ADOPTING SOFTWARE AS A SERVICE (SAAS) IN THE GOVERNMENT SECTOR OF SAUDI ARABIA

[1]MOHAMMED O. ALANNSARY, [2]YASSER M. HAUSAWI

[1,2]Department of Information Technology, Institute of Public Administration Jeddah, Saudi Arabia
E-mail: [1]Annsary@ipa.edu.sa, [2]HawsawiY@ipa.edu.sa

Abstract- Cloud computing is a new technology that has been the focus of Information Technology researchers worldwide. SaaS (Software as a Service) is one of the Cloud services that enables its users to access software based on their demand. Currently, Cloud has not been adopted, nor was SaaS utilized, or in other words neither officially nor properly implemented in government agencies of Saudi Arabia. This work demonstrates how the government of Saudi Arabia could benefit from adopting and implementing a SaaS in the Cloud, and the means that contribute to the success of such adoption and implementation with consideration to security related issues.

Index Terms- Cloud, SaaS, Saudi Arabia, Security, Saudi Vision 2030.

I. INTRODUCTION

During the past years Cloud computing has been the focus of Information Technology (IT) researchers and specialists worldwide. It is considered a solution for several technology issues that face both public and private sectors alike. In the Cloud, computing resources are provided to users as a service, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [1], and [2].

SaaS has several advantages, from the tenants prospective: the needed software is provided to their employees with less cost [3] using the pay per use or software rental revenue models [4]. In addition, technical support, and maintenance of hardware and software are the responsibility of both the Cloud and the SaaS providers. Moreover, the latest version of the software will always be available to the tenants. Finally, SaaS providers are responsible of assuring reliability, data safety, disaster recovery, and security from a higher level with minimal cost to the tenant. On the other hand, SaaS providers have the advantage of renting the SaaS instantaneously without requiring special hardware and/or software.

Software development companies are forced to move towards SaaS, this is due to the fact that SaaS is considered as a "strategic tool to compete in the market" [5]. SaaS does not require a new software development life cycle model [6]. However, SaaS is different from traditional software in two main characteristics: incorporating multi-tenancy within the design of the software, and assuring the isolation between tenants, which is usually done in the software and database layers [7], [8], [9], and [10].

During the past twenty years, government agencies in Saudi Arabia have invested heavily in the IT infrastructure. In addition, there were signed agreements and contracts with software development companies to deliver the needed software to facilitate and ease the completion of jobs and tasks. Moreover, specialists in several IT disciplines were attracted to supervise and work in the IT and computing centers to allow their operation and participate in the development and maintenance of such software.

The government of Saudi Arabia is the main funding source of the majority of its agencies – since these agencies do not have financial incomes – therefore they are considered cost centers. Thus, there exists the need to rationalize expenses and reduce costs while maintaining decent IT services that satisfy both arties, the service provider and the service user.

On April 25th, 2016, The Saudi Arabian cabinet approved the 2030 Vision [11], which is based on three pillars: vibrant community, prosperous economy, and ambitious homeland. We believe that IT will contribute majorly and play an effective role in supporting all pillars. Especially when adopting the Cloud in government agencies.

However, working towards such a transitional movement to make the government sector IT based puts Information Security on top of the issues that should be considered throughout upcoming transitional processes.

Therefore, this article proposes a solution to adopt and implement the Cloud and SaaS by the Saudi Arabian government. It exploits benefits, and redress the shortcomings of the Cloud and SaaS technologies to improve performance, rationalize expenses, and reduce cost, while guaranteeing the security of the data used. In addition, it emphasizes the importance of adopting and implementing the Cloud and SaaS to be considered as a holistic solution for IT environments in Saudi Arabia's government. Moreover, it highlights the current capabilities and success factors that Saudi Arabian government agencies have. Furthermore, the proposed solution will play a major role in Saudi Arabia's strive towards its 2030 vision.

