Journal of Applied Artificial Intelligence
https://jaai.sabapub.com
ISSN: 2709-5908

2025 Volume 6, Issue 1: 18-23
DOI: https://doi.org/10.48185/jaai.v6i1.1437

A Review of Frameworks for Evaluating the Security Performance of E-Government Systems

Ehab Husam Husni Al Shiekh Saleh[1*], Mohd Fadzil Bin Abd Kadir[1], Yousef Abubaker El-Ebiary[1]

[1]Faculty of Informatics and Computing, UniSZA, Malaysia

Received: 23.12.2024 • Accepted: 03.02.2025 • Published: 15.04.2025 • Final Version: 30.04.2025

Abstract: The use of information and communication technology (ICT) is rapidly expanding throughout society. Different ICTs are used by governments to communicate with their country's citizens and other e-government initiative stakeholders. The e-government initiative faces various internal and external challenges, including limited funding, rapid technological advancements, internet accessibility for the public, and concerns about privacy and security. To address these challenges, several frameworks have been proposed that help improve E-government performance. In order to measure the effectiveness of e-government, this paper aims to identify various constructs and their relationships by providing a summary of the proposed frameworks and models for electronic government development.

Keywords: E-government, ICTs, Frameworks, IDS, TCP

1. Introduction

Governments now place a high priority on helping citizens and the general public receive better public services, improving citizen-government communication, and integrating citizens in state governance. Governments can accomplish these goals most successfully by implementing e-government, or the integration of information and communication technology (ICT) into administrative procedures. E-government refers to providing citizens, companies, and the public at large with improved public services through the use of electronic devices and ICT [1]. It also refers to providing services to the public that improve responsiveness of government agencies to the demands of the public, facilitate citizen participation in decision-making, and expand citizens' access to government [2].

E-government systems involve the utilization of electronic technologies, such as the internet, for the provision of government services and dissemination of information to citizens, businesses, and various government bodies. The primary objectives of these systems include enhancing government operational efficiency, fostering transparency and accountability, and promoting greater citizen engagement within the democratic framework [3].

Initially, the early days of e-government didn't fully consider the potential negative consequences of the system, as it mainly focused on improving public convenience and administrative efficiency. The e-government initiative faces various internal and external challenges, including limited funding,

* Corresponding Author: ehabatele2002@gmail.com

rapid technological advancements, internet accessibility for the public, and concerns about privacy and security [4].

A major worry is the growing security threats to vital information assets and the supporting infrastructure. For businesses and e-government services, these security risks pose serious difficulties. Intrusion Detection Systems (IDS) are essential for protecting the availability, confidentiality, and integrity of computer systems [5]. Signature-based IDS (SIDS) and anomaly-based IDS (AIDS) are the two main categories into which they are divided [6]. Based on its characteristics, anomaly-based detection techniques, particularly those for AIDS, can be divided into three primary groups: static-based, knowledge-based, and machine learning-based. Static-based, pattern-based, rule-based, state-based, and heuristic-based are the five sub-classes that have been identified based on their properties because there isn't a defined classification system for anomaly-based intrusion detection.

E-Government systems can take many forms, such as: Web portals, Electronic voting, Digital identity and authentication, Open Data, and Mobile applications. E-Government systems have the potential to significantly improve government performance and citizen engagement. However, there are also privacy, security, and accessibility issues in web-based applications [7]. Governments should carefully consider these aspects when implementing e-government systems to ensure they are efficient, secure and accessible to all citizens. [8] Transmission Control Protocol/Internet Protocol (TCP/IP) is a set of protocols used for communication between computers over the Internet and other networks. TCP/IP is the primary protocol used on the Internet and ensures reliable and efficient data transmission over the network. The two primary protocols that make up TCP/IP are Internet Protocol (IP) and Transmission Control Protocol (TCP). The IP protocol is responsible for the transmission of data packets in the network. Ensures data is sent to the correct destination and broken up into smaller packets if necessary. The TCP protocol is responsible for reliable data transmission. It establishes a connection between two devices, splits the data into packets, and reassembles the packets on the target device [9].

In this review, section 2 provides a general overview of E-Government, and its challenges. Review of the related works are presented in Section 3. Sections 4 discuss performance of the existing works. the study's conclusion, which includes suggestions for further research avenues are presented in Section 5.

2. E-Government

Electronic government, or e-Gov, is another name for e-Government, which is the use of internet-based or not-so-based information and communication technology (ICT) tools and applications to improve interactions between government and business/commerce (G2B), government and citizens (G2C), government agencies (G2G), and government and households (G2H). This strategy is not without its difficulties, though. In the field of e-Government, protecting the security and privacy of data is crucial [10].

