Journal of Business Systems Innovation and Management Science

IMPACT OF ROBUST FIREWALLS ON THE PERFORMANCE OF THE E-CITIZEN PLATFORM IN KENYA

Joshua Wariua Kebuka and **Dr. Emmy Rotich, PhD**

Journal of Business Systems Innovation and Management Science
ISSN: 1849-5419
Vol.3, Issue.No.2, 2026

Impact of Robust Firewalls On the Performance of the E-Citizen Platform in Kenya

Joshua Wariua Kebuka

Corresponding Author, Jomo Kenyatta University of Agriculture and Technology

Dr. Emmy Rotich, PhD

Lecturer, Entrepreneurship and Procurement Department, School of Business and Entrepreneurship, Jomo Kenyatta University of Agriculture and Technology

Article History:
***Published on**:* 13 /07/2026

DOI:
https://doi.org/10.5281/zenodo.21334667

***How to Cite**:* Kebuka, J. W., & Rotich, E. (2026). Impact of Robust Firewalls On the Performance of the E-Citizen Platform in Kenya. *Journal of Business Systems Innovation and Management Science*, 3(2), 1–19.
https://doi.org/10.5281/zenodo.21334667

Abstract:

Purpose of the Study: The purpose of this study was to determine the impact of robust firewalls on the performance of the e-Citizen platform in Kenya. Specifically, the study examined how firewall configuration quality, response time, intrusion detection capability, and update frequency influence platform availability, reliability, security, and overall service delivery effectiveness.

Methodology: The study adopted a mixed-methods descriptive research design targeting 500 respondents comprising e-Citizen users, e-government officials, information technology staff, and cybersecurity professionals. A sample of 150 respondents was selected through stratified and simple random sampling. Quantitative and qualitative data were analysed using descriptive, inferential, and thematic techniques.

***Findings**:* The study achieved a response rate of 91.3%. Findings indicated that respondents strongly agreed firewall configuration quality, rapid threat response, and frequent updates significantly enhance platform performance. Pearson correlation analysis established a strong positive and statistically significant relationship between robust firewalls and e-Citizen platform performance ($r = 0.735$, $p < 0.001$). Regression analysis further revealed that robust firewalls significantly predicted platform performance, explaining 54.0% of the variance ($R^2 = 0.540$). The findings demonstrate that robust firewall implementation substantially improves platform availability, reliability, transaction processing, data security, and overall resilience against evolving cyber threats.

Conclusion: The study concludes that robust firewalls significantly enhance the performance of Kenya's e-Citizen platform by improving security, availability, and reliability. Continuous firewall updates, effective intrusion detection, and integration with broader cybersecurity governance and business continuity planning are essential for sustaining resilient, secure, and efficient digital government service delivery.

***Keywords**: Robust Firewalls, e-Citizen Platform, Platform Performance, Cybersecurity.*

1. INTRODUCTION

1.1 Background of the Study

The digitalisation of public service delivery has become a central pillar of government modernisation programmes worldwide, promising faster, more transparent, and more accessible services to citizens. This transformation, however, exposes government digital platforms to an expanding range of cyber threats, since consolidating thousands of sensitive services onto a single portal creates a high-value target for malicious actors. Firewalls remain the foundational layer of defence against such threats, filtering network traffic according to defined security rules and preventing unauthorised access before it reaches sensitive government systems. In Kenya, the e-Citizen platform has evolved into the principal digital gateway for public service delivery, hosting over five thousand services ranging from passport applications to business registration and tax-related transactions. The performance of this platform, measured in terms of availability, transaction speed, reliability, and data security, is therefore inseparable from the strength of the cybersecurity architecture that protects it, making the study of firewall robustness directly relevant to the platform's continued success.