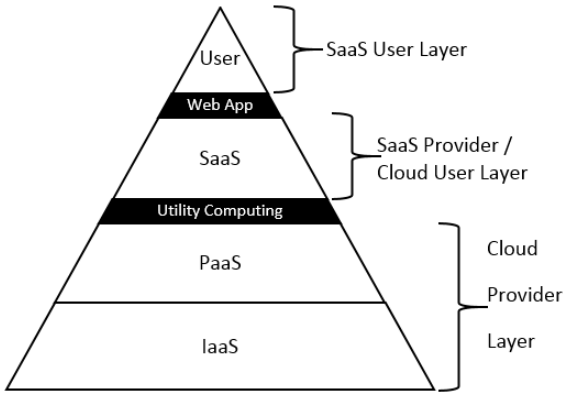


Fig. 1: SaaS structure in the Cloud

The remainder of this article is structured as follows: next section provides background information and related work. Section 3 introduces a proposed solution. Section 4 discusses the adaptation of the Cloud and SaaS to Saudi Arabian government agencies. Section 5 concludes the article and declares future direction.

II. BACKGROUND AND RELATED WORK

SaaS is different from traditional and web applications in many aspects. In SaaS, tenants are able to rent some services instead of the complete SaaS solution. In addition, new features are added regularly to the SaaS. Moreover, SaaS providers continuously apply updates to the SaaS [3], [5], and [10]. Furthermore, there are differences in the structure of the SaaS, the way it is hosted and delivered to the tenants. Finally, as mentioned above multi-tenancy [7], and [12] and isolation [10] are main SaaS characteristics.

Next, we examine in more detail one of the most important services provided by the Cloud, SaaS, and an integral part of the Cloud, its security.

A. SaaS (Software as a Service)

In the Cloud, the structure of a SaaS is based on three layers: The Cloud provider, the SaaS provider / Cloud user, and the SaaS user [1], as depicted in Fig. 1. The Cloud technology is used to enable and facilitate the delivery of software to tenants and their users. Recently, software development companies adopted the SaaS model to be able to compete. In addition, several government agencies worldwide adopted and implemented SaaS solutions in order to rationalize expenses and reduce costs.

As explained above, SaaS has two main characteristics that distinguish it from traditional and web applications, multi-tenancy and isolation. In multi-tenancy, a centralized version of the applications source code is shared between multiple tenants (each having one or more users). Applications need to adopt on of the three multi-tenant models described in [13] to be treated as a SaaS. Isolation is the process of assuring the separation in both the application and database layers between tenants.

Zhu et al. [10] discussed the advantages and differences amongst SaaS and traditional applications such as multi-tenant support, user-licensing differences, reduced user investment, ease of implementation, convenient update, and minimal to no maintenance.

Orue and Arrieta [8] explained the software system issues, such as its elevated cost, and its resource consumption. They also explained the influence that the Cloud has on changing current software development methodologies. They claim that the Cloud and SaaS are changing how software is designed, developed, and consumed. Which, as an example will result in the surfacing of new requirements such as multi-tenancy, scalability, and compliance with the Service Level Agreement (SLA) document.

Vashistha and Ahmed [9] discussed isolation issues and challenges, where they distinguished between the technical isolation issues faced by developers and those faced by service providers. They also proposed testing multiple sources for issues related to isolation.

Othman and Adbalrahman suggested developing a Cloud for Saudi Arabian universities and colleges [14]. Alkhater et al. [15] 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], [17], [18], and [19]. However, none proposed a solution that enables government agencies in Saudi Arabia to benefit from adopting and implementing a SaaS, 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.

B. Computer Security and the Cloud

Information Security can abstractly be defined as an application of integrated methods, strategies, principles, and processes that work together in order to assure information protection against inappropriate usage through ensuring its properties: confidentiality, integrity, availability, and accountability, which is achieved via auditing and non-repudiation [20].

Information Security has been considered as one of the most important challenges that Cloud Computing faces so far, as many of the customers (companies, organizations, and individuals) that rely on the Cloud as a main business facilitating tool are still skeptical about the reliability level of the security services that the Cloud service providers can assure.

Those customers are still concerned with the protection scope that the providers should take responsibility of, and which party should guarantee the protection process. In addition, there are some

legislations that mandate existence of access control for the stored and used information within the Cloud environment. For example, The American Health Insurance Portability and Accountability Act (HIPAA) has an access control existence condition for all Information Technology service companies that deal with healthcare entities [1].

