The Indonesian Journal of Computer Science
www.ijcs.net
Volume 13, Issue 6, December 2024
https://doi.org/10.33022/ijcs.v13i6.4531

Information Security Factors and Strategies in Enhancing E-Government Adoption in the Public Sector of Developing Countries: A Literature Review

Devi Febrianty[1], Muhammad Hilman[2], Setiadi Yazid[3]
devi.febrianty@ui.ac.id[1], muhammad.hilman@ui.ac.id[2], setiadi.yazid@ui.ac.id[3]
[1,2,3] Faculty of Computer Science, Universitas Indonesia

Article Information

Received : 6 Dec 2024
Revised : 11 Dec 2024
Accepted : 30 Dec 2024

Keywords

information security, E-government, Public sector, Factors, Strategies, Literature review

Abstract

The development of e-government is increasingly prioritized in developing countries as part of digital transformation efforts to improve the quality of public services. However, challenges such as low adoption rates, public trust issues, and weak information security persist. This research aims to comprehensively identify information security factors influencing e-government adoption in developing countries and propose implementation strategies. The approach used is a combination of systematic literature review and snowballing technique. We categorized security factors using the Technology, Organization, and Environment (TOE) framework to aid analysis and strategy formulation. Findings show that non-technical factors, particularly organizational and environmental aspects (41% each), dominate over technical factors (18%). These results highlight the importance of strengthening security policies, risk management, and data protection regulations by the government, as well as efforts to improve public perception of information security. This research provides theoretical contributions through a TOE-based framework and practical strategies to increase e-government adoption.

A. Introduction

Effective utilization of information and communication technology (ICT) is an essential step for the government in fulfilling its responsibilities, namely providing public services that are fast, efficient, and reach the entire community. One tangible form of this utilization is digital transformation through the implementation of e-government, designed to accelerate the service process and increase service affordability more broadly. ICT also enables governments to make real-time data-based policies, improve decision-making capacity, and distribute evidence-based services in a targeted manner [1].

The definition of e-government is the use of internet-based information technology to improve accountability and efficiency in various government functions [2]. The application of information technology in the public sector changes the dynamics of the relationship between society and government (G2C), business and government (G2B), and between government agencies (G2G), which leads to accelerated and easier access to public services [3]. The wide-ranging benefits of e-government have encouraged its increased use in both developed and developing countries [3], [4]. However, e-government implementation does not always run smoothly, especially in developing countries. One of the biggest challenges faced is the low level of adoption by the public. Early adoption and continued use of e-government services by citizens are essential factors in determining the long-term success of e-government services, especially in developing countries. Previous research shows that e-government adoption in developing countries is still relatively low [2], [4]. Factors affecting this low adoption include suboptimal system quality, limited infrastructure, low level of community digital literacy, and information security issues that are still a significant concern [2], [5], [6].

Information security, in particular, is one of the most critical factors in e-government adoption. Lack of trust in the internet, concerns about privacy risks, and the threat of data leakage are significant barriers to increasing e-government adoption [6]. Several hacking incidents have occurred against data managed by government agencies in developing countries, potentially leading to sensitive data leakage. One of the significant incidents occurred in India in 2018, when the Aadhaar database that holds information on more than 1 billion residents, including biometric data and bank accounts, was hacked [7]. In Indonesia, the hack of the National Data Center in 2024 also threatened to leak the data of millions of residents, highlighting the weakness of national data security [8]. A series of incidents related to data leaks and cybersecurity attacks on government-owned public information systems exacerbated the situation, possibly leading to a decline in public trust [9].

To increase e-government adoption, governments must identify information security-related factors and formulate effective implementation strategies. An in-depth understanding of these factors will help the government design more targeted information security initiatives, thereby increasing the use of e-government services [1], [2]. Previous research has discussed various aspects of information security in the context of e-government. However, most of them discuss e-government broadly and pay less in-depth attention to information security. Research by Mustafa et al. [2], Aleisa [10], Tremblay-Cantin, et al. [4], and

Sihotang et al. [11] analyzed the factors of e-government adoption in developing countries in general. Another study by Gupta and Chauhan [12] used TAM, TPB, and DeLone and McLean's Model, emphasizing trust factors in e-government, including cultural moderation. Similarly, Alfiani et al. [13] discussed implementation issues in general without focusing on information security. As a result, discussions about information security often lack detail, especially regarding its role in increasing public trust.

Research on information security factors oriented towards implementation solutions and sustainable use of e-government services in developing countries is minimal. Mushtaq [14] discusses information security in general and provides solutions that are not specific to the context of developing countries. To fill these limitations, this research conducts a comprehensive literature review. It analyzes relevant information security factors in terms of technology, organization, and environment in the context of developing countries. It proposes strategies that can be implemented to increase public trust in using e-government. Thus, the questions in this research include:

1. What information security factors influence developing countries' public trust and e-government adoption?
2. How can government agencies implement these factors to increase public trust and e-government adoption in developing countries?

By answering these two questions, this research aims to identify key information security factors influencing e-government adoption in developing countries through a literature review approach and provide recommendations for implementing these factors in government agencies.

This research has important implications, both academically and practically. Academically, this research adds to the literature on information security factors and strategies in e-government adoption, especially in developing countries that are still limited. Practically, these findings can help the government formulate policies and strategies for e-government development in terms of technology, organization, and a more secure and trusted environment, optimally supporting the digital transformation of the public sector. This research will encourage broader and more sustainable e-government adoption, especially in developing countries. This paper is structured as follows: Section 2 reviews relevant literature. Section 3 outlines the research method used. Section 4 presents the results of the research analysis and discussion. Finally, Section 5 provides conclusions and implications of this research and suggestions for future research.

Adoption of e-Government in Developing Countries

E-government, or electronic government, is a system that utilizes ICT to improve the quality of government services and encourage broader participation in the democratic process through innovative technologies so that services can be delivered more optimally [10], [15]. The recipients of e-government services can be individuals or organizations, both from within and outside the government [15]. The primary e-government services include Government to Government (G2G), which enables data exchange between government departments to improve efficiency, reduce costs, and avoid duplication through integrated systems; Government to Employees (G2E), which supports government employees in

optimizing internal services; Government to Business (G2B), which facilitates transactions between the public and private sectors and makes it easier to establish new businesses through online services; and Government to Citizens (G2C), which provides citizens with electronic access to government services.

