JESICA: Journal of Enhanced Studies in Informatics and Computer Applications
Journal homepage: jesica.itsk-soepraoen.ac.id
ISSN: e-ISSN: 3046-6938 p-ISSN: 3046-6997
Vol. 3, No. 1, February 2026, Pp. 1-9

Systematic Literature Review on Data Security and Privacy for e-Government

Mela Firdini Azzahra*[1], Ardhan Aghsal Dwi Putra[2], Jingga Mustika Putri[3], Maulana Aditya[4], Risqy Siwi Pradini[5]
1, 2, 3, 4, 5 Institut Teknologi Sains dan Kesehatan RS.DR. Soepraoen Kesdam V/BRW, Indonesia

***Corresponding author**
E-mail address:
23102020@student.itsk-soepraoen.ac.id

Keywords:
Cyber security, data privacy, e-government, information technology, public service

Abstract

The use of e-Government is increasing along with efforts to improve the efficiency, transparency, and quality of public services. However, advances in digitalization are also accompanied by cybersecurity risks and threats to data privacy. This study aims to examine the implementation of data security and privacy in e-Government, as well as evaluate the technologies used to mitigate data leaks and misuse. The method used is Systematic Literature Review of articles published between 2021 and 2025 through Scopus, ScienceDirect, and Google Scholar databases. The research selection followed the PRISMA 2020 guidelines, resulting in 16 articles meeting the eligibility criteria. The study findings indicate that information security implementation in government institutions remains inconsistent, with key challenges related to weak security management, technical system vulnerabilities, and low public trust in personal data protection. Several technologies considered to have potential to improve security include blockchain, advanced cryptography, and automation for vulnerability detection, although their implementation remains hampered by cost, scalability, and human resource readiness. Overall, this study emphasizes that a comprehensive approach that combines technology, management, and increased security awareness is needed to strengthen data protection in e-Government.

1. Introduction

In this era, everything is inseparable from digitalization, be it in the fields of education, business, health, or even government [1]. The government uses e-Government as a digital technology to facilitate public services for the community and other institutions to increase efficiency and transparency [2]. However, this digital transparency also carries significant privacy risks; protecting personal data in electronic systems is a form of respect for the privacy of highly sensitive individuals [3]. Along with the increasing use of e-Government and the demand for sensitive data collection, serious problems have emerged in the form of cybercrime threats and data security risks [4].

Even though these risks are known, the implementation of security in e-Government is still lacking and not appropriate [5]. One of the main challenges is the risk of personal data leaks that still overshadows the digitalization policy for public services, so it is necessary to strengthen information technology infrastructure and adjust existing regulations [6]. Not to mention the awareness and human resources in governments in several countries in addressing this problem, so that public trust in e-Government has decreased [7].

Previous research shows that privacy security risks play a major role in influencing e-Government adoption. Study [8] confirms that risks and concerns about misuse of personal data can influence people's decisions to use government digital services. Public perception of data security and privacy positively affects trust in e-Government, so service platforms need to ensure citizens' personal information is fully secure [7]. According to [9], e-Government challenges do not only come from external threats but also internal weaknesses such as suboptimal security governance and a lack of policy control. An efficient security model in the public sector should include citizen identification, identity authentication, data confidentiality, and data integrity to minimize the emergence of new vulnerabilities [10]. This shows that e-Government security issues are multidimensional and require a comprehensive approach [11].

Several technological solutions have been proposed to address this issue. Blockchain technology, for example, offers the potential to improve data integrity and security through its decentralization and immutability [12][13]. There is also static analysis, which is used to detect software vulnerabilities early in development so that risks can be minimized more quickly [14]. Given the ever-changing landscape of digital services, systematic observation of citizen attitudes and technological developments is essential to map privacy-related barriers [15]. Although various solutions have been researched, there has not been a comprehensive mapping of how these risks and privacy issues are interrelated in the context of e-Government [16].

Based on these conditions, this study uses the Systematic Literature Review (SLR) method to summarize research findings related to data security and privacy in e-Government. This study aims to identify the implementation of data security and privacy in e-Government systems, while analyzing effective technologies for mitigating data leaks and improving security and privacy levels in e-Government. Therefore, the research findings are expected to serve as a reference for governments, researchers, and system developers in designing more secure and reliable e-Government services.

