Investigating the Security Factors in Cloud Computing Adoption: Towards Developing an Integrated Framework

Madini O. Alassafi[1,2], Abdulrahman Alharthi[1], Ahmed Alenezi[1], Robert J. Walters[1], Gary B. Wills[1]
[1]*School of Electronics and Computer Science, University of Southampton, United Kingdom*
[2]*Faculty of Computing and Information Technology, Kind Abdul-Aziz University, Saudi Arabia*

Abstract

There are several benefits of using cloud computing in organizations and government agencies such as cost saving and flexibility in getting resources. Cloud computing plays a significant changing in organizations since it allows the users to access the service anytime and everywhere via networks, with paying for using only. In developing countries, such as Saudi Arabia, the cloud computing is still in its early time not widely adopted, compared to countries in the west. In order to promote the adoption of cloud computing, it is important to recognize an important and specific issue related to cloud computing is the potential and perceived security factors that posed by implementing the technology. Hence, the aim of this study is to investigate the security factors that influence organization and government agencies to adopt cloud computing in a Saudi Arabia context. This paper proposed a framework identifies the key factors for the successful adoption of cloud computing, focused on risks, social and security benefits when implementing security in the cloud services. The proposed framework is involving of three categories, social factors category, cloud security risks category and perceived cloud security benefits. The finding showed that all the proposed factors in the framework were statistically significant, except one factors under perceived cloud security benefits were not statically significant.

1. Introduction

Cloud computing is a term used to define distributed computing associated through a network to afford utility services to the end user [1]. The cloud allows users to access the service anytime and everywhere, and only pay for what they use. Cloud computing is a way of delivering computing resources based on different technologies such as cluster computing, distributed systems and web based services. It has become an attractive opportunity for enterprises as it meets their IT demand and their infrastructure.

On other hand, there are also disadvantages to using cloud computing that must be considered. The risks of adopting cloud computing have been categorized into different levels such as cost, security, governance, legal–compliance and performance concerns [2]. In the cloud, the customer may not have the kind of control over their data or the performance of the applications that they have with traditional Information and communication technologies (ICT) or the ability to audit or change the processes and policies under which users must work.

The security of the cloud, and associated privacy concerns, give many organizations pause as they think through their particular cloud computing concerns. Security concerns including physical security and simple access to facilities and equipment, as well as logical security, industry compliance requirements, auditability, and more. Although the adoption of cloud computing services can provide many advantages for the government agencies, few European countries have developed governmental cloud strategy plans [3]. Furthermore, the security risks have potential influence on the acceptance of cloud computing in most of the world. One of the main problems notable by big government organizations is the amount of spent on the IT infrastructure. For example, "*the Saudi Arabia government agencies spent around 4 million GBP in 2010 and it is predicted that the total spending for the year subsequent might have increased by 10.2% compared to 2010*" [4]. This indicates that in Saudi Arabia, there is negative potential attitude toward adopting and implementing advanced technologies. Some studies have been conducted in investigate the influence of the social and management aspects that facilitate or pose challenge on the cloud adoption in Saudi Arabia [4].

As result of the literature, there is inadequate efforts to know the factors that influence acceptance or rejection of cloud computing services due to security risks [3]. According to ICorps Technologies, by 2020 it is expected that the cloud computing market will exceed $270 billion. This forecast implies that the cloud computing industry is on the rise and the number of cloud users around the world is increasing. The increase in use of cloud computing technology is due to its low initial investment, lower maintenance cost and very high computations power [5].

As cloud computing providers have several security controls that overcome the ability of any

government or private organization, there is a low marker of using cloud in Saudi Arabia due to the security risks [6]. In order to understand the security risks associated with cloud computing adoption, this study will investigate the Saudi government agencies attitude toward security risk cloud in adoption investigating the perceived influence of cloud computing security benefits and how these security risks and benefits can affect the decision making process toward cloud adoption.

2. Literature Review

2.1. Overview of Cloud Computing Adoption

Every organization has some ideas, which are to be streamlined to achieve big profits. To implement these ideas, every organization can benefit from Information & Technology (IT) at every stage. Therefore, there is need to develop IT applications for specific use. Developing an IT application, require data centers with servers and storage devices, uninterrupted power supply, cooling systems, complicated software and experts to run those systems. The process of developing an IT application involves development, staging and production environment. When we develop many applications for an organization, the investment cost will be very high. Apart from the infrastructure, the organization need the software's to be updated all the time [7].

