digital

MDPI

Review

Mitigating Cybercrimes in E-Government Services: A Systematic Review and Bibliometric Analysis

Shahrukh Mushtaq * and Mahmood Shah

Newcastle Business School, University of Northumbria at Newcastle, Newcastle upon Tyne NE1 8ST, UK; mahmood.shah@northumbria.ac.uk

* Correspondence: shahrukh.mushtaq@northumbria.ac.uk

Abstract: Cybercrime prevention is critical for the effective functioning of e-government services. Despite its importance, internal cybercrime mitigation processes within these services are underrepresented in the existing literature. This study addresses this gap by conducting a systematic review and bibliometric analysis of e-government research from January 2015 to January 2025. Using the Web of Science and Scopus databases, 3790 studies were identified; after removing duplicates, bibliometric analysis was performed using R Studio (Build 467). The analysis revealed that Government Information Quarterly was the leading journal, with China, the USA, and the UK contributing the most publications. Nineteen major themes emerged, with "adoption" identified as the dominant theme, followed by "governance" and "development". Among 88 security-related studies, 19 specifically addressed cybersecurity in e-government services. Findings indicate a predominant focus on user-centric perspectives, such as service adoption and system vulnerabilities, while internal cybersecurity issues, including managerial practices and mitigation strategies, remain largely unexplored. Limited data availability may contribute to this gap. This study highlights the need for future research to adopt an integrated approach, emphasising management-level practices for cybercrime mitigation within e-government institutions from both developing and developed nations.

Keywords: e-government; digital government; cybercrimes; electronic government; cybercriminals; mitigation

Received: 4 November 2024
Revised: 24 January 2025
Accepted: 27 January 2025
Published: 29 January 2025

Citation: Mushtaq, S.; Shah, M. Mitigating Cybercrimes in E-Government Services: A Systematic Review and Bibliometric Analysis. *Digital* **2025**, *5*, 3. https://doi.org/10.3390/digital5010003

1. Introduction

E-government implies the provision of public services through electronic means [1]. Governments across the globe adopt e-government services as part of their broader efforts to digitise operations, foster an information society, and address the digital divide [2]. It progresses through multiple stages of growth, each focusing on ensuring cybersecurity and implementing risk assessments to protect the expanding digital infrastructure [3]. The continued integration of digital services in government functions, while beneficial, also creates vulnerabilities such as cyber threats, intensifying concerns over the protection of personal and sensitive data. These cybersecurity challenges lead directly to an increase in cybercriminal activities, particularly as governments digitise services on a large scale. Despite the increasing prevalence of cybercrimes, the extent to which policies and strategies for cybercrime prevention are effective remains fragmented in the existing literature. Notably, there is a lack of comprehensive reporting on the security dimensions of e-government services, leaving critical aspects of their cybersecurity largely unaddressed.

2. A Literature Review

2.1. Cybercrimes

The act of using a computer or technology to commit a crime is referred to cybercrime [4]. These include phishing emails, viruses, hacking, cyber pornography, cyberbullying, online blackmailing, identity theft, etc. [5]. Mainly categorised as 1. Cyber-enabled crimes (phishing, cyberstalking, identity theft, consumer fraud, online dating fraud, online threats, etc.) and 2. Cyber-dependant crimes (malware, ransomware, hacking, DDoS) [6]. The increase in the use of technology during COVID-19 provided an opportunity for cybercriminals to exploit online users. However, a major focus of existing research is on the cyber victimisation of users [5], while governments and other institutes equally face cybersecurity challenges.

For instance, ref. [7] reports ransomware, hacking, and DDoS attacks in the aviation industry. The aviation industry is part of critical infrastructure and, thus, needs better protection from cybercrimes. Similarly, e-government services are critical, including the healthcare sector, finance, transportation, etc., which require extensive application of digital security technologies. The cybercrime research is addressed towards user victimisation [4], SMEs [5], the aviation sector [6], etc.; this encompasses multiple public and private sectors. However, the state of research that is particularly directed towards cybercrime mitigation within e-government services is underexplored.

2.2. Rise of Cybercrime in E-Government

The adoption of these services, especially in the wake of accelerated digital transformation due to the COVID-19 pandemic, led to an increase in cybercrimes [8]. As government systems and businesses become more digitised, regardless of their infrastructure, they become attractive targets for cybercriminals [9]. In the past, cyberattacks have affected a wide range of sectors, including public services, critical infrastructure, and financial institutions [10], emphasising the inadequacy of traditional information security management practices [11]. Concerns about how these services store, process, and safeguard personal information continue to grow as incidents of large-scale data breaches become more frequent, costing organisations up to GBP 284.44 million annually [12]. Additionally, according to Statista, the estimated cost of cybercrimes will reach GBP 12.792 trillion by 2029 [13].

As per further reports, the industries vulnerable to cyber threats include healthcare, finance, manufacturing, professional services, and education. Globally, the highest concentrations of cybercrimes have been reported in America (43%), Europe (32%), and Asia (14%), with the lowest incidence observed in Australia (1.5%) [14]. In 2023, government agencies across the globe experienced a significant surge in cyber incidents, with reported cases increasing from 40,000 in early 2023 to 100,000 by August 2023 [14,15]. This sharp rise is alarming, highlighting the urgent need for stronger cybercrime mitigation practices in e-government services.

Despite existing cybersecurity frameworks, especially National Institute of Standards and Technology (NIST) guidelines and ISO standards [16–21], institutes remain vulnerable, making e-government cybersecurity a critical area for further exploration. However, addressing cyberthreats requires more than technical solutions; it demands a multidisciplinary approach to fully understand and mitigate cybercrime.

2.3. Cybercrime Mitigation: A Multidisciplinary Approach

E-government, positioned at the intersection of several academic disciplines—including computer science, information systems, public administration, and political science [22]—exhibits considerable diversity in the literature concerning cybercrime mitigation [23]. To develop a comprehensive understanding from a multidisciplinary perspective, it must tran-

scend purely technological solutions. The complexities involved in mitigating cybercrime cannot be addressed by simple technical fixes such as encryption, biometrics, or artificial intelligence. Instead, research must account for factors beyond the purview of computer scientists.

The monodisciplinary approaches have proven insufficient; instead, there is a need for strategies recognising the importance of human elements embedded within technological systems [24,25]. Thus, an integrated approach, considering human, organisational, and technological factors, is necessary. Moreover, the implementation of e-government services in developing countries has encountered numerous challenges, with roughly 80% of programs being classified as failures or only partially successful [26].

Cybercrime mitigation is further complicated by issues such as the "siloisation" of large volumes of public data and the lack of systematic processes for evaluating cybersecurity policies [27]. There is a growing recognition that successful cybercrime mitigation requires collaboration between developed and developing countries to share best practices and knowledge [23].

Preliminary database searches revealed scattered evidence of cybercrime mitigation across the e-government literature; however, a comprehensive and consolidated account remains absent. To address this gap, the present study aims to conduct an in-depth review and bibliometric analysis, identifying key research contributions and outlining future directions for cybercrime mitigation within the context of e-government.

2.4. Purpose and Scope of This Study

This article consolidates research on cybercrime mitigation within the context of e-government services from January 2015 to January 2025. Specifically, it conducts a comprehensive bibliometric analysis using the Web of Science and Scopus database to map the current literature on e-government and cybercrime mitigation. By using the R Studio software (build 467), this study identifies key research trends, prominent authors, and significant affiliations in the domain. Furthermore, this study evaluates the extent to which the existing literature has addressed cybercrime mitigation in e-government services and proposes a future research agenda to advance the field. This article contributes to the body of knowledge by the following:

1. Mapping the existing literature on e-government services;
2. Conducting a bibliometric analysis to identify key research, authors, and affiliations;
3. Assessing the extent to which cybercrime mitigation is addressed in e-government services;
4. Proposing a future research agenda based on this literature review.

3. Materials and Methods

With the primary objective of assembling a diverse array of relevant research, we utilised the search string; "e-government OR egovernment OR digital government AND cybercrime" as the initial query, which enabled us to cover a wide range of the relevant literature. To ensure that our analysis reflected recent research, we focused exclusively on the research articles published from January 2015 to 2025 in Web of Science (WoS) and Scopus databases. The choice of Scopus was made due to its extensive database archive, which encompasses prominent platforms, including Emerald, Elsevier, IEEE Xplore, EBSCO, Springer, etc. Not to miss any relevant studies, the WoS database was also searched. This time, the boundary was established to highlight advancements during the last decade.

Additionally, our search criteria were intentionally broad, incorporating various disciplines, such as management, political science, and security systems, among others. By avoiding restrictions to any single domain, we successfully expanded the breadth of our dataset for bibliometric analysis. Bibliometric analysis is a method used for the analysis and

exploration of a large volume of scientific data [28]. It facilitates a thorough bibliometric examination, allowing for the systematic evaluation and interpretation of findings.

For the bibliometric analysis, a complete record of 3790 research articles was loaded into R Studio (Build 467) to analyse using its Bibliometrix package. While VOSviewer is primarily designed for conducting scientometric or bibliometric analyses, it does not allow for the integration of multiple databases simultaneously. In contrast, R software excels in its ability to merge database files from multiple sources, such as Web of Science (WOS) and Scopus, as demonstrated in our case.

3.1. Publication Selection

The articles were included based on inclusion criteria tailored to address research questions effectively. To identify themes within the existing literature on e-government, the criteria for the first research objective was kept broad to include all relevant database hits. For the subsequent objectives, only articles concerning e-government services in their titles were considered. Studies were excluded if they were duplicates, did not mention e-government services in the title, were not written in English, were book chapters, or were conference papers.

3.2. Data Extraction

In accordance with the established criteria, 3790 research articles were initially identified. The 41 duplicates were automatically removed and reported by the bibliometrix package in R. The dataset, therefore, reconfigured itself by default in the software.

The next phase of the filtration involved an in-depth examination of titles and abstracts to ensure alignment with the research. Given that the first research objective is focused on mapping the existing literature, all articles were considered to provide a comprehensive overview of the e-government research landscape. The findings are presented in themes emerging within e-government research over the timeframe, additionally Table A1 is dedicated to the intersection of cybercrime and the e-government literature.