E-Government applications heavily rely on the Internet to provide extensive services to citizens. While this enhances transparency and accessibility, it also introduces significant risks due to vulnerabilities. Nevertheless, if these vulnerabilities are identified, there are mechanisms in place to address them; otherwise, they may be exploited by malicious actors.

E-government applications refer to the use of electronic technologies, particularly the Internet, to facilitate the delivery of government services, enhance administrative processes, and improve

interactions between governments and citizens. These applications leverage digital platforms and online tools to streamline and automate various government functions, making them more efficient, accessible, and transparent.

E-government applications can encompass a wide range of services and activities, including:

- Online Service Delivery: Governments provide a variety of services through digital channels, such as issuing official documents (e.g., passports, driver's licenses), processing permit applications, paying taxes, accessing healthcare information, and registering for government programs.
- Government Information Portals: Websites and online portals serve as central repositories for government information, enabling citizens to access and search for relevant information, policies, regulations, and public announcements.
- Citizen Engagement Platforms: E-government applications often include platforms for citizen engagement, such as online forums, feedback mechanisms, and e-participation tools, allowing citizens to express their opinions, participate in decision-making processes, and provide feedback to government entities.
- Digital Payment Systems: E-government applications facilitate online payment options, allowing citizens to conveniently pay fees, fines, taxes, and other government-related transactions electronically.
- Data Management and Analytics: Governments leverage e-government applications to collect, store, and analyze vast amounts of data, enabling evidence-based decision-making, performance monitoring, and policy formulation.
- Collaboration and Interagency Communication: E-government applications facilitate communication and collaboration among different government agencies and departments, streamlining workflows, sharing information, and enhancing coordination in service delivery.
- The ultimate goal of e-government applications is to improve the efficiency, accessibility, and transparency of government services, promote citizen participation and engagement, and enhance overall governance. By leveraging digital technologies, governments can overcome geographical barriers, reduce bureaucratic hurdles, and provide citizens with 24/7 access to services and information.

It's important to note that the specific e-government applications and their functionalities may vary across countries and jurisdictions, depending on local governance structures, technological infrastructure, and the level of digital adoption [11].

The storage of comprehensive citizen profiles is a fundamental aspect of E-government. However, this repository of sensitive data presents a potential risk, as malicious actors could exploit it, leading to potential breaches of confidentiality or unauthorized alterations of information, compromising its integrity [12].

An issue arises when individuals need to verify and confirm the identity of information or object owners, and conversely, when they need to gain access to specific data within E-government applications like e-voting, e-passports, or e-transactions through the E-government portal [12].

Security breaches can result in a disruption of information access for citizens, a problem particularly prevalent in developing countries where a significant number of E-government projects have faced challenges and failed [13].

3. Related Works

According to Lewandowski et al. (2001), an effective IRS framework should be created by combining data from several sources to provide a quick and dispersed defense against information attacks [14]. While the aforementioned systems proved beneficial in several instances, their capacity and efficacy to furnish automated, anticipatory, proactive reactions were restricted [15].

A framework for authentication has been presented by [16] that takes into account the specific demands and requirements of the Greek government agencies. The framework is composed of two parts: the Service Provider (SP) and the Identity Provider (IdP). In order to acquire unique IDs that will be used to access services from the service providers, users must register with IdP at a central e-government system site. Every time a user requests access to a service, SPs verify their identities with the IdP at the central portal to acquire a Single Sign On (SSO) password that may be used to access multiple SPs.

Since the technology, organisation, and environment (TOE) framework takes into account the environment, it provides a better explanation for the adoption of innovation and technology at the intra-organizational level. This is in line with the diffusion of innovations (DOI) theory, which explains innovation adoption at the organisational level [17]. Studies have also combined the TOE framework with other theories, like the institutional theory and the DOI theory.

Surveys like those by Shameli-Sendi et al. (2012), Anuar et al. (2010), and Stakhanova et al. (2007) offer a number of methods and the mechanisms they use in response to an attack [18], [19], [14].

E-government in Saudi Arabia: Obstacles, Difficulties, and Its Function The process of developing e-government is both politically and technically. A few important variables that affect the quality of e-government are the government's information policy, the quantity and caliber of users, and user motivation. To yet, no nation has been able to effectively fulfill every need for the perfect e-government model. According to this perspective, in order to meet the requirements for the success of e-government, a tailored approach to its creation and implementation is required [20].

