DIGITAL TRANSFORMATION AND ADMINISTRATION INNOVATION

Citation: Mozafari, A. (2027). Removing Barriers to the Implementation of E-Government: A Systematic Review. *Digital Transformation and Administration Innovation,* 5(1), 1-17.

Received date: 2026-04-07 Revised date: 2026-07-14 Accepted date: 2026-07-21 Initial published date: 2026-07-26 Final published date: 2027-01-01

Removing Barriers to the Implementation of E-Government: A Systematic Review

Amirreza Mozafari [1*]

1. Master's student, Department of Management and Accounting, Qa.C., Islamic Azad University, Qazvin, Iran

*Correspondence: 4311652577@iau.ir

Abstract

This study aimed to identify, classify, and synthesize the principal barriers to e-government implementation and the strategies proposed to eliminate or reduce them. This systematic review examined Persian- and English-language studies published between 2000 and 2025. Relevant publications were identified through searches of Scopus, Web of Science, ScienceDirect, SpringerLink, Emerald Insight, ProQuest, IEEE Xplore, Google Scholar, the Scientific Information Database, Magiran, Noormags, and IranDoc. Search terms addressed e-government, digital government, implementation, adoption, barriers, challenges, readiness, and facilitating strategies. After duplicate removal, title and abstract screening, full-text assessment, and methodological appraisal, 42 studies met the eligibility criteria and were included in the qualitative synthesis. Data were extracted using a researcher-developed form covering study characteristics, implementation barriers, proposed solutions, and principal conclusions. The findings were analyzed through qualitative thematic synthesis and constant comparison. The synthesis showed that e-government implementation barriers formed an interconnected socio-technical and institutional system rather than a set of isolated problems. Technological and infrastructural deficiencies were the most recurrent barriers, followed by organizational and managerial weaknesses, limited human-resource competencies, incomplete legal and regulatory frameworks, cultural resistance, financial constraints, security and privacy concerns, political and institutional instability, digital inequality, and insufficient citizen participation. The findings further indicated that infrastructure investment alone was insufficient because weak leadership, fragmented governance, poor data quality, inadequate employee readiness, and low public trust frequently prevented technological resources from producing sustainable outcomes. The most consistently proposed solutions included interoperable digital infrastructure, administrative process redesign, accountable leadership, workforce development, comprehensive legislation, stronger cybersecurity and privacy protection, sustainable financing, citizen-centered service design, public awareness, and inclusive access. Successful e-government implementation requires a coordinated, context-sensitive strategy that integrates technological modernization with organizational reform, legal development, data governance, employee capacity building, public trust, and digital inclusion.

Keywords: E-government; digital government; implementation barriers; public administration; digital transformation; systematic review

1. Introduction

The rapid expansion of information and communication technologies has fundamentally transformed the manner in which governments interact with citizens, businesses, employees, and other public institutions. Within this transformation, e-government has emerged as a central mechanism for modernizing public administration, improving access to services,

increasing operational efficiency, and strengthening the responsiveness of government institutions. E-government extends beyond the simple conversion of paper-based procedures into electronic formats; it involves the strategic use of digital technologies to redesign administrative processes, integrate governmental information systems, facilitate data exchange, and establish more transparent and citizen-centered forms of governance. In this sense, e-government represents both a technological innovation and an institutional reform agenda through which traditional bureaucratic structures are expected to become more flexible, interconnected, accountable, and capable of responding to changing public expectations. Contemporary approaches increasingly situate e-government within the broader concept of digital governance, emphasizing whole-of-government integration, cross-organizational coordination, and the development of common infrastructures rather than isolated digital projects within individual agencies (Memarzadeh et al., 2024; Muhdiarta et al., 2025; Panda et al., 2025).

The growing importance of e-government is closely associated with its potential to improve the efficiency and quality of public services. Digital platforms can reduce administrative delays, minimize repetitive procedures, lower transaction costs, and provide citizens with access to services without the limitations of time and geographical location. By integrating databases and automating routine operations, governments can reduce redundant information requests, facilitate faster decision-making, and allocate public resources more effectively. E-government may also support economic resilience by decreasing administrative costs, simplifying business-government interactions, improving regulatory implementation, and increasing the transparency of economic processes. In sectors such as taxation, the use of electronic systems can improve information exchange, strengthen monitoring capacity, and reduce opportunities for noncompliance and tax evasion when supported by adequate information and communication technology infrastructure. At the organizational level, digital government systems may also improve employee performance by clarifying procedures, increasing access to relevant information, and strengthening organizational transparency. Therefore, the value of e-government is not confined to service convenience but extends to institutional productivity, economic management, administrative discipline, and the more efficient achievement of public-policy objectives (Farahani & Babaeianpour, 2024; Gholami et al., 2024; Zamani et al., 2024).

Transparency and accountability constitute additional central objectives of e-government implementation. Digital systems can make administrative procedures more traceable, reduce discretionary interventions, facilitate the monitoring of institutional performance, and provide citizens with greater access to governmental information. When public services are delivered through standardized and documented electronic processes, opportunities for hidden decision-making, selective treatment, and informal administrative practices may be reduced. E-government can therefore contribute to the development of clearer lines of responsibility and more observable interactions between citizens and public institutions. The implementation of smart-city initiatives and integrated digital services has similarly been associated with efforts to enhance transparency and accountability in public-service delivery. However, these outcomes are not produced automatically by the introduction of technology. Transparency depends on the design of systems, the availability and accuracy of information, the willingness of organizations to disclose relevant data, and the existence of mechanisms through which citizens can evaluate or challenge administrative decisions. Consequently, e-government development must be coordinated with administrative transparency programs and governance reforms if digital platforms are to create meaningful institutional accountability rather than merely changing the technical medium through which existing procedures are performed (Chabok et al., 2025; Margareta et al., 2025; Raeisi et al., 2024).

Public trust is particularly important because the sustainability of e-government depends on citizens' willingness to use digital services and provide personal information through governmental platforms. Trust is shaped by multiple factors, including perceptions of government competence, service quality, system security, institutional integrity, responsiveness, transparency, and the protection of personal data. Evidence indicates that e-government development and the quality of governance can jointly influence public trust, suggesting that citizens evaluate digital services within the broader context of their confidence in government institutions. When digital platforms are reliable, accessible, and responsive, they may reinforce perceptions that government is capable and service-oriented. Conversely, system failures, unclear procedures, poor communication, or concerns regarding data misuse can intensify skepticism and reduce citizens' willingness to adopt electronic channels. In countries where confidence in public institutions is already fragile, the implementation of e-government may therefore face an additional legitimacy challenge. Citizens must be convinced not only that electronic systems function

technically but also that government institutions will use data responsibly, respond to problems fairly, and protect users against misuse, unauthorized access, and administrative harm (Alsaad et al., 2024; Kenfack & Check, 2024; Nguyen et al., 2024).

The continued use of e-government services is also influenced by users' experiences with system quality, information quality, service quality, and perceived usefulness. Initial adoption does not necessarily lead to sustained use, because citizens may return to face-to-face services when digital platforms are difficult to navigate, unreliable, incomplete, or unable to provide a full transaction from beginning to end. User satisfaction therefore serves as an important link between technological design and long-term acceptance. When systems are easy to use, provide accurate and relevant information, process requests efficiently, and offer appropriate technical support, citizens are more likely to continue using them and develop greater trust in digital government. Electronic loyalty is similarly affected by e-service quality and e-trust, while system anxiety may weaken the relationship between favorable perceptions and continued use. These findings demonstrate that successful implementation cannot be measured solely by the number of services placed online. It must also be evaluated through actual utilization, satisfaction, continuity of use, user confidence, and the extent to which electronic services are perceived as superior or at least equivalent to conventional administrative channels (Kala et al., 2024; Nawafleh & Khasawneh, 2024; Shahzad et al., 2024).