Governments in many countries have utilized e-government to improve transparency, efficiency, and accessibility of government services [10]. For citizens, e-government provides faster, cheaper access, enables active participation, reduces corruption, and improves collaboration between ministries [5], [10]. However, its success largely depends on citizen adoption, including the intention and willingness to use electronic services [2], [5]. Although e-government implementation is growing rapidly in various parts of the world, e-government adoption in developing countries is still inadequate [16]. This low adoption rate has been widely recognized in the literature. One study in Pakistan revealed that citizens of the country were reluctant to use e-government due to security concerns [17]. In addition, another study revealed that fear and perceived risk of data privacy are factors inhibiting the adoption and reuse of e-government services in Kuwait [18].

The low adoption of e-government in developing countries requires government efforts to improve services so that people feel satisfied and trust using them. The main factors that affect user trust and participation are service quality, security, and system privacy; if these aspects are problematic, public trust may decrease, which results in low e-government adoption [5], [10], [19]. Over the years, many studies have discussed the key factors influencing the acceptance or rejection of e-government services, as seen in Table 1. Although many studies have addressed these factors, the focus has been more on developed countries, while studies in developing countries have received less attention [2]. Social, cultural, political, economic, and e-government readiness variations in different countries emphasize the need for solutions that fit local conditions [20].

Table 1. Recapitulation of literature review research on factors influencing e-government adoption

Research	Scope of Country	Scope Of Factors	Recommen-dation	Model	Research Focus
Mustafa et al. [2]	Developing	General	No	Not Specific	Reviewing adoption factors of e-government in developing countries.
Tremblay-Cantin et al. [4]	Developed/ Not Specific	General	No	Not Specific	Developing a conceptual framework of critical factors influencing e-government services.
Aleisa [10]	Developed/ Not Specific	General	No	TOE	Analyzing key adoption factors of e-government and their implications for stakeholders.
Sihotang et al. [11]	Developing	General	No	TOE	Identifying barriers and drivers of e-government implementation in

Research	Scope of Country	Scope Of Factors	Recommen-dation	Model	Research Focus
					developing countries.
Mushtaq [14]	Developed/ Not Specific	Information Security	Yes	Theory, Context and Method (TCM)	Reviewing the literature on administrative interventions in mitigating cybercrimes in e-government.
Gupta and Chauhan [12]	Developed/ Not Specific	General	Yes	Technology Acceptance Model (TAM),	
Alfiani et al. [13]	Developing	General	Yes	Theory of Planned Behavior (TPB), dan DeLone and McLean's Model	Exploring the relationship between trust in e-government, its factors, and the role of cultural moderation.
This Study	Developing	Information Security	Yes	TOE dan UTAUT	Identifying and analyzing implementation issues of e-government in developing countries

In Table 1, we can see the similarities and differences between several previous studies with this research. The research that has the most in common with this research is Mushtaq's research [14], which both focuses on information security in e-government implementation and provides solutions for the government in managing public service security. The difference is that Mushtaq uses the TCM method, which focuses on administrative interventions without considering the context of developed or developing countries. In contrast, this study uses a more comprehensive TOE model by analyzing technological, organizational, and environmental factors. This research also highlights explicitly developing countries with different limitations and challenges than developed countries.

Information Security Factors in E-government

Information security in e-government refers to the system's ability to protect public data from unauthorized access and cyber-attacks, as well as prevention and mitigation efforts to reduce the risk of breaches. This data protection is crucial for services involving personal data and financial transactions, as data leakage and information misuse can reduce public trust and satisfaction with e-government [5], [21]. Concerns over information security, including potential data misuse, are often the main reason citizens hesitate to adopt e-government services [1].

Public trust in e-government can be enhanced through strong security and privacy guarantees, transparent policies, and the government's ability to protect data. Privacy has become increasingly important with the proliferation of ICTs and

the internet expanding the dissemination of personal information. However, third parties can often quickly access and utilize this data, which is a severe problem. In e-government, privacy includes protecting users' personal data when accessing online services, which is the primary basis of administrative services [5], [22]. Information security factors, including technological, organizational, and external aspects, are critical in building trust and increasing e-government adoption. This research provides a comprehensive understanding of these factors and offers solutions to increase public trust and adoption of e-government in developing countries through strengthening information security.

Technology, Organization, and Environment (TOE) Model

The TOE model includes three main dimensions influencing the acceptance and integration of innovations in organizations, including e-government, namely technology, organization, and environment, as shown in Figure 2. The technology dimension includes the characteristics of the innovation itself. The organization focuses on the entity implementing the innovation, while the environment dimension consists of the external conditions in which adoption occurs [23]. The TOE framework is more suitable for examining factors influencing technology adoption, including in the government sector, as it allows flexibility in customizing factors from all three dimensions. The flexibility of the TOE framework enables researchers to apply it across various academic fields and situations, adapting it to the organization's specific needs and the technology being adopted [11], [13].

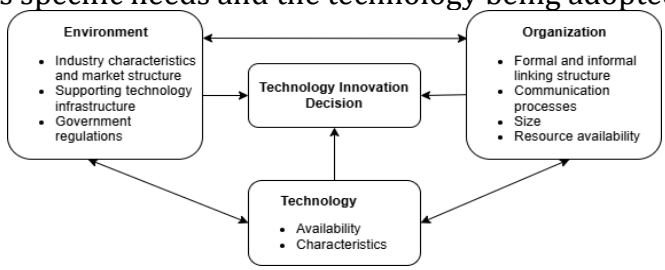

Figure 1. TOE Model by Tornatzky and Fleischer (1990) [23]

B. Research Method

This study used a systematic literature review (SLR) to collect and synthesize study findings accurately and reliably [24]. The article screening process followed the PICO (Population, Intervention, Comparison, Outcome) model to identify SLR needs, methods with specific criteria to generate quality literature and snowballing techniques. The focus of the SLR process included three main phases: Identification, Screening, and Inclusion, with the research methodology shown in Figure 3. The article screening process followed the PICO (Population, Intervention, Comparison, Outcome) model to identify SLR needs, methods with specific criteria to generate quality literature and snowballing techniques. The PICO framework is a frequently used tool for formulating research questions in SLR. The application of SLR includes three main phases: Identification, Screening, and Inclusion. Figure 3 depicts how we conducted the methodology for this literature review research.

