Available online at www.sciencedirect.com

ScienceDirect

Transportation Research Procedia 74 (2023) 1538–1545

Transportation Research Procedia

www.elsevier.com/locate/procedia

TRANSCOM 2023: 15th International Scientific Conference on Sustainable, Modern and Safe Transport

Evaluating an E-Government Stage Model by Using SOAR-AHP Process

Hemin Muhammad[a,*], Martin Hromada[a]

[a] Department of Security Engineering, Faculty of Applied Informatics, nám. T. G. Masaryka 5555, 760 01 Zlín, Czechia

Abstract:

E-government is a key component of today's efforts to give citizens improved services. As a result, participation of the general public in government policy is essential to assuring the success of e-government. Thus, when developing any e-government model, the security of personal information must be taken into account. According to earlier research, the developing countries are suffering from implementing e-government to provide e-services for their citizens. They also indicate that the biggest obstacles to implementing e-government in such countries are security and privacy. This study attempts to assess e-government stage model via using SOAR (Strengths, Opportunities, Aspirations, and Results) and Analytic Hierarchy Process (AHP). This is a new and reliable technique for evaluating e-government prior implementing. The AHP is combined with the SOAR analysis in this study's approach to analyze the phases and assess the model's viability. The study's findings demonstrate that the model is workable and appropriate for adoption.

Peer-review under responsibility of the scientific committee of the TRANSCOM 2023: 15th International Scientific Conference on Sustainable, Modern and Safe Transport

Keywords: e-government, Stage Model, AHP, SOAR;

* Corresponding author. Tel.: +964 750 444 5565.
E-mail address: muhammad@utb.cz

Peer-review under responsibility of the scientific committee of the TRANSCOM 2023: 15th International Scientific Conference on Sustainable, Modern and Safe Transport
10.1016/j.trpro.2023.11.131

1. Introduction

Governments around the world are changing how they interact with those who use their services as well as how they provide information and public services to citizens. Internet access and the vast improvements in information and communications technologies are to blame for this change. Local and national governments are automating their major and minor procedures, providing crucial information on the Internet, and corresponding electronically with their constituents throughout almost every country in the globe. The term "digital governance" or "e-government" is used to describe this situation. Security and privacy issues, which have been the focus of considerable research, are among the major obstacles to the development and application of e-government (Agbozo & Alhassan, 2018). Users are required to submit personally identifiable information to government websites in order to use these linked services. However, consumer acceptance of these services has been hampered by privacy concerns brought on by the use of these security measures to verify user identities while providing e-government services and the potential for data sharing among government agencies. This problem has received a lot of attention in the literature. Governments must concentrate their efforts on putting high-security measures into place in order to guarantee the security of their systems and the privacy of their residents. These measures will improve how the public sees the government and promote the usage of its services. At all times, secure communication must be ensured (Hernandez-Moreno & Hoyos-Marttinez, 2010).

Online privacy protection for citizens is essential for the growth of e-government. The digital divide in the population, the lack of competent e-government services, and the restricted access to technology continue to be major obstacles to the adoption and usage of e-government services in developing nations. However, by include adequate protective measures when planning e-government projects, governments can increase stakeholder participation in programs. These challenges will probably continue to exist in poor countries. E-government initiatives can be created using e-government maturity models, often known as stage models (Al-Dabbagh, 2011)(Rehak & Novotny, 2016). A growing percentage of e-government initiatives in underdeveloped nations are allegedly not adhering to current e-government trends. According to statistics, data breaches and cyberattacks are increasing in frequency in developing nations while they are declining in the West. The protection of personal information is essential in e-government systems to promote user trust since it gives citizens a sense of ownership. Citizens' private information is maintained by e-government systems utilizing secure protocols to guarantee its security. There must be organizational, social, legal, and technical safeguards in place to protect privacy. Some academics contend that enacting legislation to safeguard data privacy is crucial (Nwaeze, Zavarsky &Ruhl, 2017).