Despite the recognized benefits of e-government, its implementation remains a complex and difficult process in many countries. Governments frequently encounter technological, organizational, human, financial, legal, political, cultural, and social barriers that prevent digital initiatives from achieving their intended outcomes. Technological obstacles may include weak internet infrastructure, outdated hardware and software, fragmented databases, inadequate cybersecurity, limited interoperability, and the absence of common standards. Organizational barriers may involve resistance to change, bureaucratic rigidity, insufficient leadership commitment, unclear institutional responsibilities, poor interagency coordination, and the failure to redesign administrative processes before digitization. Human-resource constraints include limited digital literacy, inadequate training, shortages of specialized personnel, fear of job displacement, and low motivation among employees. Citizens may also encounter barriers related to insufficient digital skills, unequal access to technology, distrust of online transactions, language limitations, and the perceived complexity of electronic systems. These dimensions often interact, meaning that weaknesses in one domain may intensify barriers in another. For example, inadequate training may lead to operational errors, which reduce service quality and public trust, while poor coordination may produce incompatible systems that increase costs and frustrate users (Panda et al., 2025; Shahzad et al., 2024; Tavazooi Far, 2024).

A major implementation challenge concerns the integration of systems and data across governmental organizations. Many e-government programs have developed incrementally, with separate ministries and agencies designing independent platforms according to their own technical standards, institutional priorities, and administrative procedures. This fragmented development can produce duplicated databases, inconsistent information, repeated authentication requirements, and services that remain disconnected from one another. Unified government platforms have therefore been proposed as a means of facilitating integrated access, reducing duplication, and providing citizens with a single interface for multiple public services. Nevertheless, platform integration requires more than technical connectivity. It depends on shared data definitions, clear governance structures, institutional cooperation, secure identity-management mechanisms, and agreements concerning data ownership and responsibility. Innovation-oriented government teams may play an important role in coordinating such reforms by combining technical expertise with administrative authority, agile project management, and the capacity to work across institutional boundaries. The experience of public-sector innovation units shows that specialized and empowered teams can accelerate digital transformation, although their effectiveness depends on sustained political support, access to data, organizational legitimacy, and the ability to institutionalize innovations beyond individual projects (Chabok et al., 2025; Deligiannis & Peristeras, 2025; Popescu et al., 2024).

Data quality and data governance are equally fundamental to the effective operation of e-government. Government decisions and public services increasingly depend on the collection, processing, sharing, and analysis of large volumes of administrative data. Inaccurate, incomplete, outdated, duplicated, or inconsistent information can undermine the reliability of services, generate incorrect decisions, and reduce both employee and citizen confidence in digital systems. Data-quality problems may originate from fragmented institutional responsibilities, inconsistent registration practices, weak validation mechanisms, legacy systems, and the absence of clear data standards. These problems are particularly serious when information is shared across

organizations, because errors in one database can be transmitted throughout interconnected systems. Effective data governance therefore requires clearly defined responsibilities for data production, verification, storage, access, updating, sharing, and protection. It also requires mechanisms for monitoring data quality and resolving inconsistencies. In the Iranian context, the relationship between data quality and data governance has been identified as a major issue affecting the effectiveness and credibility of e-government. Without reliable data, even technologically advanced systems may reproduce administrative errors at greater speed and scale rather than improving governance (Popescu et al., 2024; Sahraei, 2025; Yu, 2024).

Security and privacy present another set of interrelated challenges. The concentration and exchange of governmental data can increase exposure to cyberattacks, unauthorized access, identity theft, service disruption, surveillance concerns, and the misuse of personal information. Emerging technologies such as blockchain offer potential advantages for transaction integrity, traceability, distributed verification, and tamper resistance, but they also introduce technical, regulatory, scalability, privacy, and governance risks. The adoption of advanced technologies should therefore be based on a careful assessment of public-sector needs rather than on technological enthusiasm alone. Citizens must understand how their information is collected, stored, processed, and shared, and they must have confidence that appropriate legal and technical safeguards are in place. Security must be incorporated into system architecture from the design stage and supported by encryption, authentication, access control, auditing, incident-response procedures, and continuous risk assessment. At the same time, excessive security procedures can make systems difficult to use and may discourage adoption. Successful implementation consequently requires a balance between protection, accessibility, usability, and institutional accountability (Kenfack & Check, 2024; Nawafleh & Khasawneh, 2024; Yu, 2024).

The governance of e-government implementation is also shaped by political and managerial factors. Digital transformation requires clear strategic direction, continuity of policy, stable financing, accountable leadership, and coordination among public organizations. Projects may fail when they are treated as temporary technical initiatives rather than as long-term institutional reforms. Frequent changes in political priorities, dependence on individual managers, fragmented budgeting, and competition among government agencies can prevent sustained implementation. Furthermore, the development of e-government may challenge established distributions of authority by making information more accessible, standardizing procedures, and reducing discretionary control. Organizational actors who benefit from existing arrangements may consequently resist transformation, either openly or through delayed cooperation, incomplete data sharing, and limited use of new systems. Effective governance models should therefore clarify the roles of political leaders, senior managers, information technology units, legal departments, service providers, and citizens. They should also establish measurable objectives, accountability mechanisms, and continuous evaluation procedures. In addition, e-government governance increasingly needs to support digital business development, interorganizational ecosystems, and forms of public-private interaction that extend beyond conventional administrative boundaries (Chabok et al., 2025; Deligiannis & Peristeras, 2025; Farahani & Babaeianpour, 2024).

The diversity of e-government barriers indicates that no single intervention can ensure successful implementation. Investment in infrastructure is essential, but infrastructure alone cannot resolve organizational resistance, unclear legislation, poor data quality, or low citizen trust. Employee training is necessary, but its effects may remain limited when managers do not support process change or when systems are unreliable. Similarly, legal reforms may establish the validity of digital transactions, but citizens may still avoid electronic services if platforms are difficult to use or if they lack adequate access to technology. A comprehensive approach must therefore combine technological modernization, administrative process redesign, human-resource development, legal and regulatory reform, data governance, cybersecurity, citizen participation, and mechanisms for digital inclusion. The transformation of public services should also be guided by an understanding of local administrative capacity, technological maturity, socioeconomic conditions, and public expectations. Strategies that succeed in digitally advanced settings may not be directly transferable to contexts characterized by limited infrastructure, fragmented institutions, or lower levels of digital literacy. Context-sensitive implementation is consequently essential for converting general principles of e-government into feasible and sustainable reforms (Memarzadeh et al., 2024; Muhdiarta et al., 2025; Tavazooi Far, 2024).

The growing volume of research on e-government has generated a wide range of findings regarding barriers, facilitating conditions, implementation models, and improvement strategies. However, the evidence remains dispersed across different disciplines, countries, levels of government, and methodological traditions. Some studies emphasize technological readiness

and system integration, whereas others focus on trust, service quality, transparency, organizational change, or legal and institutional capacity. This fragmentation makes it difficult for policymakers and administrators to determine which barriers are most frequently reported, how different barriers interact, and which strategies have been proposed to address them. A systematic review can contribute to this field by organizing the available evidence into coherent categories, identifying recurring and context-specific challenges, and synthesizing practical approaches for reducing implementation obstacles. Such a synthesis is particularly important because contemporary e-government initiatives increasingly involve complex interdependencies among technology, institutions, employees, citizens, and data. Understanding these relationships can help prevent governments from addressing visible technical problems while overlooking the organizational and societal conditions that ultimately determine whether digital reforms are accepted and sustained (Kala et al., 2024; Nguyen et al., 2024; Raeisi et al., 2024; Sahraei, 2025).

Accordingly, the present systematic review aimed to identify, classify, and synthesize the principal barriers to the implementation of e-government and the strategies proposed for removing or reducing these barriers.

