Core Elements Impacting Cloud Adoption in the Government of Saudi Arabia

Norah Alrebdi, Nabeel Khan
Department of Information Technology
College of Computer, Qassim University, Buraydah, Saudi Arabia

Abstract—**The Kingdom of Saudi Arabia is taking rapid steps towards digital transformation in the field of government services. Cloud computing adoption may be the next step that supports this digital transformation to providing many features and reducing costs. Therefore, this paper will present multiple factors that may make it difficult to move to the cloud by conducting several interviews and questionnaires with government sector workers, those with technical experience, and that too to take caution and develop suitable solutions in advance. This paper also presents some recommendations and suggestions useful to consider when adopting the cloud in the public sector.**

Keywords—Cloud computing; e-governance; cloud computing adoption; smart government; Saudi Arabia vision 2030

I. INTRODUCTION

Based on trends of using technology, a basis in all government transactions within the Kingdom of Saudi Arabia (KSA) and in solidarity with the 2030 vision for digital transformation, several technologies should be considered and used in several fields. Cloud computing is one of the foremost necessary technical revolutions due to the advantages it offers. Therefore, the cloud is one of the technologies that the Kingdom attached great importance during this vision [1]. The World Bank defines e-government as "the use by government agencies of information technologies (such as Wide Area Networks, the Internet, and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government" [2]. While cloud computing is defined by the National Institute of Standards and Technology as" a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [3]. The resources vary according to their type. They may be an Infrastructure, platform, or software[4]. While deployment models of cloud vary rely upon the goals. It might be a Public, Private, Hybrid, or Community cloud [5]. Cloud computing provides several features relating to performance, availability, and reducing costs [6,7]. Therefore, the government of Saudi Arabia confirmed cloud computing's value, so it worked to develop some procedures for providing government services as a cloud service [8]. On the other hand, cloud computing in the government sector correlated with specific considerations. This research would address some factors influencing cloud computing implementation in government organizations based on prior literature review [9,10]. This research aims to assist decision makers in implementing cloud computing in government organizations and make them aware of the essential concerns to put in place the necessary measures to protect their organizations.

II. LITERATURE REVIEW

This section will discuss related works that discussed the factors affecting cloud adoption in government institutions in Saudi Arabia. By studying the previous literature, Alanezi in [11] conducts several discussions with IT employees in different organizations in different fields, for instance, the health field, finance field, education field, etc., in Saudi Arabia. They examine some expected effect factors when embracing cloud computing in their public or private organization. These discussions covered two aspects: negative and positive factors. The study shows four negative factors: Security and privacy challenges, government rules, lack of experience, and control loss. While the positive aspects contain three factors: the low cost, enhance performance, and the potential of scalability and flexibility, as shown in Table I.

Al-Ruithe et al. in [12] put forward several risks that may prevent the government sector from moving to the cloud. These risks are related to many technical, security, legal, and other aspects. Likert scale was used to measure these factors' effect on adopting cloud in public organizations based on 206 public sector workers' answers. The Table II illustrates these concerns and the average measure of responses. The findings indicate that Privacy issues and Trust issues represent the biggest fear of cloud adoption.

In [8] author proposed a framework of critical security elements using the triangulation method to validate results. The triangulation method contains three steps. First, review a previous literate review to collect the elements considered as critical security elements. Second is to organize interviews with IT professionals to review the data collected in the first step, besides suggesting new elements from experts. The final step is for conducting a survey using a close-end questionnaire to assure effective operation of framework. This framework dealt with three aspects: security risk elements, Social elements, and expected security advantages, as illustrated in Table III. Security risk elements contain interface security risks, threats of sharing the same sources, steal some accounts or services, malicious insiders, violating rules and regulations, the possession of data, data protection, data Spread, and client-side encryption error. The social elements contain confidence, security, and privacy. While the expected security advantages aspect contains scalability, take benefit of the advanced

security tools in the cloud market, a system of sophisticated security, standardized security interfaces, cloud security checking, check the implementation of Service Level Agreement (SLAs), and resource concentration [13].

