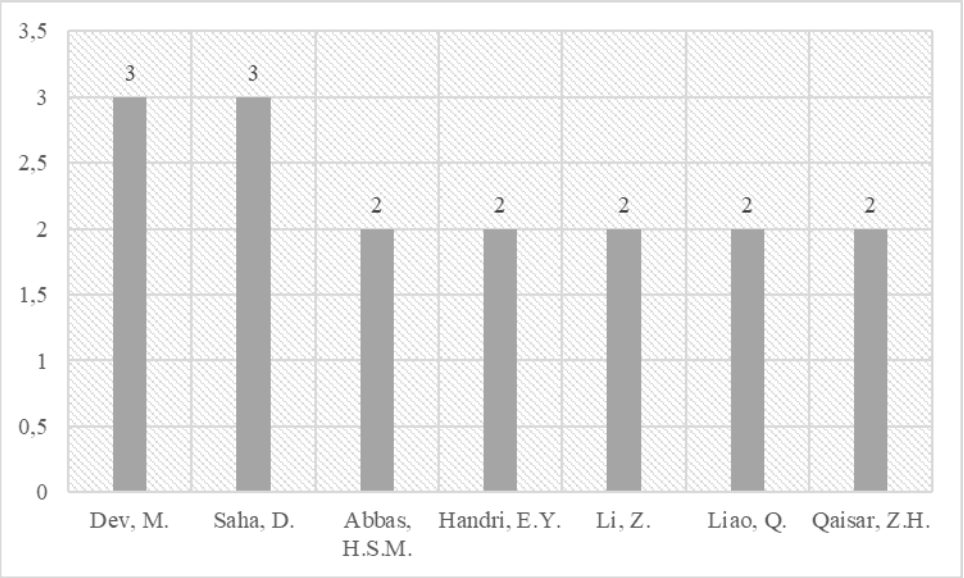
ISSN: 2406-8721 (Media Cetak) dan ISSN: 2406-8985 (Media Online)
Volume 12 Nomor 1 September 2025

Top Authors, Affiliations, and Countries in Cybersecurity and E-Government Publications

In research on cybersecurity within the context of e-government, several authors have emerged with notable contributions. The most prolific authors in this field are Dev, M. and Saha, D., each of whom has published three articles. These two authors demonstrate a strong commitment to advancing the discourse on cybersecurity in the domain of digital governance.

In addition, several other authors have made substantial contributions, albeit with a slightly lower number of publications. Abbas, H.S.M., Handri, E.Y., Li, Z., Liao, Q., and Qaisar, Z.H. each have two publications in this area. Although their publication counts are lower than those of Dev and Saha, their contributions remain significant in enriching the body of literature on cybersecurity in e-government. The growing number of publications by these authors indicates a continued expansion of research in this field and reflects the increasing scholarly interest in addressing digital security challenges within the realm of public governance.

Figure 2: Leading Authors in Cybersecurity and E-Government Research



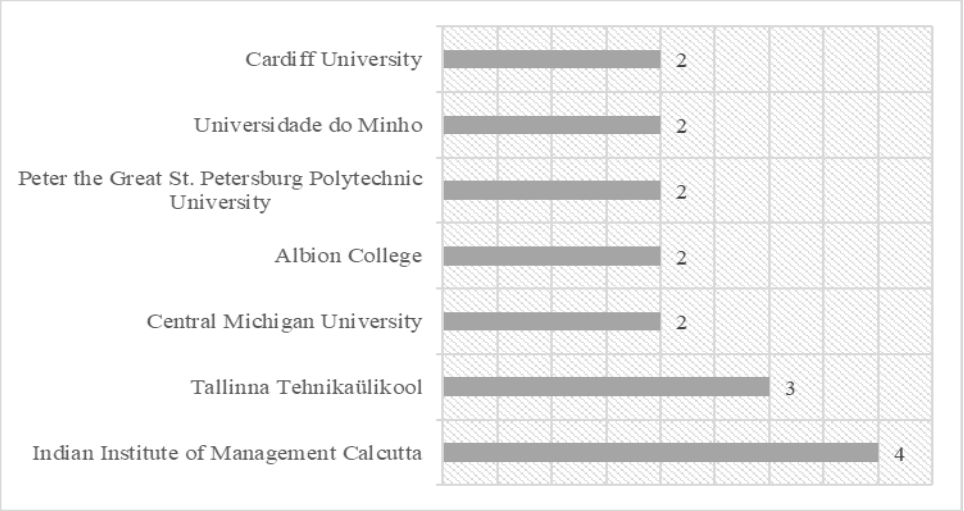
Source: (Scopus Database)

In cybersecurity research within the e-government domain, several prominent institutions have emerged with significant contributions to the academic literature. The Indian Institute of Management Calcutta leads with a total of four publications, underscoring its central role in advancing research on cybersecurity in the context of digital governance. The institution's success in producing relevant publications highlights its commitment to the development of this topic.