1.1.1 Global Perspective

Globally, governments have recognised that the performance and trustworthiness of digital public services depend heavily on the robustness of their underlying network security architecture. Estonia, widely regarded as Europe's most advanced digital government, has built its e-governance ecosystem around a distributed, encrypted data-exchange layer known as X-Road, supported by layered firewall and intrusion-detection controls that allow the country to sustain near-continuous availability of digital services despite being one of the most cyber-targeted nations in Europe (Kitsing, 2025). In Asia, research on network security architecture in Bangladesh demonstrated that deploying next-generation firewalls configured with deep packet inspection across seven layers of the network significantly improved the detection and mitigation of intrusion attempts compared with conventional firewall configurations, underscoring the direct link between firewall sophistication and system performance (Islam et al., 2023). A broader systematic review of local government cybersecurity practice similarly found that jurisdictions investing in layered technical controls, including firewalls, consistently reported fewer service disruptions and stronger public trust in digital platforms than those relying on outdated or minimally configured security infrastructure (Hossain et al., 2024). These global cases illustrate that firewall robustness is not merely a technical safeguard but a direct determinant of the continuity and credibility of digital government services.

1.1.2 Regional Perspective

Within Africa, the performance of government digital platforms has been similarly shaped by the strength, or weakness, of network security controls. In West Africa, Nigeria's telecommunications regulator has reported a sustained rise in distributed denial-of-service and ransomware incidents targeting government and financial platforms, with weak firewall configuration and delayed patching repeatedly identified among the contributing vulnerabilities

that degrade service availability (Nigeria Communications Commission, as cited in Gana et al., 2024). In Southern Africa, an evaluation of South Africa's digital government transformation found that public sector platforms which had adopted more comprehensive cybersecurity governance, including firewall management as part of a wider control framework, recorded improved service continuity and user confidence compared with agencies still reliant on fragmented, ad hoc security practices (Shibambu, 2024). A related study assessing the applicability of international cyber-resilience frameworks such as the NIST Cybersecurity Framework and ISO/IEC 27001 to developing-country e-government contexts found that South African public agencies applying structured, multi-layered security controls achieved measurably higher resilience scores than agencies applying isolated technical fixes (Rambau et al., 2026). These regional experiences reinforce that firewall robustness functions most effectively as part of a broader, well-governed security architecture rather than as an isolated technical intervention.

1.1.3 Local Perspective of Cybersecurity Integration in the e-Citizen Platform

In Kenya, the e-Citizen platform has grown into the government's principal digital service delivery channel, and its cybersecurity posture has consequently attracted sustained public and regulatory scrutiny. In July 2023, barely a month after President William Ruto relaunched the platform with an expanded catalogue of over five thousand services, a distributed denial-of-service attack claimed by a group calling itself Anonymous Sudan rendered e-Citizen and several dependent services, including electricity token purchases and mobile banking platforms, inaccessible for days (Kenya ICT Action Network, 2023). The Office of the Auditor-General subsequently reported that, for the financial year preceding the attack, the e-Citizen platform lacked an approved information and communication technology policy, a steering committee, a business continuity plan, and a secondary backup site, exposing the platform to significant operational risk (Nation Media Group, 2025). More recent incidents, including a major disruption of the platform's core payment channel in January 2025 and intermittent login failures reported in March 2026, indicate that availability challenges have persisted even after the 2023 attack (Kenyans.co.ke, 2026). These recurring disruptions underscore the practical urgency of strengthening firewall and broader network security controls to safeguard the continuity of Kenya's digital public services.

1.1.4 The e-Citizen Platform, Kenya

The e-Citizen platform is Kenya's flagship digital government portal, developed to consolidate access to public services previously scattered across multiple ministries, departments, and agencies into a single online window. Since its relaunch in June 2023, the platform has hosted services spanning passport and visa processing, national identification, business registration, driving licences, and an increasing share of national revenue collection, positioning it as critical information infrastructure under Kenya's Computer Misuse and Cybercrimes Act. The platform's centrality to public administration means that any degradation in its performance, whether through downtime, slow transaction processing, or data compromise, carries consequences that extend well beyond individual inconvenience to affect revenue collection, service delivery, and public trust in digital governance. It is within this context that the present

study examines the specific contribution of robust firewalls to sustaining and improving the platform's performance.

1.2 Statement of the Problem

The Kenyan government has invested substantially in expanding the e-Citizen platform's service catalogue and promoting its adoption as the default channel for public service delivery. Despite this investment, the platform has repeatedly experienced significant performance and security disruptions, most notably the July 2023 distributed denial-of-service attack that paralysed access to over five thousand services for several days, alongside subsequent downtime incidents affecting core payment functions in January 2025 and login access in March 2026 (Kenyans.co.ke, 2026). Compounding this concern, the Office of the Auditor-General found that the platform had, at the time of the 2023 attack, no approved information and communication technology policy, no steering committee, and no secondary backup site, findings that point directly to gaps in the underlying security architecture, including firewall governance, rather than to isolated technical failures (Nation Media Group, 2025).

