EPiC Series in Computing

Volume 58, 2019, Pages 387–396

Proceedings of 34th International Conference on Computers and Their Applications

Adopting and Implementing a Government Cloud in Saudi Arabia, An Integral Part of Vision 2030

Mohammed O. Alannsary[1] and Yasser M. Hausawi[1]

Department of Information Technology Programs
The Institute of Public Administration
Jeddah, Saudi Arabia
(Annsary, HawsawiY)@ipa.edu.sa

Abstract

Cloud computing is a relatively mature and robust technology that has promised its users with several proven advantages, such as cost reduction, immediate scalability, and resource sharing. The Cloud is built based on providing resources as services, such as providing Infrastructure, Platform, and Software as a Service. Such approach enables Cloud users to access these services based on their demand. In the government sector of Saudi Arabia, adoption and utilization of the Cloud is minimal. Despite being adopted officially, the Cloud has not been yet implemented properly. In our work we introduce how the government sector in Saudi Arabia can adopt and implement a Cloud Solution through utilizing its services and while considering issues related to its security.

1 Introduction

The Saudi Arabian Government approved the Vision 2030 program in late April 2016 [23], the vision generally is meant to achieve three goals: a vibrant community, a prosperous economy, and an ambitious homeland. We believe that implementing a Cloud solution for government agencies in Saudi Arabia will play a significant role in supporting and achieving the Vision's goals and programs. Having said that, the Cloud as a solution is the right fit to host and facilitate current and future e-government activities. Therefore; a clear and robust Cloud implementation needs to be planned and executed to assure its success.

Cloud computing is a relatively mature technology that has promised its users with several proven advantages. In the Cloud, resources are provided to customers as services, such as Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS) [7], and [17]. Figure 1 depicts the general construct of The Cloud.

In Saudi Arabia, a supreme royal decree included a directive to the Ministry of Communication and Information Technology (MCIT) to formulate providing government services and transactions electronically. This led to the establishment of the E-Government program (Yesser) as a joint project between MCIT, the Ministry of Finance, and the Communication and Information Technology Commission (CITC). Yesser is concerned with increasing the public sectors efficiency and productivity through enabling easy to use and better services to both organizations and individuals alike [20].

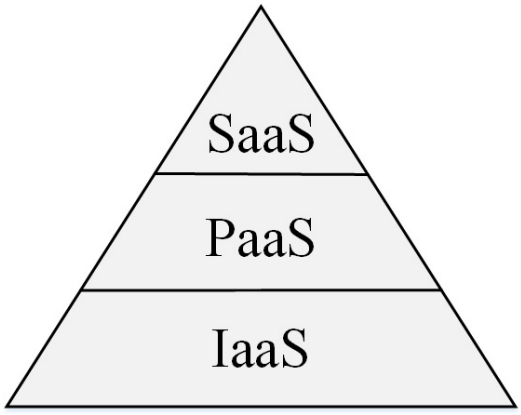

Figure 1: General Construct of the Cloud.

With the Help of Yesser, government agencies in Saudi Arabia implemented an e-government solution for their services, which led to an unprecedented investment in the Information Technology Sector, specifically building the infrastructure, developing software solutions, and hiring specialists in several IT disciplines. As a result, currently all government agencies have their own data center, a bundle of software systems, and well educated and talented professionals. One of the main concerns with this investment is that it is fully funded by the government, and contradicts with the Vision 2030 goal of rationalizing expenses and reducing cost on one hand, and maintaining an acceptable level of service on the other.

In addition, the existence of a relevant, yet very important national digital entity called National Information Center (NIC) as a unique national data center that unifies the management of national data and enables and provides the development of safe digital business solutions, products, and services that in turn help in organizing and facilitating the national data sharing and exchange between government agencies [19]. Hence, tight integration between both Yesser and NIC can better help reaching the goals of the E-government program and even move further towards smart government in Saudi Arabia. Moreover, recently there were royal decrees that established both the "National Authority of Cyber-Security", and the "Saudi Federation for Cyber Security and Programming". The former is the national entity that is responsible of cyber security and its affairs in Saudi Arabia. The latter is concerned with preparing young professionals in the fields of cyber security and programming.