In addition, several other institutions have also made noteworthy contributions, albeit with slightly fewer publications. Tallinna Tehnikaülikool (Tallinn University of Technology) in Estonia recorded three publications, while other well-regarded universities such as Central Michigan University, Albion College, Peter the Great St. Petersburg Polytechnic University, Universidade do Minho, and Cardiff University each contributed two publications. These contributions reflect the global relevance of cybersecurity in e-government and demonstrate the engagement of institutions from various regions of the world in addressing this increasingly critical issue.

ISSN: 2406-8721 (Media Cetak) dan ISSN: 2406-8985 (Media Online)
Volume 12 Nomor 1 September 2025

Figure 3: Leading Institutional Affiliations in Cybersecurity and E-Government Research

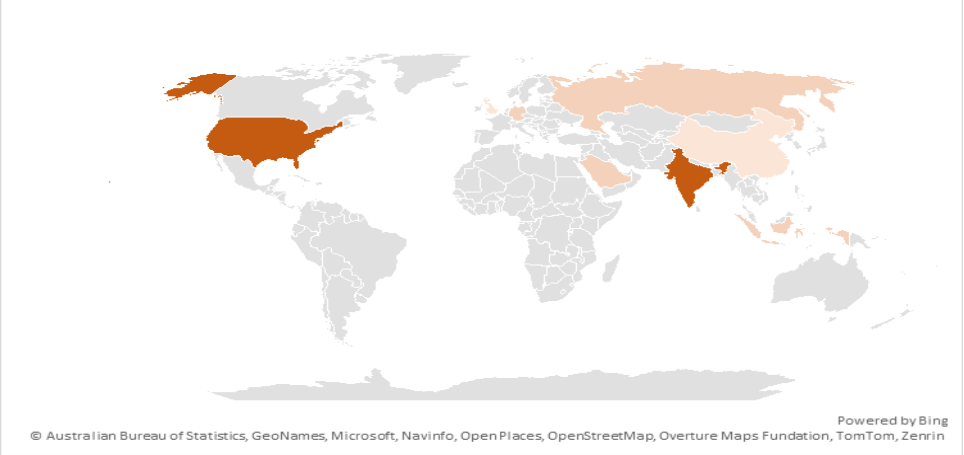


Source: (Scopus Database)

Research on cybersecurity in the context of e-government reveals that several countries play a dominant role in generating scholarly publications in this field. India and the United States lead with a total of 12 publications each, reflecting both nations' strong interest and commitment to addressing cybersecurity issues within digital governance. Their contributions have been instrumental in advancing research and innovation related to public sector cybersecurity.

In addition, countries such as Germany, Indonesia, the Russian Federation, and Saudi Arabia have each produced six publications, indicating that the topic is also receiving substantial attention from other major nations. China and the United Kingdom have made notable contributions as well, with five publications each. This global distribution of publications underscores the importance of international collaboration and knowledge-sharing in addressing increasingly complex digital security challenges at the global level.

Figure 4: Leading Countries in Cybersecurity and E-Government Research



Source: (Database Scopus)

Highly Cited Scholarly Works on Cybersecurity within E-Government

The most cited research in the field of cybersecurity within the e-government domain is the article authored by Elisa et al., (2018), titled *"A Framework of Blockchain-Based Secure and Privacy-Preserving*

ISSN: 2406-8721 (Media Cetak) dan ISSN: 2406-8985 (Media Online)
Volume 12 Nomor 1 September 2025

E-Government System." Published in the journal *Networks* in 2018, this article has received 86 citations, indicating its substantial influence on research related to the application of blockchain technology for enhancing security and privacy in digital government systems.

Following that is the article by Alharbi et al., (2017) , titled *"The Impact of Security and Its Antecedents in Behaviour Intention of Using E-Government Services,"* published in *Behaviour and Information Technology*. This publication has received 55 citations, reflecting its relevance to numerous studies examining user acceptance and the adoption of technology in the public sector. The article explores the influence of security-related factors on users' behavioral intentions to engage with e-government services, positioning it as a key reference in understanding the role of trust and perceived security in digital service usage.