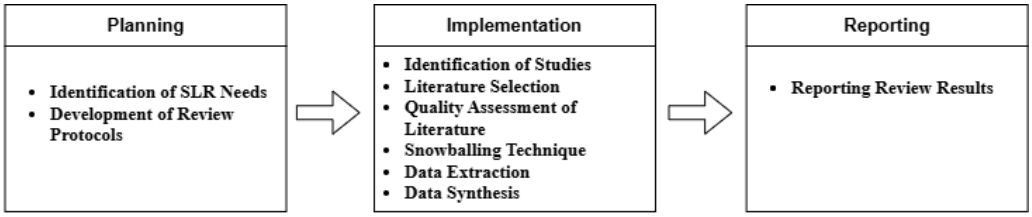

Figure 2. Research Methodology (Source: Proposed by the author)

Planning Stage

The planning stage included the process of identifying the needs of the SLR and drafting the review protocol. The criteria for formulating the research question used the PICO model with four core components: the ’population' studied, the 'intervention' applied, the 'comparison' with the control, and the 'outcome' measured [25]. Table 2 presents the results of this stage.

Table 2. Structure of Research Questions

PICO Component	*Description*
Population	Information Security, Factors, Strategies, E-government, Developing Countries
Intervention	Information security factors affecting the implementation of e-government in developing countries and strategies to apply those factors.
Control/Comparison	N/A
Results	1. Factors 2. Strategies for implementing information security factors

We used the criteria listed in Table 2 as the basis for formulating the research questions. This systematic review aimed to answer the following questions: (1) What information security factors influence e-government adoption in developing countries? (2) How to implement these factors in government agencies to increase e-government adoption in developing countries. Based on these research questions, the authors searched for relevant articles in the source database using the following search keywords: ("information security" OR "security") AND ("e-government" OR "electronic government" OR "e-gov") AND ("factor" OR "strategy" OR "challenge" OR "issue" OR "success" OR "barrier" OR "enabler") AND ("developing country" OR "developing nation" OR "emerging country").

Implementation Stage

During the implementation stage, we conducted research by accessing trusted databases, including Scopus, Science Direct, ACM Digital Library, IEEE Xplore, and Emerald Insight, to cover articles published between January 2019 and October 2024. We imported articles selected from various databases into Mendeley® and applied inclusion criteria, exclusion criteria, and quality control through in-depth reading, analysis, and comparison to ensure each article was appropriate, relevant, and feasible. This stage resulted in a proportionate number of articles for further analysis.

The inclusion criteria for selecting articles were as follows: (1) a case study, (2) written in English, (3) discussing information security factors and e-government in developing countries. The exclusion criteria to ensure the focus and

relevance of the research include: (1) unscientific books and magazine articles, (2) SLRs, conference notes, and speaker notes, (3) duplicate articles, (4) articles without full text, and (5) articles that are not relevant to discussing information security factors in e-government in developing countries.

Then a quality test was conducted with several key questions including: (1) Does the article clearly describe the purpose of the research?, (2) Does the article present the literature review, background, and context of the research?, and (3) Does the literature discuss an actual case study?. In addition, it includes: (4) Does the article present related previous research?, (5) Does the article have a clear research methodology, and (6) Does the article have research results?. After the selection process based on the inclusion, exclusion, and quality test criteria was completed, the author applied the snowballing technique to complete and expand the coverage of the literature not covered in the SLR results to obtain articles eligible for further analysis. These steps ensured the quality of the selected articles to maintain the integrity and validity of the review. With the articles screened, the next step was data extraction and synthesis. Figure 3 shows the flow of the article selection process using the SLR method and the snowballing technique to obtain the final 30 articles.

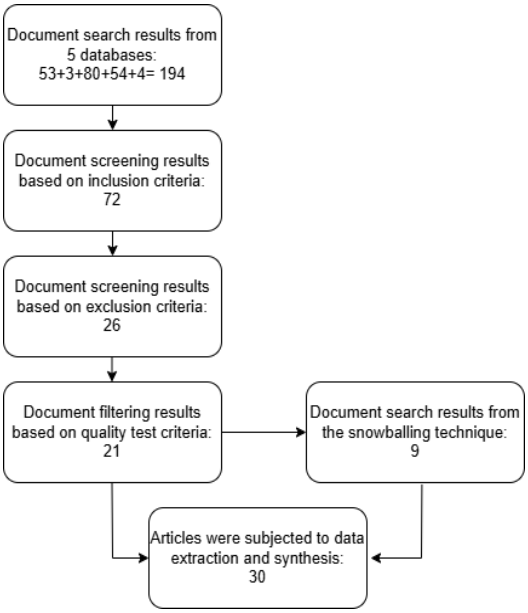

Figure 3. Article Selection Process (Source: Proposed by the authors)

Reporting Stage

In the reporting stage, the main focus was extracting and organizing information from the rigorously selected articles using a Microsoft Excel template. This template contains essential information from each study, including the author's name, year of publication, article type, place of publication, topic, title, keywords, country, institution, and research method, as well as the area of focus, namely Information Security Factors and Implementation Strategies in e-government implementation in developing countries. Data synthesis was conducted through a data-driven approach to combine empirical findings from various studies to produce an in-depth analysis. The data synthesis process also involves classifying factors into the TOE method. After the data extraction and

synthesis stages from the selected literature were completed, the author compiled a report as the final output of the SLR process.

C. Result and Discussion

In this section, the author elaborates and analyzes the results of the literature review search by the stages described in the previous section.

Data Extraction

After the article selection stage, this study extracted data from the selected articles. In this context, Table 3 presents information on the 14 developing countries that were the research locations in the extracted literature, along with the references of each country. This data provides a comprehensive overview of the geographical context of research that addresses information security factors in e-government adoption.

Table 3. Results of Country Data Extraction Literature

Number	Country	*Literature References*	*Amount of Literature*
1	Afganistan	[24], [25]	2
2	Afrika Selatan	[26]	1
3	Arab Saudi	[15], [27], [28]	3
4	China	[17], [21], [29], [30]	4
5	Indonesia	[1], [31], [32], [33], [34], [35]	6
6	Irak	[36], [37]	2
7	Kuwait	[18]	1
8	Nigeria	[38]	1
9	Pakistan	[17], [39]	2
10	Rwanda	[40], [41]	2
11	Thailand	[42]	1
12	United Arab Emirates (UAE)	[43]	1
13	Yordania	[5], [44], [45], [46]	4
14	Zambia dan Zimbabwe	[47]	1

Based on data extraction from the literature review shown in Table 3, most of the research on information security factors affecting e-government adoption in developing countries comes from Indonesia. As one of the largest developing countries in Southeast Asia with a population of more than 270 million and internet penetration reaching 73.3%, Indonesia is developing e-government significantly to optimize public services that are faster, more efficient, and can reach all corners of the region [1]. However, the rapid development of e-government in Indonesia presents complex challenges, such as maintaining information security in the face of data leaks, cyber-attacks, and digital transformation challenges involving diverse and complex infrastructure [31]. Therefore, many studies have focused on Indonesia to identify information security factors as strategic inputs for the government in improving e-government adoption safely and effectively.