In our work we propose a solution to support the Vision 2030 through implementing the Cloud by the Saudi Arabian government. We will discuss and explain its benefits and shortcomings to give a better view of its effectiveness in reducing cost, and rationalizing expenses, while maintaining an acceptable level of services. In addition, Information security (IS) is a vital aspect in any IT based transition. Therefore; considering it during the implementation of the Cloud is essential to its success. Such solution is expected to be holistic and forthcoming to the Saudi Arabian government.

The remainder of this article is structured as follows: the next section provides related work. Section 3 introduces a new method. Section 4 discusses the adaptation of the Cloud by the government of Saudi Arabia. Section 5 concludes the article and declares future direction.

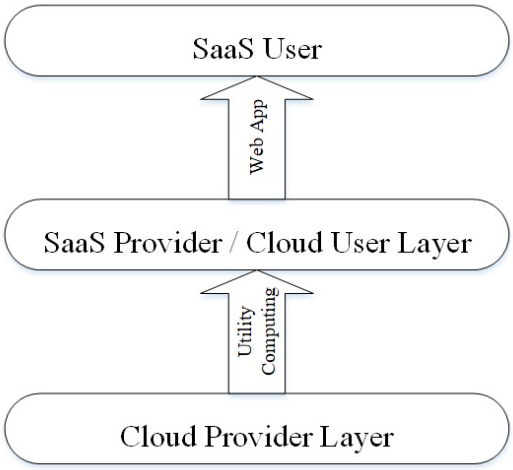

Figure 2: The General Construct of Delivering SaaS.

2 Related Work

The main advantage of the Cloud is that all computing resources are provided as a service to its intended customers, such as SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service) [7], [17]. In addition, SaaS is built and delivered using a three layer construct: Cloud provider, SaaS provider/Cloud user, and SaaS user [7]. Figure 2 shows the general construct of delivering SaaS.

Othman and Adbalrahman suggested developing a Cloud for Saudi Arabian universities and colleges [14]. Alkhater et al. [5] discussed the factors influencing the intention of adopting the Cloud in Saudi Arabian organizations. Similar to their work, other researchers investigated factors related to Cloud adoption in Saudi Arabia from different perspectives [16], [3], [4], [6], and [1]. However, none proposed a solution that enables government agencies in Saudi Arabia to benefit from adopting and implementing The Cloud, nor did they explain how it could be achieved. Furthermore, none described the means that will contribute to the success of such adoption and implementation.

Alannsary, and Hausawi [2] suggested adopting SaaS in the government sector in Saudi Arabia. their work focused on SaaS as a tool to maximize cost saving. They also suggested a National Cloud. However, this was to facilitate implementing the SaaS. With the current changes in the Vision 2030 initiatives, and the current state of Cloud with Yesser, there exist the need to further explain the adequate way to implement the Cloud.

Information security (IS) can be defined as ensuring confidentiality, integrity, availability, and accountability (which can be achieved through non-repudiation and auditing) through the application of integrated methods, principles, processes, and strategies [12]. IS is known to be one of the Clouds main challenges, Cloud customers are skeptical about the level of security that Cloud providers can assure. In fact, The Cloud technology has both internal and external security risks. Figure 3 shows the IS levels related to the Cloud. It is worth noting that Cloud providers are responsible of securing the IaaS and PaaS layers which include and are not limited to the hardware and data centers' physical security. On the other hand SaaS providers are responsible of securing the software. Generally, Cloud security solutions are based on two

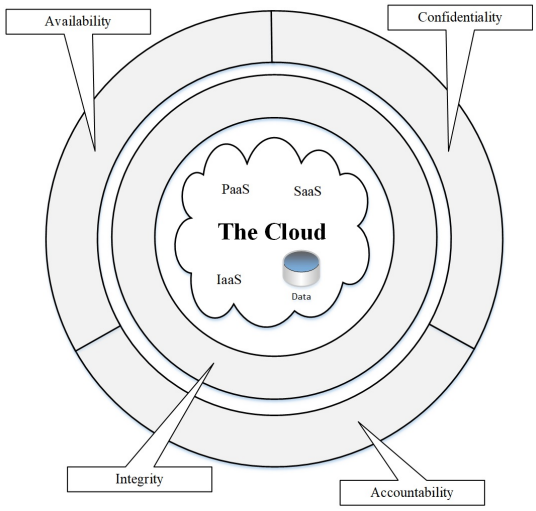

Figure 3: Information Security Levels Related to the Cloud.

ideas: Virtualization and Encryption [13]. Multi-tenancy [10] and [11], and Isolation [25] are two main characteristics of SaaS that are considered a security challenge for Cloud, SaaS providers, and end users [13], [15], [26], and [24].