Another article that has garnered significant attention is the work by Al-Besher & Kumar (2022) , titled *"Use of Artificial Intelligence to Enhance E-Government Services,"* published in *Measurement Sensors*. With 38 citations, this study examines the application of artificial intelligence (AI) in improving the efficiency and quality of e-government services. The article underscores the growing relevance of AI in modern public administration systems, highlighting its potential to transform service delivery and decision-making within digital governance frameworks.

Additionally, the article by Li & Liao (2018), titled *"Economic Solutions to Improve Cybersecurity of Governments and Smart Cities via Vulnerability Markets,"* published in *Government Information Quarterly*, has also received 38 citations. This work offers economic-based solutions for enhancing cybersecurity in government and smart city infrastructures, providing a novel perspective on the integration of economic incentives and technological safeguards. The article contributes to expanding the discourse by emphasizing how market-driven mechanisms can play a strategic role in mitigating cybersecurity risks within public digital ecosystems.

Last, the article by Hellmeier (2016), t itled *"The Dictator's Digital Toolkit: Explaining Variation in Internet Filtering in Authoritarian Regimes,"* and published in *Politics and Policy* in 2016, the article has received 33 citations. Although it primarily focuses on the political aspects of cybersecurity, this work is significant within the broader context of digital governance studies, particularly in examining internet filtering policies in authoritarian regimes.

Table 1: Highly Cited Articles

Number	Author	Title	Journal	Year	Citation
1	Elisa, N.,Yang, L., Chao, F., Cao, Y.	A framework of blockchain-based secure and privacy-preserving E-government system	Networks, 29(3), pp. 1005–1015	2018	86
2	Alharbi, N., Papadaki, M., Dowland, P.	The impact of security and its antecedents in behaviour intention of using e-government services	Behaviour and Information Technology , 36(6), pp. 620–636	2017	55
3	Al-Besher, A., Kumar, K.	Use of artificial intelligence to enhance e-government services	Measurement Sensors , 24, 100484	2022	38
4	Li, Z., Liao, Q.	Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets	Government Information Quarterly , 35(1), pp. 151–160	2018	38
5	Hellmeier, S.	The Dictator's Digital	Politics and	2016	33

ISSN: 2406-8721 (Media Cetak) dan ISSN: 2406-8985 (Media Online)
Volume 12 Nomor 1 September 2025

		Toolkit: Explaining Variation in Internet Filtering in Authoritarian Regimes	Policy , 44(6), pp. 1158–1191		

Source: (Scopus Database)

Network and Overlay Visualizations in Cybersecurity and E-Government

In the analysis of cybersecurity within e-government, network and overlay visualizations provide a clear representation of the relationships among themes, authors, and institutions involved in the publications. By utilizing the VOSviewer software, it is possible to map various clusters that emerge based on frequently occurring keywords within the literature on this topic. These visualizations aid in understanding the structural composition and dynamics of existing research, as well as in identifying how key topics related to cybersecurity and e-government have evolved over time.

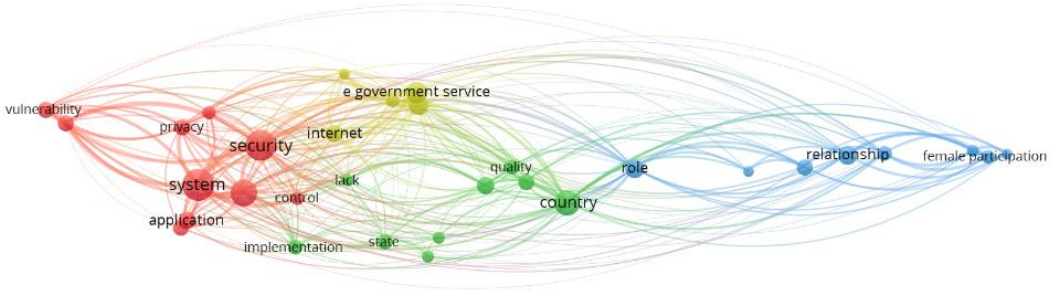


Table 2: Cluster Tema riset Cybersecurity dalam E-Government

Cluster	Themes
Cluster 1 (Red)	Application, blockchain, control, cyber attack, framework, privacy, security, system, vulnerability, website
Cluster 2 (Green)	Country, digital economy, digital technology, digital transformation, digitalization, implementation, lack, quality, state
Cluster 3 (Blue)	Cybersecurity commitment, e government development, female participation, nation, relationship, role, wellbeing, workforce
Cluster 4 (Yellow)	Artificial intelligence, citizen, e governance, e government service, internet