The author has studied numerous stage models for e-government in the literature to determine the models' strengths, flaws, and success factors. These models appear to differ from one another even though they are founded on various viewpoints and make use of a variety of e-government concepts. The author put forth a step model for e-government for local administration in developing nations based on various aspects, including social, organizational, technical, and legal issues (Wu, 2014). These must be taken into consideration before beginning an e-government project in developing nations. The protection of personal information is the focus of the six stages of the proposed e-government stage model (Requirements, Information, Awareness, Interaction, Transaction, and Integration).

The goal of this research is to create a methodical approach and offer support for a decision scenario about the implementation of an e-government stage model that is concentrated on protecting personal data in developing nations. The SOAR (Strengths, Opportunities, Aspirations, and Results) technique is used as a tool to assess both the supply and demand side. However, selecting an e-government stage model using solely the SOAR analysis is difficult because numerous qualitative considerations need to be taken into account. These characteristics are virtually undefined and linguistically problematic The Analytic Hierarchy Process (AHP) approach is utilized to get over this problem, study the SOAR components carefully, and take these variables into consideration in a hierarchical framework. The section on the e-government stage model contains illustrations of the proposed stage model. The section on assessment technique that follows discusses the SOAR group factors and the procedures used to calculate AHP (Mu & Pereyra-Rojas, 2016). The calculation of the combined techniques is also covered in this section. Tables are used to illustrate the study's conclusions, which are then discussed in the discussion section. The reference section serves as the study's conclusion.

2. E-Government Stage Model

Individual researchers have presented numerous various e-government stage models. Researchers give many models with different phases. Models that are based on a variety of phrases and events are presented to them. There are generally four to seven stages. The general phases include e-democracy, interaction, communication, transaction, and web presence. These models are not primarily concerned with security problems. Most of them argue that models focus excessively on stage names while ignoring stage security considerations. Some models fail to account for the organizational, sociological, political, and technological requirements that influence whether or not e-government projects are effective (Dewa & Zlotnikova, 2014).The six steps of the proposed stage model are depicted in Fig.1. The requirements phase, which is the initial stage, is where the ICT infrastructure is the main topic. At this stage, deficiencies in the legal and organizational aspects can be corrected. It is possible to adopt a data protection regulation or standard and make security preparations in terms of hardware and software. At this point, it is vital to consider how legal and organizational factors may affect the flow of information. The second stage, known as the Information phase, entails the development of a static website that presents essential data about each company. It is crucial to make sure the website is free of bugs or other difficulties that could have a negative influence on the opinions of users (Muhammad & Hromada, 2022).

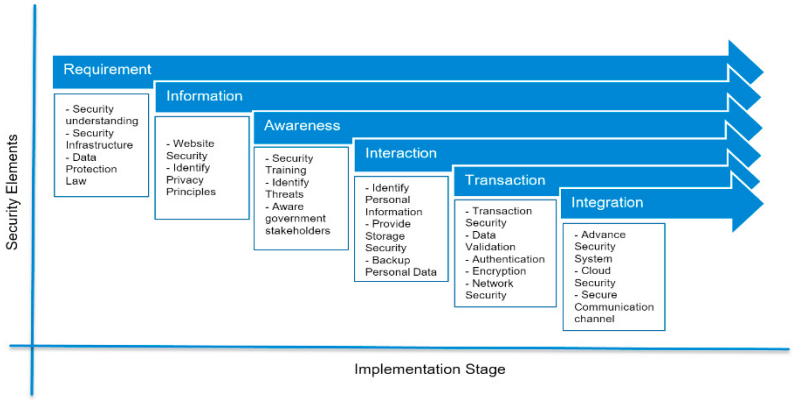

Fig.1. Proposed E-Government Stage Model

The privacy concept should be addressed in accordance with international standards. As they weren't included in earlier models that were suggested to developing countries, the Requirements and Awareness phases are unique to this model. In nations where adoption of new technology is still in its early stages, awareness is at a different stage and needs more care. At this time, training should be provided to employees of government stakeholders to make sure they are adequately knowledgeable about security and the protection of personal information. After completing this phase, the government may use forms to conduct regular business in their organizations. Customers may download the forms and manually submit their requests. Each organization maintains a high amount of storage while also backing up personal information. At this point, organizations and technology elements are evaluated. The transaction and integration stages present the largest technical difficulties since they require two-way communication between individuals and government agencies. As a result, the majority of security measures, including network security, data validation, encryption, and authentication, are now required. During the interaction phase, every government website is displayed on a single page. Advanced security and cloud security are necessary to provide a secure conduit across all websites and data processes (Muhammad & Hromada, 2022).