3 A New Method

It is known that building and maintaining an efficient and reliable IT infrastructure may drain the organizations' financial assets and resources. This may become a major issue if the IT infrastructure is not up to the challenge and/or not sufficient enough to fulfill the organizations technological needs. In addition, the rapid change and development in both the hardware and software requires additional and continuous investment from organizations. Therefore; organizations need to implement sustainable and integrated solutions while minimizing the cost to allow proper return on their investment. The Cloud is considered as such solutions.

3.1 Current State

Since the year 2000 government agency officials in Saudi Arabia strived to fulfill their agencies' technological needs through investing in IT, specifically through establishing and maintaining Data centers, training staff, and developing related Software applications. In addition, in a recent study that surveyed government employees [1], 29% of the respondents reported that yes, their agencies have already adopted some Cloud services, 16.5% responded that they do not know, and around 55% responded with no the Cloud is not adopted. Moreover, in the respondents answer to weather the organizations plan for Cloud computing adoption, 69% of them responded that their agencies intend to adopt the Cloud.

There are several factors that contribute to not adopting the Cloud in government agencies in Saudi Arabia, such as the unavailability of professionals in the field, the newness of the technology, and the technologies reputation of being hard to secure and manage. However, the fact is that the technology itself was created to reduce expenses, and allow better management

of resources. Therefore, the need to eliminate the fears to capitalize on the technology's benefit is essential.

Yesser has several initiatives and products, one of which is the Government Cloud Computing (GCC). The objective of this initiative is to allow the delivery of shared services to government agencies and sectors within a reliable, safe, and highly efficient environment. The scope of the Government Cloud Computing is based on two approaches: building upon and empowering the available and already completed services, and transforming the planned (in the future) services to the Cloud.

Yesser defines GCC as a Cloud, where in fact it is a collection of data centers that are interconnected together via a secure network to provide services through the Government Service Bus. One of the main observations is that neither Yesser nor the GCC have any control over the hardware of these data centers, which is supposed to be the IaaS and PaaS of the Cloud. In addition, the national data management is part of the tasks of the National Information Center (NIC), which makes security assurance difficult to achieve unless strong and successful integration is maintained. Moreover, Scalability, Mutli-tenancy, and Isolation are advantages of the Cloud, with the current structure of GCC all three are not available. Finally, describing and distributing services over the names of the main layers of a Cloud does not significantly mean that a Cloud is in place and available. Table1 displays the services of GCC and their distribution of the IaaS, PaaS, and SaaS Layers, existing services are shown in **bold** and *italic*

Layer	Service
IaaS.	***Government Secure Network.***
	Disaster Recovery.
	Hosting.
	Voice and Video over GSN.
PaaS.	National Enterprise Architecture (NEA).
	Government Service Bus (GSB).
	Executive Strategy Manager (ESM).
	Communication and notification (Tarasoul).
	Enterprise Program Management (EPM).
	Software Development Life Cycle (SDLC).
	IT Service Management (ITSM).
	National Contact Center (Amer).
SaaS.	***E-Correspondence.***
	E-Procurement.
	E-UnivApply.
	Government Resource Planning.
	Government Relations Management.
	Geospatial.

Table 1: Services of the GCC Layers - Existing Services are in **Bold** and *Italic*.

Yesser also has a product that is considered a pillar of the National infrastructure, the Government Service Bus (GSB). The key role of GSB is to facilitate the exchange of data between government agencies. However, each government agency that either provides or consumes services will still need to maintain a complete IT infrastructure to be able to provide and/or benefit from the data available through the GSB. Since the Government of Saudi Arabia is the main source of income to all government agencies, Such architecture does not allow reducing cost. In addition, it will be difficult to assure an elevated level of security, since the security strength