2. Methods and Materials

This study was conducted using a systematic review design to identify, classify, and synthesize the barriers to the successful implementation of e-government and the strategies proposed for removing or reducing these barriers. The review process was designed in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses guidelines to ensure transparency, methodological rigor, and reproducibility. The study population consisted of all Persian- and English-language scholarly publications addressing the barriers, challenges, limitations, facilitating conditions, and implementation requirements of e-government. Electronic searches were conducted for studies published from January 2000 to December 2025, a period selected to cover the expansion of e-government initiatives from their early development to more recent stages of digital government transformation. Following the identification and screening process, 42 studies met all eligibility criteria and were included in the final qualitative synthesis. The included sample comprised peer-reviewed journal articles, conference papers with complete methodological and findings sections, and relevant research reports that directly examined e-government implementation barriers at the national, organizational, administrative, technological, legal, social, or cultural level. Studies were included when they focused explicitly on e-government implementation, reported identifiable barriers or challenges, provided empirical or systematically developed conceptual findings, and made the full text available in either Persian or English. Studies were excluded when they addressed only technical descriptions of electronic services without examining implementation barriers, concentrated exclusively on e-commerce or private-sector digitalization, lacked sufficient methodological information, were published as editorials, book reviews, news items, dissertations without accessible full text, or duplicated findings already reported in another publication. Duplicate records were removed before screening. The titles and abstracts of the remaining studies were independently examined for relevance, after which potentially eligible papers underwent full-text assessment. Any uncertainty regarding the inclusion of a study was resolved through repeated examination of its objectives, methodology, and findings until a final decision was reached.

Data were collected through a structured literature search and a researcher-developed data extraction form. Relevant studies were identified through systematic searches of international databases, including Scopus, Web of Science, PubMed, ScienceDirect, SpringerLink, Emerald Insight, ProQuest, IEEE Xplore, and Google Scholar, as well as Persian-language databases such as the Scientific Information Database, Magiran, Noormags, and the Iranian Research Institute for Information Science and Technology. The search strategy was developed through combinations of controlled terms and free-text keywords related to e-government and its implementation barriers. The principal English search terms included “e-government,” “electronic government,” “digital government,” “e-governance,” “e-government implementation,” “adoption of e-government,” “barriers,” “obstacles,” “challenges,” “constraints,” “implementation problems,” “critical factors,” “readiness,” “resistance,” and “facilitators.” Equivalent Persian terms were also used. Boolean operators such as AND and OR were applied to combine the keywords and improve the sensitivity and specificity of the search. Reference lists of the eligible publications were also manually examined to identify additional studies that might not have appeared in the database searches. The data extraction form recorded the author or authors, publication year, country or geographical context, study purpose, research design, study population, sample characteristics, data collection method, analytical approach, identified barriers, proposed

solutions, and principal conclusions. To assess the methodological quality of the included studies, appraisal criteria appropriate to qualitative, quantitative, mixed-method, and review studies were applied. The quality assessment considered the clarity of the research question, appropriateness of the research design, adequacy of the sampling procedure, validity of the data collection tools, transparency of the analysis, consistency between the findings and conclusions, and relevance of the study to the objectives of the systematic review. Studies with serious methodological deficiencies or insufficient information for extracting findings were excluded. To improve the reliability of data collection, the extracted information was reviewed on two separate occasions, and the original full texts were re-examined whenever inconsistencies or ambiguities were detected.

The extracted data were analyzed using qualitative thematic synthesis. The analysis began with repeated reading of the findings and conclusions of all 42 included studies to obtain a comprehensive understanding of the reported barriers to e-government implementation. Relevant statements, concepts, factors, and recommendations were identified and entered into an initial coding framework. Similar concepts were compared, merged, and organized into descriptive codes. The codes were subsequently grouped into broader categories according to their conceptual similarities and their position within the process of e-government implementation. Through an iterative process of constant comparison, the identified barriers were classified into major themes, including technological and infrastructural barriers, organizational and managerial barriers, human-resource and competency barriers, legal and regulatory barriers, financial and economic barriers, cultural and social barriers, political and institutional barriers, information-security and privacy barriers, and barriers associated with digital inequality and citizen readiness. Proposed strategies for overcoming these barriers were analyzed in parallel and categorized according to the corresponding barrier domains. These strategies included the development of information and communication technology infrastructure, enhancement of interoperability among government systems, improvement of managerial commitment, redesign of administrative processes, strengthening of digital competencies, establishment of comprehensive legal frameworks, allocation of sustainable financial resources, protection of information security and personal privacy, promotion of public trust, and expansion of equitable access to electronic services. Both the frequency and conceptual significance of the identified themes were considered during interpretation. Frequency was used to determine how commonly each barrier appeared across the included studies, while conceptual significance was used to identify barriers that had a fundamental or cross-cutting influence on the implementation process, even when they were reported in a smaller number of studies. The final synthesis was developed by comparing findings across different countries, administrative contexts, research methods, and levels of government. Particular attention was paid to convergent findings, contradictory results, contextual differences, and relationships among the identified barriers. To enhance analytical credibility, the coding structure and thematic classifications were repeatedly reviewed against the original studies, and categories were refined until they were sufficiently distinct, internally coherent, and capable of representing the range of evidence included in the review.

3. Findings and Results

The systematic search and screening process resulted in the inclusion of 42 studies that met the predetermined eligibility and quality criteria. The publication years of the included studies ranged from 2001 to 2025, although most were published during the period in which e-government programs expanded from the initial digitization of public services toward more integrated forms of digital government. Of the 42 studies, 5 studies (11.9%) were published between 2001 and 2005, 7 studies (16.7%) between 2006 and 2010, 9 studies (21.4%) between 2011 and 2015, 12 studies (28.6%) between 2016 and 2020, and 9 studies (21.4%) between 2021 and 2025. In terms of geographical distribution, 14 studies (33.3%) were conducted in Asian countries other than Iran, 11 studies (26.2%) were conducted in Iran, 6 studies (14.3%) originated from European countries, 4 studies (9.5%) were conducted in African countries, 3 studies (7.1%) were undertaken in North America, 2 studies (4.8%) were conducted in Middle Eastern countries other than Iran, and 2 studies (4.8%) examined multiple countries or adopted an international comparative perspective. Regarding methodological orientation, 15 studies (35.7%) used quantitative designs, 13 studies (31.0%) applied qualitative methods, 8 studies (19.0%) used mixed-method designs, and 6 studies (14.3%) were conceptual, analytical, or secondary review studies. The quantitative studies generally relied on surveys of public-sector employees, managers, information technology specialists, citizens, and users of electronic public services, whereas the qualitative studies commonly used interviews, focus groups, expert panels, and document analysis. The reported sample sizes of empirical studies varied substantially, ranging from 12 participants in expert-based qualitative research to more than 2,000

citizen respondents in large-scale surveys. Most studies focused on national or central-government e-government programs, while others examined municipal governments, local public organizations, ministries, public universities, healthcare organizations, tax administrations, and other government agencies. Across these different contexts, the included studies consistently demonstrated that e-government implementation was influenced by an interconnected set of technological, organizational, human, legal, financial, cultural, political, security, and accessibility-related conditions.