3. Evaluating Methodology

The transformation of how the government provides services to its citizens and other stakeholders whenever and wherever they need them depends heavily on e-government. E-government system monitoring and benchmarking have been the subject of extensive research. Nonetheless, a limited amount of research has been done to assess e-government stage models overall. The majority of research on evaluating e-government systems has frequently concentrated on the different elements or sections within a model, such as strategy, policies, service supply, and ICT projects, with little to no in-depth assessment of the e-government stage model as a whole. The author argues that it

is essential to evaluate e-government systems before they are implemented since failing to do so would be a budget-wasting waste. Investors in e-government efforts are putting more and more pressure on funded programs to evaluate their effectiveness and impact using both qualitative and quantitative methodologies (Choi, Jeon & Kim, 2019)(Rehak, Hromada & Ristvej, 2017).

The Strength, Opportunities, Aspirations, and Results (SOAR) analytical approach has gained popularity as a planning and analysis tool for strategic initiatives over the past ten years. By applying this technique to identify environmental correlations, a firm can engage with its surroundings and establish business strategy. For more than 20 years, SOAR has established a reputation as a framework that provides a flexible way to think strategically and develop strategies. SOAR promotes individuals in charge of strategic planning to incorporate stakeholders beyond top management by involving the appropriate stakeholders, which helps planners comprehend the overall system (Stavros, 2013).

- S1: Protecting Personal Information in One-Way Communication
- S2: Protecting Personal Information in Two-Way Communication
- S3: Aware e-government stakeholders in protecting personal information
- S4: Personal Information Security Protocol

The opportunity factors are:

- O1: Providing a proper Personal Data Protection Law context
- O2: Developing Security Information Infrastructure
- O3: Identify Personal Information
- O4: Enhance security of communication and storages

Via the stage model the government will have the following aspiration

- A1: Reduce Cost
- A2: Obtain Law framework for protecting personal information
- A3: Provide Transparency
- A4: Improve e-service

The Results that can be obtained during implementing the model are:

- R1: Enhance security of communication channels
- R2: Provide high level of security for Personal Information within government organizations
- R3: Increase Trust of people to E-Government
- R4: Increase E-Participation

Analytic Hierarchy Process (AHP) is a multi-criteria decision-making approach that uses hierarchical formation to demonstrate a problem and then generates priority for solutions based on the user's choice (Dewa & Zlotnikova, 2014). Making judgments involves assessing a number of different factors. There are a variety of options available to us, and we must consider a variety of criteria or variables while selecting one of these options (Kampova, Lovecek & Rehak, 2020). We must choose these criteria and possibilities before assigning them a judgment score or assessment value since they will be more obvious when we make decisions as a group. Prof. Thomas L. Saaty created the Analytic Hierarchy Process (AHP), one of the techniques for generating multi-criteria choices. AHP is a multi-criteria decision-making approach that uses hierarchical formation to demonstrate a problem and then generates priority for solutions based on the user's choice. It is, in essence, a technique for constructing ratio scales from paired comparisons. The input can come from both objective measurement—price, weight, etc.—and objective judgment—satisfied feelings and preferences. Because people aren't always consistent, AHP allows for a modest amount of judgmental inconsistency. The major Eigen vectors are used to create the ratio scales, whereas the principal Eigen value is used to create the consistency index. AHP is the greatest method for making a decision when there are many criteria and possibilities. The hierarchy's structure can be used to represent Level 0, the analysis's goal (Saaty, 1987).