To discern themes, titles were carefully reviewed and classified. For subsequent objectives, this review concentrated on studies related to cybercrime mitigation, emphasising security aspects in e-government. Notably, no articles directly addressed the concept of cybercrime mitigation in e-government; instead, cybersecurity issues were highlighted to varying degrees. Consequently, research addressing security concerns within e-government services is summarised in Table A1. A visual representation of the systematic review methodology (PRISMA diagram) is provided in Figure 1.

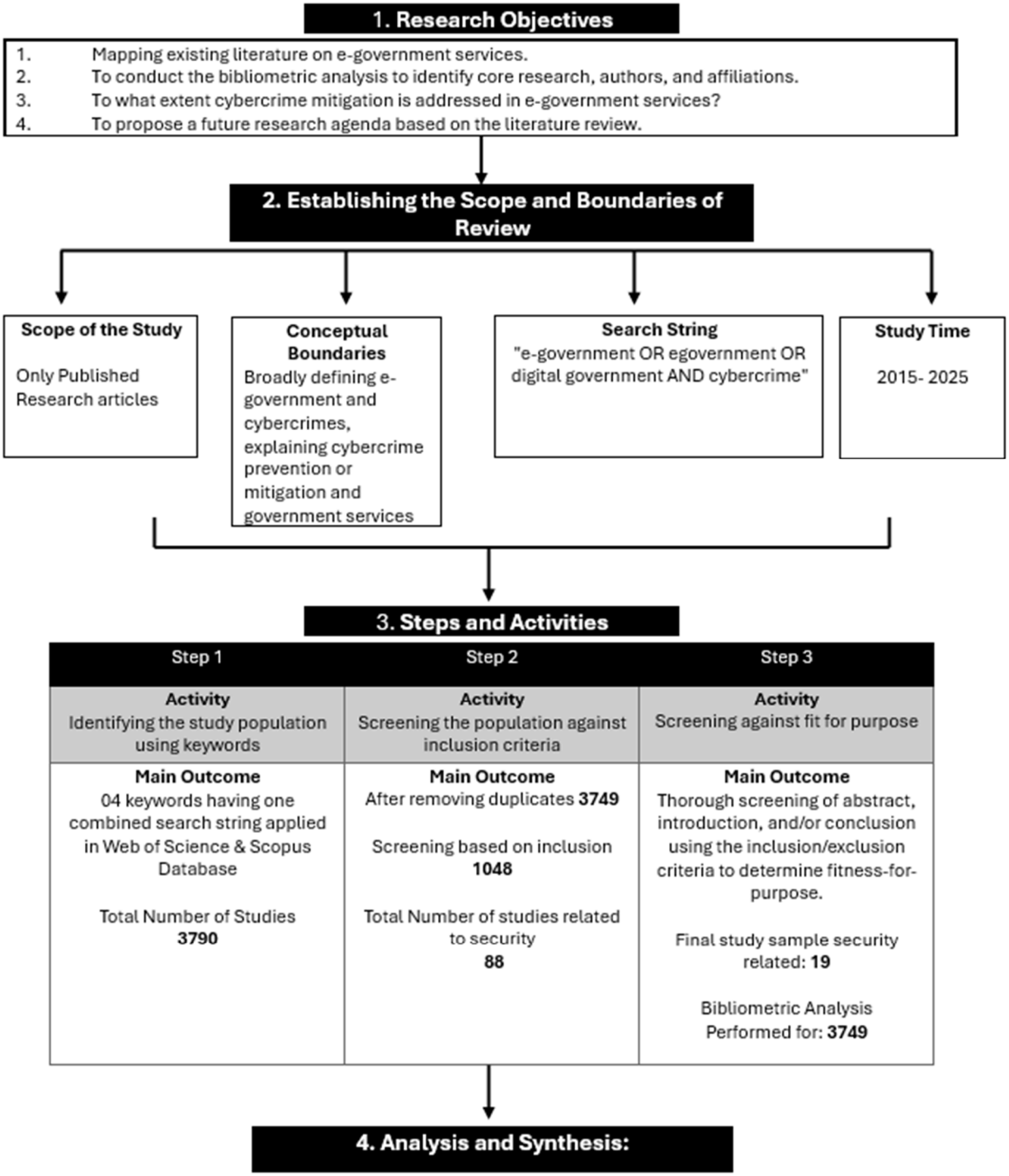

Figure 1. Review Process.

4. Results

As noted by Radanliev [29], Figure 2 is called the "Bill of Materials" for the data (the literature) examined. The analysis encompassed research published between 2015 and 2025, comprising 3790 articles (after removing duplicates, the final count is 3749) sourced from 1247 distinct publications.

The dataset reveals a downward trend in the volume of related research over the past decade. Notably, 26.36% of the articles feature international co-authorship, with contributions from 8030 authors. On average, each document includes 2.97 co-authors, featuring the inherently collaborative nature of research in this domain.

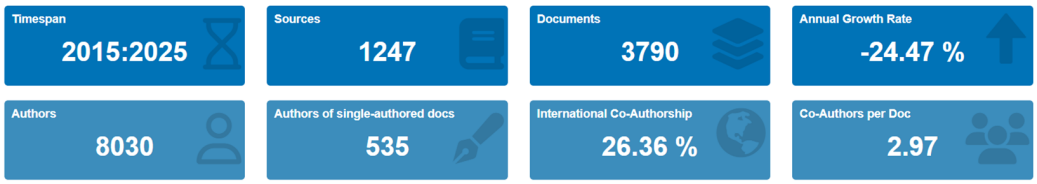

Figure 2. Key information on dataframe from WOS and Scopus combined (authors' own).

4.1. Journals

The body of research concerning e-government services is disseminated across a variety of scholarly journals. Notably, a substantial proportion of the publications identified within the databases are concentrated in *Government Information Quarterly*, as illustrated in Figure 3. The graph reflects the increasing attention and production of research in e-government and related fields. Journals dedicated to electronic government, information systems, and public administration have shown notable growth, particularly in the later years, signifying the growing significance of these areas in academic discourse.

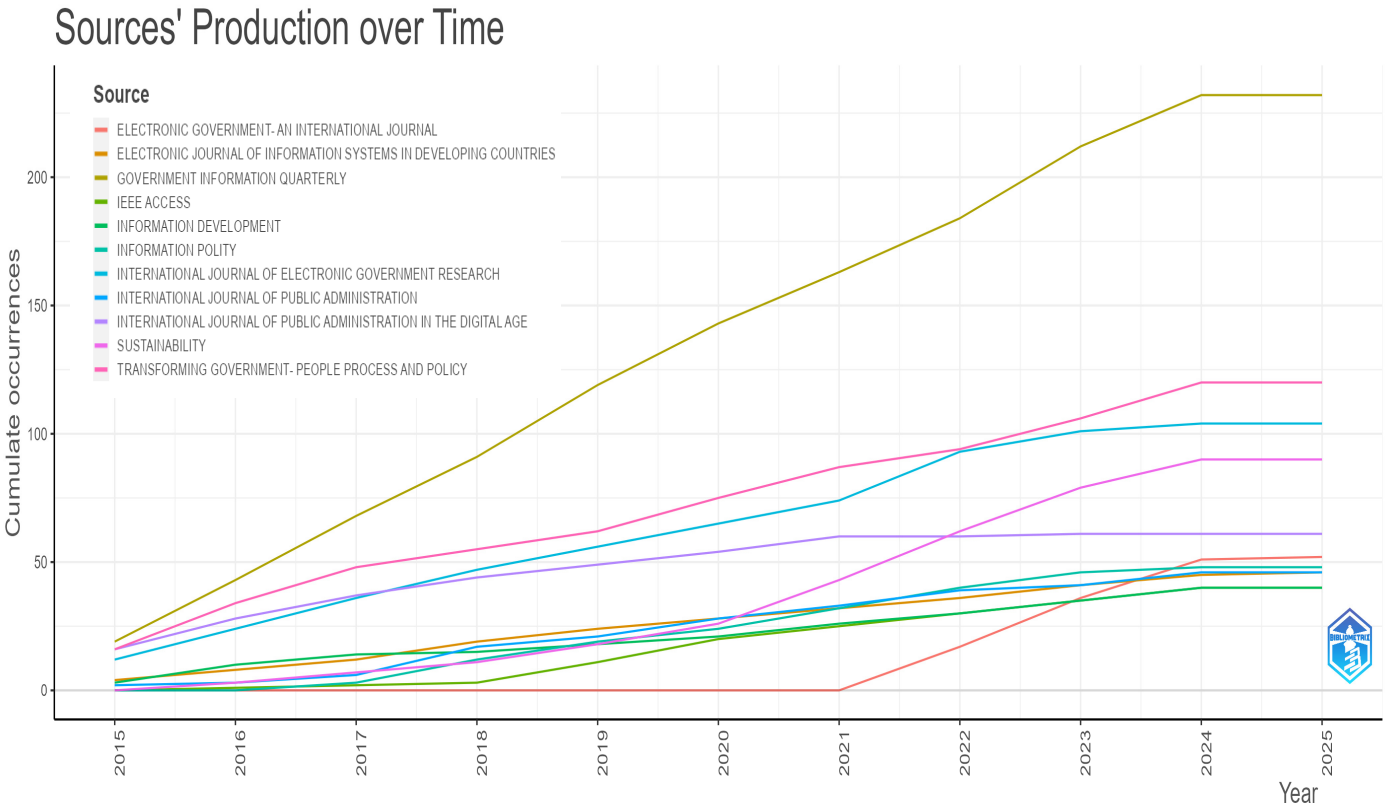

Figure 3. Top ten journals' production (authors' own).

4.2. Author Influence and Affiliation Statistics

The R Studio employs the Biblioshiny function, which facilitates an online interactive simulation for an enhanced user experience. Upon uploading the data file, the software establishes a communication link that seamlessly converts the data into a manageable data frame. In this study, the software projected the following information:

> biblioshiny();
Loading required package: shiny;
Listening on http://127.0.0.1:4129;
Converting your df collection into a bibliographic data frame.