TABLE I.   POSITIVE AND NEGATIVE FACTORS OF ADOPTING CLOUD COMPUTING

S.No	Factors Affecting Cloud Computing Adoption	
	Negative	*Positive*
1.	Security and Privacy	Low cost
2.	Government Rules	Enhance Performance
3.	Lack of Experience	Ability of Scalability and flexibility
4.	Loss of Control	

TABLE II.   SAUDI ARABIAN PUBLIC SECTOR CONCERNS ABOUT CLOUD COMPUTING

S.No.	Risks with Statistical Ratio	
	Risk	*Statistical Ratio*
1.	Unsatisfactory Financial Benefit	3.47
2.	Unripe Cloud Computing	3.76
3.	Unknown Data Storage place	3.91
4.	Lack of Functionalities	3.69
5.	Lack of Performance	3.71
6.	Loss of Control	4.04
7.	Data Governance Failure	4.03
8.	Proprietary lock in	3.67
9.	Dangerous Availability	3.8
10.	Integration problems	3.7
11.	Trust problems	4.1
12.	Privacy Problems	4.15
13.	Compliance Problems	3.86
14.	Legal Problems	3.96
15.	Security Problems	4.07

TABLE III.   FRAMEWORK OF CRITICAL SECURITY ELEMENTS

S.No.	Framework Elements Based on Security Aspects		
	Security Threats Elements	*Social Elements*	*Expected Security Advantage*
1.	Interface Security Risk	Security	Scalability.
2.	Threats of Sharing the Same Services	Confidence	Advanced Security tools in the cloud Market.
3.	Steal some accounts or services.	Privacy	System of Sophisticated Security.
4.	Malicious Insider		Security Interfaces Unified
5.	Violating rules and regulations.		Cloud Security Checking.
6.	Possesions of Data		Checking the Implementation of SLAs
7.	Data Incorporation and Service		Resource Concentration
8.	Data Spread		
9.	Client Side Encryption Error		

III. PROBLEM STATEMENT

With the growth of electronic services of Saudi Arabian government, it has become crucial to adopt cloud computing technology to make it robust and secured. Due to immense benefits offered by cloud computing, such as low cost and scalability, its necessary to guide ever emerging public sector. On the other hand, the implementation of cloud computing may bring some concerns and risks. Therefore, this paper aims to summarize the concerns that government institutions in the Kingdom of Saudi Arabia may face when adopting the cloud by reviewing previous literature to try controlling it and finding precautionary measures to avoid.

IV. RESULTS AND DISCUSSION

A. Research Method

This research incorporated quantitative research method to list factors that are important in Saudi Arabian public sector. It involves two steps; the first step was used by applying systematic literature review method which involved searching for the literature on this topic by using several approved search engines for papers such as Google Scholar and some popular databases such as ScienceDirect. In this research, authors used some keywords to help find papers related to the topic, such as: "cloud adoption," "public sector in Saudi Arabia," "affect factors," in addition to several other keywords. The research focused on papers published from 2017 to the present day of 2022. In the second step of this paper, we conducted a detailed review and analysis of the factors mentioned in the literature related to cloud adoption in the Saudi Arabian public sector. This paper introduces some of the concerns mentioned in previous literature to help researchers and government organization officials find solutions to overcome cloud adoption issues.

B. Results

Cloud usage in the public sector leads to the elimination of tremendous costs and adding several advantages. However, its adoption may pose some risks, making decision-makers hesitant about adopting it in their institutions. This study reviewed three research papers that discussed the factors affecting the implementation of cloud computing in the Saudi Arabian public sector. One of the papers mentioned in this research identifies factors affecting the public and private sectors. We noticed some similarities in the factors extracted, which may signify that there are common factors between the two sectors, so this research may help officials in the private sector also in the decision to adopt the cloud. Table IV shows general information on these papers. This review revealed that cloud and data security are the most important concerns affecting cloud adoption, in addition to the loss of control and data governance.

C. Recommendations

This section recommends solutions suggested by some researchers. In [14], its stated that Saudi government has expedite the process of restructuring and transforming the e governance strategy ensuring; cost reduction, improvement in services, time saving, increase in effectiveness and efficiency across all government organizations. "YASSER" platform has already been developed ensuring overall control of all

procedures, activities and all other issues related to implementation of effective e-governance. Moreover, the kingdom has recently taken a forward step to facilitate its adoption across government bodies by establishing committee to develop the necessary regulations for the cloud paradigm. Based on the findings in this research a comprehensive cloud system is recommended as shown in Fig. 1.