2. Research Method

This study uses the Systematic Literature Review (SLR) method to identify relevant research related to data security and privacy in e-Government implementation. This SLR method was chosen because it provides a comprehensive overview of research trends, challenges, and proposes solutions in a systematic and structured manner, in accordance with the PRISMA 2020 guidelines [17].

2.1. Research Questions and PICO

This research follows several stages, including planning, implementation, and reporting. In the planning stage, the research objectives and Research Questions (RQs) are determined. In the implementation stage, a literature search, study selection, and data extraction are conducted. In the final stage, reporting, analysis, and synthesis are undertaken to answer the RQs. The RQs to be addressed through this research are:

- RQ1: How are data security and privacy implemented in e-Government systems?
- RQ2: What technologies are effective in mitigating data breaches and enhancing e-Government data security and privacy?

To ensure focus and consistency in the literature search and selection process, this study employed the PICO (Population, Intervention, Comparison, Outcome) framework. This framework served as the basis for discussing the research questions, developing the literature search strategy, and establishing the inclusion and exclusion criteria, as shown in Table 1. The PICO framework served as the primary reference for determining keywords and developing the inclusion and exclusion criteria in the SLR [18].

Table 1. Research framework using PICO

Component	Description
Population (P)	e-Government systems in various countries or agencies that manage sensitive public data.
Intervention (I)	Implementation of security & privacy methods: encryption, access control, blockchain, and security policies.
Comparison (C)	An e-government system without security.
Outcome (O)	Methods in data security and privacy in e-Government effectiveness methods.

2.2. Data Source

The literature sources for this study are gathered from reputable scientific databases commonly used in information technology research, specifically Scopus and Google Scholar. These databases were chosen to ensure that the studies reviewed were of high quality and relevance, particularly in the areas of e-Government, cybersecurity, and data privacy. A comprehensive literature search was conducted across these scientific databases to obtain relevant and high-quality articles.

Table 2. Databases in scientific source searches

Database	Query string	Result	Date of search
Scopus	“E-Government” AND “Security”	58	23-11-2025
	“E-Government” AND “Privacy”	28	23-11-2025
	“E-Government AND Information Security”	15	17-11-2025
	“E-Government” AND “Risk”	37	17-11-2025
Google Scholar	“E-Government” AND “Cyber Crime”	1	17-11-2025

Basic details of the data used, search keywords, publication range, and the last search date are presented in Table 2. The search was conducted using various keyword combinations (query strings) arranged based on PICO components, with a focus on e-Government systems, cybersecurity, and data privacy. The Results column shows the initial number of articles obtained from each keyword combination before further filtering. Meanwhile, the Search Date column displayed in Table 2 lists the last search date, namely November 17, 2025. Recording the number of results and search time is done to maintain transparency of the research process, support reproducibility, and ensure the method's compliance with the PRISMA 2020 guidelines.

2.3. Search Strategy

The literature search process is conducted using a combination of keywords tailored to the focus of the research topic. The keyword structure utilized Boolean operators (AND and OR) to control the scope of the search results, both broadening and narrowing the articles retrieved. The main keyword combinations used in the search process include “e-Government” AND “Security”, “e-Government” AND “Privacy”, “e-Government AND “Information Security”, “e-Government” AND “Risk”, and also “e-Government” AND “Cyber Crime”.

2.4. Inclusion and Exclusion Criteria

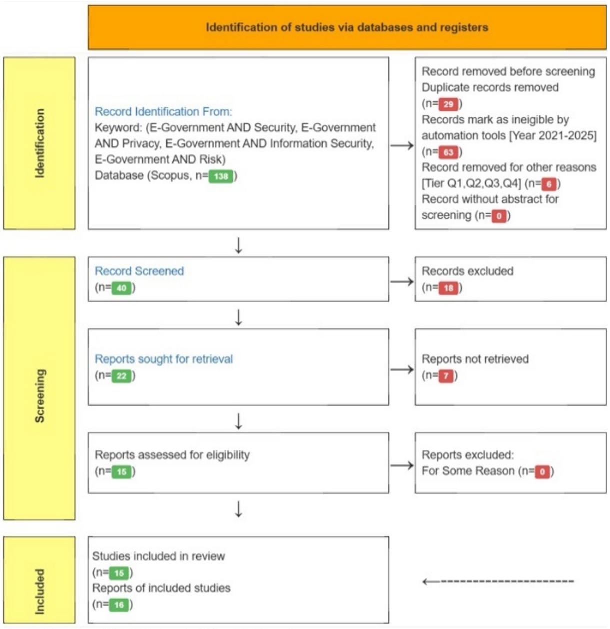
To ensure the relevance and quality of the literature used, this study established inclusion and exclusion criteria as a reference in selecting references. The inclusion and exclusion criteria used are shown in Table 3.