Source: (Scopus Database was processed using Vosviewer)

Cluster 1 (Red) highlights keywords that emphasize technical and security-related aspects, such as *application*, *blockchain*, *control*, *cyber attack*, *framework*, *privacy*, *security*, *system*, *vulnerability*, and *website*. This cluster illustrates the dominance of themes associated with technical solutions aimed at addressing cybersecurity threats in e-government, as well as the application of emerging technologies like blockchain to safeguard privacy and protect digital government systems from cyberattacks. The

ISSN: 2406-8721 (Media Cetak) dan ISSN: 2406-8985 (Media Online)
Volume 12 Nomor 1 September 2025

prominence of these terms suggests a growing demand for innovative technical solutions such as blockchain to reinforce cybersecurity in electronic government infrastructures. (Aslan & Shiong, 2023).

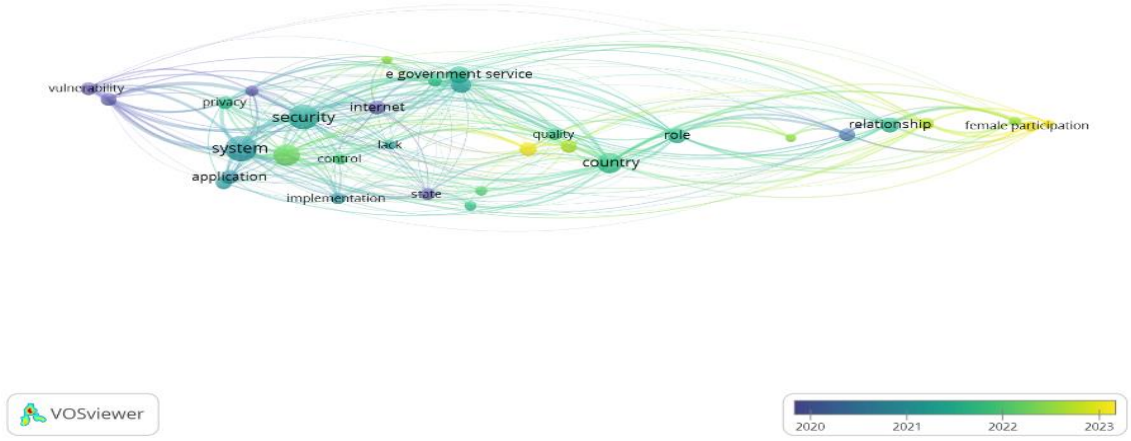
Cluster 2 (Green) connects keywords such as *country*, *digital economy*, *digital technology*, *digital transformation*, *digitalization*, *implementation*, *lack*, *quality*, and *state*. This cluster reflects a research focus on the challenges and opportunities associated with digital transformation across different countries, as well as the quality of implementation and adoption of digital technologies within government systems. It underscores how nations are progressing toward digitalization and highlights the central role of policy and transformation quality as critical issues in e-government research. Key challenges in digital transformation include disparities in digital capability, varying levels of digital literacy, and concerns related to privacy (Hagen et al., 2013).

Cluster 3 (Blue) addresses themes more closely related to cybersecurity within the broader context of e-government development, featuring keywords such as *cybersecurity commitment*, *e-government development*, *female participation*, *nation*, *relationship*, *role*, *wellbeing*, and *workforce*. This cluster highlights the importance of a strong commitment to cybersecurity as a foundational element in the advancement of e-government, as well as the critical role of societal engagement—including female participation—in ensuring the success and sustainability of secure and inclusive digital governance systems. A sustained dedication to cybersecurity is essential in e-government development, as it fosters public trust and ensures the protection of systems and data (Haddad & Binder, 2019).

Cluster 4 (Yellow) centers on innovative technologies and citizen interaction, featuring keywords such as *artificial intelligence*, *citizen*, *e-governance*, *e-government service*, and *internet*. This cluster reflects the growing application of artificial intelligence (AI) in enhancing e-government services, particularly in improving the quality of interaction between governments and citizens. It illustrates how AI technologies are being leveraged to support more efficient, personalized, and responsive e-governance systems. The integration of AI contributes significantly to optimizing service delivery and strengthening citizen engagement in digital governance processes (Singh, 2023).

