Plagiarism Detector v. 2867 - Originality Report 6/26/2025 12:49:35 PM

Analyzed document: E-GOVERNMENT-2400721993 (2).docx Licensed to: Makerere University College of Health Sciences

Comparison Preset: Rewrite Detected language: En

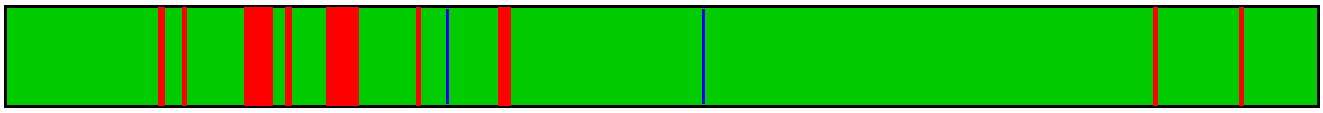
Check type: Internet Check

TEE and encoding: DocX n/a

Detailed document body analysis:

Relation chart:

Distribution graph:



Top sources of plagiarism: 47

11%	286	1.	https://open.ncl.ac.uk/theories/2/unified-theory-of-acceptance-and-use-of-technology
10%	181	2.	https://taapublications.com/tijasdr/article/download/549/605/1171
10%	278	3.	https://en.wikipedia.org/wiki/Unified_theory_of_acceptance_and_use_of_technology

Processed resources details: 250 - Ok / 17 - Failed

Important notes:

Wikipedia:	Google Books:	Ghostwriting services:	Anti-cheating:
Wiki Detected!	[not detected]	[not detected]	[not detected]

UACE: UniCode Anti-Cheat Engine report:

1. Status: Analyzer **On** Normalizer **On** character similarity set to **100%**
2. Detected UniCode contamination percent:**0%** with limit of: 4%
3. Document not normalized: percent not reached 5%
4. All suspicious symbols will be marked in purple color:Abcd...
5. Invisible symbols found: 0

Assessment recommendation:

No special action is required. Document is Ok.

Alphabet stats and symbol analyzes:

Active References (Urls Extracted from the Document):

No URLs detected

Excluded Urls:

No URLs detected

Included Urls:

No URLs detected

Detailed document analysis:

COLLEGE OF COMPUTING & INFORMATION SCIENCES SCHOOL OF COMPUTING & INFORMATICS TECHNOLOGY PROGRAMME: Master of Information Technology COURSE NAME: E-GOVERNMENT COURSE CODE: MIT7228 STUDENT NUMBER: 2400721993 REG NO: 2024/HD05/21993U Comparative Analysis of Uganda and Estonia's E-Government Development Estonia is globally recognized as a leader in e-government, having established a comprehensive digital infrastructure that facilitates efficient public service delivery. Key components of Estonia's e-government include the X-Road data exchange platform and a robust electronic identification (eID) system, enabling secure and seamless access to a wide range of services. These innovations have allowed Estonia to digitize nearly all government services, resulting in significant time and cost savings for both citizens and the government (McBride et al., 2018). In contrast, Uganda's e-government development is still in its formative stages. While initiatives such as the eCitizen portal and the Data Integration Platform (UGHub) have been launched to centralize and streamline access to government services, challenges persist. These include limited ICT infrastructure, especially in rural areas, and low levels of digital literacy among the population(Jansen et al., 2023). Moreover, Uganda's e-government efforts are often hindered by inconsistent political support and regulatory frameworks that may not fully support digital transformation (Mwesigwa, 2022). The disparity between Estonia and Uganda in e-government development underlines the necessity for an enabling policy environment, solid infrastructure, and widespread digital competence. Estonia's experience illustrates how concentrated investment in digital infrastructure and inclusive policy can result in efficient and transparent government. In order to advance its e-government agenda, Uganda will have to address infrastructural deficits, enhance digital skills across the population, and enjoy consistent political and regulatory support for digital ventures. 2. Management Approaches to E-Government Development

Plagiarism detected: **0.47%** https://taapublications.com/tijasdr/article/downl... + 4 id: **1**

The development and implementation of e-government initiatives in developing countries have followed various management approaches that aim to improve efficiency, transparency, and citizen engagement. These approaches often rely on established models and frameworks to tackle the specific challenges these nations face. 2.1.

