JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(3), SEPTEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

Enhancing Cyber Security in E - Governance System: Strategies for protecting digital public services and data privacy

[1]Emmanuel D. Dako, [2]Ore-Ofe Ajayi, [3]Imam A. Isa, [4]Aondonenge S. Dugguh, [5]Micheal Tase, [6]Nafisa Shehu Usman
[1,2,3,4&6]*Computer Engineering Department, Ahmadu Bello University, Zaria*
[5]*ICT Department, Federal Airport Authority of Nigeria*

ABSTRACT
This research paper focuses on enhancing cybersecurity in e-governance systems, a critical area given the increasing reliance on digital platforms for government services. The study aims to evaluate the current cybersecurity landscape within e-governance infrastructures, identify vulnerabilities, and propose an improved, comprehensive framework to mitigate security risks. Using a mixed-method approach, data was collected through surveys with IT administrators and interviews with cybersecurity experts. The research examines key areas, including the challenges of securing legacy systems, the risks associated with multi-platform environments, and the integration of emerging technologies like Artificial Intelligence (AI), Internet of Things (IoT), and blockchain. The findings reveal significant concerns regarding outdated infrastructures, inconsistencies in security policies across platforms, and the vulnerabilities introduced by new technologies. Based on these insights, the proposed cybersecurity framework incorporates AI-driven threat detection, robust incident response strategies, and user-centered design principles to balance usability and security. The study highlights the potential of these measures to improve response times, secure data handling processes, and protect against advanced cyber threats.

ARTICLE INFO
Article History
Received: March, 2025
Received in revised form: June, 2025
Accepted: July, 2025
Published online: September, 2025

KEYWORDS
Artificial Intelligence (AI), cyber security, e-governance, Internet of Things (IoT, threat detection

INTRODUCTION

The digital transformation of governance systems has revolutionized how public services are delivered, offering increased efficiency, transparency, and accessibility. E-Governance involves the use of information and communication technologies (ICT) to facilitate the interaction between government bodies and citizens, businesses, and other arms of government [1]. However, the reliance on digital platforms exposes these systems to significant cyber security threats. This research paper aims to investigate the current state of cyber security in e-governance systems, identify vulnerabilities, and propose strategies to enhance their resilience against cyber threats.

E-government has become the main way for governments to connect with and serve their citizens. The World Bank explains that e-government involves using technology to make government operations and services better. The growth of e-government depends on several factors, including technology, skilled workers, supportive laws, good infrastructure, and the trust of the public [2].

E-government involves using Information and Communication Technology (ICT) to transform and improve public services, ensuring they are efficient, integrated, and impactful for citizens. It aims to enhance the management of citizen relations while supporting economic and social development at local, national, and international levels. By incorporating ICT into public administration, e-government simplifies workflows, improves data management, and enhances access to services, resulting in

Corresponding author: Emmanuel D. Dako.
successdgee@gmail.com
Computer Engineering Department, Ahmadu Bello University, Zaria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(3), SEPTEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

increased efficiency, transparency, and citizen empowerment. Despite its potential to improve people's well-being, the implementation of e-government systems has faced several challenges and failures along the way [3].

E-government applications are increasingly relying on cyberspace, which is still an emerging area when it comes to digital security. Cybersecurity, which focuses on protecting the networks and systems that make up cyberspace from intrusions, plays a key role in maintaining the safety and integrity of information. However, the constantly evolving risk landscape requires governments to adopt more dynamic and flexible strategies. To address cybersecurity challenges, governments are now developing comprehensive plans and adaptable approaches to ensure the protection of their digital systems and data [4].

Previous studies have shown that the failure of e-Government implementation is often linked to a lack of dedicated leadership. Additionally, research highlights resistance to change as a major challenge in adopting e-Government programs. This resistance stems from existing work practices, such as reliance on paperwork and fear of job loss. Some believe that e-Government disrupts long-standing systems, which can interfere with entrenched bribery and corruption practices or alter traditional structures. However, not all resistance to e-Government is driven by harmful intentions; in many cases, it is simply caused by inertia or reluctance to adapt to new systems [5].