Table 1. General Characteristics of the Studies Included in the Systematic Review

Study characteristic	Category	Number of studies	Percentage
Publication period	2001–2005	5	11.9
	2006–2010	7	16.7
	2011–2015	9	21.4
	2016–2020	12	28.6
	2021–2025	9	21.4
Geographical context	Iran	11	26.2
	Other Asian countries	14	33.3
	Europe	6	14.3
	Africa	4	9.5
	North America	3	7.1
	Other Middle Eastern countries	2	4.8
	Multinational or international	2	4.8
Research design	Quantitative	15	35.7
	Qualitative	13	31.0
	Mixed methods	8	19.0
	Conceptual, analytical, or review	6	14.3
Primary unit of analysis	Government employees and managers	13	31.0
	Citizens or users of public services	10	23.8
	Information technology experts	7	16.7
	Government organizations or administrative systems	6	14.3
	Policy documents and previous studies	6	14.3
Administrative level	National or central government	19	45.2
	Ministries and specialized public agencies	10	23.8
	Provincial, municipal, or local government	8	19.0
	Multiple administrative levels	5	11.9

As shown in Table 1, the included evidence was distributed across different publication periods, geographical settings, methodological approaches, participant groups, and administrative levels. The largest proportion of studies was published between 2016 and 2020, accounting for 28.6% of the total sample. This concentration indicates that scholarly attention to implementation barriers increased during the period in which governments increasingly moved beyond the provision of isolated online services toward integrated platforms, data-sharing arrangements, digital identity systems, and more complex forms of electronic interaction. Nevertheless, nearly half of the included studies were published after 2015, demonstrating the continuing relevance of implementation barriers despite technological development and the increasing availability of digital tools. Geographically, studies from Asian countries represented the largest share of the evidence. When the 11 Iranian studies were considered alongside the 14 studies from other Asian countries, 59.5% of the included publications originated from Asia. This finding suggests that e-government implementation has attracted substantial attention in developing and transitional administrative systems, where governments have often attempted to modernize public services while simultaneously confronting infrastructural limitations, administrative fragmentation, regulatory uncertainty, unequal digital access, and public trust concerns. Quantitative studies constituted the most common methodological category, although qualitative and mixed-method research together represented half of the included sample. This methodological diversity allowed the review to integrate measurable relationships among readiness factors with deeper explanations of organizational resistance, managerial behavior, institutional culture, citizen attitudes, and implementation experiences. Government employees and managers were the most frequently examined unit of analysis, indicating that the organizational and administrative dimensions of e-government received greater attention than purely citizen-centered issues. Furthermore, 45.2% of the studies addressed national or central-government programs, whereas only 19.0% focused specifically on provincial, municipal, or local government. This distribution indicates that the evidence base has emphasized national policy and central administrative systems, while

implementation conditions at local levels, where infrastructure and human-resource inequalities may be more pronounced, have received comparatively less systematic attention.

Table 2. Identified Barriers to the Implementation of E-Government

Main barrier domain	Major barriers identified in the included studies	Number of studies reporting the domain	Percentage of studies
Technological and infrastructural barriers	Inadequate internet coverage, outdated hardware and software, unstable networks, fragmented databases, lack of interoperability, absence of common technical standards, weak system integration, limited data centers, and insufficient maintenance capacity	35	83.3
Organizational and managerial barriers	Resistance to organizational change, insufficient managerial commitment, unclear responsibilities, weak coordination, bureaucratic rigidity, fragmented decision-making, lack of implementation planning, and limited monitoring mechanisms	33	78.6
Human-resource and competency barriers	Limited digital literacy, shortage of qualified specialists, inadequate training, lack of technical support, low employee motivation, fear of job displacement, and insufficient change-management skills	30	71.4
Legal and regulatory barriers	Incomplete legislation, unclear legal validity of electronic records, weak data-protection rules, lack of digital-signature regulation, uncertainty regarding institutional accountability, and inconsistent administrative procedures	26	61.9
Cultural and social barriers	Preference for face-to-face services, low public awareness, mistrust of electronic transactions, resistance to new technologies, limited culture of information sharing, and concerns regarding the reliability of online services	25	59.5
Financial and economic barriers	High implementation and maintenance costs, inadequate budget allocation, unstable funding, limited return-on-investment assessment, unequal resource distribution, and dependence on short-term project financing	23	54.8
Information-security and privacy barriers	Cybersecurity vulnerabilities, fear of unauthorized access, identity theft, weak access controls, insufficient security protocols, lack of incident-response capacity, and public concern about misuse of personal data	22	52.4
Political and institutional barriers	Changes in political priorities, weak policy continuity, insufficient high-level support, competition among agencies, political interference, centralized decision-making, and limited institutional accountability	19	45.2
Digital-divide and accessibility barriers	Unequal access to devices and internet services, rural–urban disparities, socioeconomic inequalities, limited accessibility for older adults and persons with disabilities, and low digital readiness among disadvantaged groups	18	42.9
Citizen participation and service-design barriers	Limited user involvement, inadequate needs assessment, poor interface design, complex service procedures, insufficient feedback channels, lack of multilingual content, and low perceived usefulness	16	38.1

The findings presented in Table 2 demonstrate that barriers to e-government implementation were multidimensional and mutually reinforcing rather than isolated technical problems. Technological and infrastructural barriers were the most frequently reported category and appeared in 35 of the 42 studies, representing 83.3% of the evidence base. These barriers included inadequate communication infrastructure, obsolete information systems, fragmented databases, poor interoperability, unstable connectivity, and the absence of common technical standards across government organizations. The repeated identification of these problems indicates that the implementation of e-government depends not merely on purchasing computers or developing individual websites but on establishing an integrated digital architecture capable of supporting secure information exchange, uninterrupted service delivery, and coordination among public institutions. In many studies, separate government agencies had developed incompatible systems, resulting in duplicated data collection, repeated citizen authentication, inconsistent records, and the continued need for paper-based procedures. Therefore, technological fragmentation frequently reproduced existing administrative fragmentation rather than resolving it.

Organizational and managerial barriers were reported in 33 studies, making them the second most common barrier domain. These findings showed that even where adequate technology was available, implementation was often weakened by resistance to change, limited managerial commitment, unclear institutional responsibilities, bureaucratic procedures, and insufficient coordination among agencies. Several studies indicated that e-government projects were treated as temporary information technology initiatives rather than as comprehensive programs of administrative transformation. As a result, responsibility was commonly delegated exclusively to technical departments without corresponding changes in organizational structures, work processes, performance indicators, or decision-making arrangements. The lack of sustained leadership support also reduced the authority of implementation teams and limited their ability to resolve interdepartmental conflicts. Human-resource and competency barriers were identified in 30 studies, confirming that employee knowledge, motivation, confidence, and

adaptability constituted essential determinants of implementation success. Public employees sometimes perceived electronic systems as threats to occupational security, established routines, professional autonomy, or organizational status. Inadequate training intensified these concerns because employees were expected to use new systems without sufficient technical preparation or ongoing support. In addition, governments frequently experienced shortages of specialists in systems analysis, cybersecurity, database management, digital-service design, and project management.

Legal and regulatory barriers were found in 61.9% of the included studies. These barriers involved ambiguity regarding electronic signatures, the evidentiary value of digital documents, data ownership, interagency data sharing, privacy protection, accountability for system failures, and legal responsibility for unauthorized disclosure. The absence of comprehensive and enforceable regulations reduced both institutional willingness to exchange information and citizen confidence in electronic transactions. Cultural and social barriers were similarly important, appearing in 25 studies. These findings revealed that some citizens and employees continued to prefer traditional in-person services because they perceived physical documents, direct interaction, and handwritten signatures as more trustworthy. Low awareness of electronic services, limited understanding of their benefits, and previous negative experiences with unreliable systems also reduced adoption. Financial barriers were reported in more than half of the studies and were particularly evident in developing countries and local government settings. E-government projects required substantial initial investment as well as continuing expenditure for maintenance, security, system upgrading, training, technical support, and service redesign. Where funding was allocated only for initial system development, projects often became obsolete or nonfunctional after their formal launch.