Literature Synthesis

The authors compiled a literature synthesis to answer the first research question (RQ1) about the information security factors that influence public trust and e-government adoption in developing countries. This synthesis process

systematically identifies relevant information security factors and organizes them into a structure that allows for analysis and comparison. The synthesis results are summarized in Table 4, which serves as the primary tool of this research, providing a thorough understanding of the information security factors and supporting literature sources.

Table 4. Information Security Factor Synthesis Results

Number	Factors	*Literature References*	*Amount of Literature*
1	Perceived Security	[1], [5], [26], [27], [28], [32], [38], [39], [41], [43], [44], [47]	12
2	Perceived Privacy	[5], [18], [28], [32], [39], [41], [47]	7
3	Information Security Awareness	[34], [37], [40], [46], [48]	5
4	Privacy Law and Regulation	[24], [25], [31], [36], [37], [46]	6
5	Cybersecurity Law and Regulation	[25], [30], [40], [42], [46]	5
6	Privacy Policy	[15], [34], [40], [41], [42], [46]	6
7	Cybersecurity Policy	[15], [25], [34], [37], [40], [46]	6
8	Security Culture	[34], [40], [46]	3
9	Data Security and Privacy	[15], [29], [31], [36], [45]	5
10	Security Mechanism	[26], [37], [42]	3
11	Security Audit	[15], [31], [42]	3
12	Information, Communication, and Technology (ICT) Security	[24], [29], [30], [33], [36], [40]	6
13	Experienced privacy protection personnel	[29], [31], [37]	3
14	Security certificate	[42], [46]	2
15	Security Risk Management	[29], [30], [37], [41], [42], [43]	6

Table 4 summarizes this study's relevant information security factors, including the number of literature that discusses them and their references. The perceived security factor is the most frequently raised and discussed in 12 pieces of literature, confirming the importance of users' security perceptions in supporting the successful adoption of e-government. The findings from RQ1 are used as the basis for answering the second research question (RQ2), namely, how to implement these factors in government agencies to increase public trust and e-government adoption in developing countries. To answer RQ2, before further analysis, the factors were first classified into three main areas: technology, organization, and environment.

Classification of Factors

In an effort to facilitate the implementation of strategies for applying information security factors in e-government, the synthesis results are classified into three main domains, namely technology, organization, and environment. Table 5 presents the results of this classification.

Table 5. Classification of Factors to TOE Model

Number	Factors	Literature References	Amount of Literature
Technology (n=14)			
1	ICT Security	[24], [29], [30], [33], [36], [40]	6
2	Data Security and Privacy	[15], [29], [31], [36], [45]	5
3	Security Mechanism	[26], [37], [42]	3

Number	Factors	Literature References	Amount of Literature
Organization (n=32)			
1	Cybersecurity Policy	[15], [25], [34], [37], [40], [46]	6
2	Privacy Policy	[15], [34], [40], [41], [42], [46]	6
3	Information Security Awareness	[34], [37], [40], [46], [48]	5
4	Experienced privacy protection personnel	[29], [31], [37]	3
5	Security Culture	[34], [40], [46]	3
6	Security Audit	[15], [31], [42]	3
7	Security Risk Management	[29], [30], [37], [41], [42], [43]	6
Environment (n=32)			
1	Cybersecurity Law and Regulation	[25], [30], [40], [42], [46]	5
2	Privacy Law and Regulation	[24], [25], [31], [36], [37], [46]	6
3	Perceived Security	[1], [5], [26], [27], [28], [32], [38], [39], [41], [43], [44], [47]	12
4	Perceived Privacy	[5], [18], [28], [32], [39], [41], [47]	7
5	Security certificate	[42], [46]	2

Table 5 shows that most of the articles from the literature review that discuss information security factors in e-government adoption in developing countries fall under the categories of Organization (32 mentions out of 13 articles), Environment (32 mentions out of 22 articles), and Technology (14 mentions out of 12 articles). These results indicate that the main challenges related to information security are more dominant in non-technological aspects than technology. These non-technological factors include weaknesses in policy and legal frameworks that have not optimally supported the implementation of information security [25], low levels of public awareness and trust in data security in e-government services [36], and lack of policy consistency and coordination between government agencies [22], [25]. As a result, developing more advanced technologies is often delayed until these challenges can be overcome.

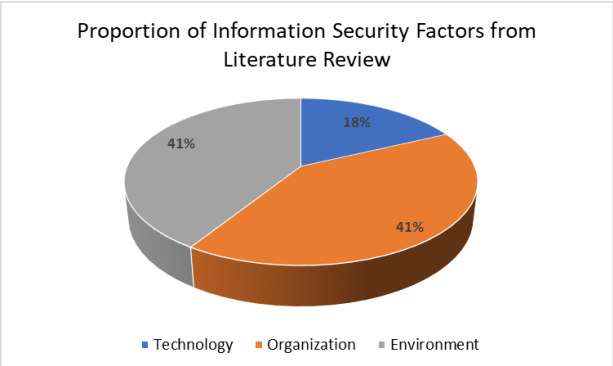

Figure 4. Proportion of Information Security Factors from the Literature Review

Figure 4 is a visual representation of the data presented in Table 5, which shows the distribution of information security factors based on the TOE classification. The Organization and Environment category has the most significant proportion (41%), followed by Technology (19%). This representation provides a more precise illustration of the dominance of non-technological factors in supporting the adoption of e-government in developing countries, especially in the

Organization and Environment category, which includes aspects of laws (UU), regulations, citizen perceptions, policies, public awareness, culture, and management of government agencies Thus, Figure 5 confirms the need to prioritize the strengthening of non-technological factors. However, the development of technological aspects remains necessary for the successful implementation of e-government.