Table 3. Inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
The journal article discusses security, data privacy, and risks in the context of e-Government	The article is not available in full-text form
Articles published between 2021 and 2025	Articles in the form of opinions, editorials or proceedings that do not have complete research data
English language articles	The article discusses data security in other sectors such as e-commerce or banking
Articles are freely accessible (open access)	The article is a duplication of another publication
Articles accredited Q4, Q2, Q3, and Q1	Unaccredited article

2.5. Study Selection Process

The literature selection process in this study is conducted systematically by adhering to the PRISMA 2020 guidelines, which include the stages of identification, screening, eligibility, and inclusion. The detailed study selection process is presented in Figure 1.


Identification of studies via databases and registers
Identification
Record Identification From:
Keyword: (E-Government AND Security, E-Government AND Privacy, E-Government AND Information Security, E-Government AND Risk)
Database (Scopus, n=138)
Record removed before screening
Duplicate records removed
(n=29)
Records mark as ineigible by automation tools [Year 2021-2025]
(n=63)
Record removed for other reasons [Tier Q1,Q2,Q3,Q4] (n=6)
Record without abstract for screening (n=0)
Screening
Record Screened
(n=40)
Records excluded
(n=18)
Reports sought for retrieval
(n=22)
Reports not retrieved
(n=7)
Reports assessed for eligibility
(n=15)
Reports excluded:
For Some Reason (n=0)
Included
Studies included in review
(n=15)
Reports of included studies
(n=16)

Generate From Watase Uake Tools, based on Prisma 2020 Reporting

Figure 1. PRISMA diagram

In the identification stage, a literature search was conducted using a combination of keywords related to e-Government, security, privacy, information security, and risk. The search focused on the Scopus database with publication years ranging from 2021 to 2025, resulting in 138 articles. Of these, 29 articles were removed due to duplication. Furthermore, an initial screening process using an automated tool eliminated 63 articles for not meeting publication year criteria, and 6 articles were excluded for not meeting accredited journal criteria (Q1–Q4).

A screening phase was conducted on 40 articles that passed the initial selection process by reviewing their titles and abstracts. The screening results showed that 18 articles were irrelevant to the research focus, namely, data security and privacy in e-Government, and therefore, they were excluded. Next, 22 articles were reviewed in full text. However, 7 articles were not fully accessible and were excluded from the selection process. At the eligibility stage, 15 full-text articles were further evaluated based on predetermined inclusion and exclusion criteria. All articles at this stage were deemed to meet the criteria, and none were eliminated. The final stage, inclusion, resulted in a total of 16 articles deemed eligible, consisting of 15 obtained from the primary database and 1 from a supplementary source. These articles were then used as the basis for analysis in the SLR study to identify security risks, data privacy issues, and technological solutions implemented in e-Government.

2.6. Quality Assessment

To ensure that the articles used in this study were of good quality and good relevance, a quality assessment was conducted. Each article that passed the selection process was then evaluated using several quality assessment criteria. The quality assessment criteria used in this study consisted of three questions, as shown in Table 4. From the quality assessment criteria used in sorting out which articles meet most of the criteria, they are declared worthy of proceeding to the data extraction and analysis stage.

Table 4. Article quality assessment criteria

Code	Assessment criteria
QA1	Does the article clearly explain the security or privacy issue?
QA2	Is the research methodology explained completely and logically?
QA3	Does the article propose solutions, frameworks, or recommendations to address the problem discussed?

2.7. Data Extraction

At this stage, important information was extracted from each article that passed the selection process. The collected data includes the author's name and year of publication, the research objectives, the methods used, and the focus of the discussion regarding data security and privacy in e-government systems. Additionally, information regarding the types of security threats, data privacy topics, and proposed solutions or technologies was recorded. This extracted data served as the basis for the analysis and discussion of the research results.