Meanwhile, the overlay visualization illustrates the temporal trends of various topics in e-government and cybersecurity from 2020 to 2023. A significant increase is observed in themes such as cybersecurity, digital transformation, and artificial intelligence (AI), indicating the growing importance of these issues in recent years. Additionally, topics related to female participation and relational dynamics within e-government also show an upward trend, reflecting increased attention to inclusivity and gender equality in the implementation of e-government systems.

Figure 5: Overlay Visualitation Cybersecurity Research in E-Government



Source: (Scopus Database was processed using Vosviewer)

ISSN: 2406-8721 (Media Cetak) dan ISSN: 2406-8985 (Media Online)
Volume 12 Nomor 1 September 2025

This discussion demonstrates that while topics such as cybersecurity and digital transformation remain central concerns, there is also a growing focus on social engagement and the role of women in advancing more inclusive and secure e-government policies. In addition, artificial intelligence and e-governance play a significant role in the modernization of public administration and the strengthening of digital security.

Word Cloud and Dominant Themes in Cybersecurity and E-Government

The transformation toward a more efficient and integrated e-government requires serious attention to several key elements, one of which is cybersecurity. In this context, frequently appearing terms in the word cloud—such as *government*, *security*, *cybersecurity*, *digital*, and *information*—reflect the core focus areas in efforts to develop technology-driven governance. E-government aims to enhance the quality of public services by leveraging advancements in digital technologies. However, the successful realization of such a system depends not only on the effectiveness of digital infrastructure but also on its resilience against evolving threats. Digital government reform must address cybersecurity challenges while simultaneously embracing emerging technologies such as big data and the Internet of Things (IoT) (Elisa et al., 2018).

Appropriate information and system security are essential for maintaining public trust in digital government services. The presence of keywords such as *development*, *framework*, and *international* highlights the need for governments to establish clear policies and procedures, while also fostering collaboration with other nations to ensure optimal cybersecurity. Building a robust framework facilitates the management of secure and reliable digital governance systems. Furthermore, international cooperation is vital in strengthening global efforts to combat escalating cyber threats such as ransomware and phishing attacks, which have become increasingly prevalent (Yongping, 2023). Therefore, cybersecurity and system integrity constitute two interdependent pillars essential for the successful implementation of secure, transparent, and efficient e-government systems.

Figure 6: Word Cloud of Cybersecurity Research in E-Government

Source: (Scopus Database was processed Nvivo 12 Plus)

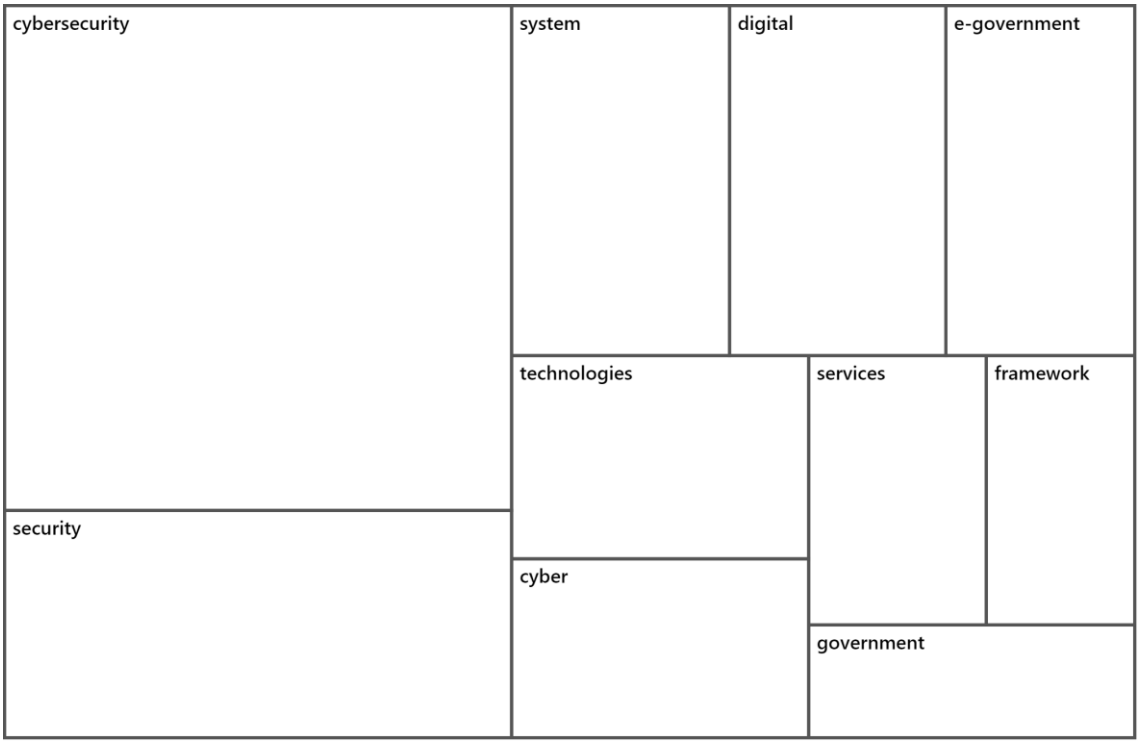
ISSN: 2406-8721 (Media Cetak) dan ISSN: 2406-8985 (Media Online)
Volume 12 Nomor 1 September 2025

