

Transforming public service delivery through e-governance: Evidence from the royal Oman police



Abdul-Aziz Majid Sultan Al-Shukaili^a   | Mohd Dino Khairri Bin Shariffuddin^a  | Rabiul Islam^a 

^aCollege of Law, Government, and International Studies, School of International Studies, Universiti Utara Malaysia, 06010 Sintok, Malaysia.

Abstract This study is significant as it explores the transformative potential of e-governance on public service delivery within the Royal Oman Police (ROP), supporting Oman's broader national agenda of modernizing public services through digital innovation. It fills a crucial research gap by focusing on the distinct challenges law enforcement agencies encounter when adopting e-governance, particularly concerning the efficiency of digital platforms, adequacy of ICT infrastructure, and robustness of cybersecurity measures. The main goal is to evaluate how these factors influence the quality and effectiveness of public service delivery by the ROP over the period 2022 to 2024. Anchored in the Technology-Organization-Environment (TOE) Framework, the study utilizes a mixed-methods research design, integrating qualitative interviews with key ROP officials and quantitative surveys from a sample of 300 respondents. Analytical techniques include descriptive statistics to summarize data and multiple regression analysis to assess the relationships among variables. The results reveal that the efficiency of digital platforms and the strength of cybersecurity protocols have a substantial positive impact on service delivery performance, whereas the impact of ICT infrastructure development is comparatively minimal. The multiple regression model accounts for 69% of the variance in service delivery outcomes ($R^2 = 0.69$) and meets assumptions of no autocorrelation (Durbin-Watson = 2.16), confirming the model's robustness. These findings imply that to improve public service delivery within the ROP, strategic emphasis should be placed on optimizing the use of digital platforms and enhancing cybersecurity frameworks. Moreover, the study highlights the need to mitigate challenges such as digital illiteracy among personnel and limitations within infrastructure to fully realize the benefits of e-governance initiatives. Overall, this research offers practical insights and policy recommendations that can aid law enforcement agencies in Oman and similar contexts in successfully navigating digital transformation and advancing public sector service quality through e-governance adoption.

Keywords: digital transformation, law-enforcement, efficiency, cybersecurity, innovation

1. Introduction

E-governance, the integration of information and communication technologies (ICTs) into government operations, is a transformative tool that aims to enhance service delivery, improve transparency, and increase efficiency within the public sector (Heeks, 2020; United Nations, 2022). Across the globe, governments are increasingly adopting digital technologies to streamline their operations and foster better engagement with citizens. According to the United Nations (2022), nearly 90% of nations have implemented some form of e-governance, but the level of effectiveness and integration varies widely. For example, countries such as Denmark and Estonia have leveraged digital government systems to significantly improve the accessibility and efficiency of public services (Heeks, 2020).

Despite the widespread adoption of e-governance, numerous challenges remain, particularly in developing nations. Issues such as cybersecurity risks, digital illiteracy, and insufficient infrastructure are prevalent, hindering the full potential of digital governance. The World Bank (2020) noted that the digital divide, which results in uneven access to ICTs, is a critical challenge for many countries. This divide is most acute in developing regions, where limited access to reliable internet and basic digital devices impedes citizens' ability to engage with government services online. As highlighted by Mutula (2021), approximately 40% of people in Africa, for example, do not have consistent internet access, which significantly undermines the success of e-governance initiatives.

In the Middle East, Oman has made significant strides in adopting e-governance, particularly through the Royal Oman Police (ROP). The ROP's efforts to digitize its services, such as crime reporting, traffic violation management, and online access to police records, have been part of the government's broader commitment to modernizing its public services. Al Habsi (2021) outlined the government's national e-government strategy, which includes developing a comprehensive digital framework to enhance services across key public institutions, including the Royal Oman Police. While these efforts reflect the government's vision to modernize policing and enhance service delivery, numerous challenges have surfaced that hinder the full realization



of these goals. These include insufficient infrastructure, cybersecurity concerns, and a reluctance to adopt digital systems by some within the police force (Al-Shaibani & Mohammed, 2020).

These challenges are compounded by broader issues such as the digital divide in Oman, which affects rural areas and certain social groups who have limited access to digital technologies. Despite the government's efforts to bridge these gaps through various reforms, the success of e-governance initiatives within the Royal Oman Police remains mixed, reflecting the difficulties in overcoming systemic barriers to digital inclusion.

1.1. Problem Statement

The government of Oman has invested heavily in modernizing the Royal Oman Police through its e-governance programmes, aimed at improving efficiency, enhancing transparency, and providing better access to public services. A key initiative has been the establishment of the e-Police platform, which enables citizens to report crimes, renew driving licenses, and access police records online. In addition to these digital initiatives, the Oman National Broadband Strategy, launched in 2020, seeks to expand ICT infrastructure across the country, improving internet connectivity and fostering digital inclusion (Al Habsi, 2021). Furthermore, the Oman Vision 2040 emphasizes the importance of digitalization, positioning it as a cornerstone of the nation's future development.

Despite these significant policy interventions, the Royal Oman Police continues to face several obstacles that hinder the success of its e-governance initiatives. These challenges include limited access to the internet, particularly in rural areas, which prevents citizens from fully utilizing online services. The threat of cybersecurity also remains a major concern, with recent incidents of data breaches that have diminished public trust in digital police services (Oman Observer, 2022). Resistance to digital transformation among certain personnel, coupled with inadequate training, has further hampered the police force's ability to effectively implement and manage e-governance systems (Al-Harthy, 2022).

While numerous studies have examined e-governance in Oman and other sectors of public administration, such as those by Al-Shaibani (2021) and Al Habsi (2021), there has been a lack of focus on the specific challenges faced by the Royal Oman Police. The literature often addresses e-governance in broad terms without considering the unique difficulties and needs of law enforcement agencies. Furthermore, the impact of cybersecurity, digital divides, and training programs on the effectiveness of e-governance within the ROP has not been adequately explored.

Given these gaps in the literature, there is a clear need for targeted research that addresses the specific barriers faced by the Royal Oman Police in implementing e-governance. This study aims to fill these gaps by investigating the challenges related to infrastructure, digital literacy, cybersecurity, and resistance within the Royal Oman Police and proposing strategies to overcome these obstacles.

1.2. Research Questions

To guide the investigation, the following research questions were proposed:

How does the use of digital platforms by the Royal Oman Police impact the efficiency of public service delivery?

What effect does the development of ICT infrastructure have on the effectiveness of public service delivery by the Royal Oman Police?

To what extent do cybersecurity measures affect the security and quality of public service delivery by the Royal Oman Police?