Information-security and privacy concerns were reported in 22 studies. These concerns were not limited to technical vulnerability but also included weak institutional procedures for access control, data classification, identity management, incident reporting, and accountability. Citizen fear regarding surveillance, misuse of personal data, and unauthorized disclosure weakened trust and reduced willingness to use online public services. Political and institutional barriers were identified in 19 studies and included policy discontinuity following changes in government, competition among public agencies, weak political ownership, and the prioritization of visible short-term projects over long-term institutional integration. Digital-divide and accessibility barriers appeared in 18 studies, showing that electronic service delivery could deepen inequality when governments failed to account for differences in income, education, age, disability, language, geographical location, and access to reliable internet services. Finally, barriers related to citizen participation and service design were reported less frequently than technological and organizational barriers, but they remained conceptually important. Systems developed without user consultation were often complex, difficult to navigate, poorly adapted to actual citizen needs, and unable to generate sufficient perceived usefulness. Collectively, these results indicate that e-government implementation should be understood as a socio-technical and institutional transformation process in which technical infrastructure, legal arrangements, administrative capacity, employee readiness, political support, and citizen trust must be developed simultaneously.

Table 3. Strategies for Removing or Reducing E-Government Implementation Barriers

Strategic domain	Recommended strategies synthesized from the included studies	Number of studies proposing the strategy	Percentage of studies
Development of integrated digital infrastructure	Expansion of broadband access, modernization of hardware and software, establishment of shared platforms, development of government cloud services, creation of interoperable databases, adoption of common technical standards, and continuous system maintenance	34	81.0
Organizational reform and process redesign	Simplification of administrative procedures, elimination of duplicated processes, clarification of organizational responsibilities, establishment of cross-agency governance structures, integration of electronic and administrative reforms, and continuous performance monitoring	32	76.2
Leadership commitment and implementation governance	Appointment of accountable senior leaders, formulation of a clear national strategy, creation of implementation roadmaps, strengthening of interagency coordination, establishment of measurable indicators, and continuity of political and managerial support	31	73.8
Capacity building and human-resource development	Continuous employee training, digital-literacy programs, recruitment and retention of information technology specialists, establishment of technical-support units, change-management education, and development of incentives for system use	29	69.0
Legal and regulatory strengthening	Enactment of comprehensive e-government legislation, recognition of electronic signatures and records, development of data-protection laws, clarification of institutional accountability, regulation of interagency data exchange, and establishment of enforceable cybersecurity standards	26	61.9

Security, privacy, and trust enhancement	Adoption of multilayer security systems, strong authentication, encryption, regular security audits, privacy-by-design practices, incident-response plans, transparent data-use policies, and public communication regarding security protections	24	57.1
Sustainable financing and resource allocation	Multiyear budgeting, prioritization of high-impact projects, lifecycle cost assessment, equitable allocation of resources, public–private cooperation under regulatory oversight, and dedicated funding for maintenance and system upgrading	22	52.4
Citizen-centered service design and participation	Involvement of users in service design, usability testing, simplification of interfaces, development of integrated service portals, provision of feedback mechanisms, multilingual access, mobile compatibility, and measurement of citizen satisfaction	21	50.0
Public awareness and cultural change	Awareness campaigns, digital-literacy education for citizens, communication of service benefits, promotion of information-sharing culture, demonstration of successful applications, and provision of assisted digital-service centers	20	47.6
Digital inclusion and equitable access	Expansion of rural connectivity, subsidized access for disadvantaged groups, accessible design for persons with disabilities, alternative service channels, public internet centers, mobile-based services, and targeted support for older adults	18	42.9

As presented in Table 3, the most frequently proposed strategy for overcoming implementation barriers was the development of integrated digital infrastructure, which was recommended in 34 studies. The synthesis showed that infrastructure development should extend beyond increasing internet availability and include interoperability, common data standards, secure shared platforms, government cloud infrastructure, reliable identification systems, and long-term maintenance arrangements. A recurring recommendation was the establishment of architecture through which public organizations could exchange verified information without requiring citizens to repeatedly submit the same documents. Integrated infrastructure was also considered essential for reducing administrative duplication, improving service speed, increasing data accuracy, and enabling coordinated decision-making. However, the reviewed studies emphasized that technical integration should be accompanied by clearly defined data-governance rules because unrestricted or poorly regulated data sharing could create new privacy and accountability risks.

Organizational reform and administrative process redesign were recommended in 32 studies. This finding indicates that digitizing inefficient procedures without first examining their necessity, sequence, and institutional logic may simply transfer bureaucratic complexity from paper-based environments to electronic platforms. The studies therefore recommended mapping existing processes, eliminating unnecessary approvals, reducing duplicated documentation, clarifying decision authority, and redesigning services around citizen needs rather than around the internal structure of government agencies. Leadership commitment and effective implementation governance were also identified as central strategies. Thirty-one studies emphasized the need for high-level political and managerial support, clear national objectives, accountable implementation structures, interagency coordination mechanisms, and measurable indicators of progress. Leadership was especially important for resolving conflicts between institutions, compelling compliance with common standards, maintaining policy continuity, and protecting long-term digital projects from frequent administrative changes. The findings further suggested that implementation responsibility should not be confined to information technology departments. Instead, e-government governance should involve senior managers, legal experts, process owners, human-resource units, security specialists, financial officers, and representatives of service users.

Capacity building and human-resource development were proposed in 29 studies. The reviewed evidence indicated that one-time introductory training was insufficient because digital systems, security threats, administrative requirements, and user expectations continually evolved. Effective capacity-building programs therefore needed to include technical skills, data protection, cybersecurity awareness, digital communication, service design, project management, and organizational change. Employees also required practical opportunities to use new systems, access to technical assistance, and incentives linked to effective adoption. The retention of skilled information technology personnel was described as particularly important because public agencies often lost qualified specialists to the private sector due to limited career progression, inflexible recruitment systems, and uncompetitive compensation. Change-management interventions were similarly required to address employee concerns about increased monitoring, reduced authority, job displacement, or disruption of familiar work practices.

Legal and regulatory strengthening was recommended by 26 studies and included formal recognition of electronic records and signatures, comprehensive data-protection legislation, regulation of digital identity, clear rules for data sharing, and explicit institutional accountability. These legal foundations were expected to reduce uncertainty among government organizations and strengthen citizen confidence in electronic transactions. Security, privacy, and trust-enhancement strategies were proposed in

24 studies. Recommended measures included encryption, secure authentication, access-control systems, regular vulnerability assessment, security audits, incident-response procedures, staff training, and transparent privacy policies. The findings showed that public trust could not be established through technical security alone. Citizens also needed clear information about what data were collected, why they were collected, how they would be used, which institutions could access them, and what remedies were available in cases of misuse or system failure.

Sustainable financing was identified as another essential strategy. Twenty-two studies recommended multiyear budgeting and lifecycle-based financial planning rather than limiting expenditure to the initial development of systems. Financial plans needed to include maintenance, staff development, cybersecurity, system integration, software licensing, data migration, user support, evaluation, and future upgrading. Some studies recommended carefully regulated public–private partnerships where government organizations lacked sufficient technical capacity, although they also warned that outsourcing without strong contractual and regulatory controls could create dependency, data-ownership disputes, and security risks. Citizen-centered service design and participation were proposed in half of the included studies. These strategies included involving citizens in needs assessment, conducting usability testing, simplifying interfaces and language, improving mobile compatibility, developing integrated portals, and creating effective complaint and feedback mechanisms. The evidence indicated that citizen adoption increased when electronic services were easier, faster, more transparent, and demonstrably more useful than conventional channels.

Public-awareness and cultural-change programs were suggested in 20 studies. These studies emphasized that governments should clearly communicate the availability, advantages, procedures, and security features of electronic services. Demonstrating successful services and providing assisted access could gradually reduce mistrust and increase familiarity. Finally, 18 studies recommended targeted measures to reduce digital inequality, including rural connectivity programs, accessible interfaces, public internet centers, mobile service delivery, support for disadvantaged citizens, and the retention of alternative service channels during transition periods. These measures were essential because compulsory digitalization without adequate access and support could exclude populations that were already vulnerable. Overall, the proposed strategies demonstrated that removing barriers to e-government implementation requires a coordinated policy package rather than a single intervention. The most effective approach combines infrastructure development, institutional reform, leadership, legal protection, employee capability, sustainable financing, security, citizen participation, and digital inclusion.