This pattern of recurring disruption, despite the platform's strategic importance, suggests that the relationship between firewall robustness and platform performance in the Kenyan context has not been systematically or empirically established, even though comparable studies elsewhere have linked firewall configuration quality and response time directly to the continuity of digital government services (Islam et al., 2023; Hossain et al., 2024). Existing Kenyan and regional literature on e-government cybersecurity has tended to focus on broad governance frameworks or general threat landscapes rather than isolating the specific contribution of firewall infrastructure to measurable platform performance outcomes (Mabonga & Nyamboga, 2024). This study therefore sought to address this gap by empirically examining the impact of robust firewalls on the performance of the e-Citizen platform in Kenya, generating evidence to inform the platform's ongoing cybersecurity investment.

Purpose of the Study

The purpose of the study was to determine the impact of robust firewalls on the performance of the e-Citizen platform in Kenya.

Research Hypothesis

H01: Robust firewalls do not significantly influence the performance of the e-Citizen platform in Kenya.

2. LITERATURE REVIEW

2.1 Introduction

This chapter presents the theoretical foundation underpinning the study, a review of relevant empirical literature on firewalls and digital platform performance, and the conceptual framework guiding the analysis.

2.2 Theoretical Review

2.2.1 Defense-in-Depth Theory

Defense-in-Depth Theory originated from military strategy and was later adapted into information security practice to guide the design of layered defences against increasingly sophisticated digital threats. The theory holds that no single security control, however well designed, can guarantee complete protection of a digital system, and that resilience is instead achieved by combining multiple, complementary layers of defence, including firewalls, intrusion detection systems, encryption, and access control measures, so that the failure of one layer does not expose the entire system to compromise. Within this layered architecture, the firewall occupies a foundational position, filtering incoming and outgoing network traffic according to defined security rules and thereby determining, in large part, what reaches the deeper layers of the system in the first place.

Applied to the e-Citizen platform, Defense-in-Depth Theory suggests that the quality, responsiveness, and update frequency of firewall configuration directly shape the platform's exposure to disruption, since a poorly configured or infrequently updated firewall weakens the very first line of defence upon which subsequent layers depend. Recent empirical work on next-generation firewalls configured with deep packet inspection across multiple network layers found that such layered configurations substantially improved intrusion detection and reduced successful breach attempts relative to conventional, single-layer firewall deployments (Islam et al., 2023). Similarly, a systematic review of local government cybersecurity practice found that jurisdictions applying structured, multi-layered technical controls, consistent with Defense-in-Depth principles, experienced fewer service disruptions than those relying on isolated or poorly maintained security tools (Hossain et al., 2024). These findings affirm the theory's continued relevance to understanding how firewall robustness, as one layer within a broader defensive architecture, shapes the performance and resilience of public digital platforms such as e-Citizen.

A recognised limitation of Defense-in-Depth Theory is that implementing multiple overlapping layers of security can increase system complexity, cost, and the likelihood of misconfiguration, which may itself introduce latency or false positives that degrade platform performance even as security nominally improves (Rambau et al., 2026). This caution is particularly relevant for resource-constrained public institutions in developing countries, where the human and financial capacity to maintain multiple, well-coordinated security layers may be limited. Despite this limitation, the theory remains a robust foundation for examining how firewall robustness contributes to the protection and performance of the e-Citizen platform, since it explains both the potential benefits of layered defence and the practical trade-offs that must be managed in its implementation.

2.2.2 The Concept of e-Citizen Platform Performance

Platform performance, within the context of digital government services, refers to the extent to which a system remains available, processes transactions promptly, safeguards user data, and recovers quickly from disruption, in a manner that meets user expectations for reliability and trust. For a platform such as e-Citizen, which hosts a large and growing share of Kenya's public administrative and financial transactions, performance is inseparable from security, since a breach or denial-of-service incident directly manifests as downtime, delayed transactions, or compromised data, all of which constitute performance failures from the perspective of the citizen user.