Strategy Analysis

In this section, the authors analyze the findings from the classification of factors based on the TOE framework and provide recommendations to government agencies in developing countries regarding strategies for implementing information security factors to increase e-government adoption.

a. Technology

Technology is the least discussed category in the previous literature, indicating that in developing countries, this category is still in development and has not become a significant obstacle to e-government adoption. In this category, the most mentioned factor is ICT Security (6 articles), which includes the development of ICT security infrastructure, including network security, securing e-government applications at various layers, secure communication between government agencies and stakeholders, and investment in modern technologies such as intrusion detection systems and secure cloud technology [15], [24], [29], [36]. The next factor is Data Security and Privacy (5 articles), which includes technical measures to protect the confidentiality, integrity, and availability of data, such as encryption of sensitive data, backup with reliable systems, and data desensitization to prevent leakage of personal information [29], [36], [37], [45]. Finally, the Security Mechanism (3 articles) consists of technical tools and methods to protect e-government from threats, such as implementing data encryption, user authentication, data validation, strong password policies, threat detection, security adaptation of trusted applications, and activity tracking such as login history [28], [36], [37], [45].

To overcome the barriers to e-government adoption in this category, government agencies that develop e-government need to implement the following strategies:

1. Strengthen ICT Security by developing ICT infrastructure that includes network security, advanced security systems, and secure communication channels to support e-government operations [36], [37]. Investments in modern technologies such as intrusion detection systems, fiber optic internet, and securing e-government applications at various layers must also be prioritized to protect data from unauthorized access [15], [24], [29]. In addition, inter-agency secure communications and collaboration through threat monitoring centers should be implemented to improve responses to security risks [30]. Cooperation with the private sector is also essential to develop innovative ICT solutions and strengthen security [29].
2. Strengthen Data Security by applying encryption to sensitive data, such as usernames and passwords in databases, and using strong algorithms such as Data Encryption Standard (DES) to prevent unauthorized access [45]. In addition, users' personal data should be backed up regularly using a reliable

storage system to protect the information from loss or damage [36]. A data desensitization process must also be implemented to ensure published data does not reveal sensitive personal information [29].

3. Strengthen the Security Mechanism by designing e-government privacy models and implementing security techniques, including five main methods: data encryption, authentication with strong passwords (a combination of at least eight characters, including uppercase letters, lowercase letters, numbers, and symbols) and Multi-Factor Authentication, login confirmation, registration confirmation, and login history tracking [36], [45]. In addition, implementing granular access control and threat detection mechanisms to protect the e-government perimeter from cyber-attacks is also essential. This step can be strengthened by adapting security mechanisms from trusted applications to increase the effectiveness of system protection [28], [31], [37].

b. Organization

Organization is one of the most discussed categories in the previous literature, showing that this category is a major barrier to e-government adoption in developing countries. The most mentioned factor is the Cybersecurity Policy (6 articles), which includes developing and implementing a systematic cybersecurity policy framework across all levels of the organization [25]. Furthermore, a Privacy Policy (6 articles) is an organizational policy that aims to protect users' rights by ensuring confidentiality, integrity, and transparency in data management, including compliance with privacy policy regulations and standards [42]. Security Risk Management (6 articles) is the process of identifying, analyzing, and managing risks, including periodic risk assessments to ensure the security of e-government information and services [29], [30].

Another factor is Information Security Awareness (5 articles), which includes efforts to create a strong awareness and understanding of the importance of information security at all levels of the organization [31], [34]. Experienced Privacy Protection Personnel (5 articles) refers to individuals with specialized data protection and privacy expertise, which is necessary to ensure information security in e-government services [29]. Security Culture (5 articles) is a set of shared norms, values, and beliefs that shape the mindset and behavior of the organization in supporting sustainable information security practices to increase the awareness and involvement of all organization members on security issues [34], [46]. Finally, Security Audit (5 articles) systematically evaluates system security to identify weaknesses and determine the necessary mitigation steps, thus ensuring data protection remains optimal [31], [42].

To overcome the challenges of e-government adoption in the organizational category, government agencies are advised to implement the following strategies:

1. Strengthen the Cybersecurity Policy by developing a cybersecurity framework that includes legal dimensions, policies, software and hardware infrastructure, and procedures to deal with security incidents effectively. This policy should be clearly designed, documented, and consistently applied across all levels of the organization to ensure good coordination when handling security incidents [25], [29], [30].
2. Strengthen Privacy Policy by ensuring all e-government websites include privacy policies in accordance with regulations, such as the Privacy Act of 1988,

implement HTTPS encryption to protect user data, and use website design templates to ensure consistency and transparency [42]. In addition, privacy policies should be aligned with IT risk and privacy, adopting international standards such as General Data Protection Regulation (GDPR) [34]. The implementation of privacy self-regulation is also necessary for government agencies to address gaps in regulation and provide more comprehensive protection [40].

3. Strengthen Security Risk Management by developing and implementing a comprehensive risk management framework to identify, analyze, and manage security risks associated with open data and e-government services [29]. In addition, periodic risk assessments need to be conducted to evaluate potential threats to government information systems. These assessments should include penetration testing and attack simulations to ensure the system's resilience to security threats [30].
4. Increase Information Security Awareness by providing regular cybersecurity training to employees to understand best practices in protecting data, complying with privacy policies, and identifying and mitigating security risks before they become serious threats [30], [31], [37]. Government agencies should adopt the Skills Framework for the Information Age to upskill employees in information security and ensure they understand best practices. [36].
5. Strengthen Experienced Privacy Protection Personnel by training employees on the latest risk management and data privacy protection techniques to enhance their competencies. Government agencies must also recruit and retain experienced employees to ensure expertise in handling security issues. In addition, it is necessary to establish a privacy response team consisting of legal experts, technicians, and risk managers to effectively handle incidents and provide strategic advice regarding data protection policies [29], [31].
6. Improve Security Culture by building a security culture supported by clear guidelines, proactive communication, and support from key figures such as executives, heads of human resources, and security professionals. This step aims to improve the understanding of the importance of information security at all levels of the organization, thereby creating a work environment that supports security practices on an ongoing basis [34], [42].
7. Conduct regular security audits to assess vulnerabilities, identify weaknesses, and ensure that the necessary mitigation measures are in place to protect data optimally. These audits help prevent the exploitation of vulnerabilities and maintain public confidence in the security of e-government services [31], [42].

c. Environment

The environment category should also be an important focus of governments and organizations in addressing e-government adoption barriers related to information security. The most discussed factor in this category is Perceived Security (12 articles), which is citizens' perception of protection against security threats, including the belief that their personal information is safe from hacking or manipulation, thus increasing their sense of security in using e-government services [1], [39]. The next factor, Perceived Privacy (7 articles), is citizens' perception of their ability to control personal information disclosure, use, and storage, influencing trust and adoption of e-government [39], [40].