In the thematic analysis conducted using NVivo 12's Autocode feature, the most prominent themes identified include *cybersecurity*, *security*, *system*, *technologies*, *cyber*, *digital*, *e-government*, *services*, *framework*, and *government*. These themes provide a comprehensive overview of how digital technologies can enhance efficiency and transparency in governance, while also underscoring the cybersecurity challenges that must be addressed in the implementation of e-government initiatives.

The dominance of *cybersecurity* and *security* as key themes reflects the critical importance of protecting data and systems used in e-government. Cybersecurity plays a vital role in safeguarding sensitive information involved in public service delivery and in mitigating threats from cyberattacks. The emergence of *system* and *technologies* highlights the need for robust infrastructure and appropriate technological tools to support the successful implementation of digital government systems. Meanwhile, the themes *digital* and *e-government* underscore that digital transformation lies at the core of public service improvement, enabling faster and more efficient access to government services.

The theme *framework* emphasizes the importance of having a well-defined policy and procedural structure in managing digital government systems, encompassing security regulations, transparency, and operational efficiency. The emergence of *government* as a theme highlights the pivotal role of the state in regulating and ensuring the effective implementation of technology and security-related policies across the public sector. Overall, the analysis conducted using NVivo 12 demonstrates that effective cybersecurity management and the adoption of appropriate technologies are essential for establishing secure, efficient, and reliable e-government systems.

Figure 7: Dominant Themes in Cybersecurity Research within E-Government



Source: (Scopus Database was processed Nvivo 12 Plus)

ISSN: 2406-8721 (Media Cetak) dan ISSN: 2406-8985 (Media Online)
Volume 12 Nomor 1 September 2025

CONCLUSION

Research on cybersecurity in e-government has shown a significant rise in attention to this issue, in parallel with the growing integration of digital technologies in public administration. Publication trends indicate a steady increase in interest since 2016, with a notable surge in the number of studies between 2021 and 2023. This increase reflects the critical need to focus on securing digital government systems in response to the rising threats of cyberattacks, such as ransomware and phishing. Thematic analysis using NVivo 12 reveals that central themes including *cybersecurity*, *security*, *digital*, and *e-government* are dominant across the literature. These findings underscore the necessity for governments to establish strong policy frameworks and secure digital infrastructures to maintain public trust in the delivery of technology-based public services.

This study is subject to certain limitations, primarily in terms of data scope, as it relies solely on publications indexed in the Scopus database. As a result, it may not capture the full breadth of relevant literature on cybersecurity in the context of e-government. Furthermore, the study does not provide an in-depth examination of the social and political factors that may influence the implementation of e-government across different national contexts. Future research is encouraged to broaden the scope of analysis by incorporating data from additional databases and sources, and by considering socio-political factors that could impact the success and challenges of cybersecurity implementation in digital governance. Further studies may also explore the application of emerging technologies, such as artificial intelligence (AI) and blockchain, in enhancing the security of e-government systems across various countries.

REFERENCE

Al-Besher, A., & Kumar, K. (2022). Use of artificial intelligence to enhance e-government services. *Measurement: Sensors*, *24*, 100484.

Alharbi, N., Papadaki, M., & Dowland, P. (2017). The impact of security and its antecedents in behaviour intention of using e-government services. *Behaviour & Information Technology*, *36*(6), 620–636.