2.3 Empirical Review

A growing body of recent literature has examined the relationship between firewall robustness and the performance of digital platforms in both public and private sector contexts. Islam et al. (2023) evaluated the deployment of a Cisco-based next-generation firewall within a scientific research organisation's network, configuring firewall policies across all seven layers of the Open Systems Interconnection model and analysing resulting intrusion attempt data. The study found that the next-generation firewall configuration substantially improved the detection and prevention of network and application-layer threats compared with the organisation's prior security posture, demonstrating that firewall sophistication translates directly into measurable gains in threat mitigation capacity relevant to sustaining platform performance.

A related study examining performance-driven architectural approaches to next-generation firewalls found that incorporating hardware acceleration alongside contextual, application-aware inspection allowed firewalls to maintain high throughput without sacrificing security accuracy, addressing a common trade-off in which stronger security controls degrade system responsiveness (International Journal of Computer Technology and Electronic Communication, 2023). This finding is particularly relevant to public platforms such as e-Citizen, where citizens expect both strong data protection and fast transaction processing.

At the regional level, Mabonga and Nyamboga (2024) conducted a comprehensive review of cybersecurity measures across East African e-government systems and found that inconsistent firewall management, limited intrusion detection capacity, and weak incident response planning were recurring vulnerabilities that undermined the reliability of digital public services across the region, a pattern consistent with Kenya's own experience of recurring e-Citizen disruptions. In South Africa, Shibambu (2024) found that government departments which had integrated stronger technical security controls into their digital transformation strategies reported improved continuity of online public services relative to departments that treated cybersecurity as a secondary concern. Extending this analysis, Rambau et al. (2026) evaluated the applicability of internationally recognised cyber-resilience frameworks, including the National Institute of Standards and Technology Cybersecurity Framework and ISO/IEC 27001, to e-government platforms in developing-country contexts, finding that agencies applying structured, framework-guided security controls, of which firewall governance forms a core component, achieved significantly higher resilience outcomes than agencies applying ad hoc technical fixes.

Taken together, these studies affirm a consistent, positive relationship between the robustness of firewall infrastructure and the performance and resilience of digital platforms across diverse global, regional, and sectoral contexts, while also cautioning that firewall investment yields its fullest benefit when embedded within a broader, well-governed security architecture, precisely the layered logic anticipated by Defense-in-Depth Theory and examined empirically in this study.

2.4 Conceptual Framework

The conceptual framework for this study proposes a direct relationship between robust firewalls, the independent variable, and e-Citizen platform performance, the dependent variable. Robust firewalls are operationalised through indicators of configuration quality, threat response time, intrusion detection rate, and update frequency. e-Citizen platform performance, the dependent variable, is operationalised through indicators of service availability, transaction speed, data security, and system reliability. Guided by Defense-in-Depth Theory, the framework conceptualises the firewall as the foundational security layer whose robustness shapes the extent to which the platform can sustain continuous, secure, and efficient service delivery to citizens.

3. RESEARCH METHODOLOGY

The study adopted a mixed-methods descriptive research design to examine the impact of robust firewalls on the performance and security of the e-Citizen platform in Kenya. Integrating quantitative and qualitative approaches enabled the collection of statistical evidence alongside in-depth insights regarding cyber threats, user experiences, and existing cybersecurity practices. The target population comprised 500 respondents, including e-Citizen users, e-government officials, information technology staff, and cybersecurity professionals with direct experience in the use or management of the platform. A sample of 150 participants, representing 30 percent of the population, was selected through stratified random sampling followed by simple random sampling within each stratum to ensure adequate representation and minimise bias. The sampling frame was derived from registered e-Citizen users and official databases of personnel responsible for platform security and management. Quantitative data were collected using structured questionnaires administered to platform users, while qualitative information was obtained through interviews with officials and information technology personnel. Data collection was undertaken after obtaining the necessary research permits and observing ethical principles, including informed consent and confidentiality. Quantitative data were analysed using descriptive and inferential statistics in the Statistical Package for the Social Sciences, while qualitative responses underwent thematic analysis, with findings presented through tables, charts, and narratives.