A comparative synthesis of the included studies further revealed that the importance and interaction of barriers varied according to the level of administrative and technological development. Studies conducted in contexts with limited digital infrastructure gave greater emphasis to connectivity, equipment, funding, and technical expertise, whereas studies from countries with relatively advanced infrastructure focused more strongly on interoperability, privacy, cybersecurity, data governance, citizen trust, and cross-agency integration. In developing administrative systems, technological barriers were often closely associated with organizational instability and limited financial capacity. Public organizations purchased systems through separate projects, used different standards, and lacked resources for maintenance or integration. By contrast, in more technologically mature settings, the primary challenge was not the absence of digital services but the difficulty of coordinating existing services, sharing data lawfully, and ensuring user-centered design. These differences indicate that strategies for removing implementation barriers should be adapted to institutional maturity rather than transferred uniformly from one setting to another.

The analysis also showed that barriers frequently formed cumulative causal chains. For example, inadequate funding limited infrastructure development and employee training; weak training increased resistance and operational errors; operational failures reduced service quality; poor service quality weakened citizen trust; and low citizen use reduced political and managerial motivation to invest further in electronic systems. Similarly, unclear legislation discouraged agencies from sharing information, which prevented system integration and required citizens to provide the same information repeatedly. These repetitive procedures reduced the perceived usefulness of electronic services and reinforced preference for face-to-face interaction. Consequently, barriers should not be prioritized exclusively according to frequency. Although technological problems appeared most often, organizational leadership, legal certainty, and public trust frequently operated as enabling conditions that determined whether technological investment produced sustainable outcomes.

Another important finding concerned the transition from e-government as service automation to digital government as institutional transformation. Earlier studies commonly defined implementation success in terms of the number of government

websites, online forms, or electronically available services. More recent studies increasingly evaluated success through integration, user experience, transparency, participation, data-driven decision-making, accessibility, and organizational change. This shift suggests that merely placing services online cannot be considered sufficient evidence of successful implementation. In several studies, services were technically available but remained underused because processes were complex, systems were unreliable, citizens were unaware of them, or users still had to visit government offices to complete identity verification, payment, or document submission. Therefore, complete service delivery, interoperability, usability, and measurable public value emerged as more meaningful indicators of implementation success.

The findings ultimately demonstrated that removing barriers to e-government requires simultaneous intervention at three interconnected levels. At the structural level, governments must establish reliable infrastructure, integrated platforms, sustainable financing, legal frameworks, and security standards. At the organizational level, they must redesign processes, clarify responsibilities, strengthen leadership, coordinate institutions, and develop employee competencies. At the societal level, they must build citizen trust, increase digital literacy, involve users in service design, and ensure equitable access. Progress at only one level is unlikely to be sufficient. Advanced infrastructure without organizational reform may leave inefficient procedures unchanged, whereas administrative reform without reliable technology may not produce accessible and continuous services. Similarly, technically and administratively effective systems may remain unsuccessful when citizens lack trust, skills, or access. The overall synthesis therefore identified integrated governance, institutional coordination, and context-sensitive implementation as the central conditions for sustainably overcoming barriers to e-government.

4. Discussion and Conclusion

The present systematic review synthesized evidence from 42 studies to identify the principal barriers to e-government implementation and the strategies proposed for overcoming them. The findings showed that technological and infrastructural barriers were the most frequently reported, followed by organizational and managerial barriers, human-resource and competency limitations, legal and regulatory deficiencies, cultural and social resistance, financial constraints, security and privacy concerns, political and institutional obstacles, digital inequality, and weaknesses in citizen participation and service design. The review also demonstrated that these barriers were not independent. Instead, they formed an interconnected system in which deficiencies in infrastructure, governance, skills, regulation, trust, and access reinforced one another. This result supports the view that e-government should be understood as a whole-of-government transformation rather than a collection of separate information technology projects. The successful establishment of digital government requires coordination across public institutions, shared infrastructures, integrated data systems, administrative process redesign, and sustained political and managerial commitment (Memarzadeh et al., 2024; Muhdiarta et al., 2025; Panda et al., 2025).

Technological and infrastructural barriers were identified in 35 of the 42 reviewed studies and therefore represented the most common category. These barriers included weak internet connectivity, outdated hardware and software, fragmented databases, poor interoperability, unstable networks, and the absence of common technical standards. This finding is consistent with the argument that e-government cannot operate effectively through isolated digital platforms developed independently by individual public agencies. Fragmented technical systems reproduce administrative fragmentation, forcing citizens to register repeatedly, submit the same information to different organizations, and move between incompatible service portals. The proposed development of unified e-government platforms is therefore important because shared architecture can facilitate data exchange, standardize access, and reduce duplication across agencies. However, technical integration requires common definitions, interoperable databases, clear institutional responsibilities, and effective governance of shared information. Accordingly, infrastructure development should not be interpreted narrowly as the provision of equipment and connectivity but as the creation of an integrated digital environment that supports continuous and coordinated public-service delivery (Panda et al., 2025; Popescu et al., 2024; Tavazooi Far, 2024).

The prominence of technological barriers also reflects differences in the digital maturity of governmental systems. In less developed contexts, implementation is often constrained by basic deficiencies in connectivity, equipment, maintenance, and access to technical expertise. In more advanced contexts, the main challenges shift toward system integration, data governance, cybersecurity, and the coordination of existing digital services. This distinction helps explain why the same general category of technological barriers can take different forms across countries. The findings of the review suggest that governments should

assess their actual level of digital maturity before selecting implementation strategies. The adoption of sophisticated technologies without reliable foundational infrastructure may increase complexity and costs rather than improve public services. Similarly, the use of innovations such as blockchain may strengthen traceability and transaction integrity, but it may also introduce new privacy, regulatory, scalability, and governance risks. Emerging technologies should therefore be adopted on the basis of clearly defined administrative needs and institutional capacity rather than symbolic modernization or technological enthusiasm (Deligiannis & Peristeras, 2025; Muhdiarta et al., 2025; Yu, 2024).

Organizational and managerial barriers were reported in 33 studies, confirming that the success of e-government depends heavily on the capacity and willingness of public organizations to change. Resistance to change, unclear responsibilities, weak interagency coordination, bureaucratic rigidity, limited managerial commitment, and insufficient implementation planning were among the most recurrent obstacles. These findings indicate that many e-government projects fail because existing procedures are transferred to electronic platforms without being redesigned. Digitizing a complex, repetitive, or inefficient process does not necessarily make it simpler; it may merely reproduce bureaucratic difficulties in digital form. The evidence therefore supports the need for administrative process reengineering before or alongside technological implementation. Public organizations must identify unnecessary approvals, duplicated records, unclear decision points, and overlapping institutional responsibilities before constructing electronic workflows. Moreover, e-government should be incorporated into organizational strategy and performance management rather than delegated exclusively to information technology departments (Chabok et al., 2025; Farahani & Babaeianpour, 2024; Raeisi et al., 2024).

The findings also emphasize the importance of leadership and implementation governance. E-government programs require senior managers who can define priorities, allocate resources, resolve interorganizational disputes, enforce common standards, and maintain continuity across political and administrative changes. The experience of specialized public-sector innovation teams demonstrates that technically capable and institutionally empowered teams can accelerate digital reform when they have direct access to decision-makers and sufficient authority to coordinate across agencies. Nevertheless, innovation teams cannot produce sustainable transformation when their work remains dependent on temporary political support or isolated from formal administrative structures. Digital reforms must therefore become institutionalized through clear mandates, stable governance mechanisms, measurable indicators, and permanent cross-agency coordination structures. This interpretation aligns with research emphasizing the role of governance models in facilitating digital business development, administrative modernization, and more integrated forms of public-sector innovation (Chabok et al., 2025; Deligiannis & Peristeras, 2025; Panda et al., 2025).