2.8. Data Analysis

The extracted data were analyzed using a descriptive analysis approach. The selected articles were grouped based on discussion topics, such as types of security risks, data privacy issues, and approaches or technologies used to enhance security in e-government systems. The results of this analysis are then used to answer the research questions and identify trends and challenges still faced in implementing data security and privacy in e-Government.

3. Results and Discussion

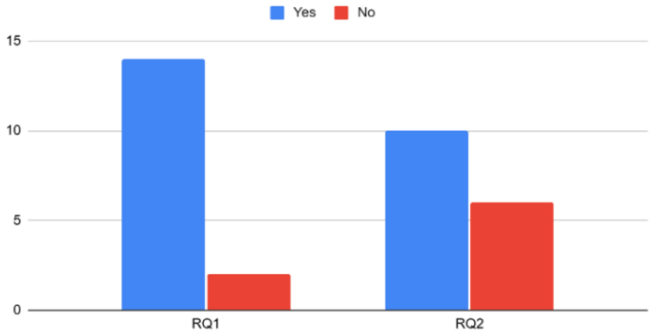


Figure 2. Distribution of article relevance to RQ

This section outlines the empirical findings obtained from a systematic synthesis of 16 selected articles spanning the period 2021 to 2025. The analysis results are mapped to answer two main research questions, namely how data security and privacy are implemented (RQ1) and the classification of proposed technology solutions (RQ2). Figure 2 shows that most of the reviewed journals are highly relevant to Research Question 1 (RQ1), with 14 journals meeting the criteria (Yes) and 2 journals not meeting the criteria (No). Meanwhile, for Research Question 2 (RQ2), there are 10 relevant journals (Yes) and 6 irrelevant journals (No), indicating variation in the scope of RQ2.

3.1. Implementation of Data Security and Privacy in e-Government Systems (RQ1)

Data extraction results from primary studies indicate a variety of implementation focuses, encompassing institutional, policy, and risk management aspects in the implementation of e-Government systems. A summary of the data security and privacy implementations identified to address RQ1. Table 5 presents the implementation of data security and privacy in e-Government systems based on selected studies that address RQ1. The results show that the approaches used in these studies are diverse, including quantitative analysis methods, structured literature reviews, and the development of technical and conceptual frameworks.

Table 5. Implementation of data security and privacy in e-Government systems (RQ1)

Author	Security methods	Data privacy aspects	Technology/standards	Results
[8]	Security risk factor analysis (Quantitative/PLS-SEM)	Protection against privac risk factors in service adoption	SmartPLS 3.2.8, PLS-SEM	Privacy, security, and institutional logic factors accounted for 61.7% of citizens' reasons for adopting services.
[5]	Framework GAUCHO (Government adaptive unified cybersecurity holistic orchestration)	Secure data exchange and protection of sensitive information	MARISMA, X-Road	Proposes a holistic framework that integrates adaptive risk management and cyber governance.
[9]	Structured Literature Review for Risk Typology	Security and system risks that affect trust	e-Government Risk Typology	Comprehensive risk classification to help system designers build more reliable services.
[7]	Meta-Analytic Structural Equation Modeling (MASEM)	The relationship between privacy and risk as determinants of trust	Statistical Analysis (MASEM)	Security and privacy are key building blocks of trust.
[12]	Blockchain Immutability Framework	Data transparency, fraud prevention, record integrity	Blockchain	Blockchain-based framework to increase transparency and public trust.
[19]	Data Security Management Review (Review)	Protection of sensitive data & government information assets	Yesser Program	Evaluation of data security policies and identification of infrastructure vulnerabilities in Saudi Arabia.
[14]	Combined Static Application Security Testing (SAST).	Vulnerability detection leak prevention	SAST Tools (Code Analysis)	The combined use of SAST tools improves the accuracy of security vulnerability detection in open-source projects.
[20]	Automated threat modeling	GDPR Compliance and Data Protection Impact Assessment (DPIA)	BPMN, OWASP Risk Rating	An automated BPMN-based methodology for identifying privacy threats/risks without the need for in-depth expertise.
[2]	Decentralized framework & Artificial Immune System (AIS)	Privacy preservation via encryption & data immunity	Blockchain (Ethereum), AIS	A decentralized system that mitigates internal/external threats while maintaining user privacy.
[21]	Institutional strategic analysis & standardization	Increased transparency and public trust mechanisms	Blockchain	A multi-faceted strategy (institutions, standards, talent) to accelerate secure blockchain adoption.