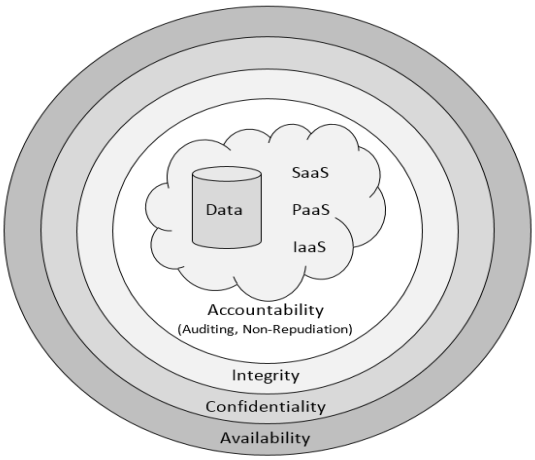


Fig. 2: Information security levels related to the Cloud

In fact, The Cloud faces both external and internal information penetration risks. For the former, most of the penetration risks are similar to the risks that typical IT centers face [1]. At the SaaS or application level, or the end-user interface, end users have more security related responsibilities than Cloud service providers do, as they have to keep their Cloud services' login credentials away from non-authorized people, and keep them only for personal usage.

On the other hand, the rest of the Cloud levels are more likely to be protected by the providers rather than the end users. For the later, Cloud and/or SaaS providers must protect the information of a tenant from the information of other tenants within the Cloud environment. In addition, tenants need to be protected from the employees whom work for the Cloud and/ or SaaS providers.

Fig. 2 shows the information security properties that are related to the Cloud along with their levels of application. The relationship between those properties and The Cloud services (SaaS, PaaS, IaaS) starts when the Cloud services become available for the customers, then confidentiality comes into the process when customers use their login credentials to gain access to such Cloud services. After the customers are granted access to the authorized Cloud services, integrity becomes a property of action in order to protect the accessed services along with the used data within the Cloud environment from improper usage and alteration. Finally, accountability (auditing and non-repudiation) ensures recording every transaction executed in the Cloud services and associate it with its party of action.

Cloud providers, whom provide PaaS and IaaS services, should take care of hardware and data centers' physical security, while SaaS providers need to assure the software's digital security. End-users are only responsible for their personal security through protecting their credentials from improper usage. In general, security solutions for the Cloud are based on two ideas: Virtualization and Encryption [21]. In order to depict the importance of information security to the Cloud, the information security properties that are shown in Fig. 2 will be associated with the Cloud as follows:

1. Confidentiality

Confidentiality is considered the most important information security property, as it is a key pillar for controlling services and information access. Successful application of confidentiality is a primary step to achieve successfulness of applying the other properties of information security. Regardless of the importance of the role that end-users should play in order to achieve the confidentiality property, multi-tenancy is one of the Cloud Computing features that is considered a challenge for the Cloud and SaaS providers due to the importance of their customers' privacy protection against one another [21].

Providing multi-tenant services that are shared simultaneously to multiple customers may lead to the possibility of having hidden adversaries who are eager to violate privacy protection for various reasons. One reason could be just gaining access, while another dangerous reason could be alteration or distortion of the Cloud services and information, a third reason may be critical, such as destroying or denying Cloud services [22]. Therefore, isolation is considered an important technique that helps protecting customers while utilizing the multi-tenancy feature.

2. Integrity

It is important to use the Cloud services along with the information being traded, processed, and stored in a proper way without any improper alteration or distortion. Once information is improperly altered, its integrity is violated and it becomes inaccurate and unreliable. The responsibility of Integrity assurance is shared by Cloud providers, SaaS providers, and end-users. End-Users should not allow unauthorized parties to alter their information on the Cloud [24]. However, both Cloud and SaaS providers hold responsibilities to take care of most security assurance tasks. They must protect multi-tenant users from violating the information integrity of one another. In addition, they should protect their customers ' information against internal violation caused by such providers' staff [23].

3. Availability

Not like other environments, availability is a critical security property and quality attribute in the Cloud, as the Cloud service should be available all times. Cloud

services unavailability may cause major losses and damages for companies and organizations that rely on Cloud services for their main businesses processes, and may put them out of service [23]. Therefore, availability is a non-tolerable need for both providers and customers. The responsibility of assuring the availability is totally on the providers, as the responsibility of the customers is limited to only providing a stable Internet connection to allow access to the providers' sites [24].