TABLE IV.   LITERATURE REVIEW COMPARISON

| Framework Elements Based on Security Aspects					
Research Reference	*Approach type*	*Sample Size*	*Year*	*Discuss Risk factors*	*Discuss Benefit factors*
	Quantitave Study	55 Universities	2021	Yes	Yes
[9]	Qualitative Study	32 Interviews	2018	Yes	Yes
[10]	Empirical Study (Quantitative)	206 Questionaries	2018	Yes	No
[8]	Mixed: Qualitative and Quantitative	12 Interviews and 32 Questionnaires	2017	Yes	Yes
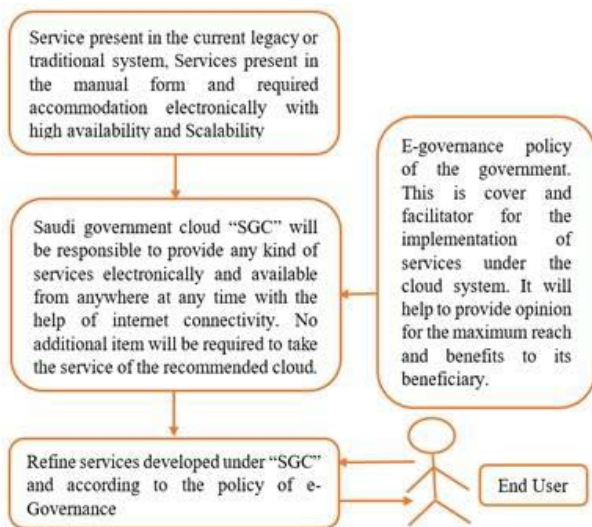
Fig. 1.   Recommended Cloud System.

In this research authors proposed to plan for an umbrella Saudi Government Cloud i.e., "SGC". A number of teams to be formed aiming to work specially in the reformation of cloud and e-governance resulting in implementation of SGC. These teams should have members from the government organizations to facilitate the process of investigating technical and financial feasibility of the system. Once the system is ready, it should be included under SGC with classification based on services and policies of e-governance.

Alannsary and Hausawi in [15] proposed a solution using cloud computing in the public organizations of Saudi Arabia. This solution is to launch a national cloud center headed by a Communication and Information Technology Commission (NCC). NCC will take responsibility for the cloud services of infrastructures and platforms. Besides the solutions and maintenance of the cloud services of software, this solution helps to decrease cost and IT resources. In contrast, SaaS's control, rules, and management will be the prerogative of each government agency. As for solutions that will provide by NCC, they propose two methods, either by studying the solutions that agencies are currently using and converting them into SaaS solutions. While the other is developing solutions they are needed from scratch, which may reduce time and cost.

In 2019, the same authors in [16] presented the previous proposal in detail and considered all parties contributing to developing and protecting this system. They proposed to create an Intelligent Government Cloud (IGC) powered by the National Center. This cloud provides services of all types to government agencies besides accountable for maintenance and verification work. The paper proposes that Riyadh be the headquarters of the IGC, with the establishment of several physical centers throughout the Kingdom to act as backup sites. The author suggests that the centers be part of Saudi universities due to many specialists who may contribute to this work's development. All government institutions must follow the Ministry of Finance regulations and the Ministry of Civil Service. IGC will provide any software solutions currently used in government organizations to a SaaS solution, which will contribute to reducing the costs paid by making them usable by any party separately. This proposal is consistent with the concern of the Kingdom in cybersecurity. Several organizations established interested in this field: The National Authority for Cyber-Security, the Saudi Federation for Cyber Security and Programming, the National Center for Information Security Technology, and the National Cyber-Security Center. Having these organizations may help implement the solution safely and accurately in compliance with government procedures and regulations.

In [17, 18], Al-Ruithe and Benkhelifa suggested a research paradigm focused on nine factors in the public organization of Saudi Arabia as helpful factors for the effective adoption of cloud data governance. These factors contribute to managing data, determining the requirements for data management, knowledge of the required functions of the data governance team, and align cloud data with other data in the organization. In addition to the ability to integrate cloud data governance functions with the cloud computing context adopted by the data-owning organization, development of the necessary contracts between the cloud consumer and the provider, the deployment of the system and the capacity to manage it in real-time, the attempt to sustain the data management program for a long period of time, the monitoring of the implementation method to ensure its correctness. Each factor contains some items that are defined from literature reviews and questionnaires. 28 hypotheses were brought up that fall under two types of hypotheses that are associative and causal. It was evaluated using Structural Equation Modelling (SEM). The results of hypothesis testing demonstrated that the model was adequate.