Figure 4 represents the publication trends of the top authors identified in the dataset. It shows the number of articles published by the top ten authors over the years, with the size of each circle corresponding to the number of articles. The chart also includes a colour scale to indicate the total citation count (TC) per year for each author, ranging from low (light blue) to high (dark blue).

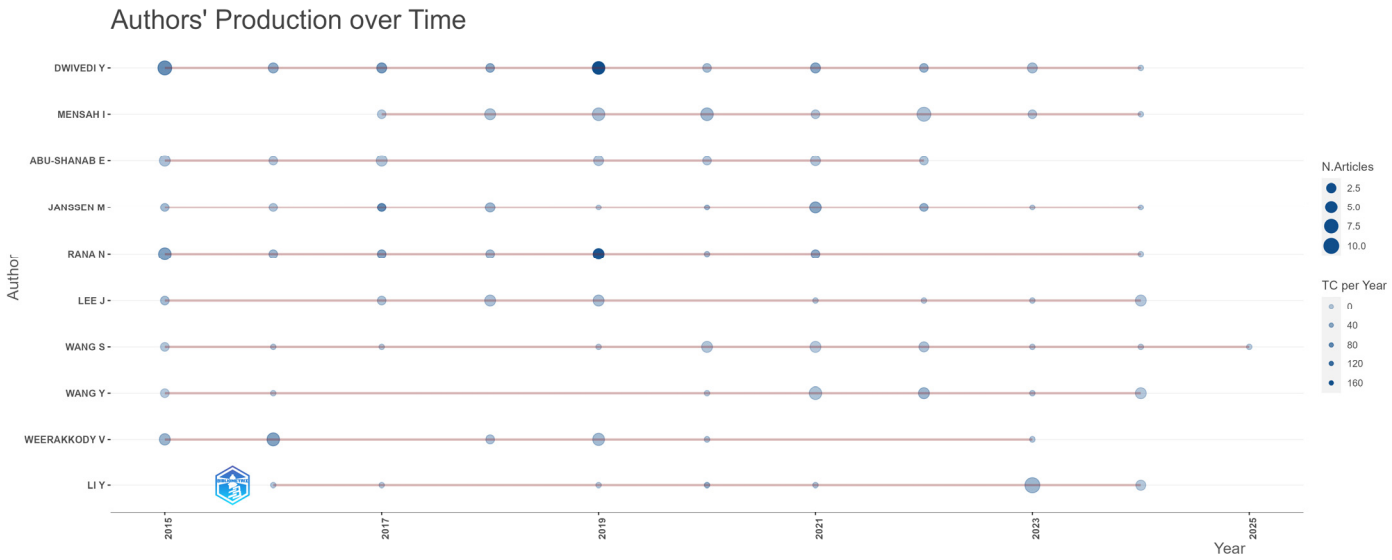

Figure 4. Authors' production with citations over years (authors' own).

Table 1 presents the most relevant authors, Dwivedi Y leads with 33 articles, followed closely by Mensah I with 31 articles. Abu-Shanab E, Janssen M, and Rana N each contributed 20 articles, while other top authors, such as Lee J, Wang S, Wang Y, Weerakkody V, and Li Y, contributed 19 and 18 articles, respectively. The "Authors' Production over Time" chart provides a clear visual of their consistent productivity, with Dwivedi Y and Mensah I showing a steady output of articles in recent years, while others like Abu-Shanab E and Rana N demonstrate fluctuating patterns.

Table 1. Most Relevant Authors.

Authors	Articles
DWIVEDI Y	33
MENSAH I	31
ABU-SHANAB E	20
JANSSEN M	20
RANA N	20
LEE J	19
WANG S	19
WANG Y	19
WEERAKKODY V	19
LI Y	18

Table 2 lists the countries with the number of publications in e-government research, highlighting the leading contributors. China tops the list with 1129 publications, followed by the USA with 787 and the UK with 417. Other notable contributors include India

(373), Spain (358), Australia (220), Ukraine (217), Germany (208), South Korea (206), and Malaysia (202).

Table 2. Contributing Countries.

Country	Freq
CHINA	1129
USA	787
UK	417
INDIA	373
SPAIN	358
AUSTRALIA	220
UKRAINE	217
GERMANY	208
SOUTH KOREA	206
MALAYSIA	202

4.3. Countries' Statistics and Collaboration

Given the interconnectedness of data, the previously mentioned information offers insights into collaboration trends. However, it remains essential to present precise information pertaining to specific datasets through rigorous statistical and mathematical analyses. Accordingly, a list of the top 10 countries contributing significantly to research in e-government services is provided. Notably, two of the top five countries producing e-government-related research are in Asia—China and India.

The following Figure 5 country chart illustrates the clusters of collaboration within e-government services research. Based on the input analysed in R Studio, the cluster represents a network visualisation of global collaborations and research contributions in e-government, with countries represented by nodes. The colour of the nodes indicates their level of involvement, where blue nodes represent countries with strong research output or centrality, and red nodes indicate relatively lower involvement.

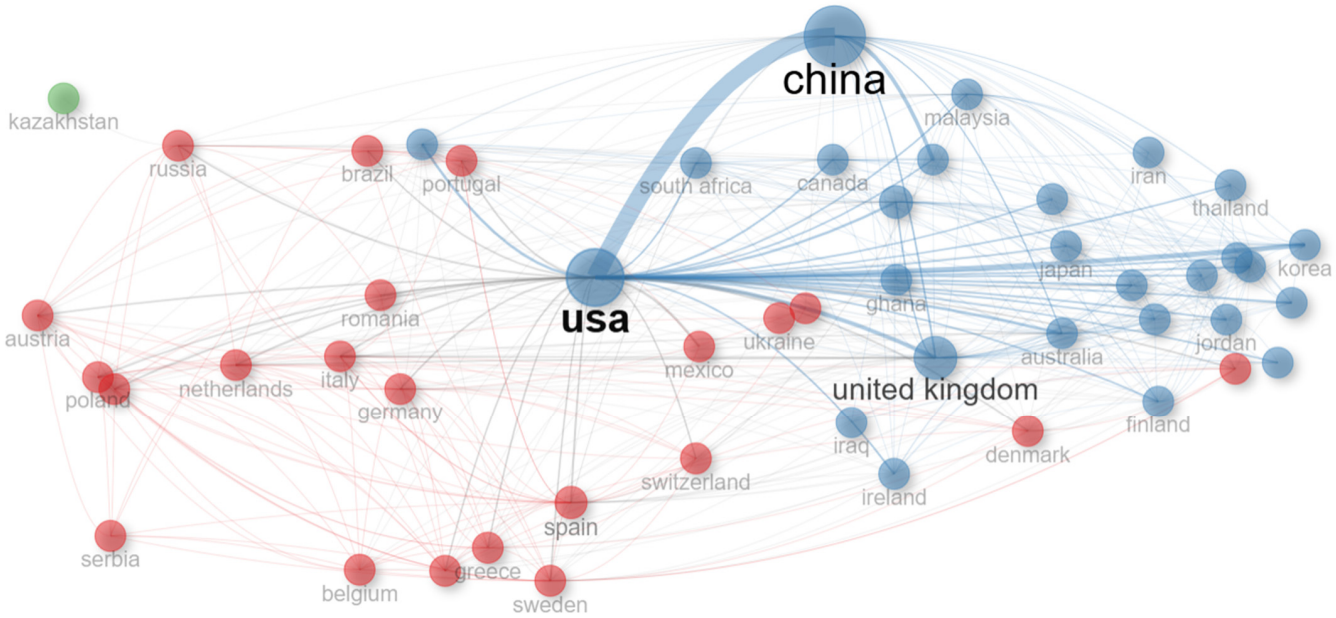

Figure 5. Countries collaboration cluster (authors' own).

4.4. Citation Network Analysis

This analysis provides the frequency of citations, a crucial metric for ranking journals based on their contributions to the field of e-government. By examining citation patterns, one can identify the most influential research works over the period. It provides valuable insights into prominent papers, leading journals, and key contributors, including countries, organisations, and affiliations. Understanding these trends is essential for assessing the impact of research in the domain and guiding future inquiries.

Among the top ten most cited articles, the leading study is cited 962 times. This research examines various algorithms, methodologies, and applications across different domains, highlighting the significance of personalised recommendations in enhancing user experience and engagement [30].

The second most cited study, with 862 citations, explores and critically reviews the UTAUT framework and proposes an alternative model to explain the acceptance and use of information systems (IS) and information technology (IT) innovations [31]. The third on the list, cited 531 times, pertains to digital transformation. It highlights how governments, responding to changing citizen expectations and external pressures such as technological advancements and supranational agreements, are shifting their operations to improve public service delivery [32]. The remaining articles with the highest citation counts over the years are detailed in Table 3.

Table 3. Most contributing authors.

Author and Publisher	Total Citations
LU J, 2015, DECIS SUPPORT SYST	962
DWIVEDI Y, 2019, INFORM SYST FRONT	862
MERGEL I, 2019, GOV INFORM Q	531
LI L, 2018, INFORM SYST J	435
DWIVEDI Y, 2017, GOV INFORM Q	368
JANSSEN M, 2017, J BUS RES	366
WIRTZ B, 2019, INT J PUBLIC ADMIN	328
BONSÓN E, 2015, GOV INFORM Q	302
CUCCINIELLO M, 2017, PUBLIC ADMIN REV	253
DWIVEDI Y, 2015, INFORM SYST FRONT	252

4.5. Trend Topics and Keywords

Thematic evolution of e-government research from 2015–2020 to 2021–2025, presented in Figure 6, reveals a shift in focus from infrastructure and security (e.g., interoperability, adoption, privacy, and cybercrime) to user-centred themes like trust, cybersecurity, usability, COVID-19, and service quality. While e-government remains a central theme, the increasing prominence of trust and security reflects growing concerns over data protection and user confidence. The trend of COVID-19 emphasises the pandemic's impact on e-government services, highlighting the need for resilient, user-friendly digital governance.

4.6. Keyword Occurrences Network

Keyword occurrences help identify themes and trends prevalent in a specific research domain. As depicted in Figure 7, it is noteworthy to observe the evolution of research in e-government concerning its internal spheres, including management, information, and governance. Additionally, a distinct cluster emerges focused on the adoption of e-government services, primarily relating to user engagement. The network map highlights

researchers' concerns regarding factors integral to the e-government adoption process, such as technology, models, trust, and satisfaction. This network aids in pinpointing the interrelated aspects of research.