MATERIALS AND METHODS

E-governance has been adopted in many developing countries to enhance government services that were previously inefficient and to support better governance systems [6]. E-governance involves the use of information and communication technologies (ICT) by governments and civil society to encourage greater citizen participation in political processes. It includes activities such as politicians and political parties using the internet to gather feedback from their constituencies and civil society organizations sharing opposing views to challenge ruling authorities. E-governance covers a wider scope, as it integrates ICT into government structures, decision-making, and the management of relationships between the state and the public. In contrast, e-government is considered a smaller part of e-governance, focusing specifically on the use of ICT to improve government services and operations [7].

In Nigeria, e-governance plays an important role in improving education and promoting innovation through digital platforms and tools that make educational activities more efficient. Strengthening e-governance can also help bridge communication gaps between the government, local communities, businesses, and the wider society. With better access to digital tools, public institutions and governments can create effective systems that improve transparency and accountability, helping to achieve goals like quality education and infrastructure development [8].

E-governance is divided into four main areas: government, population, commerce, and workforce, which are all closely linked. Each of these areas can use different frameworks to implement e-governance effectively. Cybersecurity focuses on protecting network servers, storage systems, and software applications by using the right technologies. As e-governance continues to grow, a strong and reliable cybersecurity strategy becomes essential, as shown in previous studies. Cybersecurity plays a key role in addressing major challenges at local, regional, and national levels. It helps prevent data breaches and ensures the safety and privacy of users [9]. Cybersecurity focuses on protecting critical systems and sensitive data from cyberattacks, which can come from both internal and external sources. It involves measures to secure networked systems and applications, often referred to as IT security.

A significant challenge lies in balancing safe operations with maintaining confidentiality. For effective governance, there must be transparency, accountability, integrity, and confidentiality. However, implementing e-governance comes with challenges, as cybersecurity plays a key role in addressing risks

Corresponding author: Emmanuel D. Dako.
successdgee@gmail.com
Computer Engineering Department, Ahmadu Bello University, Zaria.

associated with protecting sensitive information. With the rise of cybercrimes happening frequently, securing personal and official data has become a major concern. Government agencies handle large volumes of individual and business records, making it crucial for people to trust that their privacy and data security are well protected [10]. Digital public services evolve through various stages, including initiation, testing, implementation, and growth. Although their main goals and key functions generally stay the same, changes often occur during these phases. These changes may result from adopting new technologies, enforcing updated regulations, or introducing additional features [11].

Data privacy is essential for gaining consumer trust and can be achieved by clearly showing how data flows, along with proper authentication and authorization for activities like collecting, storing, processing, and sharing data. Risks to data privacy often arise from unauthorized actions such as collecting, using, accessing, storing, or sharing personal data. These risks can lead to data leaks and compromise user privacy, especially in healthcare, where the data is sensitive, valuable, and requires extra care. Therefore, it is important to implement proper security and protection measures to safeguard such information [12]. Data privacy focuses on the proper handling of data, including its collection, analysis, storage, and access. It emphasizes using data in a responsible way that aligns with users' preferences while ensuring protection against unauthorized access [13].

This study employed a mixed-methods approach, combining both qualitative and quantitative techniques to thoroughly investigate cybersecurity vulnerabilities in e-governance systems. The qualitative aspect involved conducting in-depth interviews with cybersecurity experts, government IT officials, and professionals involved in e-governance. These interviews provided nuanced, context-rich insights into the challenges and vulnerabilities of e-governance infrastructure, particularly concerning legacy systems, multi-platform integration, and the use of emerging technologies. The quantitative component, on the other hand, involved the distribution of structured surveys to gather measurable data on perceived vulnerabilities, the effectiveness of incident response strategies, and the balance between usability and security in e-governance.

To gather relevant data, a set of survey and interview questions were created to address specific research objectives. For the topic of legacy infrastructures and security risks, the survey asked participants whether they agreed that the lack of regular updates and patches in legacy systems poses a significant threat to e-governance security, with options ranging from "Strongly Agree" to "Strongly Disagree." The interview question for this topic focused on identifying the primary challenges in addressing security vulnerabilities in legacy systems within e-governance. Regarding multi-platform environments and vulnerabilities, the survey questioned whether security policies across different platforms in e-governance systems were well-coordinated, while the interview explored the consistency of security protocols across these platforms and the challenges resulting from any inconsistencies. In the area of emerging technologies in e-governance, the survey asked whether IoT devices integrated into e-governance systems posed a significant security risk, and the interview inquired about challenges faced when integrating technologies like AI and IoT into e-governance systems.