4. Accountability

Multi-tenancy is a key feature that the Cloud and SaaS relies on for providing services. Therefore, it is important to audit all the transactions in the Cloud environment. It is essential to determine the responsible party of each committed transaction starting from access requests to the Cloud servers, and ending by completing transactions and successful logging out. In addition, non-repudiation must be applied. Similar to availability, the responsibility of assuring accountability is totally on the providers [24].

III. PROPOSED SOLUTION

The cost of initiating and maintaining an IT infrastructure within an organization is known to be high. Which includes purchasing and upgrading hardware, software licenses, man power, and day to day operations. Such expenses are known to be the highest amongst maintaining and operating different organization assets. In addition, the cost incurred by managing an IT center is known to be continuous, due to the rapid development in the IT world. Therefore, it is essential that organizations implement integrated and sustainable solutions with reduced cost, that suit the cognitive and service return from their investment in an IT environment. One of the known solution is to utilize the Cloud technology.

A. Current situation

In Saudi Arabia, there are two main ministries, the Ministry of Finance (MoF), and the Ministry of Civil services (MoCS), whom are responsible of creating and maintaining laws, rules, and regulations related to the financial and human resources policies and procedures for all other government agencies.

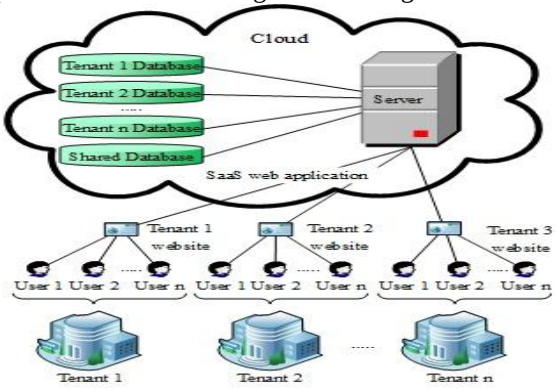


Fig. 3: An example of a SaaS solution

The MoF is concerned mainly with the financial part such as the preparation of the annual budget, funding government projects, and monitoring purchases. While the MoCS is mainly concerned with the managerial and functional part, such as vacations, and promotions. In addition, there are other government functionalities that are shared amongst other government agencies that do not fall within the responsibility of the above-mentioned ministries, such as the admissions and registrar functions available in all public universities whom are supported fully by the government.

During the last twenty years, all government agencies -individually- purchased or in house developed systems that enable automating such functionalities. For example, all public universities purchased or developed systems that automate the admission and registration processes, despite the fact that they all fall under the supervision of one ministry, and it was possible to develop or purchase one system that takes care of such functionalities and distribute it to all universities.

The Institute of Public Administration of Saudi Arabia (IPA) had a similar approach, where they internally developed most of their systems, specifically the ones related to the finance and human resource departments. Some of these systems were then given to other government agencies upon their request, that by default implement the same policies and procedures. There were some drawbacks in their approach, for example, the IPA requests certain hardware and software setup to be available. In addition, applying new updates and system patches were somewhat problematic.

It has been noticed that most of the government agencies in Saudi Arabia did not benefit from the Cloud as expected. From our point of view, this is due to several factors, such as newness of the Cloud technology, lack of specialists, and what is raised about the difficulty of managing and securing the Cloud. Needless to say that one of the objectives of the Cloud is to better manage resources, reduce expenses, and thrift government expenses on IT centers. Having said that, we propose a solution that may allow the government of Saudi Arabia utilize the Cloud as a technology to aid in its strive towards the 2030 vision.

B. Cloud and SaaS based Solution

As mentioned previously, the SaaS in the Cloud is built with multi-tenants in mind; therefore, it is adequate as an adopted solution. In addition, the Cloud does not require special hardware and/or software setup.

Fig.3 illustrates an example of a SaaS solution, where the applications' source code and any required databases are stored in the Cloud, and users belonging to subscribed tenants have access to the SaaS using a web interface.