Furthermore, Privacy Law and Regulation (6 articles) refers to the legal framework that includes national or international laws and standards to protect personal data and support e-government operations [25], [37]. Cybersecurity Law and Regulation (5 articles) covers laws and regulations for information security through technical, legal, social, and organizational controls to protect systems from cyber threats [37], [42]. Finally, Security certificates (2 articles) are digital certificates that guarantee the security of communication and data from cyber threats in e-government systems [42].

In an effort to increase e-government adoption based on factors in the environmental category, the government needs to implement the following strategies:

1. Improve Perceived Security by strengthening public awareness of e-government security regulations through clear policy statements and providing easily accessible online or telephone support [38]. In addition, reliable security mechanisms, such as two-factor authentication (2FA), should be provided to increase user protection and trust in e-government systems [28]. The implementation of encryption on all data communications is also necessary to protect information from unauthorized access and strengthen public security perceptions [39].
2. Improve Perceived Privacy by protecting users' privacy by giving them full rights to control the collection and use of personal data and ensuring accountable data management. Governments should improve transparency by providing reports that explain in detail how their personal data is managed and used [40]. In addition, e-government services, particularly on social media platforms, should provide privacy features that allow users to independently set and select their privacy preferences [39].
3. Strengthen Privacy Law and Regulation by drafting an e-government law covering electronic transactions, digital signatures, and user data privacy protection. Also, update the policy regularly to keep up with new technologies and threats [24], [25]. Compliance with privacy regulations such as the GDPR needs to be guaranteed through the establishment of an independent supervisory body to oversee its implementation [24], [31]. The government must also socialize the rights of the public regarding data privacy to increase public trust in e-government services [37].
4. Strengthen cybercrime law enforcement by increasing law enforcement agencies' capacity through regular information security training and allocation of adequate resources [25]. In addition, government agencies should align the implementation of laws and regulations with international standards such as ISO/IEC 27002, OWASP, ISO 27001, and NIST 800-53 to ensure e-government security, with the support of independent oversight bodies tasked with ensuring compliance with regulations [24], [31], [42]. Technical mitigation measures, such as cryptographic perimeter security, internal security, and real-time monitoring systems, must be implemented to quickly detect and respond to security threats [37].

Make a rule that all government agencies use security certificates that meet international standards and display certification information on the front page of the e-government website, and ensure that certificate renewals are carried out

regularly to protect communications and data from cyber threats. Automatic certification rules should also be implemented to minimize downtime caused by renewal [42].

Adoption Model Framework

Based on the findings of this study regarding information security factors that influence e-government adoption by citizens, the authors propose an e-government adoption model framework that includes these factors as a guide to increase user participation in e-government services. This model framework is developed by adapting the TOE model, highlighting technological, organizational, and environmental dimensions. Figure 5 presents the proposed model.

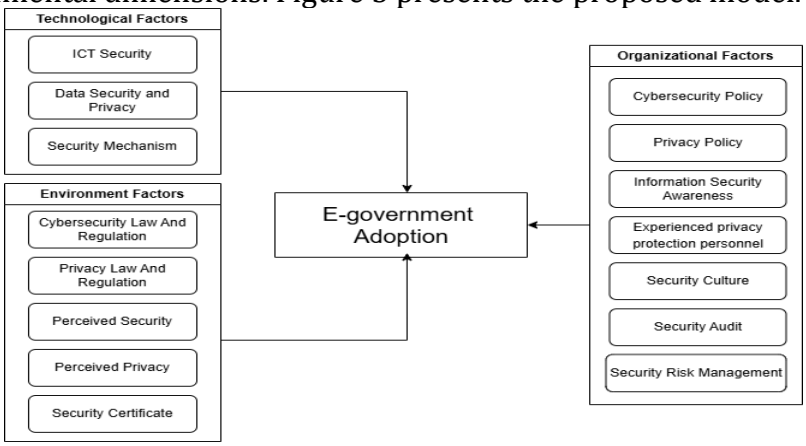

Figure 5. Proposed Adoption Model Framework (Source: Proposed by author)

D. Conclusion and Future Work

This research comprehensively analyzes information security factors that influence e-government adoption in developing countries. Through literature study, snowballing technique, and application of the Technology, Organization, and Environment (TOE) framework, we found 15 information security factors from 30 kinds of literature, consisting of 3 factors in the technology dimension, seven factors in the organization dimension, and five factors in the environment dimension. The results show that factors from the organizational and environmental dimensions are the most crucial factors (41% of mentions in the literature each), followed by technological factors (18%). This finding confirms the dominance of the discussion of non-technical information security factors over technical factors in e-government adoption.

Public perception of security and privacy, which is part of the environmental aspect, must be a major concern. The government must strengthen public awareness and trust through clear security policies and strong technological support, giving people full control over their personal data and increasing transparency in data management. The government must also strengthen policy implementation with data protection laws and regulations overseen by independent bodies. In addition, from an organizational aspect, government agencies must strengthen information security policies by developing an international standard cybersecurity framework that is documented and consistently applied at all levels of the organization. Implementing a comprehensive risk management framework to manage the security risks of open data and e-government services is also very important.

This research provides important implications, both in the academic and practical realms. Academically, this research adds to the literature on information security factors and strategies in e-government adoption, especially in developing countries where it is still limited. This research also expands the understanding of the role of TOE dimensions in supporting information security in e-government. Practically, these findings can help the government formulate policies and strategies for e-government development in terms of technology, organization, and a more secure and trusted environment, optimally supporting the digital transformation of the public sector. This research will encourage broader and more sustainable e-government adoption, especially in developing countries. Further research can test this research findings model through case studies to evaluate its influence on e-government adoption. Thus, this research provides deep theoretical insights and serves as a foundation for more effective practical implementation in the future.

E. Acknowledgment

The authors would like to thank BMKG for their support in providing scholarships during the study period at the University of Indonesia and all parties who supported this research.

F. References

[1] A. Sabani, V. Thai, and M. A. Hossain, "Factors Affecting Citizen Adoption of E-Government in Developing Countries: An Exploratory Case Study From Indonesia," *J. Glob. Inf. Manag.*, vol. 31, no. 1, pp. 1–23, 2023, doi: 10.4018/JGIM.318131.

[2] A. Mustafa, O. Ibrahim, and F. Mohammed, "E-government adoption: a systematic review in the context of developing nations," *Int. J. Innov.*, vol. 8, no. 1, pp. 59–76, 2020, doi: 10.5585/iji.v8i1.16479.