This method facilitated a comprehensive data collection, ensuring the study's findings were well-rounded, combining both measurable and experiential insights. Table 1 presents the data techniques used in this study. A systematic approach was taken to ensure that each step in the research process aligned with the study's objectives. The research focused on understanding both the broad landscape of e-governance cybersecurity through surveys and the detailed perspectives of domain experts through interviews. This approach facilitated the identification of recurring themes and patterns, which formed the basis for developing a cybersecurity framework tailored to e-governance.

Corresponding author: Emmanuel D. Dako.
successdgee@gmail.com
Computer Engineering Department, Ahmadu Bello University, Zaria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(3), SEPTEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

Data collection began with the distribution of online surveys to a diverse group of stakeholders, including cybersecurity experts, government officials, and IT professionals working in e-governance. The surveys incorporated Likert-scale questions, which enabled participants to express the degree of their agreement or disagreement on key issues, such as the effectiveness of multi-platform security policies and the vulnerabilities of IoT devices in e-governance.

Parallel to this, semi-structured interviews were conducted to gain qualitative insights into specific areas of concern identified in the literature, such as legacy infrastructure risks, incident response strategies, and challenges with emerging technologies. The interviews followed a flexible guide that allowed participants to elaborate on their experiences and perspectives while addressing the research objectives.

The sample for this study was purposively selected to ensure that participants possessed relevant expertise and experience with e-governance systems. Government officials involved in cybersecurity policymaking, IT professionals responsible for e-governance implementation, and cybersecurity specialists in both public and private sectors were targeted to provide a balanced perspective. These participants were selected based on their knowledge of the technical, operational, and policy aspects of cybersecurity in e-governance.

The research process unfolded in a structured sequence, starting with a comprehensive literature review to identify existing vulnerabilities and cybersecurity challenges within e-governance. This review helped refine the survey and interview questions to focus on key issues such as legacy systems, multi-platform integration, and emerging technologies. Following the literature review, the survey was distributed to a targeted sample, with data collected over four weeks. Concurrently, interviews were conducted, recorded, and transcribed to capture in-depth responses. Data from both the surveys and interviews were then analyzed to identify trends and patterns.

Ethical considerations were strictly adhered to throughout the study to protect participants' rights and confidentiality. All participants were informed of the study's purpose, and their consent was obtained before participation. The confidentiality of survey responses and interview transcripts was maintained, and data were anonymized to ensure privacy. Participants were also assured that their responses would be used solely for research purposes and stored securely. This ethical approach fostered a sense of trust and encouraged open and honest participation from all respondents. Table 2 presents the ethical considerations for the study.

Table 1: Data collection techniques.

Technique Type	Sample size	Purpose	Key questions	Related area
Survey	54 participants (including IT professionals, cybersecurity experts, and government officials)	To collect quantitative data on perceived vulnerabilities, security policies, and framework effectiveness.	1. How often are updates and patches applied to legacy systems? 2. How vulnerable do you think IoT devices are in e-governance systems?	Legacy Infrastructure, Multi-Platform Vulnerabilities, Emerging Technology
Interview	15 participants (cybersecurity experts and government IT administrators)	To gain in-depth qualitative insights on specific	1. What are the main security risks associated with legacy systems?	Incident Response, Cybersecurity Challenges

Corresponding author: Emmanuel D. Dako.
successdgee@gmail.com
Computer Engineering Department, Ahmadu Bello University, Zaria.

Technique Type	Sample size	Purpose	Key questions	Related area
		cybersecurity challenges and improvement areas in e-governance systems.	2. How effective are current incident response strategies?	
Focus Group	5 groups (each with 5 IT professionals from e-governance systems)	To discuss and validate the proposed cybersecurity framework design, ensuring practicality and relevance	1. How do you perceive the usability of the proposed framework? 2. Do you think the framework addresses key security needs?	Cybersecurity Framework Development
System Security Assessment	5 E-Governance platforms	To conduct a technical evaluation of network vulnerabilities and application security gaps in existing e-governance systems.	N/A (Technical results derived from automated tools and assessments)	Network Vulnerabilities, Application Security

Table 2: Ethical measures taken.