The hierarchical structure of the evaluation process is achieved at this section. The AHP structure consist of different level. The upper level is the main goal (G) which is evaluating proposed e-government stage model with considerations of protecting of personal data. The level below the upper level (second level) represents the essential targets (T) of the proposed model such as;

- T1: Improve security of personal Information
- T2: Achieve trust to E-government Services
- T3: Provide a reliable communication between Government and its stakeholders

There are numerous requirements at Level 1 made up of various components. It is also possible to add further levels of sub criteria and sub-sub criteria. The level above that is where the alternatives are, as seen in Fig.2. The relationships between factors, options, and the objective are depicted by the lines separating levels.

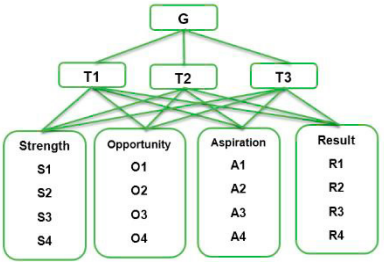

Fig. 2. AHP Structure combined with SOAR Group Factors

For calculating AHP, a hierarchical structure with a goal at the top level must be developed with respecting attributes/criteria at the second level and the alternatives at the third level. then decide which characteristics or criteria are most crucial in relation to the objective (using the fundamental scale values from table 1). This stage involves creating a pair-wise comparison matrix using the relative relevance scale (Brunelli, 2014).

Table 1. Fundamental Scale Values of Saaty

Definition	Equal Importance	Moderate Importance	Strong Importance	Very Strong Importance	Extreme Importance	Intermediate Values
Important Scales	1	3	5	7	9	2,4,6,8

After that, normalize pairwise matrix is calculated all the elements of the column divided by the sum of the column. The weighted sum value is calculated by adding up each value in the row, whereas the criteria weights are calculated by averaging all the elements in the row. To determine the ratio of weighted sub and criteria weight, equation (1) is applying (Dewa & Zlotnikova, 2014).

$$R = \frac{WS}{CW} \qquad (1)$$

Where R is the ratio, WS is weighted sum, CW is criteria weight

Calculate Lambda max (λmax) involves averaging the values derived from the equation (1).

$$\lambda_{\max} = \frac{R1+R2+R3+\cdots+Rn}{n} \qquad (2)$$

n is number of calculated ratio Rn

Results from Lambda max are used to calculate the consistency index (CI), which is calculated using the formula lambda max minus n upon n minus 1 as shown in the equation below.

$$CI = \frac{(\lambda_{\max}-n)}{(n-1)} \qquad (3)$$

By dividing the consistency index by the random index RI, the consistency ratio is obtained (equation4). The consistency index for a pairwise matrix produced at random is called the random index. The random index table for up to 10 criteria is displayed in table (2) (Sipahi & Timor, 2010).

$$CR = \frac{CI}{RI} \qquad (4)$$

Table 2. Random Index Values Based on Matrix Scales

n	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
RI	0	0.58	0.9	1.12	1.24	1.32	1.41	1.45	1.51

Finally, Verifying the hierarchy's consistency, with the condition that if the consistency ratio (Equation 4) is less than or equal to 0.1, the calculation's conclusion is deemed to be true.

4. Discussion

An essential tool that is typically applied is the SOAR analysis approach, and it is utilized in this research to evaluate the stage model for e-government. It is widely employed as a planning method. It can be connected with tools that aid in decision-making. Therefore, the SOAR and AHP techniques are combined in this study. The SOAR variables' qualitative values will be produced as a result of the integration. The AHP approach provides qualitative priorities for decision support. The aspects taken into account in SOAR analysis are given analytically defined priorities and are put on an equal footing by merging SOAR and AHP. We strengthen the quantitative data base for the evaluation of the e-government stage model by putting this integration into effect. The importance or weight of the SOAR criterion, as well as numerical results, are helpful while developing or choosing a model. It is critical to examine the supply and demand sides and any potential links between them because all elements on the numerical scale are equal.

The scaling of the second level's main targets is shown in table (3) of the AHP framework. In comparison to the other targets, the first target, which deals with protecting personal information, has a high degree. This element supports the main goal of the suggested approach, which is to protect personal information in e-government.