4. RESEARCH FINDINGS AND DISCUSSION

4.1 Response Rate

The study targeted a sample of 150 respondents drawn from three strata: e-Citizen users, e-government officials and information technology staff, and cybersecurity professionals. Out of the 150 administered questionnaires, a total of 137 were duly completed and returned, representing an overall response rate of 91.3 percent.

Table 1: Response Rate

Category	Sampled	Responded	Response Rate	Remarks
E-Citizen Users	120	113	94.2%	Included
E-Government Officials & IT Staff	21	15	71.4%	Included
Cybersecurity Professionals	9	9	100.0%	Included
Total	150	137	91.3%	

As shown in Table 1, e-Citizen users recorded a response rate of 94.2 percent, e-government officials and information technology staff recorded 71.4 percent, and cybersecurity professionals recorded 100.0 percent, yielding a composite response rate of 91.3 percent. This response rate is considered adequate for drawing valid statistical inferences. The high rate of return is attributable to the drop-and-pick-later data collection method and advance scheduling of interviews, which afforded respondents sufficient time to complete the instruments. Mugenda and Mugenda (2003) contend that a response rate of 70 percent and above is acceptable for social science research, a threshold substantially exceeded in the present study. This position is corroborated by Nulty (2022), who established that response rates above 80 percent yield more representative findings and substantially reduce the risk of non-response bias in survey-based studies.

4.2 Descriptive Analysis: Robust Firewalls

The first objective of the study sought to assess the impact of robust firewalls on the performance of the e-Citizen platform in Kenya.

Table 2: Descriptive Statistics on Robust Firewalls and Platform Performance

Statement	N	Mean	Std. Dev.
RF1: Quality firewall configuration significantly enhances the security and performance of the e-Citizen platform.	137	4.23	0.891
RF2: Firewall response time to security threats directly affects platform performance and stability.	137	4.33	0.842
RF3: The e-Citizen platform benefits from a high intrusion detection rate, blocking most unauthorized access attempts.	137	4.17	0.912

RF4: Frequent firewall configuration updates ensure the platform remains secure against evolving cyber threats.	137	4.28	0.871
RF5: Firewall configuration effectively prevents unauthorized access, improving system reliability and security.	137	4.26	0.888
RF6: The firewall's response time is fast enough to prevent disruptions in e-Citizen platform performance.	137	4.25	0.876
RF7: The firewall's ability to block malicious attempts directly contributes to high availability of the e-Citizen platform.	137	4.26	0.909

As shown in Table 2, the findings revealed that the majority of respondents strongly agreed that the quality of firewall configuration significantly enhances the security and performance of the e-Citizen platform (M = 4.23, SD = 0.891). The study also revealed that the majority of respondents strongly agreed that the firewall's response time to security threats directly affects platform performance and stability (M = 4.33, SD = 0.842), representing the highest-scoring item in this construct. The study further established that most respondents agreed that the platform benefits from a high intrusion detection rate through effective firewall deployment (M = 4.17, SD = 0.912), the lowest-rated item, suggesting comparatively greater variability in how strongly respondents perceive detection effectiveness. Frequent firewall configuration updates were similarly rated highly as a determinant of continued security against evolving threats (M = 4.28, SD = 0.871), as was the firewall's role in preventing unauthorised access (M = 4.26, SD = 0.888), maintaining adequate response speed (M = 4.25, SD = 0.876), and blocking malicious attempts to sustain platform availability (M = 4.26, SD = 0.909).

These findings are consistent with Islam et al. (2023), whose evaluation of a next-generation firewall configured across multiple network layers found substantial improvements in intrusion detection and threat mitigation capacity, reinforcing the perceived importance of configuration quality and layered deployment observed among e-Citizen stakeholders. They are further corroborated by the performance-driven firewall architecture study, which found that maintaining high threat-detection accuracy without sacrificing system responsiveness required continuous architectural refinement, a balance reflected in respondents' simultaneous emphasis on both response time and detection rate (International Journal of Computer Technology and Electronic Communication, 2023). At the same time, Mabonga and Nyamboga (2024) caution that inconsistent firewall management remains a recurring vulnerability across East African e-government systems, a caution echoed in the comparatively lower and more variable rating recorded for intrusion detection effectiveness in the present study.