[3] G. Ilieva *et al.*, "Factors Influencing User Perception and Adoption of E-Government Services," *Adm. Sci.*, vol. 14, no. 3, 2024, doi: 10.3390/admsci14030054.

[4] C. A. Tremblay-Cantin, S. Mellouli, M. Cheikh-Ammar, and H. Khechine, "E-government Service Adoption by Citizens: A Literature Review and a High-level Model of Influential Factors," *Digit. Gov. Res. Pract.*, vol. 4, no. 1, 2023, doi: 10.1145/3580369.

[5] A. Kanaan, A. Al-Hawamleh, A. Abulfaraj, H. M. Al-Kaseasbeh, and A. H. Alorfi, "The effect of quality, security and privacy factors on trust and intention to use e-government services," *Int. J. Data Netw. Sci.*, vol. 7, no. 1, pp. 185–198, 2023, doi: 10.5267/j.ijdns.2022.11.004.

[6] W. Li, "The role of trust and risk in Citizens' E-Government services adoption: A perspective of the extended UTAUT model," *Sustain.*, vol. 13, no. 14, 2021, doi: 10.3390/su13147671.

[7] A. Wibowo, W. Alawiyah, and Azriadi, "The importance of personal data protection in Indonesia's economic development," *Cogent Soc. Sci.*, vol. 10, no. 1, p., 2024, doi: 10.1080/23311886.2024.2306751.

[8] N. Gani, "Legal Politics and Data Protection in Indonesia : A Case Study of the National Data Center Hacking Najamuddin Gani," vol. 30, no. 3, pp. 296–309, 2024.

[9] L. Judijanto, F. M. Kaaffah, H. N. Muthmainah, and A. Y. Vandika, "Literature Review on Computer Network Security in the Financial Sector in Indonesia Challenges and Solutions in Facing Digital Security Threats," *Sci. du Nord Nat. Sci. Technol.*, vol. 1, no. 01, pp. 20–27, 2024, [Online]. Available: https://north-press.com/index.php/snnst/article/view/13%0Ahttps://north-press.com/index.php/snnst/article/download/13/13

[10] N. Aleisa, "Key factors influencing the e-government adoption: a systematic literature review," *J. Innov. Digit. Transform.*, vol. 1, no. 1, pp. 14–31, 2024, doi: 10.1108/jidt-09-2023-0016.

[11] D. M. Sihotang *et al.*, "A Systematic Literature Review of Barriers and Drivers E-Government in Developing Countries: TOE Framework Perspective," *2022 7th Int. Conf. Informatics Comput. ICIC 2022*, pp. 1–6, 2022, doi: 10.1109/ICIC56845.2022.10006942.

[12] P. Gupta and S. Chauhan, "Factors Influencing Trust in E-government Services : A Meta-analytic Review," *2024 Tenth Int. Conf. eDemocracy & eGovernment*, pp. 1–10, 2024, doi: 10.1109/ICEDEG61611.2024.10702083.

[13] H. Alfiani, S. Kurnia Aditya, S. Lusa, D. Indra Sensuse, P. A. Wibowo Putro, and S. Indriasari, "E-Government Issues in Developing Countries Using TOE and UTAUT Frameworks: A Systematic Review," *Policy Gov. Rev.*, vol. 8, no. 2, p. 169, 2024, doi: 10.30589/pgr.v8i2.932.

[14] S. Mushtaq, "Critical Factors and Practices in Mitigating Cybercrimes within E-Government Services : A Rapid Review on Optimising Public Service Management," *Information*, 2024.

[15] A. S. Alharbi, G. Halikias, M. Rajarajan, and M. Yamin, "A review of effectiveness of Saudi E-government data security management," *Int. J. Inf. Technol.*, vol. 13, no. 2, pp. 573–579, 2021, doi: 10.1007/s41870-021-00611-3.

[16] U. Nations, *E-Government Survey 2024*. New York: United Nations, 2024.

[17] F. Shahzad, G. Xiu, I. Khan, and J. Wang, "m-Government Security Response System: Predicting Citizens' Adoption Behavior," *Int. J. Human–Computer Interact.*, vol. 35, no. 10, pp. 899–915, Jun. 2019, doi: 10.1080/10447318.2018.1516844.

[18] K. Rouibah, H. Qurban, and N. Al-Qirim, "Impact of Risk Perceptions and User Trust on Intention to Re-Use E-Government," *J. Glob. Inf. Manag.*, vol. 30, no. 1, pp. 1–29, 2022, doi: 10.4018/jgim.307117.

[19] M. Almufti, R. Sellami, and L. H. Belguith, "Towards A Conceptual Model for Citizen's Adoption of E-Government Services in Developing Countries," *HORA 2023 - 2023 5th Int. Congr. Human-Computer Interact. Optim. Robot. Appl. Proc.*, pp. 1–5, 2023, doi: 10.1109/HORA58378.2023.10156675.

[20] T. Thi Uyen Nguyen, P. Van Nguyen, H. Thi Ngoc Huynh, G. Q. Truong, and L. Do, "Unlocking e-government adoption: Exploring the role of perceived usefulness, ease of use, trust, and social media engagement in Vietnam," *J. Open Innov. Technol. Mark. Complex.*, vol. 10, no. 2, 2024, doi: 10.1016/j.joitmc.2024.100291.

[21] Y. Li and H. Shang, "Service quality, perceived value, and citizens' continuous-use intention regarding e-government: Empirical evidence from China," *Inf. Manag.*, vol. 57, no. 3, p. 103197, 2020, doi: 10.1016/j.im.2019.103197.