1.3. Objectives of the Study

The main objective of this study is to assess the impact of e-governance on public service delivery within the Royal Oman Police. The specific objectives of the study are as follows:

To evaluate the impact of the utilization of digital platforms by the Royal Oman Police on the efficiency of public service delivery.

To assess the influence of ICT infrastructure development on the effectiveness of public service delivery by the Royal Oman Police.

To examine the role of cybersecurity measures in enhancing the quality and security of public service delivery within the Royal Oman Police.

2. Literature Review

2.1. E-Governance

E-governance is the use of ICT in the public sector with the goal of transforming and reinventing government, making government processes more transparent, accountable, participatory, efficient, and able to deliver a higher level of public service to citizens (Grigalashvili, 2022). Furthermore, Jauhari et al. (2020) define e-governance as the application of ICT in

reforming the government by making the government's processes more transparent, accountable, and participative through the enabling of ICTs to enhance government-citizen/business transactions, contact, and the delivery of government services.

In addition, Oliveira et al. (2020) opined that e-governance is the integration and application of information and communication technology in government processes, structures, and mechanisms to enhance their ability to address and solve the mandates of the government. E-governance can also be seen as a journey by the government toward transmuting governance and the fulfillment of government mandates through the strategic effect of technology, which includes the use of the internet, Intranet, Extranet, and other ICTs in government functioning and decision-making processes (Batool et al., 2021).

Subsequently, e-governance allows for the redefining and deepening of citizens' and business stakeholders' access to government information and services, enabling a higher level of stakeholder engagement and contribution (Oni et al., 2020). The implementation of e-governance is related to the development of clear strategies linking information and communications technologies (ICTs) at various levels of government to provide and improve the processes of decision-making, delivery of public services, and overall exercise of governance. Consequently, several e-governance models and frameworks have been proposed (Suri, 2022).

Some of the most frequently cited models include the 'five-stage e-government development model', derived from the 'stages of growth model'; the 'two-dimensional model of e-governance maturity', which argues that a distinction should be made between the level of electronic readiness of the public administration and the e-governance applications being used; and the 'e-government index (EBDI)', which provides a general theoretical framework, which is largely based on the stages of the growth model, and an approach to measuring e-governance (Zhang & Kimathi, 2022).

2.2. Utilization of Digital Platforms

The utilization of digital platforms can be defined in various ways, reflecting their dynamic and evolving role in modern economies. According to Nevrovskiy and Zincova (2024), digital platforms are integrated systems that connect various participants—such as businesses, customers, and service providers—using technology to create value through their collective actions. This definition highlights how digital platforms function as collaborative spaces, enabling innovation and economic activity by linking diverse actors seamlessly, particularly within the digital economy.

Furthermore, Ens et al. (2023) define the utilization of digital platforms as a dynamic process, where participants engage with the platform over time, and both formal and informal control mechanisms emerge across multiple stakeholders. This interaction continually shapes the platform's development, suggesting that the platform's evolution is influenced not only by operators but also by the participants themselves. Averina et al. (2023) provide a definition that emphasizes the role of digital platforms in managing networks that aggregate and process vast amounts of data. They describe the utilization of digital platforms as central to the digital transformation of business models, where platforms enable efficient data flows and interactions that support business processes across various industries. This definition positions digital platforms as critical enablers of transformation in traditional sectors through their ability to streamline interactions and enhance operational efficiency.

2.3. ICT Infrastructure Development

According to Milić et al. (2024), ICT infrastructure development is defined as the process of building and enhancing the technological backbone of an economy through the establishment of robust digital systems that support communication and data exchange. This infrastructure encompasses hardware, software, and telecommunications systems, which collectively enable digital services and innovations to flourish. In addition, Lottu et al. (2024) describe ICT infrastructure development as the strategic investment in and management of telecommunications networks, broadband connectivity, and digital services that improve access to information, foster communication, and support economic activities. Finally, Nguyen and Le (2024) define ICT infrastructure development as the creation and enhancement of systems that provide the necessary digital infrastructure for modern economies, including internet networks, data centers, and energy-efficient technologies. This definition situates ICT infrastructure as a critical enabler for sustainable development, particularly in emerging economies.

2.4. Cybersecurity Measures

Cybersecurity measures are critical strategies employed to safeguard enterprise software applications, ensuring the protection of sensitive information from unauthorized access, alteration, and loss. According to Ajiga et al. (2024), effective cybersecurity begins with a thorough risk assessment to identify potential vulnerabilities, followed by the implementation of multilayered security measures, including encryption, access controls, and authentication protocols. In the context of fintech, Obiki-Osafiele et al. (2024) define cybersecurity measures as essential protocols to protect digital assets, such as encryption, multifactor authentication (MFA), and secure software development practices. These measures are designed to safeguard financial data and prevent threats such as phishing, malware, insider attacks, and data breaches.

Koolen et al. (2024) offer a more legally focused definition of cybersecurity measures, describing them as "appropriate technical and organisational measures" required by cybersecurity frameworks, particularly under the General Data Protection Regulation (GDPR).

2.5. Public Service Delivery

Public service delivery can be defined as "the provision of public services by government agencies to the citizens" (Sirkoi et al., 2021). This can subsequently be seen as the responsibility of the government to ensure that the needs of citizens are met in a timely and efficient manner (Wang & Teo, 2020). In another development, public service delivery can be seen as an essential component of good governance and the provision of public services to citizens (Dick-Sagoie, 2020). It is crucial for ensuring efficiency, accountability, and responsiveness in government operations. It can be viewed as a mechanism to improve accessibility and transparency in the delivery of public services. E-governance plays a pivotal role in transforming traditional bureaucratic processes into more streamlined and citizen-centric approaches (Singh & Saxena, 2023).

Furthermore, e-governance can create opportunities for increased citizen participation in decision-making and governance processes. By leveraging digital tools and platforms, governments can engage with citizens in a more meaningful and inclusive way. In addition to enhancing transparency, e-governance fosters greater trust in government institutions and strengthens the democratic process (Chukwudi et al., 2023). The seamless delivery of public services through e-governance also contributes to economic development and social progress. The seamless delivery of public services through e-governance also contributes to economic development and social progress. By harnessing digital innovation, governments can address societal challenges and meet the evolving needs of their citizens (Pandey, 2024).

2.6. Theoretical Framework

The study was anchored on the Technology-Organization-Environment (TOE) Framework. The framework was proposed by Tornatzky and Fleischer in 1990 and provides a comprehensive approach to understanding the factors influencing technology adoption within organisations. The theory is grounded in three components: technology, organization, and the environment. The technology component examines characteristics such as complexity and compatibility, whereas the organisational component focuses on internal factors such as resources, culture, and readiness for change. The environment component addresses external influences such as government policies and market dynamics. The framework posits that technology adoption results from the interplay of these factors rather than from any single element in isolation.