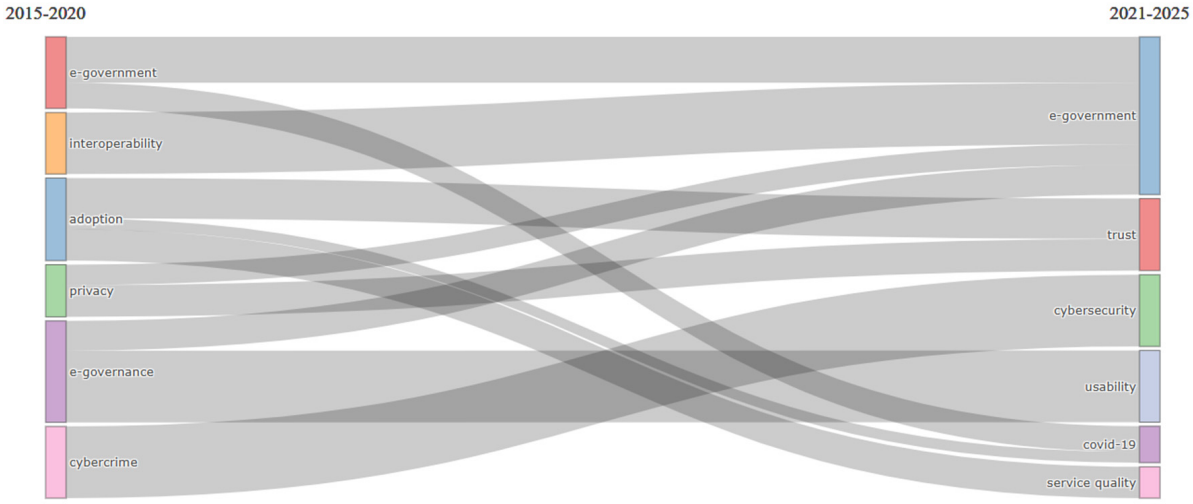

Figure 6. Trending topic, time-sliced (authors' own).

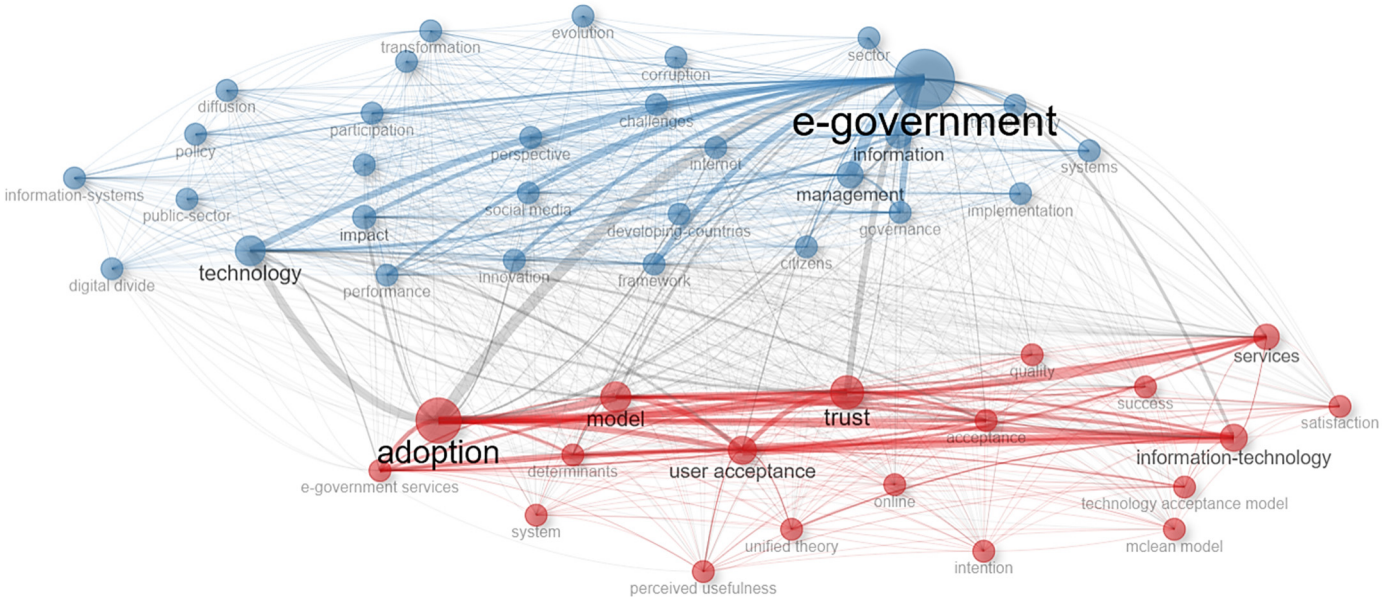

Figure 7. Keyword occurrences (authors' own).

4.7. Identified Themes

In total, 19 themes were identified, as illustrated in Figure 8. These include various aspects of e-government services, with all potential themes from the dataset. Each research paper was categorised according to its title, resulting in the following distribution: adoption (260); governance (249); development (236); implementation (113); value (116); performance (98); corruption (99)' challenges (92); security (88); application (88); transformation (107); acceptance (67); blockchain (61); accessibility (37); readiness (35); effectiveness (34); efficiency (42); barriers (29); and comparison (21). However, the extensive number of articles within some of these major themes was subsequently refined based on publication quality, resulting in the reporting of only selected papers from these prominent themes.

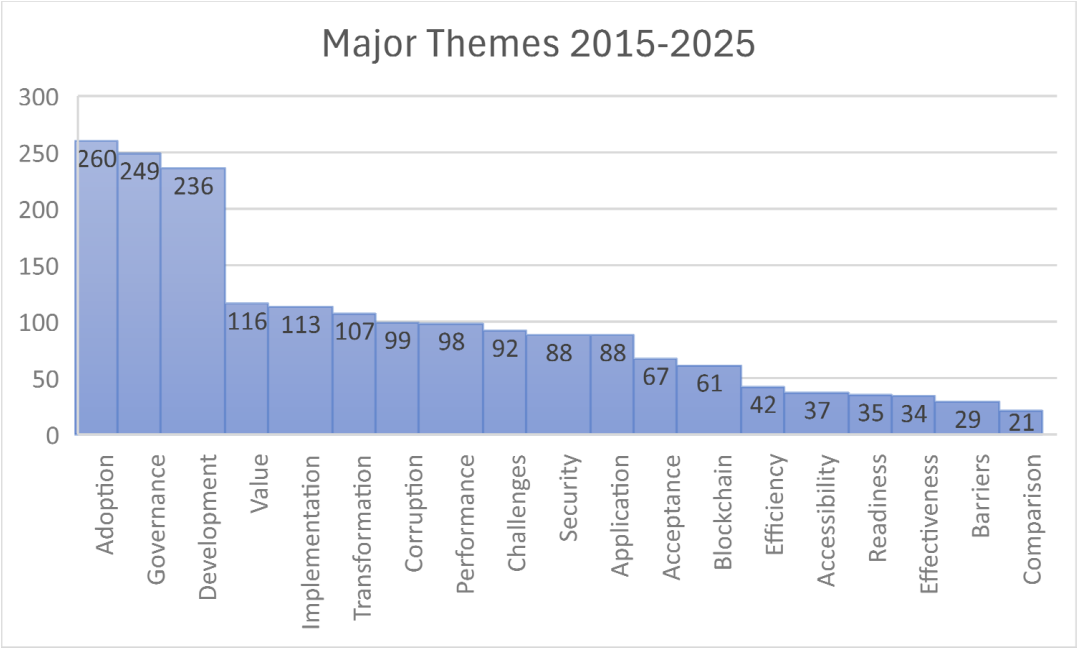

Figure 8. E-government literature themes identified (authors' own).

4.8. Cybersecurity and E-Government Research

A total of 88 research papers on security in e-government services were identified in WOS and Scopus databases; the initial scrutiny resulted in 25 studies as the main feature in the paper title. Considering the quality of these articles and suitable relevance, 19 research articles are reported particularly directed towards security within e-government services. The final sample was analysed based on each study's focus, location, findings, data, and methodologies.

5. Discussion

The e-government research contains key themes such as adoption, governance, development, value, implementation, transformation, corruption, etc. Security concerns are studied in both the adoption and development stages, while privacy emerges as a common concern in the adoption and implementation phases. Additionally, the specific theme of "security" is further explored in this study. The limited empirical data on e-government security suggest that despite its frequent discussion, practical insights into the current state of security are still lacking [33]. These recurring themes align, to some degree, with findings from a bibliometric analysis [23].

5.1. Development

E-government development refers to the systems that enable service functionality, relying on coherent government policies to promote high levels of financial and information security [34]. Integrating robust cybersecurity is essential for advancing e-government systems [35]. Research indicates that secure and resilient cybersecurity measures are essential in supporting digitalisation during the developmental stages of e-government. However, in developing countries, where corruption is often high, strict administrative measures are necessary to protect information [36]. Table 4 provides a literature-based classification of factors relevant to development studies in e-government services.

Table 4. Research Themes Identified.

Mapping of E-Government Research Themes			
Theme	**Interest**	**Concepts**	**Sources**
Development	Widespread	Decision-making, evolution, public value, transparency, efficiency, engagement, website useability, user's perception of quality, government effectiveness, culture, cybersecurity, information sharing, interconnection of services, human development, international collaborations.	[34,36–47]
Adoption	Widespread	Environment, process, information, value, capacity, usefulness, behaviour, resistance to change, content delivery, interactions, and emotional aspects.	[48–54]
	Factors	Website quality, technology adoption, trust, privacy, security risk, age, transparency, corruption, forced adoption, fairness in customer support, internet connection quality, complexity, performance, and cost–benefit expectancy and security.	[55–64]
Implementation	Widespread	National financial position, e-readiness, infrastructure, innovation, communication, political and legal framework, promotion, technological, organisational, and environmental tools, e-participation, e-transparency and e-services, population size, age, privacy.	[48,65–68]
Corruption	Widespread	Mitigation, income inequality, maturity, e-government participation.	[69–73]
Governance	Factors	E-governance, social role, public value.	[74,75]
Performance	Factors	Budget, satisfaction, relationship with adoption, measurement models, access, public value.	[76–81]
Value	Factors	Public value of websites, perceived value, service value chain, relation with performance.	[49,81–84]

5.2. Adoption

Interestingly, research has an increased focus on the adoption of e-government services, surpassing interest in their development and implementation. This trend likely reflects the rapid technological expansion, with greater emphasis on adoption as these services become functional globally. User adoption is influenced by factors such as risk and privacy concerns, with age identified as a significant factor [56].