Ethical measure	Description	İmplementation details
Confidentiality	The anonymity and confidentiality of participants, especially in survey and interview responses.	Data anonymization techniques were applied; responses were recorded, and identifying details were removed from all reports.
Informed Consent	The participants are fully informed about the research purpose, procedures, and their rights.	A consent form was provided, explaining the study's goals, the voluntary nature of participation, and data usage.
Data Security	Protects collected data from unauthorized access or breaches.	All Data are well handled and secured and accessible only to authorized research personnel. Multi-factor authentication (MFA) was used for access.
Right to withdraw	The participants are granted the freedom to not to be provide any information without penalty.	Participants were informed of their right to withdraw in both the survey and interview.
Minimizing Harm	Prevents physical, emotional, or reputational harm to participants during and after the research.	Sensitive questions were carefully phrased; participants were assured of the anonymity and non-disclosure of their responses.

Corresponding author: Emmanuel D. Dako.
successdgee@gmail.com
Computer Engineering Department, Ahmadu Bello University, Zaria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(3), SEPTEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

Transparency of Findings	The research findings are shared openly with participants and stakeholders, reflecting honest and accurate results.	A summary of research findings was made in order to bring out full reports for better output.
Privacy in data Handling	Avoids misuse or over-collection of personal data beyond the study's scope.	Only essential information was collected, following the principle of data minimization. Data was processed strictly for the purposes stated in the study.
Fair Participant treatment	All participants were treated with respect and ensures fair handling of all participant-related activities.	Equal consideration and respect were given to all participants. Procedures were standardized to prevent bias.
Compliance with Regulations	Adheres to institutional and legal guidelines for research involving human participants.	All research activities were conducted to attend a specific goal

RESULTS

The proposed system tested thoroughly to ensure it met the requirements. The survey results table presented in Table 3 provides a comprehensive overview of respondents' perceptions regarding key cybersecurity issues in e-governance, covering legacy infrastructure risks, multi-platform environments, emerging technologies, cybersecurity frameworks and response strategies, usability, and overall security measures. With 54 responses analyzed, the data reveals critical insights into current vulnerabilities and potential areas for improvement in e-governance systems.

A significant portion of participants, approximately 75%, identified the lack of regular updates as a major risk. This highlights a strong concern about legacy systems and their inability to meet current cybersecurity requirements. Compared to industry standards that emphasize regular patching as a key security measure, the findings reflect a significant gap between ideal practices and the current state of these systems. This suggests that outdated infrastructure continues to pose serious vulnerabilities within e-governance environments, emphasizing the need for regular updates and upgrades Figure 1 presents the legacy infrastructures and security risks.

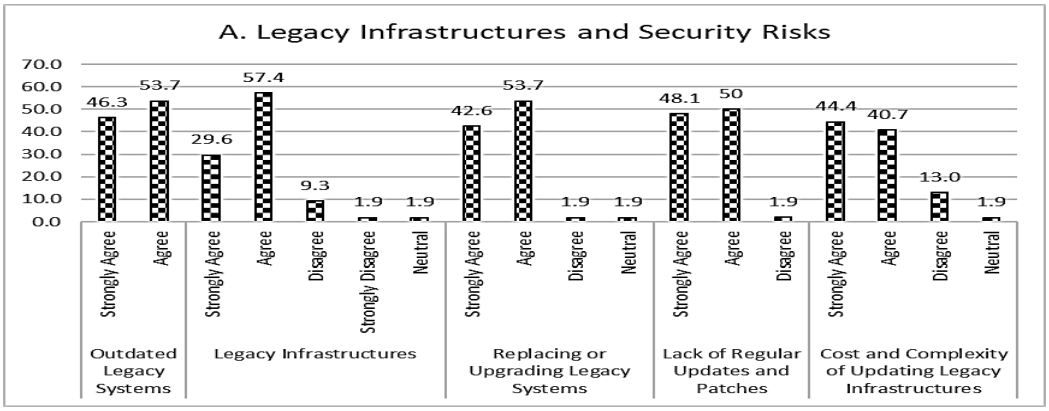

Figure 1. Legacy and Security Risks.

Corresponding author: Emmanuel D. Dako.
successdgee@gmail.com
Computer Engineering Department, Ahmadu Bello University, Zaria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(3), SEPTEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

Table 3. Summary of Survey Responses by Section (Total Responses: 54).