Part of the proposed solution is to initiate a National Cloud Center (NCC), that works under the supervision of the Communication and Information Technology Commission, such center would host the majority of government employees whom are specialized in Computer Science, Information Technology, and other related fields. The NCC would be responsible of the Clouds' IaaS and PaaS layers.

As for the SaaS layer, the NCC develops, supports, and maintains SaaS solutions. However, each government agency that creates and maintains laws, rules, and regulations of any government-shared system will be the owner of a SaaS that is hosted in the National Cloud. For example, the MoF becomes the owner of the financial SaaS, which would be available to its tenants (government agencies) and their users.

Fig. 4 illustrates the government SaaS proposed solution. The source code of many SaaS applications is located centrally in the government Cloud, all government agencies are tenants, and their authorized users have access to these SaaS solutions. Fig. 5 illustrates the multi-tenant model proposed for the government SaaS. The application and database layers of all SaaS solutions are shared among different government agencies and their authorized users.

Within a Cloud there can be physical sites that are located in separate geographical locations. Such sites could be dedicated as backup sites, or they could be used as a main site for a SaaS to balance the load between the main Cloud site and other Cloud sites. In our proposed solution of creating a NCC, we suggest transforming IT centers located in public universities to Cloud sites.

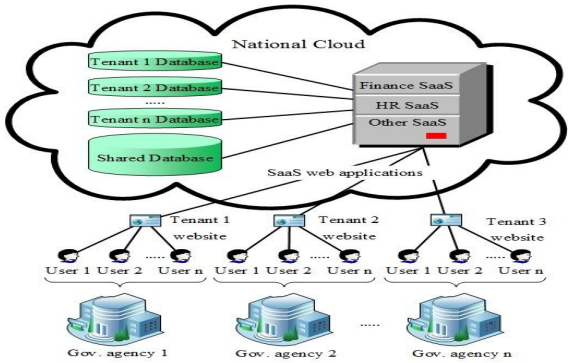


Fig. 4: Government SaaS proposed solution

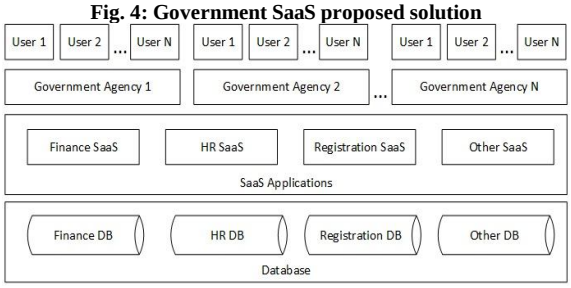


Fig. 5: Proposed government SaaS multi-tenant model

Our suggestion is based on the fact that each major city or town within Saudi Arabia houses a main campus or a branch of a public university, while there are government agencies that do not have offices in major cities. Therefore, our selection of universities is more adequate. In addition, the expertise and knowledge that university IT center employees have, and the direct support that they gain from Computing Faculty, may contribute effectively to better maintain the Cloud site.

There are two approaches to provide the SaaS solutions that are shared across a majority of government agencies and need to be hosted in the government Cloud. The first, is to analyze the current applications developed or purchased by the government agencies to select the best solution amongst them, and then work on converting that solution to a SaaS [13]. The second, is to develop the needed SaaS solution from scratch, such approach will consume both time and money. However, it is possible to utilize trusted open source SaaS solutions to decrease the cost.

There exist government agencies whom use applications that could not be used by or shared with other government agencies. Since we propose to downsize IT centers in all government agencies, such applications can be converted to a SaaS solution and then be hosted in the Cloud. This may enable such government agencies gain access to the latest versions of operating systems, database systems, and hardware from the government Cloud. In addition, the NCC can assure the security and quality of the SaaS solution.