V.   CONCLUSION

Due to the tremendous interest exhibited by Saudi Arabia in providing government services electronically, the next step

for Saudi's government sector should be in adopting the cloud. For this reason, this paper discusses several previous research that discussed concerns related to cloud adoption in the government sector. This research provides a thorough overview of the risks that can arise when adopting a cloud to prepare for it and create innovative solutions before it crashes into failure. This review illustrates that the security element occupies a large proportion of concerns. Besides this, loss of control and data governance is potentially severe concerns.

As future work, we look forward to making a case study for one of the government organizations that adopted the cloud and investigating the amount of reduced costs after adopting it. As well as understanding the consequences and difficulties they faced at present and how they overcome them.

REFERENCES

[1] The Council of Economic and Development Affairs, Cloud and E-Governance Program, https://vision2030.gov.sa/ar/node/386, Accessed on June 24, 2022.

[2] M. M. Alkhusaili, "The Evolution of E-government Project in GCC Countries," pp. 2001–2012, 2020.

[3] I. Ahmed, "A brief review: Security issues in cloud computing and their solutions," Telkomnika (Telecommunication Comput. Electron. Control., vol. 17, no. 6, pp. 2812–2817, 2019.

[4] U. A. Butt, M. Mehmood, S.B. H, Shah, R. Amin, M.W. Shaukat, S.M. Raza, D.Y. Suh, M.J. Pilan, "A review of machine learning algorithms for cloud computing security," Electron., vol. 9, no. 9, pp. 1–25, 2020.

[5] A. Ullah, N. M. Nawi, and M. H. Khan, "BAT algorithm used for load balancing purpose in cloud computing: an overview," Int. J. High Perform. Comput. Netw., vol. 16, no. 1, p. 43, 2020.

[6] A. Albelaihi and N. Khan, "Top benefits and hindrances to cloud computing adoption in Saudi Arabia: A brief study," Journal of Information Technology and Management, 2020.

[7] M. Hosseini Shirvani, "An iterative four-phase cloud adoption decision model for IT outsourcing based on TCO," J. Soft Comput. Information Technology, vol. 9, no. 1, pp. 1–13, 2019.

[8] M. O. Alassafi, A. Alharthi, R. J. Walters, and G. B. Wills, "A framework for critical security factors that influence the decision of cloud adoption by Saudi government agencies," Telemat. Informatics, vol. 34, no. 7, pp. 996–1010, 2017.

[9] N.S.Aldahwan, M.S. Ramzan; "Factors Affecting the Organizational Adoption of Secure Community Cloud in KSA"; Security and Communication Networks; Volume, 10 Spetember, 2021.

[10] N.S.Aldahwan, M.S. Ramzan; "The Descriptive Data Analysis for the Adoption of Community Cloud in HEI-Based Factor Adoption"; BioMed Research International; Volume, 8 June, 2022.

[11] M. A. Alanezi, "Factors influencing cloud computing adoption in Saudi Arabia's private and public organizations: A qualitative evaluation," International Journal of Advance Computing and Science Application, 2018.

[12] M. Al-Ruithe, E. Benkhelifa, and K. Hameed, "Key Issues for Embracing the Cloud Computing to Adopt a Digital Transformation: A study of Saudi Public Sector," in Procedia Computer Science, 2018.

[13] F. Aldosari, A. Almiman; "Investigating the Effect of Cloud Computing Adoption on Improving the Digital Competitiveness Index-An Empirical Study: Case of Kingdom of Saudi Arabia"; International Journal of Computer Science and Network Security, Vol 22, No.4, April, 2022.

[14] A.Ali, D. Manzoor, A. Alouraini, "The Implementation of Government Cloud for the Services Under E-Governance in the KSA", Science Internation (Lahore), Vol. 33,no.3, pp 249-257, 2021.

[15] M. O. Alannsary and Y. M. Hausawi, "Adopting Software As a Service (Saas) in the," no. 3, pp. 124–130, 2017.

[16] M. O. Alannsary and Y. M. Hausawi, "Adopting and implementing a government cloud in Saudi Arabia, an integral part of vision 2030," in Proceedings of 34th International Conference on Computers and Their Applications, CATA 2019, 2019.

[17] M. Al-Ruithe and E. Benkhelifa, "Determining the enabling factors for implementing cloud data governance in the Saudi public sector by structural equation modelling," Futur. Gener. Comput. Syst., 2020.

[18] A. Almukhlifi, H. Deng, and B. Kam, "E-Government Adoption in Saudi Arabia: The Moderation Influence of Transparency," Journal of Advance Information Technology., 2019.