However, vulnerabilities in e-government service websites may also hinder adoption [33]. Trust plays a crucial role, as it positively affects users' intentions to utilise these services [61]. Consequently, both user age and trust levels impact e-government service adoption. Many studies in this domain draw on the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT) frameworks, which provide foundational insights into factors influencing service acceptance and use. Constructs from these frameworks—such as perceived usefulness, ease of use, social influence, and behavioural intentions—are frequently used to examine e-government service adoption and usage [53,85].

5.3. Implementation

The implementation of e-government services requires a thorough consideration of national factors, including legal, political, technological, e-readiness, financial, infrastructural, and technological elements [65]. Table 4 summarises several contextual studies that address these issues. Among these factors, the legal and administrative frameworks that support implementation are particularly important [86]. Moreover, the execution of

e-government services at the local level should be examined through three key dimensions: e-participation; e-transparency; and e-services [67]. It is also essential to analyse the implementation mechanisms within the specific contexts they are designed for, focusing on the processes and performance of the services [48]. Similar evaluations are recommended for assessing the adoption of e-government services.

Given the critical importance of cybersecurity systems in development, according to Abbas, Qaisar [35], their implementation must incorporate privacy considerations from the outset. This involves addressing user needs and ensuring alignment with existing legal frameworks and best practices [68].

5.4. Corruption

E-government services provide technological support for governmental functions. However, the effectiveness of an e-government system in combating corruption is contingent upon the existence of a robust legal framework that has been established and implemented at the national level [69]. Consequently, the rule of law is crucial for the successful anti-corruption outcomes anticipated through e-government services. Notably, in contrast to previous research, some authors suggest that higher levels of technology adoption may inadvertently intensify corruption.

As previously noted, cybersecurity is present at each stage of e-government service development. In developing countries, implementing robust security and privacy frameworks is critical to effectively protect sensitive information [36]. Since governments anticipate widespread use of these technologies, it is imperative for users to trust these systems to facilitate the adoption of the services [61]. Thus, a secure and protective system is necessary to ensure the safety of information. Therefore, a country with an effective rule of law and e-government services can pose a mature posture of e-government services [87]. Mapping e-government research has yielded enough evidence to consider corruption as a major topic of debate, as evidenced in Table A1.

5.5. Performance

Performance monitoring is a critical factor that contributes to the effective functioning of e-government programs. Evaluating service performance enhances our understanding of their successes and failures. During the development and implementation phases, it is imperative to prioritise realistic execution over aspirational goals. Programs should be founded on well-defined policies and thorough assessments of requirements [76]. Conversely, in many developing countries, the implementation of programs often reflects the personal preferences of various ministries, resulting in the initiation of projects that may be impractical or unfeasible [1]. This misalignment is a primary cause of the failure of numerous e-government service initiatives. Citizens expect these services to enhance their daily lives rather than merely facilitating information sharing from the government [77]. Notably, research has demonstrated a negative correlation between the use of these services and their overall performance [88]. Thus, continuous monitoring post-implementation is vital for maintaining a successful system. Table 4 documents extensive research evidence evaluating these programs.

5.6. Value

The perceived value of e-government services significantly influences their usage. The quality of government websites is linked to the overall ranking of e-government portals [82]. Additionally, citizens appreciate the cost and time savings associated with these services, which, in turn, enhances their satisfaction [49]. The service quality increases emotional value and trust among users [84]. These factors are critical in shaping the public value of e-government services. Furthermore, incorporating environmental sustain-

ability into the public value framework proves effective in assessing the performance of e-government initiatives.

5.7. Governance

Integration of e-government development with the specific contextual factors of each country or region, including technology, organisation, culture, socio-economic conditions, and sectoral knowledge, can further assist governments. For instance, despite governments' strong preference for e-government to enhance efficiency, many citizens still prefer face-to-face interactions due to low digital literacy. If digital transformation is not aligned with these contextual factors, its positive impact on governance is diminished [75].

5.8. Security in E-Government Services

The literature focuses more on the e-government service's security from users' perspectives, particularly in terms of service usage and adoption. Notably, little is discussed about the internal working for cybercrime prevention. One reason could be due to a lack of data availability. For instance, e-government services are offered by public institutes; it is difficult to obtain clearance or access to government institutes' internal data compared to accessing the service users for research purposes.

The studies focused on security within e-government services, emphasising it as a critical factor. This includes both technical security measures, such as encryption and firewalls, as well as non-technical measures, including user education and awareness. Table A1 presents research specifically focused on cybersecurity as it pertains to e-government services. Based on the established inclusion criteria, only 19 research articles explicitly addressing both e-government services and cybersecurity in their titles were identified.

Krishna and Sebastian [43], Ejdys, Ginevicius [89], Thoinpson, Mullins [33] identified numerous e-government websites inadequately protected against cyberattacks. The observed vulnerabilities were outdated certificates used to verify identity and encrypt data exchanged between the website and users. Consequently, implementing robust security testing measures is essential to validate that e-government websites meet acceptable security standards [90]. Furthermore, the adoption of standardised templates and the conduct of regular security audits are necessary to enhance overall security [33].

Though e-government services are accessible through a single digital resource—the internet—there are significant differences in resources, infrastructure, technology, and adoption that contribute to the vulnerabilities of these services. For instance, research by Zhang, Tang [91] indicates that China faces limited resources for implementing cybersecurity measures in its e-government portals. Additionally, a centralised provision of these services is recommended to enhance the existing systems. In contrast, in Vietnam, the emphasis is placed on the legal aspects at the national level that are crucial for establishing effective and cybersecure e-government services [92]. This perspective is further supported by the concept of legitimacy [93].

Politanskyi, Lukianov [92] note that the e-government service implementation often leads to information security challenges, and due to the complexity of the domain, there is limited scientific research on this topic. Krishna and Sebastian [43] illustrate, through publicly available archival data from 127 countries, that developing e-government services is associated with cybersecurity commitment. This is corroborated by research in Poland explaining that security variables can serve as a promotional factor in increasing the usage of these services [89], thereby enhancing public confidence and alleviating fears of potential losses [36]. However, service administrators must consider the impact of social media threats, as these can lead to significant reputational damage to e-government services [94].

The studies from Ukraine and South Africa showed the importance of security parameters, software integration, and governance [74,95]. Studies from Saudi Arabia underscore the role of financial investment, employee training, and regulatory compliance in strengthening cybersecurity [96,97]. Studies from South Korea and Saudi Arabia also highlight the positive influence of organisational culture and legal frameworks on security effectiveness. Additionally, citizens' trust is crucial, with research from Pakistan showing that factors like privacy concerns and technology anxiety impact adoption behaviour [98,99].

The studies conducted in Pakistan also explored blockchain, suggesting its potential for improving legal compliance, though challenges related to privacy and decentralisation persist [98,99]. Legal and regulatory frameworks are central to addressing e-government security, with blockchain technology offering solutions; yet, unresolved issues around privacy and alignment remain. These findings stress the importance of a comprehensive approach, combining governance, technology, and public trust to ensure effective e-government security systems.

Corresponding to some previously discussed concepts, access features such as work-from-home and bring-your-own-device policies, along with complex hardware and software requirements—including decentralised controls—hinder the secure operation of these services [34]. Ultimately, security measures are essential for protecting valuable user information from cyberattacks. Therefore, standard operating procedures developed by the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) are crucial for securing information and preventing data breaches [100].

To address Objective 1: By mapping the existing literature on e-government services, we reviewed the literature from the last decade within the e-government research field. Notable themes have emerged, such as development, adoption, implementation, corruption, governance, performance, and value. This thematic mapping corresponds with previous bibliometric analyses [23]. Objective 2 was further explored by conducting a detailed bibliometric analysis using the WOS and Scopus merged collection, extending previous work in this area. This approach allowed us to systematically identify key research contributions, leading authors, and affiliations within the domain of e-government services.

For Objective 3: Assessing the extent to which cybercrime mitigation is addressed in e-government services, our review finds limited studies directly focused on cybercrime mitigation. Existing research predominantly addresses cybersecurity as a preventative approach, focused on safeguarding systems against data breaches and other cyber threats. This trend suggests that security is primarily emphasised during the development, implementation, and adoption phases of e-government services, potentially overshadowing specific cybercrime mitigation measures. Notably, one study collecting insights from employees involved in e-government services identified security issues as a barrier to service adoption. Additionally, standards set by NIST and ISO are highlighted as essential frameworks for maintaining security and safety in e-government services.

6. Conclusions

This study mapped research on e-government services in the past decade, shedding light on existing themes. It presented a complex landscape, including dimensions such as development, adoption, and governance through a multitude of constructs. While significant attention has been devoted to security, privacy, and user trust, the literature reveals a notable gap in discussions regarding the strategies employed by e-government institutions to mitigate cybercrime, leaving this critical aspect largely unexplored. This highlights the scarcity of the literature addressing cybercrime mitigation within these services. More attention is paid towards cybercrime victimisation from a user's perspective,

perhaps because access to data from government institutes is not easy, especially accessing the managers within these government services.

However, emerging evidence suggests that cybersecurity frameworks, such as those established by the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO), through their standards, can uplift the cybersecurity posture of these services. Despite this potential, much of the existing research tends to concentrate on the security of e-government websites and software, often overlooking broader cybersecurity within institutes. Furthermore, the focus predominantly centres on users, while the internal mechanisms related to the implementation of mitigation strategies by e-government management remain insufficiently examined in the literature.