Survey section	Question	Strongly agree	Agree	Disagree	Strongly disagree	Total responses
Legacy Infrastructure Risks	Legacy systems are a major security risk due to outdated protocols.	18 (33%)	21(39%)	10(19%)	5(9%)	54
	Lack of regular updates and patches is a significant threat to e-governance security.	20(37%)	19(35%)	10(19%)	5(9%)	54
	The cost of updating legacy infrastructures hinders cybersecurity improvements.	22(41%)	15(28%)	12(22%)	5(9%)	54
Multi-Platform Environments	Security policies across different platforms are well-coordinated.	10(19%)	15(28%)	17(31%)	12(22%)	54
	Inconsistent security measures across platforms increase vulnerability.	25(46%)	15(28%)	8(15%)	6(11%)	54
Emerging Technologies (IoT, AI)	IoT devices pose a significant security risk in e-governance systems.	30(56%)	12(22%)	8(15%)	4(7%)	54
	The integration of AI for threat detection is critical for enhancing e-governance security.	32(59%)	10(19%)	7(13%)	5(9%)	54
Cybersecurity Framework & Response	Incident response strategies in e-governance are adequate for rapid handling of cyberattacks.	14(26%)	20(37%)	12(22%)	8(15%)	54
	Cyber incident response teams are sufficiently equipped to manage emerging threats.	17(31%)	18(33%)	10(19%)	9(17%)	54
Usability & Accessibility in Security	Accessibility concerns are well-addressed in e-governance cybersecurity measures.	12(22%)	16(30%)	15(28%)	11(20%)	54

The results show that only 30% of participants believe security policies are well-coordinated across platforms. This reveals significant challenges in unifying security protocols within multi-platform environments. The findings align with existing research that points to

Corresponding author: Emmanuel D. Dako.
successdgee@gmail.com
Computer Engineering Department, Ahmadu Bello University, Zaria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(3), SEPTEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

difficulties in managing consistent security measures across diverse systems. Such fragmentation increases vulnerability to cyber threats, highlighting the need for more integrated and standardized security policies across all platforms in e-governance systems. Figure 2 presents the multi-platform environments vulnerabilities.

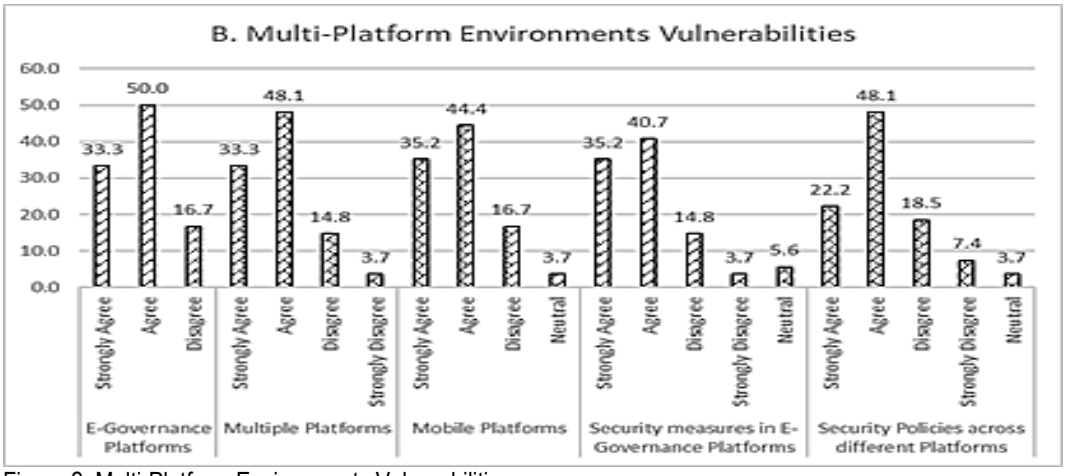

Figure 2. Multi-Platform Environments Vulnerabilities.