[4]	Privacy preservation instruments	Privacy by Design, privacy control, data lifecycle protection	Privacy Model (Misuse prevention)	Privacy controls and impact assessments greatly influence citizens' trust in services.
[22]	Data Taxonomy Analysis on public portals	Risk of personal data exposure due to transparency initiatives	LOTAIP, Web Portals	Found that transparency initiatives without adequate protections leave citizens' data (including children's) vulnerable to exfiltration attacks.
[13]	Security issue literature review	High level of data integrity & privacy through decentralization	Blockchain	Identify critical security challenges and the need for data reliability research in decentralized systems.
[23]	Self-Sovereign Identity (SSI)	Full user control over identity (User-centric control)	Blockchain, SSI	Blockchain-based identity solutions to address centralized system vulnerabilities (Africa case study).

In terms of security methods, several studies use statistical approaches and structural modeling to analyze the role of security and privacy in the adoption and trust in e-Government services, such as Partial Least Squares Structural Equation Modeling and Meta-Analytic Structural Equation Modeling [7], [8]. In addition, several studies focus on developing an integrated cybersecurity framework, risk classification, and automated threat modeling to identify security and privacy risks in digital government systems [5], [9], [20].

In the aspect of data privacy, the main focus of the research includes protecting sensitive data, preventing information leaks, increasing data transparency, and strengthening privacy controls by [4], [12], [22], [23]. Several studies specifically highlight the relationship between privacy, risk, and the level of public trust in e-Government services [4], [7], while other research on the importance of compliance with data protection regulations and the implementation of data protection impact assessments [20].

Viewed from a technology and standards perspective, blockchain technology is the most frequently used approach to guarantee data integrity, increase transparency, and support digital identity management in e-Government systems [2], [12], [13], [21], [23]. In addition to blockchain, several studies also utilize other technologies and standards, such as static application security testing, business process models and notations, OWASP risk ratings, and government data exchange platforms to support the implementation of data security and privacy [5], [14], [20]. Overall, the results presented in Table 5 show that the implementation of data security and privacy in e-Government systems is carried out through a combination of policy, methodological, and technological approaches, with a focus on data protection, risk management, and strengthening public trust mechanisms.

3.2. The Effective Technologies in Addressing Data Leaks and Improving the Security and Privacy of e-Government Data (RQ2)

Data extraction results from primary studies indicate that the technologies used are diverse and encompass security at the data, software, business process, and infrastructure levels. A summary of the technologies understood to address RQ2 is presented in Table 6. Based on a mapping of the ten selected articles, it can be identified that e-Government security approaches encompass a combination of technical, policy, and managerial aspects. Each study makes a specific contribution to strengthening data protection and increasing public trust in digital government systems.

In the conceptual and managerial realm, risk typology and trust management are proposed as a foundation in system design [25]. This approach focuses on classifying systemic risks to assist e-Government architecture designers in minimizing user distrust. In line with the policy aspect, the effectiveness of data security management policies is evaluated through the Yesser Program, which emphasizes the importance of formal policies in protecting critical government information assets [19].

From a technical perspective, blockchain technology has emerged as the dominant approach. The immutability of the blockchain framework demonstrated can ensure transparency and preventing manipulation of government transaction records through its tamper-proof nature [12]. This finding is reinforced by the results of other studies, which show that blockchain decentralization provides higher data integrity than centralized database systems [13]. In addition, the importance of technical standardization in blockchain implementation is also emphasized to ensure interoperability and improve public trust mechanisms [21]. Further innovation is offered through the integration of blockchain with the

Artificial Immune System (AIS), which enables automatic intrusion detection by mimicking the mechanisms of the biological immune system [2].

Table 6. Effective technologies for e-Government security and privacy (RQ2)