A hybrid model derived from the "The strategic framework of e-government" and "Citizen comprehensive vision acknowledged" models was put out by Mateen et al. (2017) in an effort to show how best practices can be improved in any e-government endeavor [21]. The process of combining various computer knowledge systems to create a single crossover program has become more and more common. These combination models' execution files have proven to be better than their separate parts when used independently. A survey study was carried out to make sure the suggested model is more advantageous and efficient. survey that uses questionnaires and computes results by using statistics to analyse the information obtained. Writing surveys was a behaviour to develop a new model. Every internal variable was covered by the suggested model's open association survey of e-government. It arranged these components into four main metrics: people, technology, processes, and strategy. Each of the four e-government measurements was examined in depth, as well as the relationships between them. The study's findings supported the exploration theories by showing that, although with different weights, each of the four measurements affects how the e-government model is implemented.

Noe Elisa et al. (2018) proposed an e-government framework that uses blockchain technology to enforce privacy and security in the public sectors [22]. Blockchain technology allows for the creation of decentralized, highly secure, and privacy-preserving systems in which no third-party organization controls the transactions. Existing data and new data are stored using blockchain technology in a sealed compartment of blocks (a ledger) dispersed throughout the network in an unchangeable and

verifiable manner. Blockchain technology improves information security and privacy by distributing encrypted data throughout the network.

The last ten years have seen a significant increase in the amount of research on congestion control algorithms, with a primary focus on congestion management for "best-effort" dependable data transmission.

Regarding the TCP congestion control design, Al Shiekh Saleh et al. (2023) made the assumption that the network is a "black box" that does not provide sources with explicit feedback [23]. As a result, they created the end-to-end concept, which is largely responsible for the Internet's success. Specifically, when congestion is detected by a timeout or the receipt of three duplicate acknowledgments (3 packs), a TCP source employs an additive increase mechanism to utilize all available bandwidth and a multiplicative decrease technique to significantly shorten the connection window. This study looks at a few new problems with Jordanian e-government system security detection. Additionally, the primary goal of this study is to accelerate the TFRC protocol's training by grouping losses and markings that happened within the same round-trip time using the receiver. To be more specific, they raise stop-to-stop probing techniques that may boost bottleneck bandwidth in addition to arbitrary, Precise assessment of network capacity is essential for network administration software, as well as adaptable Internet apps and protocols that actively monitor and adjust to fluctuating network resource usage.

4. Discussion

This review sheds light on the development of frameworks and models for e-government assessment. To determine crucial elements, the current study presented the frameworks and models for E-government performance assessments that are currently in use. The goal would assist in creating a framework that is appropriate for assessing how well e-government initiatives are performing while taking into account the perspectives of all stakeholders. Research in this field is trending upward, with the majority of these studies and research works coming out in recent years. The findings of this study demonstrate that over the past ten years, a substantial amount of research has been conducted on congestion control algorithms, mostly concentrating on congestion control for "best-effort" dependable data flow.

5. Conclusion

This study reviews existing articles to understand factors for assessing e-governance. The majority of the literature uses citizens as the target stakeholder and as the analytical unit. Nonetheless, future study investigations must concentrate on the government and the service provider. Our study highlights that it presented the frameworks and models for E-government performance assessments that are currently in use to determine crucial elements. The results of this study show that the last ten years have seen a significant increase in the amount of research on congestion control algorithms, with a primary focus on congestion control for "best-effort" reliable data traffic.

References

[1] J. P. F. Gomes and R. M. S. Laureano, “Impacts of Electronic Public Procurement in the Portuguese Construction Sector: several years after implementation.” *Advances in Electronic Government, Digital Divide, and Regional Development*, pp. 363-383, 2018, doi: 10.4018/978-1-5225-3731-1.ch017.

[2] I. K. Mensah, “E-Government Services Adoption: The Important Elements of Trust and Transparency.” *International Journal of Electronic Government Research*, vol. 14, no. 3, pp. 12-31, 2018, doi: 10.4018/ijegr.2018070102.

[3] M. J. Moon, “The Evolution of E-Government among Municipalities: Rhetoric or Reality?” *Public Administration Review*, vol. 62, no. 4, pp. 424-433, 2002, doi: 10.1111/0033-3352.00196.

[4] O. Gibreel and A. Hong, “A Holistic Analysis Approach to Social, Technical, and Socio-Technical Aspect of E-Government Development.” *Sustainability*, vol. 9, no. 12, p. 2181, 2017, doi: 10.3390/su9122181.