Human-resource and competency barriers were identified in 30 studies, indicating that employees remain central actors in e-government implementation. New systems alter job roles, work routines, authority structures, and relationships between departments. Employees may resist electronic systems when they perceive them as threats to job security, professional autonomy, or established organizational status. Resistance may be further intensified when systems are introduced without sufficient consultation, training, or technical support. The findings therefore suggest that training should extend beyond basic software instruction and include digital literacy, information security, data management, user support, process redesign, and change management. Employees should also understand why new systems are being introduced and how they are expected to improve organizational performance and public-service quality. Research showing that e-government can enhance employee performance through organizational transparency further supports the importance of aligning digital systems with human-resource development and transparent work procedures (Gholami et al., 2024; Memarzadeh et al., 2024; Muhdiarta et al., 2025).

Data quality emerged as a cross-cutting issue underlying technological, organizational, and managerial barriers. Integrated services cannot function reliably when government databases contain incomplete, inconsistent, duplicated, or outdated information. Poor-quality data may lead to incorrect administrative decisions, repeated requests for documentation, and loss of public confidence. The findings of this review therefore support the need for comprehensive data-governance frameworks that clearly assign responsibility for data creation, validation, updating, storage, sharing, and protection. Data governance is particularly important in environments where multiple agencies contribute information to shared systems. Without common standards and accountability mechanisms, interoperability may transmit errors across institutions rather than improving efficiency. The relationship between data quality and data governance is especially relevant to e-government development in

Iran, where institutional fragmentation and inconsistent data-management practices may weaken the reliability of electronic services (Popescu et al., 2024; Sahraei, 2025; Tavazooi Far, 2024).

Legal and regulatory barriers were reported in 26 studies and included uncertainty concerning electronic signatures, digital records, privacy protection, data sharing, institutional accountability, and responsibility for system failures. These findings demonstrate that legal reform is not a secondary issue but a necessary foundation of e-government. Government organizations may be unwilling to exchange information when the legal conditions for data sharing remain unclear, while citizens may avoid digital services when they are uncertain about the validity of electronic transactions or the protection of personal information. Comprehensive legislation should therefore establish the legal status of electronic records, define the responsibilities of public institutions, regulate data exchange, and provide remedies for privacy violations and unauthorized access. Legal frameworks must also remain adaptable because new technologies continuously create forms of risk and interaction that may not be adequately covered by traditional administrative law (Alsaad et al., 2024; Kenfack & Check, 2024; Yu, 2024).

Information-security and privacy barriers were identified in more than half of the studies, reflecting the central role of trust in digital government. Citizens are unlikely to use e-government services when they fear identity theft, unauthorized surveillance, data misuse, or insecure transactions. The findings align with previous research showing that trust is shaped by both technical service characteristics and broader perceptions of governmental quality, competence, and integrity. Security measures such as encryption, strong authentication, access control, regular audits, and incident-response plans are essential, but technical protection alone is insufficient. Governments must also explain how personal data are used, which organizations can access them, and what safeguards exist when violations occur. Transparent communication is particularly important because citizens may not be able to directly evaluate the technical security of a system and must therefore rely on institutional reputation and perceived accountability (Alsaad et al., 2024; Kenfack & Check, 2024; Nguyen et al., 2024).

The review further showed that cultural and social barriers were reported in 25 studies. Preference for face-to-face services, low awareness of digital platforms, limited information-sharing culture, and distrust of online interactions reduced citizen and employee adoption. These findings suggest that e-government implementation is partly a behavioral and cultural process. Citizens do not adopt a service merely because it is available online; they compare it with traditional alternatives in terms of convenience, reliability, familiarity, and perceived risk. Where physical procedures are better understood or where online transactions have previously failed, users may continue to prefer conventional channels. Public-awareness campaigns, assisted digital-service centers, demonstrations of successful applications, and clear communication of service benefits may therefore be necessary during the transition. Smart-city initiatives that emphasize transparency and accountability can also strengthen the perceived public value of digital services when citizens can observe practical improvements in service delivery (Kala et al., 2024; Margareta et al., 2025; Nguyen et al., 2024).

Citizen satisfaction, service quality, and continued-use intention were closely related to cultural acceptance and trust. The reviewed evidence indicated that systems may be technically operational but remain unsuccessful when they are difficult to use, provide incomplete services, or require citizens to complete significant parts of the process in person. Research based on technology acceptance and information-system success frameworks shows that user satisfaction increases when systems are useful, easy to navigate, reliable, and supported by high-quality information. Satisfaction, in turn, strengthens continued-use intention and citizen trust. E-service quality also contributes to electronic loyalty through e-trust, although system anxiety can weaken these relationships. These findings confirm that the evaluation of e-government should move beyond counting the number of online services and include usability, completion rates, satisfaction, trust, and continued use as indicators of actual implementation success (Kala et al., 2024; Nawafleh & Khasawneh, 2024; Shahzad et al., 2024).

Financial and economic barriers were reported in 23 studies. E-government requires substantial expenditure not only during initial development but throughout the entire system lifecycle. Costs include infrastructure, software, cybersecurity, maintenance, technical support, employee training, system integration, data migration, evaluation, and periodic upgrading. Projects may fail when budgets cover only the design and launch stages while neglecting ongoing operation. The findings therefore support multiyear financial planning and the prioritization of high-impact projects. E-government investment should also be connected to broader economic and administrative objectives, including resource efficiency, transparency, tax compliance, and resistance-economy goals. In taxation, for example, effective electronic services can improve monitoring and reduce opportunities for evasion, but only when information and communication technologies are sufficiently developed and

institutions can use the resulting data effectively (Farahani & Babaeianpour, 2024; Muhdiarta et al., 2025; Zamani et al., 2024).

Digital inequality and accessibility barriers were identified in 18 studies, showing that the expansion of electronic services may unintentionally increase exclusion. Citizens differ in access to devices, internet connectivity, digital skills, language competence, age-related abilities, and physical accessibility needs. Rural residents, low-income groups, older adults, and persons with disabilities may face particular difficulties. E-government implementation should therefore include assisted digital channels, mobile-compatible systems, accessible interface design, public internet facilities, and continued availability of alternative channels during transitional periods. A citizen-centered approach requires that service design reflect the capabilities and circumstances of diverse users rather than an assumed technologically proficient population. Inclusive access is also essential for public trust because digital reforms perceived as benefiting only privileged groups may weaken the legitimacy of government modernization programs (Kenfack & Check, 2024; Nguyen et al., 2024; Popescu et al., 2024).

Overall, the findings demonstrate that the removal of e-government implementation barriers requires coordinated intervention at structural, organizational, and societal levels. At the structural level, governments need reliable infrastructure, integrated platforms, strong legal frameworks, high-quality data, cybersecurity, and sustainable financing. At the organizational level, they need committed leadership, process redesign, interagency coordination, employee training, and clear accountability. At the societal level, they need public trust, citizen participation, digital literacy, usability, and equitable access. The interaction among these levels explains why isolated reforms often produce limited results. Technology without administrative reform may digitize inefficiency; administrative reform without reliable infrastructure may produce unstable services; and effective systems without trust or access may remain underused. The reviewed evidence therefore supports a comprehensive and context-sensitive strategy in which technical modernization is inseparable from institutional and social transformation (Alsaad et al., 2024; Chabok et al., 2025; Panda et al., 2025).