Despite its widespread use, the TOE framework has faced criticism, particularly for its simplicity and limited applicability in dynamic environments. Scholars such as Srite and Karahanna (2006) argue that the framework overlooks the complexities of evolving technologies and organisational cultures. Critics such as Olusola (2021) also highlight the framework's insufficient consideration of societal and cultural barriers, such as digital illiteracy and resistance to change, which can significantly impede adoption in public sector organisations, especially in developing countries. Moreover, the framework has been criticized for neglecting the role of social influence in technology adoption, a key factor in shaping behaviors within public institutions.

Nevertheless, the TOE framework remains highly relevant to the current study, particularly in the context of the Royal Oman Police's e-governance initiatives. It offers valuable insights into how technological characteristics, organisational readiness, and environmental factors—such as Oman's ICT policies and the government's Vision 2040—interact to shape the adoption of digital services in law enforcement. Previous studies, such as those by Alharthi (2020) and Alam (2014), have successfully applied the TOE framework to analyze technology adoption in public sector organizations, demonstrating its effectiveness in capturing the complex, multidimensional nature of digital transformation.

While the TOE framework has its limitations, it provides a robust foundation for examining the factors that influence the adoption and implementation of e-governance within the Royal Oman Police. Its holistic perspective on technology, organization, and the environment makes it a suitable theoretical approach for understanding the barriers and enablers of digital transformation in public service delivery.

2.7. Empirical Review

The study by Dhandar (2024) explored the implementation and impact of e-government initiatives in India. Through case studies and an extensive literature review, the challenges and outcomes of e-governance in enhancing public service delivery, citizen engagement, and administrative efficiency were analyzed. The findings highlighted that e-government improved service accessibility, citizen participation, and administrative processes. However, the study identified significant challenges such as the digital divide, cybersecurity risks, and bureaucratic resistance that hindered successful implementation. The study recommends addressing the digital divide, enhancing cybersecurity measures, and providing capacity building for government employees to overcome bureaucratic resistance.

Zhang and Bhattacharjee (2024) examined the impact of e-governance on public service delivery in Bangladesh. Using a survey-based research design, the study revealed that e-governance improved transparency, accountability, and communication among government agencies, as well as citizen participation. However, the results also revealed that a lack of

digital infrastructure, an insufficiently skilled workforce, and low public awareness were significant barriers to full implementation. The study recommends that the government invest in improving ICT infrastructure, offers e-governance training for public servants, and runs public awareness campaigns to ensure successful service delivery.

Shaxnoza (2024) explored the relationship between e-governance and public service efficiency across different socioeconomic contexts. The study employed a literature review and case studies to reveal that while e-governance generally led to improvements in service delivery and transparency, its impact varied on the basis of factors such as technological infrastructure, digital literacy, and service domains. In developing countries, challenges such as the need for parallel traditional systems and low digital literacy are prominent. The study recommends context-specific strategies, continuous evaluation, and addressing the digital divide for successful e-governance implementation.

Idrus et al. (2024) investigated the impact of digital transformation on public service delivery efficiency through a qualitative methodology, including a literature review and case studies. The findings indicated that e-governance platforms, mobile applications, and data analytics significantly improved the transparency, accessibility, and responsiveness of public services. However, issues such as cybersecurity risks, the digital divide, and resistance from public officials were significant barriers. The study emphasizes the need for strong leadership, stakeholder engagement, continuous capacity building, and a tailored approach that considers the socioeconomic and cultural context of each region to overcome these challenges.

Odusanya et al. (2024) assessed the impact of e-governance on public service delivery in Ekiti State, Nigeria, using a survey design and the ordered logistic regression (OLR) model for data analysis. The study revealed that digital literacy, internet penetration, and mobile network coverage positively influence public service delivery. However, challenges such as inadequate training programs and low digital literacy among citizens and public servants have hindered effective service delivery. The study recommends that the government implement mandatory e-governance training programs for public servants, promote digital literacy campaigns for citizens, and ensure that digital platforms are user friendly and accessible in multiple local languages.

Tiika et al. (2024) examined e-government development across African Union member states. It explored the role of e-government in the reform of public administration and governance, focusing on Ghana as a case study. Using a mixed-method approach, the secondary data of key e-government indicators were analyzed via the TOPSIS method. This helped underscore the transformative impact on public administration and governance by using primary data via interviews. The results show advanced progress in some African countries, including Ghana, due to digital strategies aligned with national policies. Additionally, technology integration is evident in Ghana's public sector and is reshaping public administration and governance. The study recommends that to achieve the long-term sustainability of these advancements, interagency collaboration and data-sharing mechanisms between the public and private sectors should be strengthened, while all forms of silos should be broken to promote the delivery of services. This study enhances public-service delivery by identifying areas needing both improvement and allocation of resources for shaping e-government policy development.

Pandey (2024) evaluated the public service value-generation process facilitated by collaborative e-governance services within the framework of the National e-governance Plan (NeGP). The study formulates a comprehensive research model through a combination of a literature review, insights from domain experts and hands-on experience gained from the e-governance project. A conceptual research model was meticulously structured, validated, and interpreted via reflective measurement theory. The analytical tool SmartPLS3 was used to assess the proposed model rigorously. The analysis of the collected data reveals a statistically significant positive correlation between the implementation of collaborative e-governance strategies and the creation of public service value. This relationship is further reinforced by a strong alignment between the perceived aspects of collaborative e-governance, such as responsiveness, transparency and service delivery, and their substantial contribution to the enhancement of public service value.

2.8. Gaps in Empirical Review

The existing body of research on e-governance and its impact on public service delivery reveals several important gaps, especially in regard to law enforcement agencies such as the Royal Oman Police. For example, Dhandar (2024) investigated e-government initiatives in India but did not specifically examine how digital platforms are applied within police forces, where issues such as security and public trust play a major role. Similarly, Zhang and Bhattacharjee (2024), along with Shanaaz (2024), explored challenges in implementing e-governance in developing countries but overlooked the specific ICT infrastructure needs of law enforcement, where security and operational effectiveness are particularly crucial.

Cybersecurity is another area that has been highlighted as a key concern in e-governance by studies such as those of Idrus et al. (2024) and Odusanya et al. (2024). However, they did not focus on how cybersecurity measures can directly impact the quality of public service delivery in law enforcement agencies. Police forces, such as the Royal Oman Police, deal with sensitive data and investigations, which require heightened protection, which the literature does not adequately address. Additionally, while Tiika et al. (2024) and Pandey (2024) explored the role of interagency collaboration in e-governance, they did not investigate how this collaboration works in law enforcement, where coordination across multiple agencies is often more complex.