Author	Technology	Effectiveness of solution
[9]	Risk Typology & Trust Management	Classifying systemic risks to help system designers build architectures that minimize user distrust.
[12]	Blockchain Immutability Framework	Ensure transparency and prevent manipulation of government transaction records through blockchain's tamper-proof nature.
[19]	Data Security Management Policy	Evaluation of the effectiveness of data security policies (Yesser Program) in protecting critical government information assets.
[14]	Static Application Security Testing (SAST)	Early detection of security holes in application source code before release to prevent exploitation.
[2]	Blockchain & Artificial Immune System (AIS)	Combining blockchain decentralization with AIS to automatically detect intrusions like the body's immune system.
[21]	Blockchain & Technical Standardization	Blockchain implementation strategy through technical standardization to increase transparency and public trust mechanisms.
[22]	Transparency Taxonomy Analysis	Identify data exposure risks on transparency portals and suggest stricter access controls on public data.
[13]	Blockchain and Decentralization	Offers high levels of data integrity through decentralization to address vulnerabilities in centralized database systems.
[24]	Privacy-Preserving Data Analysis (PPDA)	Implementing Differential Privacy and Homomorphic Encryption to analyze sensitive data without revealing individual identities.
[25]	Zero Trust Network Architecture (ZTNA)	Implementing the “Never Trust, Always Verify” principle with continuous authentication and network micro-segmentation.

In the context of application security, the implementation of Static Application Security Testing (SAST) has proven effective in detecting vulnerabilities in source code from the early stages of development, thereby preventing exploitation before the application is released to the production environment [14]. This finding emphasizes the importance of implementing security from the early phases of the software development lifecycle.

Data protection and privacy issues also receive significant attention. The Privacy-Preserving Data Analysis (PPDA) approach, utilizing Differential Privacy and Homomorphic Encryption, enables the analysis of sensitive data without revealing individual identities [24]. This approach complements findings that identified data exposure risks on government transparency portals and recommended stricter access controls to public data [22]. Finally, a modern network security approach is represented by the implementation of Zero Trust Network Architecture (ZTNA). Based on the principle of Never Trust, Always Verify, this model implements continuous authentication and network micro-segmentation to reduce the risk of threats, both internal and external [25].

Overall, this mapping demonstrates that effective e-government security is achieved through a multidimensional approach that combines policy and risk management, blockchain-based data integrity, privacy protection through advanced encryption techniques, and adaptive security architectures such as Zero Trust. This integrated approach is a critical foundation for building a secure, transparent, and trustworthy digital government system.

3.3. Discussion

Based on the results of RQ1 and RQ2, it can be seen that data security and privacy issues in e-Government systems are not only influenced by the availability of technology, but also by the accompanying methodological approaches, policies, and institutional governance. The findings of RQ1 indicate that data security and privacy are consistently positioned as the main factors influencing public trust and adoption of e-Government services, while RQ2 identifies technologies used to address data leak risks and privacy breaches.

The results of RQ1 confirm that many studies place privacy, security, and risk as key determinants of public trust in e-government services. Analytical approaches, such as structural modeling and meta-analysis, demonstrate that perceived risk and privacy protection are directly related to the intention to use government digital services. This indicates that the success of e-government depends not only on service functionality but also on the system's ability to reliably guarantee citizen data protection. In other words, security and privacy serve as fundamental prerequisites for the public's willingness to widely adopt e-government services.

Furthermore, the findings of RQ2 complement RQ1 by demonstrating that the technologies used to address security and privacy challenges are multi-layered, spanning data, software, business processes, and infrastructure. The dominance of blockchain technology in both RQs demonstrates a tendency for research to leverage its integrity, transparency, and decentralization to address data manipulation issues and increase public trust. However, these findings also indicate that blockchain is more often used as a technical solution, while aspects of governance, organizational readiness, and human resource capacity remain relatively under-explored.

In addition to blockchain, other technologies such as static application security testing and automated threat modeling demonstrate a shift in focus from a reactive to a preventative approach. This approach signals a growing awareness that data breaches are caused not only by external attacks but also by weaknesses in software and internal government processes. This aligns with the findings of RQ1, which highlighted the importance of risk and trust management, as failures at the technical level can directly impact public perceptions of government credibility.

The integration of the results of RQ1 and RQ2 also demonstrates a strong link between security technology and non-technical factors, such as privacy policies, regulations, and institutional controls. Several studies in RQ1 emphasized the importance of compliance with data protection regulations and the implementation of privacy impact assessments, while RQ2 demonstrated that supporting technology for these requirements is readily available. However, the link between technology implementation and the effectiveness of privacy policies in the operational context of e-Government remains under-explored in most studies.

Overall, this discussion shows that while various technologies have been proposed and implemented to enhance e-Government security and privacy, the main challenge lies in the integration of technical solutions, policies, and institutional governance. The findings of RQ1 and RQ2 together indicate that a holistic approach, combining technology, risk management, regulation, and enhancing public trust, remains a key requirement in developing secure e-Government systems that prioritize citizen data protection.