Plagiarism detected: **0.56%** https://www.globalscientificjournal.com/researc... + 2 id: **2**

New Public Management (NPM) and Public Value Frameworks The New Public Management (NPM) approach has played a key role in reforming public sector management by focusing on efficiency, performance measurement, and customer-oriented services. In the realm of e-government, NPM encourages the use of private sector practices to enhance public service delivery. However, critics argue that NPM may miss the larger public interest and democratic values (Adolph, 2016). Alongside NPM, the Public Value Framework aims to create value for citizens through e-government services. This approach evaluates e-government performance based on factors like service quality, transparency, trust, and citizen satisfaction. By prioritizing public value, governments work to ensure that e-government initiatives meet citizens' needs and expectations (Adolph, 2016). 2.2.

Plagiarism detected: **2.36%** https://web-crawler.plagiarism-detector.com/ge... + 4 id: **3**

Diffusion of Innovation (DOI) Theory The Diffusion of Innovation (DOI) theory explains how new ideas and technologies spread within a society. In the realm of e-government, DOI has been applied to understand the adoption and implementation processes of digital services (Apleni & Smuts, 2020). Factors influencing diffusion include relative advantage, compatibility, complexity, trialability, and observability.

By leveraging DOI, policymakers can identify barriers to adoption and develop strategies to facilitate the uptake of e-government service(Aleisa, 2024). 2.3.

Plagiarism detected: **0.39%** https://web-crawler.plagiarism-detector.com/ge... id: **4**

Technology Organization Environment (TOE) Framework The Technology-Organization-Environment (TOE) framework provides a comprehensive perspective on the factors influencing e-government adoption. It considers technological readiness, organizational capabilities, and environmental factors such as regulatory support and societal needs. By analyzing these dimensions, governments can develop

tailored strategies that address specific challenges and leverage existing strengths to implement effective e-government solutions (Mahlangu & Ruhode, 2021). 2.4.

Plagiarism detected: **2.66%** https://open.ncl.ac.uk/theories/2/unified-theory-... + 29 id: **5**

resources!

Unified Theory of Acceptance and Use of Technology (UTAUT) The Unified Theory of Acceptance and Use of Technology (UTAUT) model identifies key determinants of user acceptance and usage behavior concerning new technologies. In the context of e-government, UTAUT highlights factors such as performance expectancy, effort expectancy, social influence, and facilitating conditions. Understanding these factors enables governments to design user-centric e-government services that

encourage adoption and sustained use(Aleisa, 2024). 2.5. Strategic Planning and Stakeholder Engagement Effective e-government development requires strategic planning that aligns with national development goals and involves key stakeholders. Engaging stakeholders including government agencies, private sector partners, and citizens ensures that e-government initiatives are responsive to diverse needs and foster a sense of ownership. Moreover, strategic planning facilitates resource allocation, risk management, and the establishment of clear objectives and performance indicators (Matsieli & Sooryamoorthy, 2022). 3. Trends in Digital Infrastructure and Connectivity The advancement of digital infrastructure and connectivity is pivotal

Plagiarism detected: **0.43%** https://taapublications.com/tijasdr/article/downl... + 5 id: **6**

resources!

for the successful implementation of e-government initiatives in developing countries.

Several key trends have emerged, reflecting both progress and ongoing challenges in this domain. 3.1. Expansion of Mobile Broadband and Leapfrogging Technologies Developing nations are increasingly using mobile broadband technologies to get around the limitations of fixed-line infrastructure. This method, often called

Quotes detected: **0.04%** id: **7**

"leapfrogging,"

allows countries to skip traditional stages of technological development. For example, studies show that moving directly to 4G networks in areas without connections can be a cost-effective way to provide universal broadband service in African countries, including Uganda (Ndlovu & Newman, 2020). 3.2. Investment in Digital Public Infrastructure (DPI) There is a growing emphasis on developing Digital Public Infrastructure (DPI) to support e-government services. DPI encompasses foundational systems such as digital identification, payment platforms, and data exchange mechanisms. These systems are essential for delivering public services efficiently and securely. However, challenges

Plagiarism detected: **0.99%** https://www.researchgate.net/publication/37880... id: **8**

such as inadequate infrastructure, regulatory gaps, and socio-economic disparities continue to hinder the effective adoption and integration of digital technologies in developing regions