7. Future Research Implications

While substantial investments have been made in cybersecurity infrastructures, the literature overlooks the interplay between managerial practices and technical frameworks in addressing cybercrimes in e-government services. Future research should explore cybersecurity frameworks that integrate managerial perspectives with technical infrastructures to provide a more nuanced understanding of digital governance challenges. This approach has the potential to advance theoretical models by uncovering how the alignment of human and technological elements fosters resilience in e-government systems.

From a managerial perspective, the findings emphasise the necessity of addressing human vulnerabilities while leveraging cutting-edge technologies such as AI and blockchain. AI can transform threat detection and incident response processes through automation and predictive analytics, while blockchain offers enhanced data security and transparency to reduce risks associated with cyber breaches. These technologies, when combined with strategic training initiatives, updated policy, and decision-making processes, can empower e-government institutions to design adaptive cybersecurity strategies.

Author Contributions: Conceptualization: S.M.; methodology, M.S. and S.M.; software, S.M.; validation, S.M.; investigation, S.M.; data curation, S.M.; writing—original draft preparation, S.M.; writing—review and editing, S.M. and M.S.; visualisation, S.M.; supervision, M.S. All authors have read and agreed to the published version of this manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

Table A1. E-Government services and cybercrime mitigation.

E-Government Services and Cybercrime Mitigation						
NO	**Focus**	**Location**	**Findings**	**Sources**	**Data**	**Technique**
1	Software Security Assessment	Norway and Vietnam	For security, SAST tools should be used for practical performance and in combination with triangulated approaches for human-driven vulnerability assessment in real-world projects of e-government.	[90]	Semi Structured Interviews	Static Application Security Testing (SAST)
2	Moderating effect of Cybersecurity	Asian Countries	Secured and strong cybersecurity and corruption control network systems speed up digitalization, development, and sustainability.	[35]	Cybersecurity Index	Fixed-effect regression analysis and random forest (RF) algorithm

Table A1. *Cont.*

E-Government Services and Cybercrime Mitigation						
NO	**Focus**	**Location**	**Findings**	**Sources**	**Data**	**Technique**
3	Socio-Technical Analysis	China	There is lack of resources to implement cybersecurity in e-government portals. Collaborative construction of cybersecurity systems and centralized procurement of cybersecurity services are recommended, especially at the county level and in smaller prefecture-level cities and when planning to strengthen cybersecurity capabilities of existing e-government systems.	[91]	Open-ended interviews	Based on constructs from Prior Survey Research
4	Legal Aspects	Ukraine	The implementation of e-government causes problems related to information security. Modern computer security is a complex phenomenon whose perspectives are influenced by different internal and external factors, the most important being the political situation. The issues in functioning aspect of information security in e-government are quite difficult, which explains its little scientific research.	[92]	Review of Ukrainian Information legislation	N/A
5	E-Government Website Security	Australia and Thailand	Standardised templates of government websites ensure validity of the content. Delivered through a content management system, which can result in improving security administration. Routine site audits should be scheduled to alert security administrators.	[33]	Review of Australian and Thailand's e-government websites	Web Content Analysis of Policies and encryption + Security Vulnerability testing
6	Relationship between e-gov development and cybersecurity	127 countries	E-government development demonstrated a stronger association with cybersecurity commitment and business usage. Mitigating cybercrimes is one way of saving cost in billions of USD for the nation, and thus keeping a tab on the budget balance.	[43]	Publicly available archival data	Structural equation modelling to analyse the country level variable
7	Perceived risk and security levels in building trust	Poland	The statistically important relationship between perceived security and trust in e-government technology indicated the practical utility of using a security variable in the promotion and encouragement of the public to use e-government services.	[89]	Quantitative Data	Correlation and Structural Equation Modelling
8	Privacy, Security, Trust, Risk and Optimism bias in e-government use	Zimbabwe and Zambia	Robust security measures on e-government transactions mitigate fears associated with a potential loss by citizens. Perceived lack of privacy, security, trust; perceived risk and optimism bias were all confirmed as salient factors affecting the utilisation of e-government systems by citizens.	[36]	Quantitative Data from E-Government Users	Structural Equation Modelling

Table A1. *Cont.*

E-Government Services and Cybercrime Mitigation						
NO	**Focus**	**Location**	**Findings**	**Sources**	**Data**	**Technique**
9	Information System Security for sustainable development	Korea	Information system security effectiveness depends on the path through legitimacy, influenced by normative and coercive isomorphism, which is stronger than that through organizational cynicism.	[93]	Quantitative Data from 30 departments of government	Partial Least Square
10	Social Networks in e-government	AZERBAIJAN	Social media threats can cause reputation loss in government-to-citizen relations, which may result in social–political conflicts.	[94]	Experimental Design	Fuzzy TOPSIS
11	Financial and information security of country	10 different countries	The main reasons leading to the problems of safe operation of e-government systems can be attributed to the complexity and heterogeneity of software and hardware used in e-government systems; a large number of control nodes in e-government systems; external access to the e-government system; functioning of maintenance and information security groups.	[34]	E-Government Development Index, Global Cybersecurity Index indicators	Comparison
12	Impact of information systems security laws and standards on the e-government. Cyberthreats and vulnerabilities	Saudi Arabia	The cyber-attackers intend to steal information; therefore, NIST and ISO developed standard operating procedures required for the safety and security of information to prevent data breach. The major vulnerabilities found in the literature are weak security systems, lack of awareness, and enterprise failure.	[100]	N/A	Mixed Method
13	E-Government Systems–Increasing its Security	Ukraine	Identification of critical quality of service concepts and security parameters that influence the operational security of Ukraine's electronic government system.	[95]	Reports	Qualitative
14	E-Government Projects Security	South Africa	The main problems identified were the lack of software integration and information security governance, policy, and administration.	[74]	Government Databases	Qualitative
15	E-Government Information System Security	South Korea	Using institutional theory and organisational behaviour, this study concludes that innovative culture and legitimacy positively influence ISS effectiveness.	[101]	Questionnaire—security managers	Quantitative—PLS SEM
16	Security in Intention of Using E-Government	Saudi Arabia	User interface quality, security culture, and cybersecurity law affect security perception positively.	[96]	Both collected from Saudi citizens	Mixed Method—Focus Group and SEM
17	Cybersecurity practices and quality of e-government services	Saudi Arabia	Financial investment in cybersecurity, employee training, and adherence to regulations significantly influence the adoption of strong cybersecurity practices.	[97]	Users	PLS—SEM
18	Perceived Security in Adoption Behaviour	Pakistan	Perceived privacy, perceived security, technology anxiety, effort expectancy, and performance expectancy positively influence citizens' adoption behaviour. It suggests that policymakers and relevant authorities in the Pakistani government should focus on enhancing citizens' trust.	[98]	Citizens	PLS—SEM

Table A1. *Cont.*

E-Government Services and Cybercrime Mitigation						
NO	**Focus**	**Location**	**Findings**	**Sources**	**Data**	**Technique**
19	Legal, technical and ethical security in E-Government	Pakistan	It identifies blockchain's potential in data governance and its role in ensuring legal compliance. However, challenges around privacy, decentralization, and regulatory alignment remain unresolved.	[99]	N/A	Qualitative Evaluation.

References

1. Malodia, S.; Dhir, A.; Mishra, M.; Bhatti, Z.A. Future of e-Government: An integrated conceptual framework. *Technol. Forecast. Soc. Change* **2021**, *173*, 121102. [CrossRef]
2. Kumar, R.; Mukherjee, A.; Sachan, A. Factors influencing indirect adoption of e-Government services: A qualitative study. *Inf. Syst. E-Bus. Manag.* **2023**, *21*, 471–504. [CrossRef]
3. Cremer, F.; Sheehan, B.; Fortmann, M.; Kia, A.N.; Mullins, M.; Murphy, F.; Materne, S. Cyber risk and cybersecurity: A systematic review of data availability. *Geneva Pap. Risk Insur.-Issues Pract.* **2022**, *47*, 698–736. [CrossRef] [PubMed]
4. Chandra, A.; Snowe, M.J. A taxonomy of cybercrime: Theory and design. *Int. J. Account. Inf. Syst.* **2020**, *38*, 100467. [CrossRef]
5. Lee, C.S.; Wang, Y. Typology of cybercrime victimization in Europe: A multilevel latent class analysis. *Crime Delinq.* **2024**, *70*, 1196–1223. [CrossRef]
6. Van de Weijer, S.; Leukfeldt, R.; Moneva, A. Cybercrime during the COVID-19 pandemic: Prevalence, nature and impact of cybercrime for citizens and SME owners in the Netherlands. *Comput. Secur.* **2024**, *139*, 103693. [CrossRef]
7. Florido-Benítez, L. The types of hackers and cyberattacks in the aviation industry. *J. Transp. Secur.* **2024**, *17*, 13. [CrossRef]
8. Schmitt, M. Securing the Digital World: Protecting Smart Infrastructures and Digital Industries with Artificial Intelligence (Ai)-Enabled Malware and Intrusion Detection. *J. Ind. Inf. Integr.* **2023**, *36*, 100520. [CrossRef]
9. Mee, P.; Chandrasekhar, C. *Cybersecurity Is Too Big a Job for Governments or Business to Handle Alone*; European Union Agency for Law Enforcement Training (CEPOL): Budapest, Hungary, 2021.
10. Yeboah-Ofori, A.; Opoku-Boateng, F.A. Mitigating cybercrimes in an evolving organizational landscape. *Contin. Resil. Rev.* **2023**, *5*, 53–78. [CrossRef]
11. Soomro, Z.A.; Shah, M.H.; Ahmed, J. Information security management needs more holistic approach: A literature review. *Int. J. Inf. Manag.* **2016**, *36*, 215–225. [CrossRef]
12. Lohrke, F.T.; Frownfelter-Lohrke, C. Cybersecurity research from a management perspective: A systematic literature review and future research agenda. *J. Gen. Manag.* **2023**, *48*, 03063070231200512. [CrossRef]
13. *Estimated Cost of Cybercrime Worldwide 2018–2029*; Statista: Hamburg, Germany, 2024.
14. CloudSEK. Share of Cyber Incidents Targeting Government Agencies Worldwide in 2022, by Attack Vector. Available online: https://www.statista.com/statistics/1428581/government-worldwide-targeted-cyber-incidents-by-attack-vector/ (accessed on 20 October 2024).
15. Blackberry. Number of Cyber Incidents Targeting Government Agencies Worldwide from December 2022 to August 2023. Available online: https://www.statista.com/statistics/1428595/government-worldwide-targeted-cyber-incidents-number/ (accessed on 20 October 2024).
16. Annarelli, A.; Clemente, S.; Nonino, F.; Palombi, G. *Effectiveness and Adoption of NIST Managerial Practices for Cyber Resilience in Italy*; Springer: Berlin/Heidelberg, Germany, 2021.
17. Anwary, I. Evaluating Legal Frameworks for Cybercrime in Indonesian Public Administration: An Interdisciplinary Approach. *Int. J. Cyber Criminol.* **2023**, *17*, 12–22. [CrossRef]
18. Brumfield, C.; Haugli, B. *Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework*, 1st ed.; Wiley: Newark, NJ, USA, 2022.
19. National Institute of Standards and Technology. NIST Cybersecurity Framework. Available online: https://www.nist.gov/cyberframework/framework (accessed on 15 December 2023).
20. Roy, P.P. A high-level comparison between the nist cyber security framework and the iso 27001 information security standard. In Proceedings of the 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA), Durgapur, India, 7–8 February 2020.
21. Thompson, E.C. *Building a HIPAA-Compliant Cybersecurity Program: Using NIST 800-30 and CSF to Secure Protected Health Information*, 1st ed.; Apress: Berkeley, CA, USA, 2017.
22. Dias, G.P. Fifteen years of e-government research in Ibero-America: A bibliometric analysis. *Gov. Inf. Q.* **2019**, *36*, 400–411. [CrossRef]