IV. DISCUSSION

The main advantage that the government of Saudi Arabia could gain from implementing a national Cloud is rationalizing its expenses, and reducing the cost of operating and maintaining IT centers across all government agencies, while maintaining decent IT services that satisfy each agency, its employees, and its customers. The government agencies in Saudi Arabia are composed of 21 ministries, 11 directorates, 45 authorities, 13 corporations, 8 councils, 1 department, 5 dewans or courts, 5 faculties, 29 universities, 8 funds, 13 emirates or provinces, 16 municipalities, 4 presidencies, and 53 other agencies, all totaling in 232 agencies most of which are completely funded by the government. Assuming each agency spends $5 million USD annually for IT services, which is a shy assumption, this will total in $1.2 billion USD annually of the government's budget spent on IT services and infrastructure. Through implementing a Cloud solution, we expect the amount to be reduced by at least 50%.

It is worth mentioning that the operation expenses of Amazon Web Services (AWS) in the year 2015 was $6 billion USD, while its net sales was $7.9 billion USD in the same year. AWS is Amazon's Cloud solution that is located in 12 geographical locations around the world, and consists of 33 availability zones or sites,

and provides more than 70 Cloud services such as storage, database, analytics, etc. to its 1 million customers [25]. The government Cloud solution that this article proposes is somewhat equal in its size and cost to one of AWSs Cloud centers in the 12 locations. Another advantage of implementing a SaaS solution for government agencies is the ability to share resource, and the convenience of applying patches and updates to both the applications and databases. This is due to having the applications source code and databases located in a centralized location.

An additional advantage that government agencies can gain from a government Cloud is the simplicity of creating offices immediately without the need of creating a datacenter. Furthermore, our proposed solution could be a starting point of creating government service centers, where one physical location can host multiple government agencies to serve the public.

It is worthy to emphasize that our proposed solution does not call for eliminating or shutting down IT centers currently available in government agencies. There still exists the need to have a small IT center to oversee the local network, maintain the internet connection, and provide technical support to the agencies' employees. Furthermore, the NCC and its sites can utilize and employ the excess number of IT employees in government agencies.

In the year 2012, Saudi ARAMCO was a victim of a large-scale cyberattack [26]. Based on this incident, the Saudi Arabian government responded by creating the National Center for Information Security, and forced all government agencies to host their websites and save their data on machines located within Saudi Arabia. Our proposed solution is parallel to such enforcement, since the NCC and other Cloud sites must be located in Saudi Arabia.

Our proposed solution can be applied to both military and civil government agencies. However, due to the nature of military agencies, we suggest not to mix between both, and create a separate Cloud center for agencies with military nature that ensures a higher level of both digital and physical security.

Furthermore, the NCC could act as the host or backbone of the Internet of Things (IoT) technology when needed by any of the government agencies.

Finally, the NCC may be utilized to act as a profit center instead of a cost center. Saudi Arabia is part of the Gulf Cooperation Council (GCC), the NCC may benefit from its IaaS and PaaS layers and become a Cloud provider to the private sector within Saudi Arabia, and the government and private sectors of other GCC countries.

CONCLUSION

This article introduces the Cloud and SaaS as technologies to be adopted and implemented by the Saudi Arabian government. A proposed solution was provided to facilitate the adoption and implementation; such solution can be considered as a holistic solution for IT environments in Saudi Arabia's government. In addition, several advantages were highlighted such as rationalizing expenses, and reducing cost. Moreover, the proposed solution will play a major role in Saudi Arabia's strive towards its 2030 vision. Furthermore, due to the number of security related concerns that the Cloud needs to deal with and address, the article covered the relationship between the Cloud and Information Security. 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] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin I. Stoica, and M. Zaharia, "A view of cloud computing." Communications of the ACM 53, no. 4 (2010): 50-58.

[2] NIST (The National Institute of Standards and Technology). (2012). "The NIST definition of Cloud computing". Special publication 800-145, 2011.

[3] B. Waters, "Software as a service: A look at the customer benefits." Journal of Digital Asset Management 1, no. 1 (2005): 32-39.

[4] A. Ojala, "Software-as-a-Service Revenue models.", In IT Professional Magazine, vol. 15, IEEE Computer Society, (2013), 54-59.

[5] A. Ojala, "Software renting in the era of cloud computing.", In Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on, pp. 662-669. IEEE, 2012.

[6] N. B. Ruparelia, "Software development lifecycle models.", ACM SIGSOFT Software Engineering Notes 35, no. 3 (2010): 8-13.