A large majority of respondents, about 80%, view IoT devices as highly vulnerable, while 85% acknowledge the importance of AI for threat detection. These responses emphasize the dual role of emerging technologies in e-governance systems. While IoT devices are seen as a significant risk due to their security limitations, AI is recognized as a crucial tool for enhancing threat detection and improving system defenses. These findings reflect the growing need to strengthen IoT security while leveraging AI-based solutions to address modern cybersecurity challenges. Figure 2 presents the emerging technologies (AI, IoT, Blockchain) in e-governance

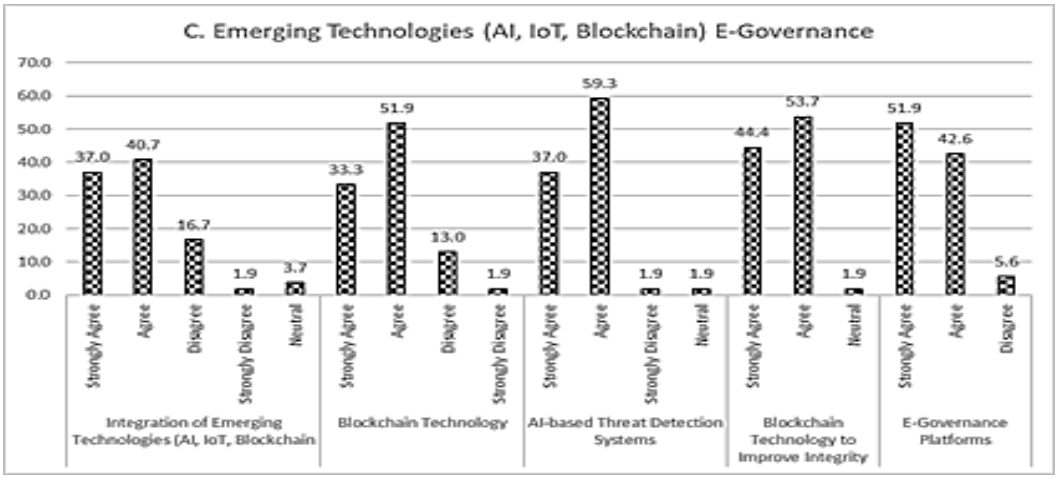

Figure 3. Emerging Technologies (AI, IoT, Blockchain) E-Governance

Corresponding author: Emmanuel D. Dako.
✉ successdgee@gmail.com
Computer Engineering Department, Ahmadu Bello University, Zaria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(3), SEPTEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

The survey results on incident response adequacy were mixed, with about 50% of participants expressing moderate satisfaction. This indicates that while existing frameworks may provide some level of defense, they are not entirely sufficient to address increasingly complex cybersecurity threats. Enhancing incident response strategies, including faster detection and proactive measures, is essential to minimize the impact of potential security breaches. This need becomes even more critical as cyber threats evolve and demand a more robust and efficient response system. Figure 4 presents Cybersecurity framework and incident report.

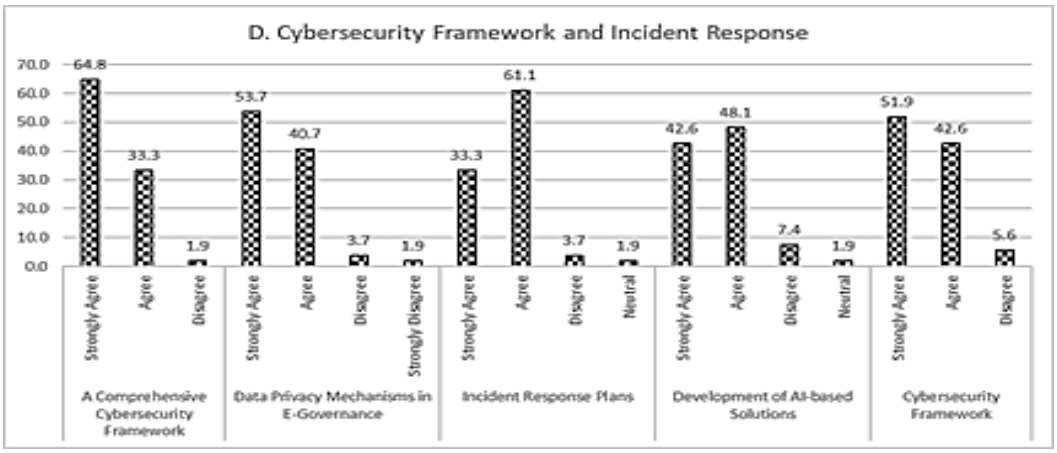

Figure 4. Cybersecurity Framework and Incident Response

Participants widely acknowledged the difficulty of balancing usability and security in e-governance systems. This finding reflects a common challenge within the industry, where efforts to improve security often compromise user experience. Balancing both elements is crucial to ensure that security measures are effective without alienating users. This is particularly important for public-facing services, where accessibility and ease of use significantly impact user satisfaction and system adoption. Figure 5 presents usability and availability in cybersecurity.