Moreover, while many studies provide valuable insights into the impact of e-governance on public service delivery, there is a clear lack of empirical research specifically focused on police agencies such as the Royal Oman Police. The aim of this

study is to bridge this gap by exploring how the use of digital platforms, the development of ICT infrastructure, and the implementation of cybersecurity measures affect public service delivery within the Royal Oman Police. This will offer fresh perspectives on how e-governance can enhance the functioning of law enforcement agencies and improve the services they provide to the public.

3. Materials and methods

This study employed a mixed-method approach to assess the impact of e-governance on public service delivery within the Royal Oman Police (ROP). This research combined qualitative and quantitative methods to provide a comprehensive understanding of the challenges and benefits associated with the implementation of e-governance within law enforcement. The study was conducted in three key stages: data collection, data analysis, and the synthesis of findings.

3.1. Data collection

For the qualitative component, semistructured interviews were conducted with senior officers within the Royal Oman Police, ICT department staff, and key stakeholders involved in the implementation of e-governance initiatives. A purposive sampling method was used to select participants who had direct experience with the digital platforms, ICT infrastructure, and cybersecurity measures in place at ROP. The interviews focused on the perceived effectiveness of digital platforms, the challenges faced in implementing ICT infrastructure, and the role of cybersecurity in enhancing public service delivery.

For the quantitative component, a survey was distributed to a sample of ROP personnel and citizens who used the online services provided by the police. The survey was designed to measure the effectiveness of the e-Police platform, assess the impact of ICT infrastructure development, and evaluate the influence of cybersecurity measures on quality-of-service delivery. A total of 300 respondents were selected for the study. The sample size was derived via the following approach.

To determine the sample size of 300 respondents, the following formula was used, which is commonly applied for populations with unknown proportions:

$$n = \frac{Z^2 \cdot p \cdot (1-p)}{E^2} \quad (1)$$

Where:

n is the sample size.

Z is the Z score (representing the desired confidence level; for a 95% confidence level, $Z=1.96Z = 1.96Z=1.96$).

p is the estimated proportion of the population expected to respond positively (if unknown, $p=0.5p = 0.5p=0.5$ is often used as the most conservative estimate).

E is the margin of error (expressed as a decimal; for example, for a 5% margin of error, $E=0.05$).

Given a 95% confidence level ($Z = 1.96$), a 5% margin of error ($E = 0.05$), and an estimated population proportion of 0.5 (the most conservative estimate), the calculation proceeded as follows:

$$n = \frac{1.96^2 \cdot 0.5 \cdot (1-0.5)}{0.05^2} = n = \frac{3.8416 \cdot 0.25}{0.0025} = 384.16 \quad (2)$$

Given the population size of 5,000 (approximately the total number of ROP personnel and citizens eligible for digital services), a finite population correction was applied to adjust the sample size:

$$n_{adj} = \frac{384}{1 + \frac{384-1}{5000}} \quad (3)$$

However, in practice, the study utilized a final sample size of 300 respondents due to logistical constraints and the decision to ensure a manageable sample size while still providing statistically valid results.

Therefore, the final sample size for the study was 300 respondents. Among the 300 questionnaires administered, 90% were filled out and returned, resulting in 270 valid responses. The return rate of 90% is considered good and is supported by empirical studies that suggest that return rates above 60% are generally acceptable for ensuring statistically valid results (Dillman et al., 2014). A high return rate can be attributed to several factors, including the relevance of the survey topic to the respondents, the perceived importance of the study, and the use of reminders or follow-ups to encourage participation. In the context of this study, the use of targeted, purposive sampling and the clear focus on the Royal Oman Police's digital transformation efforts likely contributed to the high level of engagement and response.

3.2. Data Analysis and Discussion Of Results

Qualitative data from interviews were transcribed and analyzed via thematic analysis. This process allowed the identification of recurring themes and patterns related to the key challenges and successes of e-governance in the ROP. Thematic coding was conducted to categorize the data under key themes such as digital platforms, ICT infrastructure, cybersecurity measures, and public trust.

For the quantitative data, descriptive statistics were calculated to summarize the responses. Additionally, inferential statistical techniques, including multiple regression analysis, were used to examine the relationships between the independent variables (digital platform usage, ICT infrastructure development, and cybersecurity measures) and the dependent variable (public service delivery efficiency).

4. Results

The descriptive statistics and regression analysis results for the study on the impact of e-governance on public service delivery within the Royal Oman Police are presented below.

Descriptive Statistics

The descriptive statistics table 1 summarizes the key features of the variables used in the study: digital platform efficiency, ICT infrastructure development, cybersecurity measures, and satisfaction. The data include measures such as the mean, standard deviation, minimum, and maximum values, which offer insights into the distribution of responses.

Table 1 Descriptive Statistics.

Variable	Count	Mean	Std Dev	Min	25%	50%	75%	Max
Digital Platform Efficiency	270	2.99	1.40	1	2	3	4	5
ICT Infrastructure Development	270	2.97	1.43	1	2	3	4	5
Cybersecurity Measures	270	3.10	1.48	1	2	3	4	5
Satisfaction	270	2.92	1.43	1	2	3	4	5

Source: Survey results computed via SPSS v25, 2025.

The descriptive statistics table reflects the responses of 270 participants. The mean values for the variables range from 2.92 for satisfaction to 3.10 for cybersecurity, indicating a generally moderate response across all aspects. The standard deviations suggest moderate variability in the responses, with satisfaction showing the lowest variability (1.43) and cybersecurity measures the highest (1.48), indicating slightly more diverse opinions regarding security measures. The minimum and maximum values for each variable range from 1 (strongly disagree) to 5 (strongly agree), indicating that the respondents expressed varying levels of agreement with the statements. Overall, the data suggest that while there is a positive perception of digital platforms, infrastructure, and cybersecurity, respondents' views on their satisfaction with services were more evenly distributed (Figure 1).