23. Ramzy, M.; Ibrahim, B. The evolution of e-government research over two decades: Applying bibliometrics and science mapping analysis. *Libr. Hi Tech* **2022**, *42*, 227–260. [CrossRef]
24. Leukfeldt, R.; Holt, T.J. *The Human Factor of Cybercrime*; Routledge: Abingdon, UK, 2019.
25. Dupont, B.; Holt, T. The Human Factor of Cybercrime. *Soc. Sci. Comput. Rev.* **2021**, *40*, 860–864. [CrossRef]
26. Tremblay-Cantin, C.-A.; Mellouli, S.; Cheikh-Ammar, M.; Khechine, H. E-government Service Adoption by Citizens: A Literature Review and a High-level Model of Influential Factors. *Digit. Gov. Res. Pract.* **2023**, *4*, 1–24. [CrossRef]
27. Dupont, B. Enhancing the effectiveness of cybercrime prevention through policy monitoring. *J. Crime Justice* **2019**, *42*, 500–515. [CrossRef]
28. Donthu, N.; Kumar, S.; Mukherjee, D.; Pandey, N.; Lim, W.M. How to conduct a bibliometric analysis: An overview and guidelines. *J. Bus. Res.* **2021**, *133*, 285–296. [CrossRef]
29. Radanliev, P. Digital security by design. *Secur. J.* **2024**, *37*, 1640–1679. [CrossRef]
30. Lu, J.; Wu, D.; Mao, M.; Wang, W.; Zhang, G. Recommender system application developments: A survey. *Decis. Support Syst.* **2015**, *74*, 12–32. [CrossRef]
31. Dwivedi, Y.K.; Rana, N.P.; Jeyaraj, A.; Clement, M.; Williams, M.D. Re-examining the Unified Theory of Acceptance and Use of Technology (UTAUT): Towards a Revised Theoretical Model. *Inf. Syst. Front.* **2019**, *21*, 719–734. [CrossRef]
32. Mergel, I.; Edelmann, N.; Haug, N. Defining digital transformation: Results from expert interviews. *Gov. Inf. Q.* **2019**, *36*, 101385. [CrossRef]
33. Thompson, N.; Mullins, A.; Chongsutakawewong, T. Does high e-government adoption assure stronger security? Results from a cross-country analysis of Australia and Thailand. *Gov. Inf. Q.* **2020**, *37*, 101408. [CrossRef]
34. Yarovoy, T.S.; Kozyrieva, O.V.; Bielska, T.V.; Zhuk, I.I.; Mokhova, I.L. The e-Government Development in Ensuring the Country Financial and Information Security. *Financ. Credit Act.-Probl. Theory Pract.* **2020**, *2*, 268–275. [CrossRef]
35. Abbas, H.S.M.; Qaisar, Z.H.; Xu, X.D.; Sun, C.X. Nexus of E-government, cybersecurity and corruption on public service (PSS) sustainability in Asian economies using fixed-effect and random forest algorithm. *Online Inf. Rev.* **2022**, *46*, 754–770. [CrossRef]
36. Munyoka, W.; Maharaj, M.S. Privacy, security, trust, risk and optimism bias in e-government use: The case of two Southern African Development Community countries. *S. Afr. J. Inf. Manag.* **2019**, *21*, 9. [CrossRef]
37. Ravanos, P.; Karagiannis, G. Tricks with the BoD model and an application to the e-Government Development Index. *Socio-Econ. Plan. Sci.* **2022**, *81*, 100955. [CrossRef]
38. Zhang, Y.; Kimathi, F.A. Exploring the stages of E-government development from public value perspective. *Technol. Soc.* **2022**, *69*, 101942. [CrossRef]
39. Butt, N.; Warraich, N.F.; Tahira, M. Development level of electronic government services an empirical study of e-government websites in Pakistan. *Glob. Knowl. Mem. Commun.* **2019**, *68*, 33–46. [CrossRef]
40. Aljukhadar, M.; Belisle, J.F.; Dantas, D.C.; Senecal, S.; Titah, R. Measuring the service quality of governmental sites: Development and validation of the e-Government service quality (EGSQUAL) scale. *Electron. Commer. Res. Appl.* **2022**, *55*, 101182. [CrossRef]
41. Wallis, J.; Zhao, F. e-Government Development and Government Effectiveness: A Reciprocal Relationship. *Int. J. Public Adm.* **2018**, *41*, 479–491. [CrossRef]
42. Kumar, S.; Baishya, K.; Sreen, N.; Sadarangani, P.H.; Samalia, H.V. Impact of National Culture on E-Government Development: A Longitudinal Study. *J. Glob. Inf. Manag.* **2021**, *29*, 1–22. [CrossRef]
43. Krishna, B.; Sebastian, M.P. Examining the relationship between e-government development, nation's cyber-security commitment, business usage and economic prosperity: A cross-country analysis. *Inf. Comput. Secur.* **2021**, *29*, 737–760. [CrossRef]
44. Ma, D.; Zhou, J.J.; Zuo, M.Y. Inter-agency information sharing for Chinese e-government development: A comparison between vertical and horizontal dimensions. *Inf. Technol. Dev.* **2022**, *28*, 297–318. [CrossRef]
45. Zakovec, L.; Ondria, P. Development and Current State of E-government in the Federal Republic of Germany. *Politicke Vedy* **2022**, *25*, 231–260. [CrossRef]
46. Silal, P.; Saha, D. E-Government as a Tool for Human Development: The Moderating Influence of National Culture. *J. Glob. Inf. Technol. Manag.* **2021**, *24*, 235–258. [CrossRef]
47. Cho, B.; Rethemeyer, R.K. Whom do we learn from? The impact of global networks and political regime types on e-government development. *Int. Public Manag. J.* **2022**, *26*, 507–527. [CrossRef]
48. Tan, H.B.; Zhao, X.J.; Zhang, N. Technology symbolization: Political mechanism of local e-government adoption and implementation(1). *Int. Rev. Adm. Sci.* **2022**, *88*, 511–532. [CrossRef]
49. Aranyossy, M. User adoption and value of e-government services (Citizen-centric empirical study from Hungary). *Acta Oeconomica* **2022**, *72*, 477–497. [CrossRef]
50. Mensah, I.K. Impact of Government Capacity and E-Government Performance on the Adoption of E-Government Services. *Int. J. Public Adm.* **2020**, *43*, 303–311. [CrossRef]
51. Chen, L.J.; Aklikokou, A.K. Determinants of E-government Adoption: Testing the Mediating Effects of Perceived Usefulness and Perceived Ease of Use. *Int. J. Public Adm.* **2020**, *43*, 850–865. [CrossRef]