4. Conclusion

Based on the SLR analysis of 16 selected articles, it can be concluded that the implementation of data security and privacy aspects in e-Government information has been carried out through security policies, audits, and data protection techniques. However, this implementation still feels disjointed among various agencies, resulting in uneven levels of security maturity. This situation impacts the effectiveness of data protection and triggers low levels of public trust in digital services provided by the government. Thus, the objective of the first study has been answered, namely, achieving a comprehensive understanding of the actual state of data security and privacy implementation in e-Government. Regarding the objectives of the second study, the results demonstrate that technologies such as blockchain, advanced cryptography, and automation in vulnerability detection have significant potential to improve security and reduce the risk of data breaches. However, the success of these implementations depends heavily on infrastructure readiness, human resource skills, and stable policy support. The impact of this research is to provide a map of problems and solutions that can be used as a reference by the government and system developers in creating a more secure e-government. Recommendations include improving security management structures, increasing security awareness among officials and the public, standardizing personal data protection, and developing applicable research information related to the suggested security technologies.

References

[1] S. Weiland, "Open access and the unfinished transformation of scholarly communications," in *International Encyclopedia of Education*, 4th ed., R. J. Tierney, F. Rizvi, and K. Ercikan, Eds. Amsterdam, The Netherlands: Elsevier, 2023, pp. 63–73, doi: 10.1016/B978-0-12-818630-5.02090-X.

[2] N. Elisa, L. Yang, F. Chao, N. Naik, and T. Boongoen, "A Secure and Privacy-Preserving E-Government Framework Using Blockchain and Artificial Immunity," *IEEE Access*, vol. 11, pp. 8773–8789, 2023, doi: 10.1109/ACCESS.2023.3239814.

[3] K. M. Angnesia and S. A. Wiraguna, "Analisis Pertanggungjawaban Hukum Pemerintah dalam Menegakkan Pelindungan Data Pribadi di Era Digital," *Perspektif Administrasi Publik dan Hukum*, vol. 2, no. 2, pp. 176–187, 2025, doi: 10.62383/perspektif.v2i2.249.

[4] H. Alabdali, M. Albadawi, M. Sarrab, and A. Alhamadani, "Privacy preservation instruments influencing the trustworthiness of e-Government services," *Computers*, vol. 10, no. 9, Sep. 2021, doi: 10.3390/computers10090114.

[5] V. Figueroa, L. E. Sánchez Crespo, A. Santos-Olmo, D. G. Rosado, and E. Fernández-Medina, "Building a holistic cybersecurity framework for e-Government based on a systematic analysis of proposals," *Int J Inf Secur*, vol. 24, no. 3, Jun. 2025, doi: 10.1007/s10207-025-01024-0.

[6] L. P. A. Subarkah, B. Mulyani, and M. A. Idrus, "Implications of Government Policy on Digitalization of Public Services in Realizing Smart Government," *Journal La Sociale*, vol. 6, no. 3, pp. 842–859, May 2025, doi: 10.37899/journal-la-sociale.v6i3.1702.

[7] P. Gupta, A. Hooda, A. Jeyaraj, J. J. M. Seddon, and Y. K. Dwivedi, "Trust, Risk, Privacy and Security in e-Government Use: Insights from a MASEM

Analysis," *Information Systems Frontiers*, vol. 27, no. 3, pp. 1089–1105, Jun. 2025, doi: 10.1007/s10796-024-10497-8.

[8] A. Bayaga, "Examining the predictive relevance of security, privacy risk factors, and institutional logics for e-Government service adoption," Jan. 01, 2022, *John Wiley and Sons Inc*. doi: 10.1002/isd2.12201.

[9] B. Distel, H. Koelmann, R. Plattfaut, and J. Becker, "Watch who you trust! A structured literature review to build a typology of e-Government risks," *Information Systems and e-Business Management*, vol. 20, no. 4, pp. 789–818, Dec. 2022, doi: 10.1007/s10257-022-00573-4.

[10] M. M. Ahmed and A. Musa Ahmed, "Citizens' Data Protection in E-Government System," *International Journal of Innovative Computing*, vol. 13, no. 2, pp. 1–9, Nov. 2023, doi: 10.11113/ijic.v13n2.389.