Table 3. The calculation essential Targets.

Targets/Criteria	T1	T2	T3	WS	CW	R	λmax	CI	CR
T1	0.723	0.50	1.44	2.660	0.587	4.532			
T2	0.103	0.07	0.04	0.215	0.081	2.671	3.066	0.033	0.057
T3	0.103	0.35	0.21	0.663	0.332	1.995			

The comparison of SOAR variables with respect to the first target (T1) is shown in table (4). The table demonstrates that strength and opportunity variables have higher worth than goals and accomplishments. It should be clear that all strength factors relate to protecting personal information to varied degrees. The stage model also allows the government additional opportunities to move toward creating a safe infrastructure for its e-services while adhering to the crucial objectives.

Table 4. The calculation of SOAR factors with Respect to T1.

Targets/Criteria	S	O	A	R	WS	CW	R	λmax	CI	CR
S	0.516	0.929	0.403	0.362	2.209	0.605	3.652			
O	0.172	0.310	0.403	0.362	1.246	0.227	5.498	4.229	0.076	0.084
A	0.172	0.103	0.134	0.121	0.530	0.122	4.355			
R	0.057	0.034	0.027	0.040	0.159	0.047	3.413			

The importance of the factors within the SOAR groups can be observed in table (5). There are four elements in each group. The table demonstrates that the first strength component, which is concerned with protecting personal data in one-way communication, will be given top attention. This is crucial since, starting with the first form of communication, personal data is being stored by the government. The development of a secure information infrastructure, which is the second opportunity group factor, will be given high priority in the stage model that has been provided. On the other hand, it is evident that a successful e-government depends on secured communication and information infrastructure in order to achieve its objectives. One of the key successes of e-government is transparency. As a result, transparency will be given top emphasis in the suggested paradigm. The greatest value among the result factors is (0.059), which is represented by the four group factor values in the result group. This affirms that the model's implementation will increase the stakeholders' trust in e-government services, enhance security of communication channels, provide high level of security for Personal Information within government organizations and increase E-Participation.

Table 5. Calculation of Factors within the SOAR Groups

Alternatives (S Factors)	S1	S2	S3	S4	WS	CW	R	λmax	CI	CR
S1	0.627	0.596	0.989	0.499	2.712	0.627	4.321			
S2	0.125	0.119	0.066	0.166	0.477	0.119	4.000	4.192	0.064	0.071
S3	0.125	0.358	0.198	0.166	0.847	0.198	4.283			
S4	0.070	0.040	0.066	0.055	0.231	0.055	4.164			

Alternatives (O Factors)	O1	O2	O3	O4	WS	CW	R	λmax	CI	CR
O1	0.303	0.215	0.511	0.292	1.321	0.303	4.357			
O2	0.606	0.429	0.511	0.292	1.839	0.429	4.285	4.219	0.073	0.081
O3	0.101	0.143	0.170	0.292	0.707	0.170	4.151			
O4	0.101	0.143	0.057	0.097	0.398	0.097	4.083			
Alternatives (A Factors)	**A1**	**A2**	**A3**	**A4**	**WS**	**CW**	**R**	**λmax**	**CI**	**CR**
A1	0.655	0.741	0.925	0.491	2.811	0.655	4.295			
A2	0.093	0.106	0.062	0.164	0.424	0.106	4.006	4.179	0.060	0.066
A3	0.131	0.318	0.185	0.164	0.797	0.185	4.310			
A4	0.073	0.035	0.062	0.055	0.224	0.055	4.107			
Alternatives (R Factors)	**R1**	**R2**	**R3**	**R4**	**WS**	**CW**	**R**	**λmax**	**CI**	**CR**
R1	0.292	0.237	0.388	0.314	1.230	0.292	4.214			
R2	0.584	0.474	0.646	0.314	2.018	0.474	4.255	4.158	0.053	0.059
R3	0.097	0.095	0.129	0.209	0.530	0.129	4.106			
R4	0.097	0.158	0.065	0.105	0.424	0.105	4.057			