Aslan, A., & Shiong, P. K. (2023). Learning in the Digital Age Full of Hedonistic Cultural Values Among Elementary School Students. *Bulletin of Pedagogical Research*, *3*(2), 94–102.

Bisoyi, B., Nayak, B., & Das, B. (2020). Secured and sustainable e-governance: hedging the risk by cybersecurity. *International Journal of Scientific and Technology Research*, *9*(3), 829–832.

Cavelty, M. D. (2015). *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. *August*.

Elisa, N., Yang, L., Chao, F., & Cao, Y. (2018). A framework of blockchain-based secure and privacy-preserving E-government system. *Wireless Networks*, *29*(3), 1005–1015. https://doi.org/10.1007/s11276-018-1883-0

Haddad, C., & Binder, C. (2019). Governing through cybersecurity: national policy strategies, globalized (in-)security and sociotechnical visions of the digital society. *Osterreichische Zeitschrift Fur Soziologie*, *44*, 115–134. https://doi.org/10.1007/s11614-019-00350-7

Hagen, L., Depaula, N., Dincelli, E., Caidi, N., & Rorissa, A. (2013). Electronic government around the world: Current trends and future prospects. *Proceedings of the ASIST Annual Meeting*, *50*(1). https://doi.org/10.1002/meet.14505001023

Hellmeier, S. (2016). The dictator's digital toolkit: explaining variation in internet filtering in authoritarian regimes. *Politics & Policy*, *44*(6), 1158–1191.

Janowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly*, *32*(3), 221–236. https://doi.org/10.1016/j.giq.2015.07.001

Li, Z., & Liao, Q. (2018). Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets. *Government Information Quarterly*, *35*(1), 151–160. https://doi.org/10.1016/j.giq.2017.10.006

Mijwil, M. M., Unogwu, O. J., Filali, Y., Bala, I., & Al-Shahwani, H. (2023). Exploring the Top Five

ISSN: 2406-8721 (Media Cetak) dan ISSN: 2406-8985 (Media Online)
Volume 12 Nomor 1 September 2025

Evolving Threats in Cybersecurity: An In-Depth Overview. *Mesopotamian Journal of CyberSecurity*, *2023*, 57–63. https://doi.org/10.58496/MJCS/2023/010

Sadar, S.IP., M. I. (2023). *E-Government (Konsep, Implementasi dan Evaluasi E-Government di Indonesia)*. 1–23.

Singh, A. (2023). E-Governance: Moving Towards Digital Governance. *Vidya - a Journal of Gujarat University*, *2*(1), 204–215. https://doi.org/10.47413/vidya.v2i1.173

Trubetskaya, O. V. (2020). Digitalization Of The State Sector: Foreign Experience And The Russian Future. *European Proceedings of Social and Behavioural Sciences*, 275–279. https://doi.org/10.15405/epsbs.2020.04.35

V. Weerakkody, MFWHA Janssen, Y. D. (2011). Transformational change and business process reengineering (BPR): Lessons from the British and Dutch public sector. *Government Information Quarterly: An International Journal of Information Technology Management, Policies, and Practices*, *28*(2), 320–328.

Wandaogo, A. (2022). Does digitalization improve government effectiveness? Evidence from developing and developed countries. *Applied Economics*, *54*(33), 3840–3860. https://doi.org/10.1080/00036846.2021.2016590

Wirtz, B. W., & Muller, W. M. (2019). An integrated artificial intelligence framework for public management. *Public Management Review*, *21*(7), 1076–1100. https://doi.org/10.1080/14719037.2018.1549268

Yildiz, M. (2007). E-government research: Reviewing the literature, limitations, and ways forward. *Government Information Quarterly*, *24*(3), 646–665. https://doi.org/10.1016/j.giq.2007.01.002

Yongping, G. (2023). The Past, Conundrums, and Future of International Cybersecurity Governance. *International Journal of Frontiers in Sociology*, *5*(4), 61–65. https://doi.org/10.25236/ijfs.2023.050411

Zioło, M., Niedzielski, P., Kuzionko-Ochrymiuk, E., Marcinkiewicz, J., Łobacz, K., Dyl, K., & Szanter, R. (2022). E-Government Development in European Countries: Socio-Economic and Environmental Aspects. *Energies*, *15*(23), 1–17. https://doi.org/10.3390/en15238870