(Oughton, 2021). 3.3. Addressing the Digital Divide The digital divide persists despite developments. There are continual challenges around limited internet access, affordability, and digital literacy in developing countries and particularly in Africa. Efforts to combat these issues include investment in infrastructure, inclusive policies, and increased digital skill development among the populations (Panagiotopoulos et al., 2019). 3.4. Emphasis on Interoperability and Cross-Border Integration As e-government services continue to grow, there is a growing interest in systems that are interoperable and can operate on different systems and across different nations. Developing countries are looking into architectures that allow for the safe and smooth transport of data which is relevant for services such as digital identity and transactions across borders (Krimmer et al., 2023). 3.5. Integration of Emerging Technologies Digital infrastructure is incorporating evolving technologies, such as cloud computing, artificial intelligence (AI), and the Internet of Things (IoT), to improve service delivery. While evolving technologies create innovative possibilities, they typically involve the need for regulatory frameworks and established and functional infrastructure to use it effectively and ethically (Younus et al., 2025). 4. Key Pillars of Cyber security, Data Governance, and Privacy in Digital Transformation of Developing Countries Digital transformation within developing nations needs a comprehensive framework for cyber security, data governance, and privacy to promote trust, guarantee data accuracy and security, and protect the rights of citizens in a digital world. The following pillars represent the foundations that can support this transformation: 4.1. Cyber security Governance and Strategic Frameworks Cyber security governance includes formalized frameworks that comply with

International standards such as ISO/IEC 27001 and the National Institute of Standards and Technology (NIST) (Metin et al., 2024). These frameworks define a means of (1) risk assessment; (2) incident reporting; and (3) monitoring and evaluating cyber security measures. Governance frameworks help create proactive resilience and preparedness for revenge; recovering/adapting from the emergence of new threats (Mijwil et al., 2023). 4.2. Development of Cyber security Culture and Capacity Building Human factors sometimes represents the 'weakest link' in cyber security. Promoting a cyber-security aware culture, through regular training, awareness initiatives, and through the establishment of

Quotes detected: **0.09%** id: **9**

"Security Champion"

teams can help mitigate risks by enabling employees to identify security threats and respond accordingly (AKSOY, 2024). 4.3. Comprehensive Data Protection Legislation and Enforcement Data protection laws are essential and require enforcement and implementation. Legislative frameworks should include laws regarding the collection, processing, storage, and sharing of data which should ensure there is transparency and accountability. The African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention), provides a continental framework, even though there are inconsistent implementations mesures that are in the member states there (ahad et al. 2021). 4.4. Emphasis on Data Sovereignty and Localization Data sovereignty signifies a nation's control over data produced on its soil. By enacting policies that would require data to remain domestic, management can be increased over data flows and protection of national interests. However, these measures need to strike a balance between the advantages of data control and the potential challenges of international data and economic integration (Tan et al., 2022). 4.5. Continuous Monitoring and Adaptive Security Measures The dynamic nature of cyber threats necessitates continuous monitoring and the ability to adapt security measures promptly. Implementing real-time threat detection systems and regularly updating security protocols ensure that digital infrastructures remain resilient against evolving threats(Metin et al., 2024). 5. Current Trends in Digital Skilling Pertinent to E-Government Portal Development in Developing Countries The development of e-government portals in developing countries necessitates a workforce equipped with relevant digital skills. Recent peer-reviewed literature highlights several trends in digital skilling that are particularly pertinent to such initiatives: 5.1. Emphasis on Lifelong Learning and Continuous Skill Development Digital transformation requires ongoing learning to keep pace with technological advancements. A systematic review by Salin et al. (2024) underscores the importance of lifelong learning approaches, including micro learning and modular training, to enhance digital competencies among working adults. These methods offer flexibility and adaptability, crucial for public sector employees involved in e-government services. 5.2. Integration of Artificial Intelligence (AI) in Skill Development The coexistence of AI and human workers is reshaping skill requirements. Research by Salin et al. (2023) indicates that understanding AI's role in the workplace is essential for developing relevant digital skills. Training programs must, therefore, incorporate AI literacy to prepare employees for collaborative environments involving AI technologies (Zirar et al., 2023). 5.3. Utilization of Educational Technologies for Skill Enhancement Innovative educational tools, such as chatbots, are being employed to promote digital literacy. A study by Salin et al. (2025) demonstrates that educational chatbots can effectively enhance online evaluation skills, offering interactive and personalized learning experiences. Such technologies can be integrated into e-government training modules to facilitate user engagement and comprehension(Siqueira et al., 2019). 5.4. Focus on Assessing and Bridging Digital Skill Gaps Identifying existing skill gaps is critical for targeted training. The development of assessment frameworks, as discussed by Salin et al. (2024), enables organizations to evaluate digital competencies systematically. These frameworks inform the design of customized training programs, ensuring that employees acquire the necessary skills for effective e-government service delivery. 5.5. Policy-Level Initiatives to Promote Digital Skills Government policies play a pivotal role in fostering digital literacy. An evaluation by Salin et al. (2024) of digital skills policies in Italy reveals that outreach-oriented initiatives can significantly impact digital skill development. Such policies, when adapted to the local context, can support the widespread adoption of e-government services by enhancing the digital capabilities of the populace. 6. Roadmap for Developing Uganda’s National E-Government Portal Based on Estonia’s X-Road Platform Drawing from the reviewed literature and best practices in e-government implementation, the following roadmap outlines key considerations for Uganda's Ministry of ICT in developing a national e-government portal akin to Estonia's X-Road platform. 6.1. Establishing a Robust Baseline Assessment of Current E-Government Maturity