52. Zhang, B.H.; Zhu, Y.H. Comparing attitudes towards adoption of e-government between urban users and rural users: An empirical study in Chongqing municipality, China. *Behav. Inf. Technol.* **2021**, *40*, 1154–1168. [CrossRef]
53. Al Mansoori, K.A.; Sarabdeen, J.; Tchantchane, A.L. Investigating Emirati citizens' adoption of e-government services in Abu Dhabi using modified UTAUT model. *Inf. Technol. People* **2018**, *31*, 455–481. [CrossRef]
54. Monteiro, J.; Bernando, M.; Ferreira, M.; Rocha, T. Validation of e-Government Information Delivery Attributes: The Adoption of the Focus Group Method. *J. Univers. Comput. Sci.* **2021**, *27*, 1069–1095. [CrossRef]
55. Mohammadi, M.K. Factors influencing the adoption of e-government websites in Afghanistan from the citizens' perspective. *Electron. J. Inf. Syst. Dev. Ctries.* **2022**, *88*, e12216. [CrossRef]
56. Bayaga, A. Examining the predictive relevance of security, privacy risk factors, and institutional logics for e-government service adoption. *Electron. J. Inf. Syst. Dev. Ctries.* **2022**, *88*, e12201. [CrossRef]
57. Mensah, I.K.; Mi, J.N. Exploring the Impact of Demographic Factors on E-Government Services Adoption. *Inf. Resour. Manag. J.* **2018**, *31*, 1–16. [CrossRef]
58. Kumar, R.; Sachan, A.; Mukherjee, A.; Kumar, R. Factors influencing e-government adoption in India: A qualitative approach. *Digit. Policy Regul. Gov.* **2018**, *20*, 413–433. [CrossRef]
59. Vazquez-Lopez, A.; Marey-Perez, M. Factors Affecting e-Government Adoption by Dairy Farmers: A Case Study in the North-West of Spain. *Future Internet* **2021**, *13*, 206. [CrossRef]
60. Ramirez-Madrid, J.P.; Escobar-Sierra, M.; Lans-Vargas, I.; Hincapie, J.M.M. Factors influencing citizens' adoption of e-government: An empirical validation in a Developing Latin American Country. *Public Manag. Rev.* **2022**, *26*, 185–218. [CrossRef]
61. Barbosa, J.D.S.; Mota, F.P.B. Adoption of e-government: A study on the role of trust. *Rev. De Adm. Publica* **2022**, *56*, 441–464. [CrossRef]
62. Alzahrani, L.; Al-Karaghouli, W.; Weerakkody, V. Investigating the impact of citizens' trust toward the successful adoption of e-government: A multigroup analysis of gender, age, and internet experience. *Inf. Syst. Manag.* **2018**, *35*, 124–146. [CrossRef]
63. Verkijika, S.F.; De Wet, L. E-government adoption in sub-Saharan Africa. *Electron. Commer. Res. Appl.* **2018**, *30*, 83–93. [CrossRef]
64. Olesen, K.; Wood, L.C.; Chong, J.L.L. Citizen Adoption in E-Government Systems: A Meta Analysis. *J. Glob. Inf. Manag.* **2021**, *29*, 1–28. [CrossRef]
65. Glyptis, L.; Christofi, M.; Vrontis, D.; Del Giudice, M.; Dimitriou, S.; Michael, P. E-Government implementation challenges in small countries: The project manager's perspective. *Technol. Forecast. Soc. Change* **2020**, *152*, 119880. [CrossRef]
66. Olumoye, M.Y.; Govender, I. An empirical investigation of factors influencing integrated e-Government implementation in Nigeria: A case of housing and urban development agency. *Electron. J. Inf. Syst. Dev. Ctries.* **2018**, *84*, e12012. [CrossRef]
67. Dias, G.P. Determinants of e-government implementation at the local level: An empirical model. *Online Inf. Rev.* **2020**, *44*, 1307–1326. [CrossRef]
68. Gerunov, A.A. A Privacy-by-Design Implementation Methodology for E-Government. *Int. J. Electron. Gov. Res.* **2022**, *18*, 1–20. [CrossRef]
69. Park, C.H.; Kim, K. E-government as an anti-corruption tool: Panel data analysis across countries. *Int. Rev. Adm. Sci.* **2020**, *86*, 691–707. [CrossRef]
70. Wu, A.M.; Yan, Y.F.; Vyas, L. Public sector innovation, e-government, and anticorruption in China and India: Insights from civil servants. *Aust. J. Public Adm.* **2020**, *79*, 370–385. [CrossRef]
71. Khan, A.; Krishnan, S. Conceptualizing the impact of corruption in national institutions and national stakeholder service systems on e-government maturity. *Int. J. Inf. Manag.* **2019**, *46*, 23–36. [CrossRef]
72. Nam, T. Examining the anti-corruption effect of e-government and the moderating effect of national culture: A cross-country study. *Gov. Inf. Q.* **2018**, *35*, 273–282. [CrossRef]
73. Wang, L.H.; Luo, X.; Jurkat, M.P. Understanding Inconsistent Corruption Control through E-government Participation: Updated Evidence from a Cross-Country Investigation. *Electron. Commer. Res.* **2022**, *22*, 979–1006. [CrossRef]
74. Ramtohul, A.; Soyjaudah, K.M.S. Information security governance for e-services in southern African developing countries e-Government projects. *J. Sci. Technol. Policy Manag.* **2016**, *7*, 26–42. [CrossRef]
75. Zou, Q.; Mao, Z.; Yan, R.; Liu, S.; Duan, Z. Vision and reality of e-government for governance improvement: Evidence from global cross-country panel data. *Technol. Forecast. Soc. Change* **2023**, *194*, 122667. [CrossRef]
76. Lulaj, E.; Zarin, I.; Rahman, S. A Novel Approach to Improving E-Government Performance from Budget Challenges in Complex Financial Systems. *Complexity* **2022**, *2022*, 2507490. [CrossRef]
77. Ma, L.; Zheng, Y.P. National e-government performance and citizen satisfaction: A multilevel analysis across European countries. *Int. Rev. Adm. Sci.* **2019**, *85*, 506–526. [CrossRef]
78. Chen, Y.C.; Hu, L.T.; Tseng, K.C.; Juang, W.J.; Chang, C.K. Cross-boundary e-government systems: Determinants of performance. *Gov. Inf. Q.* **2019**, *36*, 449–459. [CrossRef]
79. Sharma, P.N.; Morgeson, F.V.; Mithas, S.; Aljazzaf, S. An empirical and comparative analysis of E-government performance measurement models: Model selection via explanation, prediction, and parsimony. *Gov. Inf. Q.* **2018**, *35*, 515–535. [CrossRef]

80. Abdulkareem, A.K.; Ramli, R.M. Evaluating the Performance of e-government: Does Citizens' Access to ICT Matter? *Pertanika J. Soc. Sci. Humanit.* **2021**, *29*, 1507–1534. [CrossRef]
81. Deng, H.P.; Karunasena, K.; Xu, W. Evaluating the performance of e-government in developing countries A public value perspective. *Internet Res.* **2018**, *28*, 169–190. [CrossRef]
82. Verkijika, S.F.; De Wet, L. Quality assessment of e-government websites in Sub-Saharan Africa: A public values perspective. *Electron. J. Inf. Syst. Dev. Ctries.* **2018**, *84*, e12015. [CrossRef]
83. Li, Y.; Shang, H.P. Service quality, perceived value, and citizens' continuous-use intention regarding e-government: Empirical evidence from China. *Inf. Manag.* **2020**, *57*, 103197. [CrossRef]
84. Kumar, R.; Kumar, R.; Sachan, A.; Gupta, P. An examination of the e-government service value chain. *Inf. Technol. People* **2021**, *34*, 889–911. [CrossRef]
85. Mensah, I.K.; Adams, S. A Comparative Analysis of the Impact of Political Trust on the Adoption of E-Government Services. *Int. J. Public Adm.* **2020**, *43*, 682–696. [CrossRef]
86. Sukhonos, V.; Pakhomov, V.; Pylypenko, V.; Kolesnikova, M.; Maletov, D. Administrative and legal bases of implementation of e-government in Ukraine. *Amazon. Investig.* **2022**, *11*, 24–36. [CrossRef]
87. Arayankalam, J.; Khan, A.; Krishnan, S. How to deal with corruption? Examining the roles of e-government maturity, government administrative effectiveness, and virtual social networks diffusion. *Int. J. Inf. Manag.* **2021**, *58*, 102203. [CrossRef]
88. Ma, L.; Zheng, Y.P. Does e-government performance actually boost citizen use? Evidence from European countries. *Public Manag. Rev.* **2018**, *20*, 1513–1532. [CrossRef]
89. Ejdys, J.; Ginevicius, R.; Rozsa, Z.; Janoskova, K. The Role of Perceived Risk and Security Level in Building Trust in e-Government Solutions. *Econ. Manag.* **2019**, *22*, 220–235. [CrossRef]
90. Nguyen-Duc, A.; Do, M.V.; Hong, Q.L.; Khac, K.N.; Quang, A.N. On the adoption of static analysis for software security assessment-A case study of an open-source e-government project. *Comput. Secur.* **2021**, *111*, 102470. [CrossRef]
91. Zhang, H.P.; Tang, Z.W.; Jayakar, K. A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-government services. *Telecommun. Policy* **2018**, *42*, 409–420. [CrossRef]
92. Politanskyi, V.; Lukianov, D.; Ponomarova, H.; Gyliaka, O. Information Security in E-Government: Legal Aspects. *Cuest. Politicas* **2021**, *39*, 361–372. [CrossRef]
93. Choi, M.; Lee, J.; Hwang, K. Information Systems Security (ISS) of E-Government for Sustainability: A Dual Path Model of ISS Influenced by Institutional Isomorphism. *Sustainability* **2018**, *10*, 1555. [CrossRef]
94. Alguliyev, R.; Aliguliyev, R.; Yusifov, F. Role of Social Networks in E-government: Risk Security Threats. *Online J. Commun. Media Technol.* **2018**, *8*, 363–376. [CrossRef]
95. Zubareva, O.O.; Byelov, S.V. Electronic Government System of Ukraine and a Method for Increasing Its Security. *Cybern. Syst. Anal.* **2015**, *51*, 481–488. [CrossRef]
96. Alharbi, N.; Papadaki, M.; Dowland, P. The impact of security and its antecedents in behaviour intention of using e-government services. *Behav. Inf. Technol.* **2017**, *36*, 620–636. [CrossRef]
97. Al-Hawamleh, A.M. Investigating the multifaceted dynamics of cybersecurity practices and their impact on the quality of e-government services: Evidence from the KSA. *Digit. Policy Regul. Gov.* **2024**, *26*, 317–336. [CrossRef]
98. Muneer, F.; Azam, A.; Yang, H.; Saeed, M. Examining Perceived Privacy, Perceived Security and Technology Anxiety into UMEGA in Improving Adoption Behavior of E-Government Services: An Evidence from Pakistan. *Int. J. Hum.-Comput. Interact.* **2024**, *40*, 1–13. [CrossRef]
99. Mustafa, G.; Rafiq, W.; Jhamat, N.; Arshad, Z.; Rana, F.A. Blockchain-based governance models in e-government: A comprehensive framework for legal, technical, ethical and security considerations. *Int. J. Law Manag.* **2025**, *67*, 37–55. [CrossRef]
100. Mishra, S.; Alowaidi, M.A.; Sharma, S.K. Impact of security standards and policies on the credibility of e-government. *J. Ambient Intell. Humaniz. Comput.* **2021**, *12*, 1–15. [CrossRef]
101. Hwang, K.; Choi, M. Effects of innovation-supportive culture and organizational citizenship behavior on e-government information system security stemming from mimetic isomorphism. *Gov. Inf. Q.* **2017**, *34*, 183–198. [CrossRef]