4.3 Descriptive Analysis: e-Citizen Platform Performance

The study further sought to measure the overall performance of the e-Citizen platform as influenced by firewall robustness.

Table 3: Descriptive Statistics on e-Citizen Platform Performance

Statement	N	Mean	Std. Dev.
EPP1: The e-Citizen platform is consistently available for use without frequent downtime.	137	4.10	0.930
EPP2: Transactions on the e-Citizen platform are processed quickly and without unnecessary delay.	137	4.22	0.874
EPP3: The e-Citizen platform safeguards my personal data and information from unauthorized access.	137	4.31	0.852
EPP4: The platform recovers quickly whenever it experiences disruption or downtime.	137	4.05	0.968
EPP5: I trust the e-Citizen platform to handle my transactions securely.	137	4.27	0.860
EPP6: The overall reliability of the e-Citizen platform has improved over the past year.	137	4.14	0.921
EPP7: The e-Citizen platform's performance meets my expectations of a government digital service.	137	4.19	0.887

As shown in Table 3, respondents rated the platform's ability to safeguard personal data from unauthorised access most highly (M = 4.31, SD = 0.852), followed closely by trust in the platform's ability to handle transactions securely (M = 4.27, SD = 0.860). Transaction processing speed was also positively rated (M = 4.22, SD = 0.874), and respondents generally agreed that the platform's overall reliability had improved over the past year (M = 4.14, SD = 0.921) and that its performance met their expectations of a government digital service (M = 4.19, SD = 0.887). The item concerning consistent availability without frequent downtime recorded a comparatively lower mean (M = 4.10, SD = 0.930), while the platform's speed of recovery from disruption recorded the lowest mean and highest standard deviation in the construct (M = 4.05, SD = 0.968), indicating greater variability in respondents' experience of the platform's resilience following outages.

These comparatively more modest ratings for availability and recovery speed align closely with Kenya's documented experience of recurring e-Citizen disruptions, including the July 2023 distributed denial-of-service attack and subsequent downtime incidents in January 2025 and March 2026 (Kenyans.co.ke, 2026), as well as the Auditor-General's finding that the platform previously lacked an approved business continuity plan and secondary backup site (Nation Media Group, 2025). This pattern is consistent with Rambau et al. (2026), who found that developing-country e-government platforms applying only partial or ad hoc security controls tended to recover more slowly from disruption than those guided by structured, framework-

based resilience planning, underscoring that firewall robustness alone, without complementary continuity planning, may not fully resolve availability and recovery challenges.

4.4 Inferential Analysis

4.4.1 Pearson Correlation Analysis

Pearson's product-moment correlation was conducted to assess the strength and direction of the bivariate linear relationship between robust firewalls and e-Citizen platform performance.

Table 4: Pearson Correlation Matrix

	Robust Firewalls	e-Citizen Platform Performance
Robust Firewalls – Pearson Corr.	1	.735**
Sig. (2-tailed)	-	.000
N	137	137
e-Citizen Platform Performance – Pearson Corr.	.735**	1
Sig. (2-tailed)	.000	-
N	137	137

*Note: **Correlation is significant at the 0.01 level (2-tailed).*

The correlation analysis revealed a strong, positive, and statistically significant relationship between robust firewalls and e-Citizen platform performance ($r = .735$, $p < .001$, $N = 137$). This finding indicates that as firewall configuration quality, response time, intrusion detection rate, and update frequency improve, platform performance in terms of availability, security, and reliability improves correspondingly. This strength of association is consistent with Islam et al. (2023), who similarly found a marked improvement in threat detection and system protection following the deployment of a well-configured next-generation firewall.

4.4.2 Model Summary

The model summary presents the overall explanatory power of the regression model relating robust firewalls to e-Citizen platform performance.

Table 5: Model Summary

Model	R	R^2	Adjusted R^2	Std. Error of Estimate
1	.735a	.540	.537	.398

Predictors: (Constant), Robust Firewalls. Dependent Variable: e-Citizen Platform Performance.