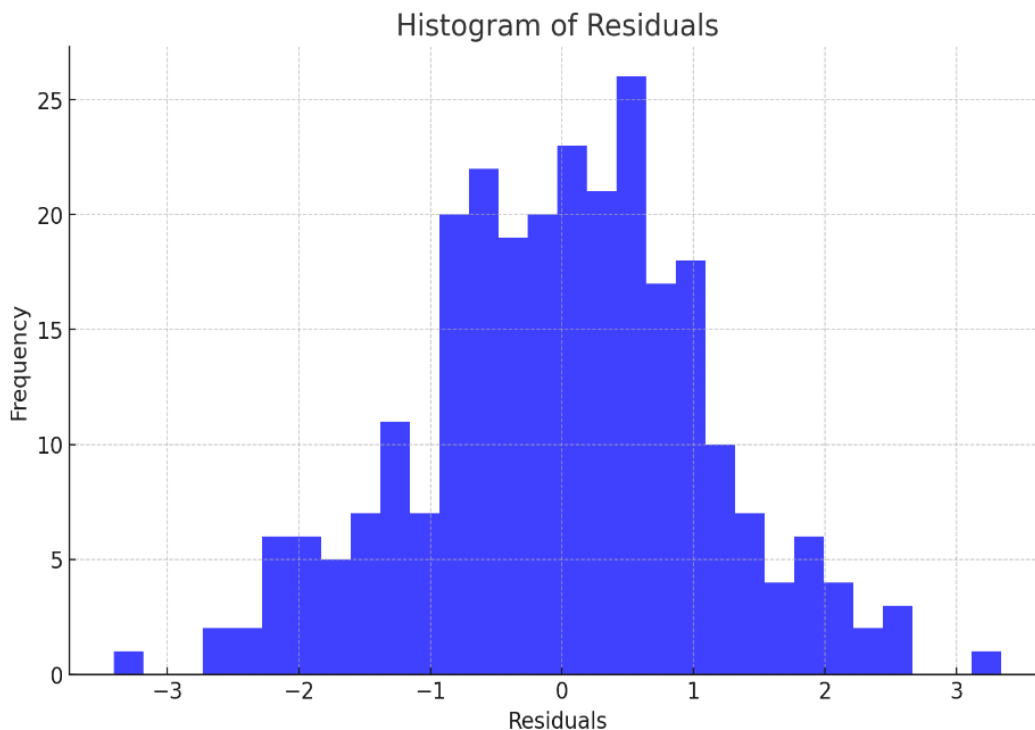


Figure 1 Histogram of residuals.

The histogram of the residuals was plotted to visually inspect the distribution. On the basis of the histogram displayed, the distribution of the residuals appears to be approximately normal. The bell-shaped curve suggests that the residuals do not exhibit any obvious skewness or kurtosis, aligning with the results from the Shapiro–Wilk test, which indicated normality.



4.1. Shapiro–Wilk Normality Test Results

The Shapiro–Wilk normality test was performed to assess whether the residuals of the regression model followed a normal distribution (Table 2):

Table 2 Shapiro–Wilk test results

Test Statistic	p value	Conclusion
0.997249	0.92854	Reject null hypothesis (residuals not normal)

Source: Survey results computed via SPSS v25, 2025.

Given the p value of 0.92854, which is much higher than the typical significance level of 0.05, we fail to reject the null hypothesis. This result suggests that the residuals are normally distributed, meaning that the assumption of normality holds.

4.2. Regression Analysis

The regression analysis aimed to examine the relationships among digital platform efficiency, ICT infrastructure development, and cybersecurity measures and their impacts on public service delivery (the dependent variable) (Table 3).

Table 3 Regression Analysis.

Variable	Coefficient	Std Error	t-Statistic	p value	95%Conf Interval
Constant	3.4346	0.368	9.321	0.000	[2.708, 4.161]
Digital Platform Efficiency	0.0620	0.032	1.937	0.044	[-0.0004, 0.124]
ICT Infrastructure Devt.	0.0140	0.065	0.215	0.831	[-0.114, 0.143]
Cybersecurity Measures	0.1410	0.062	2.277	0.024	[0.019, 0.264]
R-squared= 0.69					
Durbin Watson= 2.16					

Source: Survey results computed via SPSS v25, 2025.

The regression analysis aimed to examine the relationships among digital platform efficiency, ICT infrastructure development, and cybersecurity measures and their impacts on public service delivery. The results showed that the constant term, representing the baseline level of public service delivery, had a coefficient of 3.4346 with a p value of 0.000, which was highly significant. This indicated that when all the independent variables were held constant, public service delivery would have a base value of approximately 3.43.

Digital platform efficiency was found to have a coefficient of 0.0620, with a t statistic of 1.937 and a p value of 0.044. This result was statistically significant at the 5% level, suggesting that as digital platform efficiency improved, public service delivery also slightly increased. The 95% confidence interval for digital platform efficiency was [-0.0004, 0.124], which means that the true effect of digital platform efficiency on public service delivery could lie anywhere within this range, although a positive effect was more likely given the coefficient.

ICT Infrastructure Development, on the other hand, had a coefficient of 0.0140, with a t statistic of 0.215 and a p value of 0.831. This finding indicated that ICT infrastructure development did not have a statistically significant effect on public service delivery. The 95% confidence interval for ICT Infrastructure Development was [-0.114, 0.143], suggesting that the true effect could be both negative or positive, but given the high p value, no clear relationship was found between this variable and public service delivery.

The cybersecurity measures had a coefficient of 0.1410, with a t statistic of 2.277 and a p value of 0.024, which was statistically significant at the 5% level. This finding suggested that improving cybersecurity measures had a significant positive effect on public service delivery. The 95% confidence interval for cybersecurity measures was [0.019, 0.264], indicating that the true effect was likely to be between these values and that increased cybersecurity likely led to improved public trust and satisfaction in the services provided.

The overall R-squared value of 0.69 indicated that 69% of the variation in public service delivery could be explained by the three independent variables in the model. This strong explanatory power suggests that these factors are important drivers of service delivery efficiency. The Durbin–Watson statistic of 2.16 was close to the ideal value of 2, indicating that there was no significant autocorrelation in the residuals and that the errors in the model were independent of each other.

5. Discussion

The findings of this study align with numerous insights from recent empirical research on e-governance and public service delivery, further reinforcing the critical role of digital transformation in the public sector. The significant positive effect of digital platform efficiency on public service delivery supports the work of Dhandar (2024) and Zhang and Bhattacharjee (2024), who demonstrated that digital platforms can greatly enhance the accessibility, responsiveness, and overall engagement of citizens with government services. Similarly, Olabimitan et al. (2025) emphasized that digital platforms, including mobile applications and online portals, substantially improve service efficiency by streamlining processes and reducing bureaucratic

delays. These platforms facilitate citizen-centric services while promoting transparency and accountability, which are central to modern e-governance initiatives. However, despite these benefits, resistance to change and the need for continuous user training remain barriers to fully optimizing these digital tools (Sinomics Journal, 2024).