5. Conclusions

Governments are increasingly turning to electronic government as a must rather than an option to better serve their constituents. Citizens must be at the heart of the system for e-government to succeed and to align with the objectives of the government. Thus, it is crucial to protect their personal information. This article applied the SOAR analysis method to identify the priority variables and to concentrate on the most important elements of e-government. The SOAR group considered a number of factors, some of which are concrete and others which are not. Hence, determining the amount of client happiness would be very difficult. The AHP technique has been used to provide a quantitative evaluation of the influence of each factor on decision-making. The evaluation revealed that the proposed approach had admirable traits and crucial elements that could support model implementation. Achieving trust in e-government services, improving the security of personal information, and providing dependable communication between the government and its stakeholders were the three key aims for the evaluation technique, which was based on the circumstances in developing nations. Based on the study's primary objective, which is to evaluate the proposed model and take these aims into account, Various group factors are developed and examined.

References

Agbozo, E., Alhassan, D., Spassov, K. (2018). Personal Data and Privacy Barriers to E-Government Adoption, Implementation and Development in Sub-Saharan Africa: In Proceedings of the International Conference on Electronic Governance and Open Society Challenges in Eurasia, 82–91.

Hernández-Moreno, S., de Hoyos-Martinez, J. (2010). Indicators of Urban Sustainability in Mexico: Theoretical and Empirical Researches in Urban Management, 5, 46–60.

Al-Dabbagh, M. (2011). Electronic Government in Iraq Challenges of Development and Implementation: Orboro University, 1-16.

Rehak, D., Novotny, P. (2016). Bases for modelling the impacts of the critical infrastructure failure: Chemical Engineering Transactions, 53: 91-96.

Nwaeze, A.C., Zavarsky, P., Ruhl, R. (2011). Compliance Evaluation of Information Privacy Protection in E-Government Systems in Anglophone West Africa Using ISO/IEC 29100: In Proceedings of the 2017 Twelfth International Conference on Digital Information Management (ICDIM), 98–102.

Wu, Y. (2014). Protecting Personal Data in E-Government: A Cross-Country Study: Government Information Quarterly, 31, 150–159.

Mu, E., Pereyra-Rojas, M. (2016) Practical Decision Making: An Introduction to the Analytic Hierarchy Process (AHP) Using Super Decisions V2: Springer.

Dewa, M., Zlotnikova, I. (2014). Citizens' Readiness for E-Government Services in Tanzania: Advances in Computer Science: An International Journal, 3, 37–45.

Muhammad, H., Hromada, M. (2022). Proposing an E-Government Stage Model in Terms of Personal Information Security in Developing Countries. In Proceedings of the 2022 IEEE International Carnahan Conference on Security Technology (ICCST), 1–5.

Choi, J.P., Jeon, D., Kim, B. (2019). Privacy and Personal Data Collection with Information Externalities: Journal of Public Economics, 173, 113–124.

Rehak, D., Hromada, M., Ristvej, J. (2017). Indication of critical infrastructure resilience failure. In Safety and Reliability - Theory and Applications: Proceedings of the 27th European Safety and Reliability Conference (ESREL 2017), 963-970.

Stavros, J. (2013). The Generative Nature of SOAR: Applications, Results, and the New SOAR Profile: AI Practitioner: International Journal of Appreciative Inquiry, 15, 6–26.

Kampova, K., Lovecek, T., Rehak, D. (2020). Quantitative approach to physical protection systems assessment of critical infrastructure elements: Use case in the Slovak Republic: International Journal of Critical Infrastructure Protection, 30.

Saaty, R.W. (1987). The Analytic Hierarchy Process—what It Is and How It Is Used. Mathematical modelling, *9*, 161–176.

Brunelli, M. (2014). Introduction to the Analytic Hierarchy Process: Springer, 2014.

Sipahi, S., Timor, M. (2010). The Analytic Hierarchy Process and Analytic Network Process: An Overview of Applications: Management Decision, *48*, 775–808.