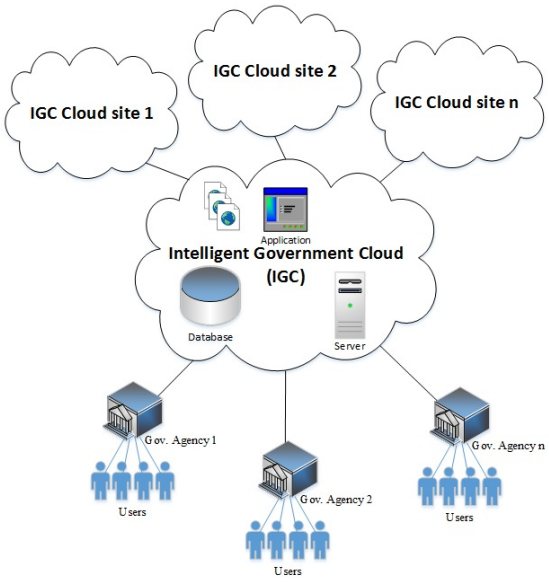

Figure 4: Overall Structure of the Proposed IGC.

of the GSB and all participating government agencies will be equal to the security strengths of the weakest link.

Another product of Yesser is the Government Secure Network (GSN), the key role of GSN is to connect government agencies with the e-Government data center. The e-government data center is the host of the national portal called "Saudi", the data center was built using highest security and technical standards. However, since GSN is concerned with connecting government agencies to each other network wise, it does not actually work or act as a Cloud in its conventional structure, in other words, there is no IaaS, PaaS, nor SaaS, the only advantage of GSN is connecting government agencies to each other securely.

3.2 Adopting the Cloud

In our work we propose a solution that will allow the Saudi Arabian government to correctly utilize the Cloud technology. Our suggestion is based on establishing an Intelligent Government Cloud (IGC) that is operated and supervised by the National Information Center(NIC) similar to the Intelligent Cloud Computing Center of the National Information Resources Services agency (NIRS) of South Korea [22]. The overall structure of the IGC is depicted in Figure 4. The IGC's main goal is to supervise the government Cloud, secure it, and provide government agencies with the IaaS, PaaS, and needed SaaS. SaaS development, Verification, validation, and maintenance could also be part of IGC's duties to standardize the software development process.

The IGC needs to be centrally located in Riyadh (the capitol of Saudi Arabia). In addition, the IGC also needs to be connected to several physical Cloud sites, that need to be distributed around the country, and act as backup sites to allow the IGC to better operate and serve its customers.

In Saudi Arabia, there are more than 25 public universities that are distributed around the countries major cities and towns. These universities have invested heavily in their IT

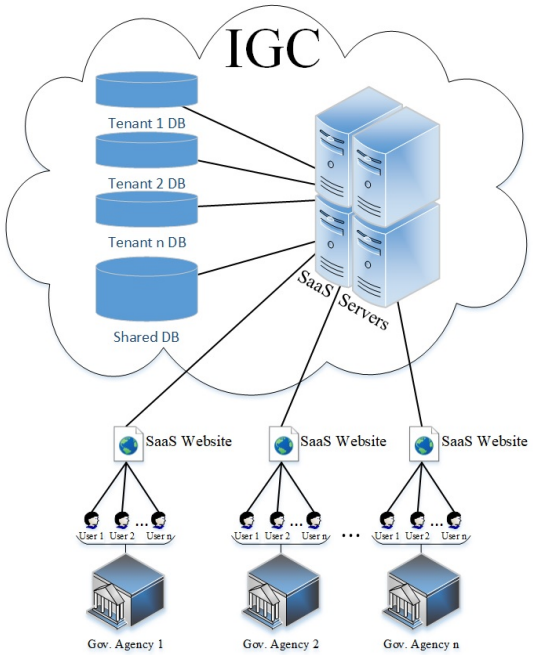

Figure 5: Proposed Structure of the Government SaaS.

infrastructure, kept their IT staff up to date with recent technologies, and hosts a verity of computing faculty. These capabilities make transforming university IT centers to be Cloud physical sites a more suitable and viable solution.

We also suggest that the IGC and its sites host, hire, and manage current work professionals of government agencies in Computer science, IT, and related fields. This will allow gathering all talented individuals in a centralized location to have better outcomes. In addition, it will result in downsizing the number of IT professionals in government agencies, and reduce or eliminate these agencies investment in data centers.

All government agencies in Saudi Arabia need to abide by the rules and regulations set forth by the ministry of Finance(MOF) and the Ministry of Civil Services (MCS). Therefore, all software solutions developed by different agencies provide the same functionalities when it comes to Human Resources and/or Finance. In addition, there are software solutions that serve individual and special needs based on the role of the government agency. Having said that, when the e-Government project was initiated, most of the government agencies have either worked relentlessly to in-house develop software solutions, or contracted software development companies to develop the software solutions.