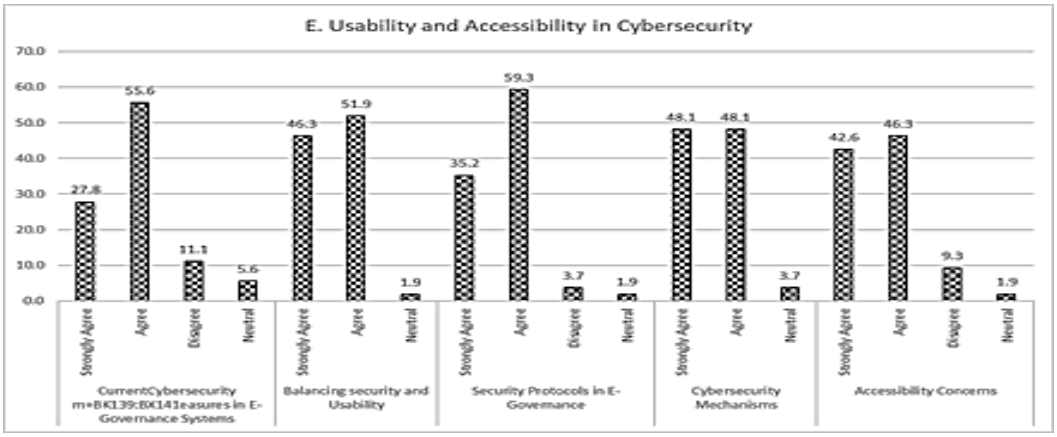

Figure 5. Usability and Availability in Cybersecurity

Corresponding author: Emmanuel D. Dako.
successdgee@gmail.com
Computer Engineering Department, Ahmadu Bello University, Zaria.

Interviews provided deeper insights into the survey findings, revealing specific challenges and operational issues. For legacy systems, participants cited the high costs and technical difficulties involved in upgrading outdated infrastructure, noting that while essential for security, updates are often resource-intensive. Emerging technology challenges were also highlighted, with one participant describing IoT devices as offering convenience but being easily exploited without proper controls. Experts emphasized the importance of faster and more proactive incident response frameworks, recommending automated detection systems to improve response times. Additionally, participants discussed the struggle to balance usability and security, particularly in public-facing systems, where accessibility must be maintained alongside robust security measures. This qualitative data adds depth to the survey findings, highlighting areas for improvement and practical challenges faced by e-governance systems.

The findings reveal critical cybersecurity challenges and opportunities within e-governance systems. Legacy infrastructure remains a significant risk, with 72% of respondents identifying outdated systems and financial constraints as barriers to regular updates, underlining the need for resource allocation to modernize infrastructure. Multi-platform environments expose vulnerabilities due to inconsistent security protocols, as 74% of participants agreed, emphasizing the importance of standardization. Emerging technologies present both risks and opportunities; while 78% viewed IoT devices as highly vulnerable, an equal percentage recognized the role of AI in enhancing threat detection, highlighting the need for improved IoT security and AI integration.

Incident response frameworks received mixed feedback, with 63% expressing confidence and 37% identifying gaps, indicating the necessity for advanced tools and team upskilling. Balancing usability and accessibility remains a concern, with divided opinions reflecting gaps in user-centric security designs. General confidence in emerging technologies was observed among 72% of respondents, though 28% remained skeptical, pointing to the importance of transparency and rigorous testing. Interviews further revealed high costs associated with updating legacy systems, the dual challenges of IoT, and the need for faster, proactive incident responses. Case studies, such as Estonia's X-Road and India's Aadhaar, provided practical insights into enhancing data security through encryption and AI-driven solutions. Recommendations include adopting multi-factor authentication, blockchain for data integrity, regular staff training, advanced access controls, and awareness campaigns to build a resilient cybersecurity foundation for e-governance systems.