[5] J. Sisodia, A. Nayak, and R. Boghey, “An Improved Index Price/Movement Prediction by using Ensemble CNN and DNN Deep Learning Technique,” Journal of Applied Artificial Intelligence, vol. 5, no. 1, pp. 41–53, Mar. 2024, doi: https://doi.org/10.48185/jaai.v5i1.980.

[6] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, “Survey of intrusion detection systems: techniques, datasets and challenges.” *Cybersecurity*, vol. 2, no. 1, 2019, doi: 10.1186/s42400-019-0038-7.

[7] Mahmoud Khalid Baklizi et al., “Web Attack Intrusion Detection System Using Machine Learning Techniques,” *International journal of online and biomedical engineering*, vol. 20, no. 03, pp. 24–38, Feb. 2024, doi: https://doi.org/10.3991/ijoe.v20i03.45249.

[8] R. Heeks, *Implementing and Managing EGovernment*. SAGE, 2006.

[9] D. Comer, Internetworking with TCP/IP. 6th ed., vol. 1. Addison-Wesley, 2014.

[10] R. Clarke, “Privacy and Data Protection for E-Government.” *Edward Elgar Publishing*, 2018.

[11] P. T. Jaeger, "Transparency and Social Media Communication about Government Stimulus Funding.” *Government Information Quarterly*, 461-471, 2018.

[12] T. Guberek, A. McDonald, S. Simioni, A. H. Mhaidli, K. Toyama, and F. Schaub, “Keeping a Low Profile? Technology, risk and privacy among undocumented immigrants.” *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, doi: 10.1145/3173574.3173688.

[13] J. Vitak, Y. Liao, P. Kumar, M. Zimmer, and K. Kritikos, “Privacy Attitudes and Data Valuation Among Fitness Tracker Users.” *Transforming Digital Worlds*, pp. 229-239, 2018, doi: 10.1007/978-3-319-78105-1_27.

[14] Lewandowski, S.M. et al. (2001) ‘Sara: Survivable autonomic response architecture’, *Proceedings DARPA Information Survivability Conference and Exposition II. DISCEX’01* [Preprint]. doi:10.1109/discex.2001.932194.

[15] N. Stakhanova, S. Basu, and J. Wong, “A taxonomy of intrusion response systems.” *International Journal of Information and Computer Security*, vol. 1, no. 1, p. 169, 2007, doi: 10.1504/ijics.2007.012248.

[16] D. Prokopios, G. Dimitris, G. Stefanos, L. Costas, L. Mitrou, “Towards an enhanced authentication framework for e-government services: The Greek case.” *Trust and Security*, pp. 189-196, 2009.

[17] T. Oliveira, M. F. Martins, “Literature review of information technology adoption models at firm level.” *Electronic journal of information systems evaluation*, vol. 14, no. 1, pp. 110-121, 2011.

[18] A. Shameli-Sendi, N. Ezzati-Jivan, M. Jabbarifar, M. Dagenais, “Intrusion response systems: survey and taxonomy.” *Int. J. Comput. Sci. Netw. Secur*, vol. *12, no. 1*, 1-14, 2012.

[19] N. B. Anuar, M. Papadaki, S. Furnell, and N. Clarke, “An investigation and survey of response options for Intrusion Response Systems (IRSs).” *2010 Information Security for South Africa*, 2010, doi: 10.1109/issa.2010.5588654.

[20] A. Basahel and M. Yamin, “Measuring success of e-government of Saudi Arabia,” *International Journal of Information Technology*, vol. 9, no. 3, pp. 287–293, Jul. 2017. doi:10.1007/s41870-017-0029-4.

[21] A. Mateen, S. Sabir, K. Ullah, "A development of hybrid framework for E-Government.” *arXiv preprint arXiv:1702.02442*, 2017.

[22] N. Elisa, L. Yang, F. Chao, and Y. Cao, “A framework of blockchain-based secure and privacy-preserving E-government system.” *Wireless Networks*, vol. 29, no. 3, pp. 1005-1015, 2018, doi: 10.1007/s11276-018-1883-0.

[23] E. H. H. Al Shiekh Saleh, M. F. Bin Abd Kadir, Y. A. El-Ebiary, “Bottleneck Bandwidth And Round-Trip Propagation Time Algorithm Using TFRC Protocol By Artificial Intelligence Algorithm.” *Journal of Pharmaceutical Negative Results*, vol. 13, no. 5, pp. 841-849, 2022.