Having such vast amount of software solutions that serve the same purpose may lead to complications in maintaining, updating, and monitoring these solutions for each agency individually. In addition, the cost related to such activities increases annually. Therefore, transforming these software solutions to a SaaS solution that serves all agencies at once is considered an excellent approach for all. The proposed approach of implementing a SaaS in the IGC is depicted in Figure 5. The IGC will host both the application servers that run the different SaaS solutions, and the databases needed by these SaaS solutions. In addition, the government agencies will

have access to the SaaS via connecting to the IGC.

To benefit from the current collection of similar software solutions when implementing the Cloud and providing SaaS to government agencies, we suggest that all similar software solutions be analyzed and evaluated to select the most useful one, which then can be transformed into a SaaS to make it available and utilizable by other government agencies [9]. Another option is to develop a completely new SaaS from scratch to serve the functionalities of MCS and MOF. As for the software solutions that serve individual and special agency needs, we suggest to simply host them in the Cloud instead of the government agencies data center. Needless to say that all software solutions need to be evaluated, verified, and validated.

4 Discussion

The above sections have provided literature review (background information and related work) and introduced the proposed solution for both adopting and adapting the Intelligent Government Cloud (IGC) as a primary pillared technology on which can be relied to benefit the government. This section discusses the rationales of introducing such proposal based on financial, performance, security, and regional view points; as currently the Saudi Arabian government is under national transformation aiming to achieve the goals of vision 2030 relying on most recent technology.

Having 232 governmental entities participating in Yesser and supervised by ministries, authorities, corporations, and agencies; the Saudi Arabian government can rely on the Cloud to rationalize and reduce IT related expenditure. According to [18], the total spending on IT in 2017 was expected to reach $14.2 billion, where government sector holds 12.9% of such total spending (i.e.: $1.83 billion). However, adopting the Cloud solution can help reducing at least 50% of the governments annual IT expenditure. Amazon Web Services (AWS) is considered the largest company that provides Cloud services to more than a million individual customers, whom are served through 13 worldwide locations, while providing more than 70 different Cloud services, yet its operational expenses in the year 2016 was $8 billion [21]. Based on the number of Cloud clients, the Saudi Arabian government is only in need of one Cloud center, which would cost 1/13 of the AWS operation expenses. Meanwhile, the Saudi government approximate annual operational cost would only be 33.6% of the total IT spending based on the year of 2017.

One more efficiency benefit that can be achieved from adopting the proposed IGC is centralizing immediate actions needed to perform updates and changes on shared applications and systems. For example, some reforming and transforming decisions need quick implementation such as patches on running systems to be reflected. While the current situation requires each of the 232 government entities to implement and apply the needed changes, having a unified service used by all entities and controlled by a unique entity would make it faster, integral, consistent, and more accurate. Furthermore, government agencies will be able to share resources, and simply disseminate successful experiences and practices. In addition, it would become easier for any governmental entity to establish branches and offices without having to pay huge IT infrastructure, operations, and maintenance expenses. Moreover, some government agency's infrastructure requirements change throughout the year, the IGC will allow those agencies to scale their infrastructure up or down based on their needs. Of course, there still exists the need to have IT units within each governmental entity to maintain stability and business continuity of IT services, and provide technical support to local staff.

During the recent six years, the government of Saudi Arabia has made several important decisions related to national Cyber-Security. Many governmental entities have been established

such as the National Authority for Cyber-Security, the Saudi Federation for Cyber-Security and Programming -mentioned previously-, The National Center for Information Security Technology, and the National Cyber-Security Center. Moreover, Saudi ARAMCO has established a national security center after the security incident of 2012 where a large-scale cyber attack targeted part of ARAMCO's IT infrastructure causing damages and losses [8]. The adoption of the proposed IGC can fit along within the recent national attention to cyber security, as having a single point of control, which can assure applying security standards, regulations, and polices properly. In addition, security monitoring and quick response to incidents can be done professionally. Furthermore, the proposed IGC can become a profit center not like the current IT services that are cost centers, as expanding the domain of the IGC services to cover the Gulf Cooperation Council can bring profitable business.

However, despite all the above-mentioned advantages and benefits, there are some downsides of adopting the Cloud technology in general. Such downsides can happen to any Cloud environment once the ingredients exist. For example, single point of failure is one possible disadvantage, both internal and external security and privacy breaches are also possible disadvantages despite the existence of their solutions.