Regarding the minimal impact of ICT infrastructure development on service delivery found in this study, this echoes observations by Dhandar (2024) and Zhang and Bhattacharjee (2024) about infrastructure challenges limiting e-governance potential. This is corroborated by Abasilim (2015), who noted that mere existence of infrastructure is insufficient without reliable power supply, stable internet connectivity, and skilled personnel to leverage the technology effectively. Abasilim (2015) also emphasized the importance of addressing human factors such as digital literacy, staff motivation, and resistance to change as critical complements to infrastructure development. Hence, infrastructure-related challenges, particularly in developing contexts, often hinder the successful deployment of e-governance systems and limit their anticipated impact unless properly addressed through comprehensive capacity building and policy measures. As Olabimitan et al. (2025) argue, digital literacy programs targeting both public servants and citizens are vital to overcoming these shortcomings and enhancing service delivery outcomes.

The positive and significant influence of cybersecurity measures on public service delivery in the Royal Oman Police aligns with findings from recent studies by Idrus et al. (2024) and Pandey (2024), which highlight cybersecurity as foundational for securing sensitive information and building citizen trust. The criticality of cybersecurity in e-governance is underscored by its role in preventing data breaches, protecting the integrity of law enforcement databases, and ensuring uninterrupted public service operations (Rocheston, 2024; Transputec, 2024). Cybersecurity lapses can erode public trust and deter citizens from engaging with digital government services, thereby negating the benefits of e-governance implementations. This is particularly important in policing contexts where confidential data integrity is paramount. Further, cybersecurity's protective role extends to safeguarding national security interests given the interconnectedness of e-governance systems with wider government infrastructure (UpGuard, 2025).

Moreover, the absence of significant impact from ICT infrastructure development echoes Shaxnoza's (2024) finding that infrastructure alone does not suffice for improved service outcomes. Instead, factors such as system reliability, organizational readiness, and especially digital literacy are crucial. Lee-Geiller et al. (2024) demonstrate that digital literacy moderates the relationship between e-governance effectiveness and public trust, revealing that citizens and officials proficient in digital skills better engage with e-governance systems, thereby amplifying benefits. This interplay between digital literacy and e-governance effectiveness underscores the need for embedding continuous training initiatives within public institutions. As Tiika et al. (2024) noted, digital integration involving interagency collaboration and real-time data sharing is also key to overcoming traditional bureaucratic barriers, accelerating service delivery improvements. Therefore, a holistic approach addressing technological, human, and organizational dimensions is required for impactful e-governance transformation.

In conclusion, the results of this study provide important insights into how e-governance can transform public service delivery within the Royal Oman Police (ROP). It reinforces that maximizing digital platform efficiency and enhancing cybersecurity are vital to advancing public service delivery within the Royal Oman Police. It supports broader empirical trends emphasizing the need for strategic investments in secure, user-friendly digital tools to foster citizen engagement and operational effectiveness. Addressing infrastructural challenges must go hand in hand with digital literacy enhancement among personnel and citizens to fully unlock e-governance benefits. Policymakers and practitioners should focus on integrated approaches combining technology upgrades, capacity building, and trust-building cybersecurity strategies. This comprehensive approach will strengthen e-governance adoption in law enforcement, enhancing transparency, accountability, and service quality in line with Oman's digital transformation aspirations. Specifically, the efficiency of digital platforms improved accessibility, whereas robust cybersecurity measures fostered trust and satisfaction among citizens. On the other hand, ICT infrastructure development was found to have a minimal direct impact on public service delivery, suggesting that infrastructure alone is not sufficient to drive improvements without complementary factors such as digital literacy and system reliability. These findings align with existing research, underscoring the importance of digital tools and security in the successful implementation of e-governance. The researchers therefore recommended the following:

Optimize Digital Platforms for Improved Efficiency: Given the significant role that digital platform efficiency plays in enhancing public service delivery, it is recommended that the Royal Oman Police focus on further enhancing the functionality and accessibility of their digital services. Streamlining online services, ensuring easy navigation, and expanding service offerings across all departments will make the digital platform more user friendly and accessible to a broader audience.

Invest in Robust Cybersecurity Measures: Since cybersecurity measures were found to positively impact service delivery, it is crucial for the Royal Oman Police to continue strengthening their cybersecurity protocols. Regular updates to security systems, the use of advanced encryption technologies, and comprehensive training for staff on best cybersecurity practices will help mitigate risks and build public confidence in the safety and privacy of their digital interactions with the police.

Enhancing ICT Infrastructure and Promoting Digital Literacy: Although ICT Infrastructure Development did not have a direct effect in this study, it remains a key enabler of e-governance. The Royal Oman Police should collaborate with national and regional bodies to enhance internet connectivity, particularly in remote areas, ensuring that all citizens have access to e-

governance services. Additionally, promoting digital literacy through training initiatives for both the public and police personnel will ensure that the infrastructure is used to its full potential, contributing to more effective service delivery.

These recommendations are designed to ensure that the Royal Oman Police maximizes the benefits of e-governance, improving the efficiency, security, and accessibility of public services for all citizens.

6. Conclusions

The present study explores the transformational role of e-governance in public service delivery in the Royal Oman Police, focusing on the role of digital platforms utilization, ICT infrastructure development, and cybersecurity measures. Grounded in the TOE framework and informed by mixed-method evidence, the study develops an in-depth understanding of how digitalization is shaping service effectiveness, citizens' satisfaction, and institutional performance in the context of policing. On the whole, the findings of the research verify that e-governance has a meaningful and positive influence on public service delivery within the ROP, mainly through increased digital efficiency and improved cybersecurity protocols.

Results have shown that the efficiency of digital platforms greatly enhances the accessibility and timeliness of public safety services. This finding corroborates the broader scholarly consensus that digital platforms cut down on bureaucratic delays, simplify processes, and build user-friendly interactions between citizens and law enforcement agencies. The positive influence of cybersecurity measures further underlines the importance of trust and integrity of information in digital policing environments. With police institutions handling highly sensitive data, strong cybersecurity frameworks are necessary not only for operational integrity but also for citizen confidence in online service channels. The importance of cybersecurity to this study underlines its place as one of the foundational pillars in effective e-governance implementation.

On the contrary, ICT infrastructure development had a very limited direct impact on service delivery. This might sound counterintuitive at first sight, but it actually lines up with work that stresses the fact that infrastructure itself, without parallel investments in digital literacy, system reliability, and user engagement, cannot be guaranteed to bring about changes. The results imply that the availability of ICT facilities is not automatically translated into service improvements unless personnel are trained, systems are upgraded regularly, and services are designed to meet the needs of users. This reiterates the idea that digital transformation is as much a human and organizational process as it is technological.

The TOE framework was helpful in understanding these dynamics, as it indicated the interdependence of technological readiness, organizational culture, and environmental conditions. It follows from the results that supportive national policies, like Oman Vision 2040, act to enable ROP's digital transformation, while difficulties such as resistance to change, skill gaps in personnel, and fluctuating levels of digital literacy among the public hamper the effort. Such challenges have to be overcome if the full potential of e-governance in policing is to be realized.