Uganda should begin by conducting a comprehensive assessment of its current e-government maturity, identifying existing digital services, infrastructure capabilities, and stakeholder readiness. This baseline will inform strategic planning and resource allocation. Benchmarking against Estonia’s Model Understanding the structural and operational aspects of Estonia's X-Road platform can provide valuable insights. Estonia's emphasis on interoperability, data security, and user-centric services should guide Uganda's adaptation strategy. 6.2. Adopting Effective Management Approaches Interoperability Framework Development Implementing a national interoperability framework is crucial. This framework should define standards for data exchange, service integration, and communication protocols among government agencies. Such a framework facilitates seamless interaction between disparate systems, enhancing service delivery efficiency. Stakeholder Engagement and Governance Establishing a multi-stakeholder governance structure ensures inclusive decision-making. Engaging public institutions, private sector partners, and civil society organizations fosters collaboration and shared ownership of the e-government initiative. 6.3. Enhancing Digital Infrastructure and Connectivity Investment in ICT Infrastructure Prioritizing investments in ICT infrastructure, particularly in underserved rural areas, is essential. Expanding broadband connectivity and ensuring reliable power supply will bridge

Plagiarism detected: **0.43%** https://www.researchgate.net/publication/28837... + 4 resources! id: **10**

the digital divide and enable equitable access to e-government services

(Alfiani et al., 2024). Leveraging Cloud-Based Solutions Adopting cloud-based platforms can offer scalable and cost-effective solutions for e-government services. Cloud computing facilitates resource optimization and rapid deployment of services, aligning with the dynamic needs of digital governance (Joshi et al., 2017). 6.4. Strengthening Cyber security, Data Governance, and Privacy Development of Comprehensive Legal Frameworks Formulating and enforcing robust legal frameworks addressing data protection, privacy, and cyber security is paramount. These laws should align with international standards to ensure trust and compliance in digital interactions. Implementation of Security Protocols Integrating advanced security measures, such as encryption and multi-factor authentication, will safeguard sensitive information. Regular security audits and risk assessments should be institutionalized to proactively address vulnerabilities. 6.5. Promoting Digital Skilling and Capacity Building Comprehensive Digital Literacy Programs Launching nationwide digital literacy campaigns will equip

Plagiarism detected: **0.47%** https://taapublications.com/tijasdr/article/downl... id: **11**

citizens with the necessary skills to access and utilize e-government services

effectively. Tailored training programs should address diverse user needs, including marginalized groups. Capacity Building for Public Servants Investing in the continuous professional development of public servants ensures competent management and delivery of digital services. Training should encompass technical skills, change management, and user-centric service design. 6.6. Phased Implementation Strategy Pilot Projects and Scaling Initiating pilot projects in select ministries or regions allows for testing and refinement of the e-government portal. Lessons learned from these pilots can inform broader rollout strategies, ensuring scalability and adaptability. Monitoring and Evaluation Mechanisms Establishing robust monitoring and evaluation frameworks will track progress, measure impact, and inform continuous improvement. Key performance indicators should be defined to assess service quality, user satisfaction, and operational efficiency. REFERENCES