This systematic review had several limitations. First, although multiple international and Persian-language databases were considered, some relevant studies may not have been identified because of differences in indexing, terminology, publication language, or database coverage. Second, the included studies were heterogeneous in terms of geographical context, research design, sample characteristics, administrative level, and definitions of e-government implementation, which limited direct comparison among findings. Third, the review relied mainly on qualitative thematic synthesis, and the frequency with which a barrier was reported does not necessarily represent its causal importance or practical severity. Fourth, publication bias may have affected the evidence base because unsuccessful government projects, internal evaluations, and politically sensitive implementation problems may not have been publicly reported. Finally, the inclusion of conceptual and review studies alongside empirical research increased the breadth of the synthesis but may also have introduced variation in the strength of evidence supporting individual themes.

Future research should use longitudinal and comparative designs to examine how e-government barriers change across different stages of implementation and levels of digital maturity. More studies are needed at municipal and local-government levels, particularly in rural and underserved settings where infrastructure and human-resource inequalities may be greater. Researchers should also investigate causal relationships among barriers rather than examining them as independent factors. Mixed-method studies could clarify how leadership, data quality, employee readiness, legal certainty, trust, and service quality interact over time. Future systematic reviews may apply meta-analytic methods where sufficiently comparable quantitative evidence becomes available. Greater attention should also be given to emerging challenges related to artificial intelligence, blockchain, automated decision-making, algorithmic accountability, digital identity, and cross-border data governance. Studies involving citizens with disabilities, older adults, low-income groups, and individuals with limited digital literacy are particularly necessary to ensure that future digital-government models are inclusive.

Government organizations should adopt an integrated implementation roadmap that links infrastructure development with administrative reform, legal regulation, data governance, employee development, and citizen engagement. Before digitizing services, agencies should simplify procedures, eliminate unnecessary documentation, clarify responsibilities, and establish interoperable data standards. Senior managers should be held accountable for implementation outcomes, while permanent interagency governance structures should coordinate system design and data exchange. Continuous training, technical support, and change-management programs should be provided for employees. Governments should also conduct regular security

audits, publish transparent privacy policies, and establish clear complaint and remedy mechanisms. Citizen participation should be incorporated into service design through needs assessments, usability testing, and satisfaction monitoring. Finally, digital inclusion should be treated as a core implementation requirement by maintaining assisted service channels, supporting rural connectivity, ensuring accessibility for persons with disabilities, and designing mobile-friendly systems that can be used by individuals with different levels of digital competence.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Alsaad, A., Alkhawaldeh, A., Elrehail, H., & Almomani, R. (2024). Linking e-government development and quality of governance to trust in government: evidence from OECD member countries. *Transforming Government: People, Process and Policy*, *18*(4), 575-593. https://doi.org/10.1108/TG-03-2024-0060

Chabok, F., Dadashkarimi, Y., & Irani, F. N. H. (2025). Identifying the components of the e-government governance model with an approach to creating and developing digital businesses. *Digital Transformation and Administration Innovation*, *5*(1), 1-17. https://doi.org/10.61838/dtai.299

Deligiannis, A., & Peristeras, V. (2025). Pioneering public sector innovation: The case of Greece's e-government team. *Administrative Sciences*, *15*(8), 306. https://doi.org/10.3390/admsci15080306

Farahani, F., & Babaeianpour, M. (2024). The Role of Influential Components of E-Government in Achieving the Goals of Resistance Economy. *Interdisciplinary Strategic Knowledge Studies*, *54*(1), 157-178. https://smsnds.sndu.ac.ir/article_3027.html

Gholami, Z., Shafiei, S., & Barakhas, H. (2024). The Role of E-Government in Employee Performance at the Sports and Youth Administration of Qazvin Province With the Mediating Role of Organizational Transparency. *Sports Management Studies*. https://smrj.ssrc.ac.ir/article_4324.html?lang=en

Kala, D., Chaubey, D. S., Meet, R. K., & Al-Adwan, A. S. (2024). Impact of User Satisfaction With E-Government Services on Continuance Use Intention and Citizen Trust Using TAM-ISSM Framework. *Interdisciplinary Journal of Information Knowledge and Management*, *19*, 001. https://doi.org/10.28945/5248

Kenfack, P. D. B., & Check, N. (2024). Reinforcing of Citizen's Trust in E-Government: The Cameroon's Case. *Journal of Computer and Communications*, *12*(01), 77-109. https://doi.org/10.4236/jcc.2024.121006

Margareta, Putri, A. V., Maskut, D. N., Kwuta, R. M., & Sipayung, B. (2025). Tarakan Smart City: Meningkatkan Transparansi Dan Akuntabilitas Layanan Publik Melalui E-Government. *Tumoutou Social Science Journal*, *2*(1), 61-73. https://doi.org/10.61476/89n39p90

Memarzadeh, G., Mobini, M., & Faghihi, M. (2024). *E-Government*. Andishehaye Goharbar.

Muhdiarta, U., Mulyaningsih, S., Wibisono, O. N., Musa, A. E. Z., & Judijanto, L. (2025). Revolutionizing Public Services: The Transformative Power of E-Government in Shaping Efficient Digital Governance. *Journal of Information Systems Engineering and Management*, *10*(54s). https://doi.org/10.52783/jisem.v10i54s.11146

Nawafleh, S., & Khasawneh, A. S. (2024). Drivers of Citizens E- Loyalty in E-Government Services: E-Service Quality Mediated by E-Trust Based on Moderation Role by System Anxiety. *Transforming Government People Process and Policy*, *18*(2), 217-240. https://doi.org/10.1108/tg-04-2023-0053

Nguyen, T. T. U., Nguyen, P. V., Huynh, H. T. N., Vrontis, D., & Ahmed, Z. U. (2024). Identification of the determinants of public trust in e-government services and participation in social media based on good governance theory and the technology acceptance model. *Journal of Asia Business Studies*, *18*(1), 44-61. https://doi.org/10.1108/JABS-04-2023-0160

Panda, S., Chandani, A., & Wagholikar, S. (2025). Digital governance across whole-of-the-government: Opportunities and challenges. *Financial Internet Quarterly*, *21*(1). https://doi.org/10.2478/fiqf-2025-0005

Popescu, M. A. M., Barbu, A., Costea-Marcu, I.-C., & Dumitriu, D. (2024). Conceptual Framework for Unified E-Government Web Platform. *Proceedings of the International Conference on Business Excellence*, *18*(1), 3503-3514. https://doi.org/10.2478/picbe-2024-0284

Raeisi, N., Jafarinea, S., & Zare, H. (2024). Testing the Model for Enhancing Administrative Transparency in Interaction with E-Government Development Programs in the Social Security Organization. *Dynamic Management and Business Analysis*, *3*(1), 320-334. https://doi.org/10.61838/dmbaj.3.1.18

Sahraei, F. (2025). An analysis of data quality in e-government and its impact on data governance in Iran. *State Studies*, *11*(41), 133-186.

Shahzad, K., Tahir, Z., Cheema, U., & Ahmad, M. A. (2024). Barriers Towards Adoption of E-Government Services. *Journal of Business and Social Review in Emerging Economies*, *10*(2). https://doi.org/10.26710/jbsee.v10i2.2966

Tavazooi Far, H. (2024). Comprehensive Study of E-Government in Iran: Opportunities, Challenges, and Improvement Strategies. 12th International and National Conference on Management, Accounting, and Law Studies, Tehran. https://civilica.com

Yu, J. (2024). Exploration of the application of blockchain in e-government: Opportunities and risks coexist. *Information Services & Use*, *44*(3), 255-266.

Zamani, L., Barzooiyan Shirvan, S., Karimi Jafari, F., & Ansari, M. (2024). Investigating the impact of e-government services on tax evasion with the moderating role of information and communication technology. *Tax Research Journal*, *32*(61), 170-218. https://doi.org/10.61186/taxjournal.32.61.170