5 Conclusion

The Saudi Arabian government is currently under a reforming process to achieve the goals of its promising vision 2030. This research work proposed the establishment of an Intelligent Government Cloud (IGC) as a holistic IT solution that provides all types and levels of Cloud services: SaaS, PaaS, and IaaS to all government entities. Within this work, advantages (rationalizing and reducing expenditure, resource sharing, quick updates, dissemination of experiences and practices); and disadvantages (single point of failure, security and privacy) of adopting the proposed IGC solution were discussed.

Future direction is working towards evaluating the application of the Cloud and SaaS in Saudi Arabia government agencies, to study the financial feasibility, and proof the validity and concept of operation.

References

[1] Majid Al-Ruithe, Elhadj Benkhelifa, and Khawar Hameed. Current State of Cloud Computing Adoption-An Empirical Study in Major Public Sector Organizations of Saudi Arabia (KSA), 2017.

[2] Mohammed O. Alannsary and Yasser M. Hausawi. Adopting Software as a Service (SaaS) in the Govewrnment Sector of Saudi Arabia, 2017. ISBN: 978-93-86291-85-1.

[3] Adnan Mustafa AlBar and Md Rakibul Hoque. Determinants of Cloud ERP Adoption in Saudi Arabia: an Empirical Study, 2015.

[4] Ahmed Albugmi, Robert Walters, and Gary Wills. A Framework for Cloud Computing Adoption by Saudi Government Overseas Agencies, 2016.

[5] Nouf Alkhater, Gary Wills, and Robert Walters. Factors influencing an Organisation's intention to adopt cloud computing in Saudi Arabia, 2014.

[6] Nouf Alkhater, Gary Wills, and Robert Walters. Factors Affecting an Organisation's Decision to Adopt Cloud Services in Saudi Arabia, 2015.

[7] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. A View of Cloud Computing, April 2010.

[8] Christopher Bronk and Eneken Tikk-Ringas. The Cyber Attack on Saudi Aramco, 2013.

[9] Scott Chate. Convert your web application to a multitenant SaaS solution, Dec 2010. DeveloperWorks.

[10] Chang Jie Guo, Wei Sun, Ying Huang, Zhi Hu Wang, and Bo Gao. A Framework for Native MultiTenancy Application Development and Management, 2007.

[11] Jun Guo, Hao Huang, Xiaofeng Shi, Fang Liu, and Bin Zhang. Research on SaaS Service Performance Prediction Method in Dynamic Resource Environment, 2013.

[12] Yasser M Hausawi. Towards a Usable-Security Engineering Framework for Enhancing Software Development, 2015.

[13] Santosh Kumar and RH Goudar. Cloud Computing-Research Issues, Challenges, Architecture, Platforms and Applications: a Survey, 2012.

[14] Abdelrahman Osman, Saad Mamoun Abdalrahman, and Abusfian Elgelany. Proposed academic cloud computing for saudi universities and higher institutes, 2013.

[15] Mark D Ryan. Cloud Computing Security: The Scientific Challenge, and a Survey of Solutions, 2013.

[16] AlAlaa N Tashkandi and Ibrahim M Al-Jabri. Cloud Computing Adoption by Higher Education Institutions in Saudi Arabia: an Exploratory Study, 2015.

[17] The National Institute of Standards and Technology. The NIST Definition of Cloud Computing, 2011.

[18] "https://mcit.gov.sa/en/media-center/news/92185. Ministry of Communication and Information Technology.

[19] https://www.moi.gov.sa. Saudi Arabian Ministry of Interior.

[20] https://www.yesser.gov.sa/en/Pages/default.aspx. Saudi Arabian E-Government Program - Yesser.

[21] http://www.annualreports.com/HostedData/AnnualReports/PDF/NASDAQ_AMZN_2016.pdf. Amazon corporation, 2016 annual report.

[22] http://www.ncis.go.kr/eng/index.jsp. The National Information Resources Services Agency.

[23] "http://www.vision2030.gov.sa/en. Saudi Arabian Vision 2030.

[24] Zhifeng Xiao and Yang Xiao. Security and Privacy in Cloud Computing, 2013.

[25] Yangpeng Zhu and Jing Zhang. Research on Key Technology for SaaS, July 2012.

[26] Dimitrios Zissis and Dimitrios Lekkas. Addressing Cloud Computing Security Issues, 2012.