[7] C. J. Guo, W. Sun, Y. Huang, Z Wang, and B. Gao, "A framework for native multi-tenancy application development and management.", In The 9th IEEE International Conference on E-Commerce Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services (CEC-EEE 2007), pp. 551-558. IEEE, 2007.

[8] L. Arrieta, and E. Orue, "From Software as a good to software as a service: Preparing the evolution of software products into the cloud.", In 2012 IEEE 6th International Workshop on the Maintenance and Evolution of Service-Oriented and Cloud-Based Systems (MESOCA), pp. 58-59. IEEE, 2012.

[9] A. Vashistha, and P. Ahmed, "SaaS Multi-Tenancy Isolation Testing-Challenges and Issues.", International Journal of Soft Computing and Engineering 2, no. 5 (2012): 49-50.

[10] Y. Zhu, and J. Zhang, "Research on key technology for SaaS.", In Computer Science & Education (ICCSE), 2012 7th International Conference on, pp. 207-210. IEEE, 2012.

[11] Vision 2030, http://www.vision2030.gov.sa/en.

[12] J. Guo, H. Huang, X. Shi, F. Liu, and B. Zhang. "Research on SaaS Service Performance Prediction Method in Dynamic Resource Environment.", In Service Oriented System Engineering (SOSE),2013 IEEE 7th International Symposium on, pp. 416-420. IEEE, 2013.

[13] S. Chate, "Convert your web application to a multi-tenant SaaS solution.", White paper, Developer-Works, IBM 14 (2010).

[14] A. Osman, S. M. Abdalrahman, and A. Elgelany. "Proposed Academic Cloud Computing for Saudi Universities and Higher Institutes." In e-Learning", Best Practices in Management, Design and Development of e-Courses:

Standards of Excellence and Creativity", Fourth International Conference on, pp. 113-119. IEEE, 2013.
[15] N. Alkhater, G. Wills, and R. Walters, "Factors influencing an organisation's intention to adopt cloud computing in Saudi Arabia.", In Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on, pp. 1040-1044. IEEE, 2014.
[16] A. Tashkandi, and I. M. Al-Jabri, "Cloud Computing Adoption by Higher Education Institutions in Saudi Arabia.", In 2015 International Conference on Cloud Computing, Riyadh, Saudi Arabia. 2015.
[17] A. M. AlBar, and M. R. Hoque, "Determinants of cloud ERP adoption in Saudi Arabia: an empirical study.", In Cloud Computing (ICCC), 2015 International Conference on, pp. 1-4. IEEE, 2015.
[18] A. Albugmi, R. Walters, and G. Wills, "A framework for cloud computing adoption by Saudi government overseas agencies.", In Future Communication Technologies (FGCT), 2016 Fifth International Conference on, pp. 1-5. IEEE, 2016.
[19] N. Alkhater, G. Wills, and R. Walters, "Factors Affecting an Organisation's Decision to Adopt Cloud Services in Saudi Arabia.", In Future Internet of Things and Cloud (FiCloud), 2015 3rd International Conference on, pp. 553-557. IEEE, 2015.
[20] Y. M. Hausawi, "Towards a Usable-Security Engineering Framework for Enhancing Software Development.", PhD diss., Florida Institute of Technology, 2015.
[21] S. Kumar, and R. H. Goudar, "Cloud Computing-Research Issues, Challenges, Architecture, Platforms and Applications: A Survey.", International Journal of Future Computer and Communication 1, no. 4 (2012): 356.
[22] M. D. Ryan, "Cloud computing security: The scientific challenge, and a survey of solutions.", Journal of Systems and Software 86, no. 9 (2013): 2263-2268.
[23] D. Zissis, and J. Dimitrios, "Addressing cloud computing security issues.", Future Generation computer systems 28, no. 3 (2012): 583-592.
[24] Z. Xiao, and Y. Xiao, "Security and privacy in cloud computing.", IEEE Communications Surveys & Tutorials 15, no. 2 (2013): 843-859.
[25] Amazon Corporation, “2015 Annual Report”, http://www.annualreports.com/Company/amazoncom-inc . 2015.
[26] C. Bronk, and E. Tikk-Ringas, "The cyber attack on Saudi Aramco.", Survival 55, no. 2 (2013): 81-96.

★★★