CONCLUSIONS

The findings of this study demonstrate that the developed cybersecurity framework can address critical challenges within e-governance systems. Participant feedback highlighted significant improvements, such as faster incident response through structured protocols, enhanced threat detection with AI, and better IoT security controls that include encryption and centralized device management. By unifying security policies across platforms and incorporating blockchain for data protection, the framework effectively reduces vulnerabilities and ensures a cohesive security approach. However, legacy systems remain a major concern, as they lack compatibility with modern security standards and create risks for data breaches. The study also emphasized the need for regular personnel training and a balanced approach to usability and security, which improves user experience without compromising system integrity.

Contributions of the study include the development of a structured framework that integrates AI-based tools and IoT controls, policy recommendations for consistent security standards, and enhanced security awareness in public institutions. Despite these contributions, the study faced limitations, such as resource constraints for upgrading legacy systems, the requirement for specialized technical expertise, and the rapidly evolving nature of cybersecurity threats. Recommendations for future work include exploring emerging technologies like AI, IoT, and

Corresponding author: Emmanuel D. Dako.
successdgee@gmail.com
Computer Engineering Department, Ahmadu Bello University, Zaria.

blockchain in real-world applications, cost-effective strategies for legacy system upgrades, and longitudinal studies to evaluate the framework's long-term effectiveness. Comparative research across regions and user-centered security designs were also suggested to address unique challenges and promote best practices globally. This research highlights the importance of an adaptive, multi-layered cybersecurity approach in e-governance systems, ensuring the protection of sensitive data, improved incident response, and a secure, user-friendly environment for digital governance services.

REFERENCES

[1] Shah, I. A., Wassan, S., & Usmani, M. H. (2022). E-Government Security and Privacy Issues: Challenges and Preventive Approaches. In *Cybersecurity measures for e-government frameworks* (pp. 61-76). IGI Global.

[2] Avotra, A. A. R. N., Chengang, Y., Sandra Marcelline, T. R., Asad, A., & Yingfei, Y. (2021). Examining the impact of e-government on corporate social responsibility performance: the mediating effect of mandatory corporate social responsibility policy, corruption, and information and communication technologies development during the COVID era. *Frontiers in Psychology, 12*, 737100.

[3] Arief, A., Wahab, I. H. A., & Muhammad, M. (2021, May). Barriers and challenges of e-government services: A systematic literature review and meta-analyses. In *IOP conference series: Materials science and engineering* (Vol. 1125, No. 1, p. 012027). IOP Publishing.

[4] Shah, I. A. (2022). Cybersecurity Issues and Challenges for E-Government During COVID-19: A Review. *Cybersecurity Measures for E-Government Frameworks*, 187-222.

[5] Samsor, A. M. (2021). Challenges and Prospects of e-Government implementation in Afghanistan. *International Trade, Politics and Development, 5*(1), 51-70.

[6] Addo, A., & Senyo, P. K. (2021). Advancing E-governance for development: Digital identification and its link to socioeconomic inclusion. *Government Information Quarterly, 38*(2), 101568.

[7] Grigalashvili, V. (2022). E-government and E-governance: Various or Multifarious Concepts. *International Journal of Scientific and Management Research, 5*(01), 183-196.

[8] Lyulyov, O., Pimonenko, T., Saura, J. R., & Barbosa, B. (2024). How do e-governance and e-business drive sustainable development goals?. *Technological Forecasting and Social Change, 199*, 123082.

[9] Bokhari, S. A. A., & Myeong, S. (2023). The influence of artificial intelligence on e-Governance and cybersecurity in smart cities: A stakeholder's perspective. *IEEE Access*.

[10] Shah, I. A., Habeeb, R. A. A., Rajper, S., & Laraib, A. (2022). The influence of cybersecurity attacks on e-governance. In *Cybersecurity Measures for E-Government Frameworks* (pp. 77-95). IGI Global.

[11] Wouters, S., Janssen, M., Lember, V., & Crompvoets, J. (2023). Strategies to advance the dream of integrated digital public service delivery in inter-organizational collaboration networks. *Government Information Quarterly, 40*(1), 101779.

[12] Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data protection and privacy of the internet of healthcare things (IoHTs). *Applied Sciences, 12*(4), 1927.

[13] Amiri-Zarandi, M., Dara, R. A., Duncan, E., & Fraser, E. D. (2022). Big data privacy in smart farming: a review. *Sustainability, 14*(15), 9120.

Corresponding author: Emmanuel D. Dako.
successdgee@gmail.com
Computer Engineering Department, Ahmadu Bello University, Zaria.