Governments around the world are dynamically into cloud computing as a wealth of growing efficiency and reducing cost [8]. Cloud adoption in general is a considered move by organizations to reducing cost, mitigating risk and realizing scalability of data base capabilities. The growth in computing lies in Cloud Computing technology, where the main objectives is reducing IT costs while increasing productivity, availability, reliability and flexibility and reducing the response times [9].

The report of National Institute of Standards and Technology (NIST) titled "The NIST Definition of Cloud Computing" provides the following definition for cloud computing: " Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction" [10].

Most of the recent studies in the cloud adoption demonstrations that the security is the most importance have to consider it if thinking to adopt cloud computing services in government agencies [11]. It usually categorized the top cloud computing adoption concern. Thus, to shed some lights on the security fundamental in the cloud adoption, firstly, cloud security definition is worth to be mentioned. According to Cloud Security Alliance (CSA) is '*Security is a set of control-based technologies and policies designed to follow to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use'.*

2.2. Cloud Adoption Benefits

The most significant benefits of cloud adoption are (Pay as you go pricing model, Scalability, Availability, Low maintenance and Easy implementation). Moreover, the cloud adoption has many benefits for organizations and the one of the most benefit is that, the cloud be able to decrease costs and saving money for the companies and small or large enterprises due to the cloud adoption is offering an outsourcing model that lets them to get resources and pay as they use of services. For example, the money that company spends on to run their system, instead of building up in-house IT infrastructure as a principle expenditure. Furthermore, the maintenance of IT resources and the upgrades are achieved by a third party, which endorse organizations to allocation responsibility and saving money [12].

2.3. Characteristics of Cloud Computing

The five essential characteristics of cloud computing are [10]:

- On-Demand Self-Service: A consumer can separately provide computing capabilities such as server, network, and storage as needed automatically, without requiring human interaction with a service provider.
- Resource Pooling: The providers' computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned, and reassigned according to consumer demand.
- Broad Network Access: Capabilities are available over the network and accessed through standard mechanisms that promote their use by mixed thin- or thick-client platforms.
- Rapid Elasticity: Capabilities can be changed to quickly scale up, and rapidly released to quickly scale down.
- Measured Service: Resource usage can be monitored, controlled and reported, thereby providing transparency for both the provider and consumer of the service.

2.4. Cloud Service Models

Cloud service models define how the cloud computing services are made available to the clients. Three different categories of service are provided by cloud computing [13].

- The Infrastructure as a Service (IaaS) model supplies infrastructure components to customers. Those components may be virtual machines, storage, networks,

firewalls, load balancers, operating system, database, and so on. The consumer is able to deploy these components in their infrastructure [8]. Examples of the IaaS model are Amazon Web Services and Dropbox.

- The Platform as a Service (PaaS) model delivers a pre-built application platform to the customer. PaaS automatically scales and supplies the demand for infrastructure components dependent on varying application requirements. PaaS solutions supply an API, which has a set of tasks for platform management and for development. Google App Engine is considered a popular PaaS provider, and Amazon Web Services also supplies some PaaS solutions [8].
- The Software as a service (SaaS) model is software provided by a third party developer, available on demand, generally through the internet and remotely configurable. Examples of the SaaS model are Salesforce CRM and Google Docs.

2.5. Cloud Deployment Models

Most recently, four-cloud deployment models have been accepted by the majority of cloud users.

- **Public Clouds,** provided for the public under a utility-based pay-per-use consumption model. Public clouds may be owned, managed, and operated by a business, academic, or government organization. Any user that is aware of the service location can access the infrastructure. Examples are Microsoft's Azure Service Platform and Amazon's AWS.
- **Private Clouds,** the cloud infrastructure is provided for exclusive use by a single organization comprising multiple consumers (e.g. business units). A Private Cloud is built to be operated and managed by that organization for its internal use only to support its business operations. Public, private, and government organizations worldwide are adopting this model to exploit the cloud benefits of flexibility, cost reduction, agility [14]. Examples are Amazon Virtual Private Cloud and eBay.
- **Hybrid Clouds,** merging two or more clouds may accomplish maximum benefits with cost reduction. Thus, an internal cloud can be employed within an enterprise to protect confidential data, while a community or public cloud can be used to attain cost reduction (Gong, et al., 2010). Few hybrid clouds are actually in use, though initiatives such as by IBM and Juniper do exist [15].
- **Community Clouds,** the goal of this deployment model is to provide free or low-cost services to organizations with common interests [16].