[22] A. Bayaga, "Examining the Challenges of Integration and Interoperability of a

Security and Privacy Policy Framework for e-Government Services: The Case of South Africa," *2020 Conf. Inf. Commun. Technol. Soc. ICTAS 2020 - Proc.*, 2020, doi: 10.1109/ICTAS47918.2020.233974.
[23] L. G. Tornatzky, "The processes of technological innovation," *Lexington/DC Heath Co.*, 1990.
[24] A. M. Samsor, "Challenges and Prospects of e-Government implementation in Afghanistan," vol. 5, no. 1, pp. 51–70, 2021, doi: 10.1108/ITPD-01-2020-0001.
[25] E. Ismail, A. A. Alariqi, A. Jawid, J. Wall, and M. Abdulrab, "Strategy, Policy, and Legal Barriers to E-Gov Implementation in Afghanistan," *IEEE Access*, vol. 10, pp. 13800–13812, 2022, doi: 10.1109/ACCESS.2022.3144198.
[26] F. Maphumula and K. Njenga, "Innovation in Tax Administration: Digitizing Tax Payments, Trust And Information Security Risk," in *2019 Open Innovations (OI)*, 2019, pp. 304–311. doi: 10.1109/OI.2019.8908232.
[27] M. Alajmi, M. Mohammadian, and M. Talukder, "The determinants of smart government systems adoption by public sector organizations in Saudi Arabia," *Heliyon*, vol. 9, no. 10, p. e20394, 2023, doi: https://doi.org/10.1016/j.heliyon.2023.e20394.
[28] M. S. Al-Zahrani, "Integrating IS success model with cybersecurity factors for e-government implementation in the Kingdom of Saudi Arabia," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 5, pp. 4937–4955, 2020, doi: 10.11591/ijece.v10i5.pp4937-4955.
[29] Y. Li, R. Yang, and Y. Lu, "A privacy risk identification framework of open government data: A mixed-method study in China," *Gov. Inf. Q.*, vol. 41, no. 1, p. 101916, 2024, doi: https://doi.org/10.1016/j.giq.2024.101916.
[30] Z. Mao and Y. Zhu, "Tension between the safe flow of government data across organizational boundaries and fragmentations in secure collaboration: the Chinese e-government," *Aslib J. Inf. Manag.*, vol. 76, no. 4, pp. 629–652, Jan. 2024, doi: 10.1108/AJIM-10-2022-0461.
[31] M. Yusuf, M. K. Sophan, A. K. Darmawan, B. D. Satoto, A. Muntasa, and R. A. Nugroho, "E-Government Service Management System (E-GovService) to Improve Local e-Government Using DevOps Approach," in *2023 6th International Conference on Information and Communications Technology (ICOIACT)*, 2023, pp. 309–314. doi: 10.1109/ICOIACT59844.2023.10455931.
[32] G. K. Avianto, F. Elliyana, and D. I. Sensuse, "Satisfaction Factors of Indonesian National Civil Servant Recruitment System," in *2021 9th International Conference on Information and Communication Technology (ICoICT)*, 2021, pp. 371–376. doi: 10.1109/ICoICT52021.2021.9527470.
[33] D. I. Sensuse and A. Syahrizal, "Upsurging of Quality: Antencendent Framework for EServices Quality Measurement," in *2020 3rd International Conference on Computer and Informatics Engineering (IC2IE)*, 2020, pp. 311–316. doi: 10.1109/IC2IE50715.2020.9274680.
[34] V. S. Kasma, S. Sutikno, and K. Surendro, "Design of e-Government Security Governance System Using COBIT 2019: (Trial Implementation in Badan XYZ)," *Proceeding - 2019 Int. Conf. ICT Smart Soc. Innov. Transform. Towar. Smart Reg. ICISS 2019*, vol. 2019, pp. 5–10, 2019, doi: 10.1109/ICISS48059.2019.8969808.
[35] D. Madyatmadja, "Citizen Attitude : Potential Impact of Social Media Based

Government," pp. 128–134, 2019, doi: 10.1145/3371647.3371653.
[36] H. Muhammad and M. Hromada, "Evaluating a Proposed E-Government Stage Model in Terms of Personal Data Protection," *Appl. Sci.*, vol. 13, no. 6, 2023, doi: 10.3390/app13063913.
[37] H. Muhammad and M. Hromada, "Proposing an E-Government Stage Model in Terms of Personal Information Security in Developing Countries," *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2022-Septe, pp. 1–5, 2022, doi: 10.1109/ICCST52959.2022.9896521.
[38] O. M. Okunola and J. Rowley, "User experience of e-government: the Nigeria Immigration Service," *Libr. Hi Tech*, vol. 37, no. 3, pp. 355–373, Jan. 2019, doi: 10.1108/LHT-09-2018-0138.
[39] S. Khan, R. Umer, S. Umer, and S. Naqvi, "Antecedents of trust in using social media for E-government services: An empirical study in Pakistan," *Technol. Soc.*, vol. 64, 2021, doi: 10.1016/j.techsoc.2020.101400.
[40] C. Mutimukwe, E. Kolkowska, and Å. Grönlund, "Information privacy practices in e-government in an African least developing country, Rwanda." Wiley, Rwanda, 2019.
[41] C. Mutimukwe, E. Kolkowska, and Å. Grönlund, "Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior," *Gov. Inf. Q.*, vol. 37, no. 1, p. 101413, 2020, doi: https://doi.org/10.1016/j.giq.2019.101413.
[42] N. Thompson, A. Mullins, and T. Chongsutakawewong, "Does high e-government adoption assure stronger security? Results from a cross-country analysis of Australia and Thailand," *Gov. Inf. Q.*, vol. 37, no. 1, p. 101408, 2020, doi: https://doi.org/10.1016/j.giq.2019.101408.
[43] R. Eid, H. Selim, and Y. El-Kassrawy, "Understanding citizen intention to use m-government services: an empirical study in the UAE," *Transform. Gov. People, Process Policy*, vol. 15, no. 4, pp. 463–482, 2020, doi: 10.1108/TG-10-2019-0100.
[44] A. Althunibat *et al.*, "Sustainable applications of smart-government services: A model to understand smart-government adoption," *Sustain.*, vol. 13, no. 6, pp. 1–28, 2021, doi: 10.3390/su13063028.
[45] A. S. Al-Sherideh *et al.*, "Development of a Secure Model for Mobile Government Applications in Jordan," *J. Stat. Appl. Probab.*, vol. 13, no. 1, pp. 145–155, 2024, doi: 10.18576/jsap/130110.
[46] A. Alkhwaldi, M. Kamala, and R. Qahwaji, "Security Perceptions in Cloud-based e-Government Services: Integration between Citizens' and IT-staff Perspectives," *Proc. 2019 Ieee 12th Int. Conf. Glob. Secur. Saf. Sustain.*, pp. 158-+, 2019.
[47] W. Munyoka and M. S. Maharaj, "Privacy, security, trust, risk and optimism bias in e-government use: The case of two Southern African Development Community countries," *SA J. Inf. Manag.*, vol. 21, no. 1, pp. 1–9, 2019, doi: 10.4102/sajim.v21i1.983.
[48] H. Muhammad and M. Hromada, "Evaluating an E-Government Stage Model by Using SOAR-AHP Process," *Transp. Res. Procedia*, vol. 74, pp. 1538–1545, 2023, doi: https://doi.org/10.1016/j.trpro.2023.11.131.