[11] S. Malodia, A. Dhir, M. Mishra, and Z. A. Bhatti, "Future of e-Government: An integrated conceptual framework," *Technological Forecasting and Social Change*, vol. 173, p. 121102, 2021, doi: 10.1016/j.techfore.2021.121102.

[12] D. Ahmad, N. Lutfiani, A. D. A. Rizki Ahmad, U. Rahardja, and Q. Aini, "Blockchain Technology Immutability Framework Design in E-Government," *Jurnal Administrasi Publik: Public Administration Journal*, vol. 11, no. 1, pp. 32–41, Jun. 2021, doi: 10.31289/jap.v11i1.4310.

[13] M. Štaka, M. Stefanović, D. Stefanović, Đ. Pržulj, and V. Fabri, "Review of security issues in the application of blockchain technology in e-Government," *Centre for Evaluation in Education and Science (CEON/CEES)*, May 2024, pp. 84–93. doi: 10.5937/imcsm24059s.

[14] A. Nguyen-Duc, M. V. Do, Q. Luong Hong, K. Nguyen Khac, and A. Nguyen Quang, "On the adoption of static analysis for software security assessment–A case study of an open-source e-Government project," *Comput Secur*, vol. 111, Dec. 2021, doi: 10.1016/j.cose.2021.102470.

[15] I. Savveli, M. Rigou, and S. Balaskas, "From E-Government to AI E-Government: A Systematic Review of Citizen Attitudes," Sep. 01, 2025, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/informatics12030098.

[16] S. Mushtaq and M. Shah, "Mitigating Cybercrimes in E-Government Services: A Systematic Review and Bibliometric Analysis," Mar. 01, 2025, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/digital5010003.

[17] M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," Mar. 29, 2021, *BMJ Publishing Group*. doi: 10.1136/bmj.n71.

[18] M. B. Eriksen and T. F. Frandsen, "The impact of patient, intervention, comparison, outcome (Pico) as a search strategy tool on literature search quality: A systematic review," *Journal of the Medical Library Association*, vol. 106, no. 4, pp. 420–431, Oct. 2018, doi: 10.5195/jmla.2018.345.

[19] A. S. Alharbi, G. Halikias, M. Rajarajan, and M. Yamin, "A review of effectiveness of Saudi E-Government data security management," *International Journal of Information Technology (Singapore)*, vol. 13, no. 2, pp. 573–579, Apr. 2021, doi: 10.1007/s41870-021-00611-3.

[20] D. Granata, M. Rak, G. Salzillo, G. Di Guida, and S. Petrillo, "Automated threat modelling and risk analysis in e-Government using BPMN," *Conn Sci*, vol. 35, no. 1, 2023, doi: 10.1080/09540091.2023.2284645.

[21] J. Yu, "Exploration of the application of blockchain in e-Government: Opportunities and risks coexist," *Inf Serv Use*, vol. 44, no. 3, pp. 255–266, Nov. 2024, doi: 10.3233/ISU-240013.

[22] C. Paguay-Chimarro, D. Cevallos-Salas, A. Rodríguez-Hoyos, and J. Estrada-Jiménez, "Transparency Unleashed: Privacy Risks in the Age of E-Government," *Informatics*, vol. 12, no. 2, Jun. 2025, doi: 10.3390/informatics12020039.

[23] G. Mandinyenya, V. Malele, and G. Mandinyenya, "'A Blockchain-based Identity Management Solution for Secure Personal Data Sharing in Africa: A Systematic Literature Review' A Blockchain-based Identity Management Solution for Secure Personal Data Sharing in Africa: A Systematic Literature Review A Blockchain-based Identity Management Solution for Secure Personal Data Sharing in Africa: A Systematic Literature Review," *Latin-American Journal of Computing (LAJC)*, vol. 12, no. 2, 2025, doi: 10.5281/zenodo.15742071.

[24] Y. M. D. Ali, "Privacy-Preserving data analysis," *Advances in Engineering Innovation*, vol. 7, no. 1, pp. 32–36, Apr. 2024, doi: 10.54254/2977-3903/7/2024029.

[25] Kipkoech Denzel, "A survey of security in zero trust network architectures," *GSC Advanced Research and Reviews*, vol. 22, no. 2, pp. 182–214, Feb. 2025, doi: 10.30574/gscarr.2025.22.2.0036.