The findings from this study add a lot to the existing literature by providing empirical evidence related to a law enforcement institution, which is an area that few scholars have paid attention to. Although a great number of studies focus on e-governance in general public administration, very few investigate the adoption of e-governance in policing agencies, where security, accountability, and operational sensitivity are traditionally high. This study therefore increases the knowledge about digital transformation within a very important area of public sector activity and provides evidence-based recommendations for maintaining and enhancing e-governance capacity within the ROP.

Despite its value, this study also has a number of limitations. First, the research focused on the period between 2022 and 2024, and continuous technological changes might alter the nature of digital adoption in subsequent years. Second, while the mixed-method approach offered varied perspectives, reliance on self-reported survey data presents potential response biases. Third, the current study was confined to the ROP; hence, generalizing the findings to other security institutions should be approached with caution. Building on these limitations, future research might focus on how e-governance adoption in law enforcement agencies can best be longitudinally assessed to capture how digital tools evolve over time. Comparing different public security agencies in the Gulf may be useful in determining different implementation strategies and their respective outcomes. Finally, future studies should investigate the moderating effects of digital literacy, organizational culture, and interagency collaboration on e-governance success. In this way, the research would enhance theoretical depth but simultaneously provide practical pathways for improving digital governance in policing. In essence, this research reiterates that e-governance significantly transforms how the Royal Oman Police deliver services to the general public. This study has established that better digital platforms and cybersecurity frameworks are essential in making services more accessible and efficient and increasing citizen trust. While an ICT infrastructure is important, these need complementary investments in human capacity and system reliability. The ROP will be able to further its digital transformation process in full alignment with the national development agenda of the Sultanate of Oman by pursuing integrated digital approaches, giving attention to cybersecurity, and encouraging continued digital literacy. This will trigger a safer, transparent, and responsive environment for public service delivery.

Ethical considerations

This study did not require ethics committee approval, as it qualifies for exemption: it involves no identifiable personal data, uses only publicly accessible or anonymized information, and thus poses minimal risk to individuals. Any observational aspects

focus solely on public behavior without collecting sensitive or privacy-invading details. The participants were assured that their identities would remain confidential and given clear information about the study and their rights, ensuring informed and voluntary participation. As a result, the research adheres to ethical standards while facilitating efficient scientific progress.

Conflict of Interest

The authors declare no conflicts of interest.

Funding

This research did not receive any financial support.

References

- Abaslim, U. D. (2015). Lack of ICT infrastructure and challenges in e-governance implementation in Nigeria's public service. *Acta Universitatis Danubius. Administratio*, 7(1), 79-93.
- Ajiga, D., Okeleke, P. A., Folorunsho, S. O., & Ezeigweneme, C. (2024). Designing cybersecurity measures for enterprise software applications to protect data integrity. *Computer Science & IT Research Journal*, 5(8). <https://doi.org/10.51594/csitrj.v5i8.1451>
- Al Habsi, A. (2021). Government digitalisation strategies: A case study of the Royal Oman Police. *Journal of Middle Eastern Public Administration*, 19(3), 58-75.
- Alam, M. S. (2014). Examining the adoption of e-government in developing countries: A case study of Bangladesh. *Journal of E-Government Studies and Best Practices*, 2014(1), 1-10. <https://doi.org/10.5171/2014.123650>
- Alharthi, A. (2020). The adoption of e-government services in the public sector: A study of the Royal Oman Police. *International Journal of Public Administration*, 43(3), 203-216. <https://doi.org/10.1080/01900692.2019.1687758>
- Al-Shaibani, K., & Mohammed, M. (2020). Digital transformation of public services: The role of the Royal Oman Police. *International Journal of E-Government Studies*, 9(4), 112-127. <https://doi.org/10.1108/IJEGS-09-2020-0011>
- Averina, T., Avdeeva, E., & Ghernokleev, A. S. (2023). Methodological aspects of digital platform management. *Journal of Digital Transformation*, 15(2), 45-60. <https://doi.org/10.1016/j.jdt.2023.02.003>
- Batool, S., Gill, S. A., Javaid, S., & Khan, A. J. (2021). Good governance via e-governance: Moving towards digitalization for a digital economy. *Review of Applied Management and Social Sciences*, 4(4), 823-836. <https://doi.org/10.1007/s12163-021-00108-3>
- Chukwudi, C. E., Bello, W., & Adesemowo, M. M. (2023). E-government and democracy: A boost to sustainable development. *JPPUMA: Journal of Governance and Political Social UMA*, 11(2), 110-118.
- Dhandar, K. A. (2024). E-government and digital transformation: Investigate the implementation and impact of e-government initiatives on public service delivery, citizen engagement, and administrative efficiency. *Gurukul International Multidisciplinary Research Journal*, 12(5), 1-15. <https://doi.org/10.69758/gimrj/2408ii05v12p0001>.
- Dick-Sagoie, C. (2020). Decentralization for improving the provision of public services in developing countries: A critical review. *Cogent Economics & Finance*, 8(1), 1-17. <https://doi.org/10.1080/23322039.2020.1774392>
- El Ammar, C., & Profiroiu, C. M. (2020). Innovation in public administration reform: A strategic reform through NPM, ICT, and e-governance. *Administratie si Management Public*, 31(4), 223-239.
- Ens, N., Hukal, P., & Jensen, T. (2023). Dynamics of control on digital platforms. *Journal of Technology Governance*, 18(3), 128-141. <https://doi.org/10.1108/JTG-08-2023-0214>
- Grigalashvili, V. (2022). E-government and e-governance: Various or multifarious concepts. *International Journal of Scientific and Management Research*, 5(1), 183-196.
- Harthy, M. (2022). E-Governance and its implications for the Royal Oman Police. *Oman Journal of Public Administration*, 15(1), 22-30.
- Heeks, R. (2020). *Implementing and managing e-government: International challenges*. SAGE Publications.
- Idrus, S. H., Sumartono, E., Wartono, W., Suharto, S., & Syahriar, I. (2024). Harnessing digital transformation for improved public service delivery: Lessons from global administrative practices. *Join: Journal of Social Science*, 6(2), 122-140. <https://doi.org/10.59613/k8s6s859>.
- Jauhari, A., Abd Majid, M. S., Basri, H., & Djalil, M. A. (2020). Are e-government and bureaucratic reform promoting good governance towards a better performance of public organizations? *Calitatea*, 21(3), 8-18.
- Koolen, C., Wuyts, K., Joosen, W., & Valcke, P. (2024). From insight to compliance: Appropriate technical and organisational security measures through the lens of cybersecurity maturity models. *Comput. Law Secur. Rev.*, 52, 105914. <https://doi.org/10.1016/j.clsr.2023.105914>
- Lee-Geiller, S., & others. (2024). The moderating effect of digital literacy on the link between e-government effectiveness and public trust. *Journal of Public Sector Studies*, 39(4), 77-93.
- Lottu, O. A., Jacks, B. S., Ajala, O. A., & Okafor, E. S. (2024). Theoretical frameworks for ICT for development: Impact assessment of telecommunication infrastructure projects in Africa and the U.S. *World Journal of Advanced Research and Reviews*. <https://doi.org/10.30574/wjarr.2024.21.3.0721>
- Milić, M., Borocki, J., & Vekić, A. (2024). The power of ICT infrastructure in fostering innovation. *2024 47th MIPRO ICT and Electronics Convention (MIPRO)*, 1905-1910. <https://doi.org/10.1109/MIPRO60963.2024.10569834>
- Mushka, D. (2024). Digital platforms as tools for modern digital marketing. *International Journal of Digital Business*, 12(1), 32-47. <https://doi.org/10.1016/j.ijdigital.2024.01.004>
- Nevrovskiy, A., & Zincova, M. (2024). Definitions and classifications of digital platforms. *Journal of Digital Economy Studies*, 7(1), 98-113. <https://doi.org/10.1016/j.jdes.2024.01.002>
- Nguyen, V. C. T., & Le, H. (2024). The impact of ICT infrastructure, technological innovation, renewable energy consumption, and financial development on carbon dioxide emission in emerging economies: New evidence from Vietnam. *Management of Environmental Quality: An International Journal*. <https://doi.org/10.1108/meq-09-2023-0325>