The regression model yielded a correlation coefficient of .735, confirming a strong positive linear relationship between robust firewalls and platform performance. The coefficient of

determination (R^2 = .540) demonstrates that robust firewalls alone explained 54.0 percent of the variance in e-Citizen platform performance, a substantial proportion for a single-predictor model in public sector digital governance research. The adjusted R^2 of .537 confirms the model's robustness after accounting for sample size. This explanatory strength is broadly consistent with Hossain et al. (2024), whose systematic review found that technical security controls, including firewalls, were consistently among the strongest predictors of digital platform continuity in local government contexts.

4.4.3 Analysis of Variance

The Analysis of Variance test was performed to determine the overall statistical significance of the regression model.

Table 6: ANOVA Results

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	33.399	1	33.399	158.51	.000b
Residual	28.451	135	.211		
Total	61.850	136			

a. Dependent Variable: e-Citizen Platform Performance. b. Predictors: (Constant), Robust Firewalls.

The results confirm that the regression model was statistically significant ($F(1, 135) = 158.51$, $p < .001$). The regression sum of squares was substantially larger than the residual sum of squares, confirming that the model accounted for a considerably greater proportion of variance in platform performance than remained unexplained. This result validates the utility of the regression model and affirms that robust firewalls significantly predict variation in e-Citizen platform performance, consistent with the significant relationships reported by Islam et al. (2023) and Shibambu (2024) in their respective evaluations of firewall and broader security control effectiveness.

4.4.4 Regression Coefficients

The regression coefficients indicate the contribution of robust firewalls to e-Citizen platform performance.

Table 7: Regression Coefficients

	B	Std. Error	Beta (β)	t	Sig.
(Constant)	1.052	.201		5.234	.000
Robust Firewalls (X)	.731	.058	.735	12.603	.000

Dependent Variable: e-Citizen Platform Performance.

Based on the unstandardised coefficients, the fitted regression equation is expressed as: e-Citizen Platform Performance = 1.052 + 0.731 (Robust Firewalls). The coefficient indicates that a unit improvement in robust firewalls is associated with a 0.731-unit increase in platform

performance, holding other factors constant (B = .731, β = .735, t = 12.603, p < .001). This finding provides strong empirical support for rejecting the null hypothesis and concluding that robust firewalls significantly and positively influence the performance of the e-Citizen platform in Kenya. The magnitude and significance of this coefficient corroborate the findings of Islam et al. (2023), who demonstrated that layered, well-configured firewall deployment produced measurable improvements in network protection, and of Rambau et al. (2026), who found that structured technical security controls were significant contributors to e-government platform resilience in developing-country contexts.

5. SUMMARY OF THE STUDY

This study set out to determine the impact of robust firewalls on the performance of the e-Citizen platform in Kenya. The descriptive findings revealed strong agreement among respondents that firewall configuration quality and response time are central to sustaining platform security and stability, although intrusion detection effectiveness and post-disruption recovery speed emerged as comparatively weaker dimensions. Correlation analysis established a strong, positive, and statistically significant relationship between robust firewalls and platform performance (r = .735, p < .001), while regression analysis confirmed that robust firewalls significantly predicted platform performance outcomes, accounting for 54.0 percent of the variance. These findings are consistent with global, regional, and Kenyan evidence affirming that firewall robustness, when embedded within a broader, well-governed cybersecurity architecture, substantially strengthens the availability, security, and reliability of digital government platforms.

6. CONCLUSION

The study concludes that robust firewalls exert a significant and substantial positive influence on the performance of the e-Citizen platform in Kenya. The strength of the relationship established in this study demonstrates that continued investment in firewall configuration quality, rapid threat response capability, and regular rule updates is likely to yield measurable improvements in platform availability, security, and citizen trust. At the same time, the comparatively weaker ratings recorded for intrusion detection effectiveness and disruption recovery speed, together with the Auditor-General's documented findings on the platform's historical absence of a business continuity plan and backup infrastructure, indicate that firewall robustness alone cannot fully guarantee platform resilience. Consistent with Defense-in-Depth Theory, firewalls function most effectively as one layer within a broader, coordinated security architecture that also encompasses governance structures, continuity planning, and complementary technical controls.