- Obiki-Osafiele, A. N., Agu, E. E., & Chiekezie, N. R. (2024). Protecting digital assets in fintech: Essential cybersecurity measures and best practices. *Computer Science & IT Research Journal*, 5(8). <https://doi.org/10.51594/csitrj.v5i8.1449>
- Odusanya, O. S. E., Uroye, A., Onibon, M. G. T., & Efunade, A. O. (2024). An assessment of e-governance impact on public service delivery in Ekiti State, Nigeria. *Mitteilungen Klosterneuburg*, 7(1), 25-40. <https://doi.org/10.61586/nyanx>.
- Olabimitan, A. O., Ogunmodede, K., & Alaba, O. (2025). E-Governance and public service delivery: Evidence from Nigeria. *ORGANIZE: Journal of Economics, Management and Finance*, 4(1), 110-122. <https://doi.org/10.58355/organize.v4i1.149>
- Olusola, O. (2021). The digital divide and technology adoption in public sector organizations: A critical analysis. *Journal of Information Technology and Development*, 27(2), 159-177. <https://doi.org/10.1002/itdj.10223>
- Oman Observer. (2022). Cybersecurity challenges in Oman's e-governance. *Oman Observer*. Retrieved from <https://www.omanobserver.om>
- Oni, S., Oni, A. A., Ibietan, J., & Deinde-Adedeji, G. O. (2020). E-consultation and the quest for inclusive governance in Nigeria. *Cogent Social Sciences*, 6(1), 1823601. <https://doi.org/10.1080/23311886.2020.1823601>
- Pandey, J. K. (2024). Evaluating public service value within collaborative e-governance: A study in the Indian context. *Digital Transformation and Society*, 3(2), 197-213. <https://doi.org/10.1186/s40820-024-00351-z>
- Rocheston. (2024, October 21). The importance of cybersecurity in e-government. <https://u.rocheston.com/the-importance-of-cybersecurity-in-e-government/>
- Shaxnoza, J. (2024). Impact of e-governance on public service efficiency. *International Journal of Law and Policy*, 5(3), 108-120. <https://doi.org/10.59022/ijlp.229>.
- Singh, M. K., & Saxena, R. (2023). Good governance and e-governance. *Idealistic Journal of Advanced Research in Progressive Spectrums (IJARPS)*, 2(12), 19-26. <https://doi.org/10.4018/978-1-7998-6452-8.ch007>
- Sinomics Journal. (2024). Digital transformation in public service management. *Sinomics Journal*, 3(4), 1248.
- Sirkoi, K. R., Omboto, P., & Musebe, R. (2021). Perceived influence of performance standards on quality public service delivery in national government administration in Elgeyo Marakwet County. *East African Journal of Interdisciplinary Studies*, 3(1), 116-127. <https://doi.org/10.46912/eajis.2021.033012>
- Srite, M., & Karahanna, E. (2006). The role of espoused national cultural values in technology acceptance. *MIS Quarterly*, 30(3), 679-704. <https://doi.org/10.2307/25148757>
- Suri, P. K. (2022). Effectiveness of strategy implementation and e-governance performance. *Evaluation and Program Planning*, 77, 101-112. <https://doi.org/10.1016/j.evalprogplan.2022.101123>
- Tornatzky, L. G., & Fleischer, M. (1990). *The process of technological innovation*. Lexington Books.
- Transputec. (2024, September 25). Importance of cybersecurity in public sector. <https://www.transputec.com/blogs/cybersecurity-in-public-sector/>
- United Nations. (2022). *E-Government Survey 2022: The future of digital government*. United Nations Department of Economic and Social Affairs. <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2022>
- UpGuard. (2025, July 1). Guarding governance: Cybersecurity in the public sector. <https://www.upguard.com/blog/cybersecurity-in-the-public-secto>
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425-478. <https://doi.org/10.2307/30036540>
- Wang, C., & Teo, T. S. H. (2020). Online service quality and perceived value in mobile government success: An empirical study of mobile police in China. *International Journal of Information Management*, 50, 44-56. <https://doi.org/10.1016/j.ijinfomgt.2019.04.002>
- World Bank. (2020). *Digital government: Pathways to create public value*. World Bank Group. <https://openknowledge.worldbank.org/handle/10986/35167>
- Zeamari, I., & Laurier, W. (2024). Defining digital platforms: A systematic literature review. *Journal of Digital Platforms and Innovation*, 9(2), 85-101. <https://doi.org/10.1007/s40797-024-00124-5>
- Zhang, M., & Bhattacharjee, B. (2024). Evaluating the impact of e-governance on public service delivery: A case study of Bangladesh. *Malaysian Journal of Social Sciences and Humanities (MJSSH)*, 9(9), 2950-2965. <https://doi.org/10.47405/mjssh.v9i9.2960>.
- Zhang, Y., & Kimathi, F. A. (2022). Exploring the stages of e-government development from public value perspective. *Technology in Society*, 68, 101-115. <https://doi.org/10.1016/j.techsoc.2022.101433>