7. RECOMMENDATIONS

Based on the study's findings, the agencies responsible for the e-Citizen platform should institutionalise continuous firewall rule updates and regular penetration testing to ensure that

configurations remain responsive to evolving threat patterns. Investment should be directed towards strengthening intrusion detection capabilities, including the adoption of machine learning-based anomaly detection, to address the comparatively weaker performance recorded for this dimension. The platform's custodians should also formalise a comprehensive business continuity plan, complete with a secondary backup site, to address the gaps previously identified by the Office of the Auditor-General and to improve recovery speed following any future disruption. Finally, firewall investment should be pursued as part of a broader, coordinated cybersecurity governance framework, encompassing clear policy, a dedicated steering committee, and continuous staff capacity building, rather than as an isolated technical measure.

8. AREAS FOR FURTHER RESEARCH

Future research should consider comparative studies examining the influence of firewall robustness on the performance of other Kenyan e-government platforms, to establish whether the relationship identified in this study holds across different digital service contexts. Longitudinal studies tracking e-Citizen platform performance over successive years, particularly following major security incidents, would provide valuable insight into the durability of firewall-driven performance gains. Additionally, further research could examine the specific organisational and governance factors, such as staff cybersecurity competence, incident response protocols, and budgetary allocation, that moderate the relationship between firewall robustness and digital platform performance in resource-constrained government contexts.

9. REFERENCES

Gana, I. M., Ibrahim, A. F., Oluwaseyi, W. A., & Wali, A. I. (2024). Cyber warfare and national security in Nigeria: Threats and responses. Kwararafa Security Review, 1(2), 1–18. https://www.researchgate.net/publication/389026012_Cyber_Warfare_and_National_Security_in_Nigeria_Threats_and_Responses

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Local government cybersecurity landscape: A systematic review and conceptual framework. Applied Sciences, 14(13), 5501. https://doi.org/10.3390/app14135501

Islam, M. S., Uddin, M. A., Ahmed, M. S., & Moazzam, G. (2023). Analysis and evaluation of network and application security based on next generation firewall. International Journal of Computing and Digital Systems, 13(1), 193–202. https://doi.org/10.12785/ijcds/130116

International Journal of Computer Technology and Electronic Communication. (2023). Next-generation firewalls: A performance-driven approach to contextual threat prevention. International Journal of Computer Technology and Electronic Communication, 6(1), 6339–6346. https://doi.org/10.15680/IJCTECE.2023.0601003

Kenya ICT Action Network. (2023). E-Citizen attack: How cyber insecurity enables inaccessibility. KICTANet. https://www.kictanet.or.ke/e-citizen-attack-how-cyber-insecurity-enables-inaccessibility/

Kenyans.co.ke. (2026, March 5). eCitizen platform experiences outage as Kenyans decry service delays. https://www.kenyans.co.ke/news/121402-ecitizen-platform-experiences-outage-kenyans-decry-service-delays

Kitsing, M. (2025). E-government as a development strategy: The case of Estonia. International Journal of Public Administration, 48(2), 1–15. https://doi.org/10.1080/01900692.2024.2316128

Mabonga, E., & Nyamboga, T. O. (2024). Cybersecurity measures in East African e-government systems. IAA Journal of Social Sciences, 10(2), 12–24. https://doi.org/10.59298/IAAJSS/2024/102.122400000

Mugenda, O. M., (2003). Research methods: Quantitative and qualitative approaches. African Centre for Technology Studies. https://ir-library.ku.ac.ke/items/0769481e-46cb-4710-b595-5806ae7db90e

Nation Media Group. (2025, August). Hackers' paradise: Auditor-General warned, hackers listened. Daily Nation. https://nation.africa/kenya/news/hackers-paradise-auditor-general-warned-hackers-listened-5268236

Nulty, D. D. (2022). The adequacy of response rates to online and paper surveys: What can be done? Assessment & Evaluation in Higher Education, 47(1), 1–14. https://doi.org/10.1080/02602930701293231

Rambau, T. M., Munyoka, W., Phahlamohlaka, L. J., & Kadyamatimba, A. (2026). Evaluating cyber resilience frameworks for e-government: Applicability of NIST CSF, ISO/IEC 27001 and COBIT 2019 in developing country contexts. Information & Computer Security. https://doi.org/10.1108/ICS-09-2025-0376

Shibambu, A. (2024). Transformation of digital government services in the public sector in South Africa. Africa's Public Service Delivery & Performance Review, 12(1), a753. https://doi.org/10.4102/apsdpr.v12i1.753