2.6. The Fundamental Elements of Cloud Computing for Governemnt Agencies

The author David et al. (2009) recommended that the importance proposition of cloud computing has unlimited appeal to governments due to the dynamic nature of IT demands and exciting economic situations various governments face. These eight elements are dynamic in qualifying the cloud computing government agencies and it is important that there be:

- Universal Connectivity, user's requirement has nearby global contact to the internet.
- Open Access, user's requirement has fair, non-preferential contact to the internet.
- Reliability, the cloud must purpose at stages equivalent to or better than existing separate systems.
- Interoperability and User Choice, users have ability to shift through the cloud platform.
- Security, users' data must be safe.
- Privacy, users' privileges to their data have to clearly defined and secured.
- Economic value, the cloud obligation brings tangible savings and benefits.
- Sustainability, the cloud requirement increase energy effectiveness, and decrease environmental influence.

3. The Proposed Framework

The proposed framework is intended to investigate the security factors that influence the adoption of cloud computing in Saudi Arabian context. This framework proposed the successful adoption of cloud computing focused on security factors when implementing security in the cloud system [18]. The proposed framework is consisting of three categories:

- **The first is Social Factors category**, which has three components: trust, privacy and security culture.
- **The second is Cloud Security Risks category**, which comprises of cloud technology security risks such as malicious insider, insecure interfaces and shared technology.
- **The third category is Perceived Cloud Security Benefits** that includes well-known cloud security features such as smart scalable security mechanism, centralized auditing, and standardized security policies interfaces.

The framework factors were identified by critically reviewing studies found in the literature

together, with factors from the industrial standards within the context of Saudi Arabia. The framework's categories and factors are illustrated in **Table 1**.

3.1. Perceived Cloud Security Risk Factors

The perceived cloud security risk factors describe cloud security risk factors, which are related to the nature of the cloud security and set of known security risks that highlighted by the security organization industries and research studies of the cloud technology and identifies the factors that affect an organization's decision to adopt this technology.

- **Insecure interfaces and application programing interfaces:** consumers manage and react with cloud services out of interfaces and APIs. Providers have to guarantee that security is inserted and considered at their service models. However, the users should understand and be aware of security risks in the use.
- **Share technology risk:** infrastructure as a service is constructed on shared infrastructure that is frequently not considered to accommodate a multi-tenant architecture such as CPU caches and GPUs.
- **Account or service hijacking**: according to CSA, the service traffic hijacking was recognized as the third highest cloud computing security risk. It is regularly with stolen identifications and it considered the strong two factors authentication techniques.
- **Malicious insiders**: a risk to an organization, because it is a current or previous operate provider, or other one who had authorized access to an organization's system or have access to potential sensitive data. However, it is important for the government organizations to understand what providers are doing to identify and protect beside the malicious insider risk.
- **Failure of Compliance with Regulations,** according to Gartner compliance with regulation is one of the important risk factors that the government should be aware of it before adopting the cloud even when it is held through a service provider. Compliance with regulation is an effective factor that can make a secure reluctant transferring to the cloud computing. This risk derives from the fact, which there are no governmental regulations or directions that can support the firm in the event of a data breach. The lack of IT standards is a big problematic may hinder the adoption decisions of cloud computing.
- **Data ownership**: this factor is critical security risk that the government organization requirements to be carefully think through and qualify since the organization logically and actually defends the data it owns.
- **Service data integration**: every organization must be sure for their own data is protected since it is moving between the end user and the cloud data center. However, the risk is bigger for organizations which using a cloud computing model because unsecured data is more liable to interception when it transmission.
- **Data leakage:** according to CPNI, it is weakness of security access rights to more than domains and weakness of physical transport system for cloud data and backups.

3.2. Social Factors

Social factors are related to the Saudi organization security behavior and attitude toward the usage of cloud computing in term of security in cloud adoption perspective.

- **Trust**: mentions to support on another entity, the belief that this entity will function as expected Trust in the cloud computing with difficulty consists on trusting the service itself and the provider to supply a trusted level of authentication, confidentiality, and integrity related to the service and stored the data.
- **Security culture:** security culture can support most of organizational effectiveness in a way that information security can be normal part in daily activities of all employee. Security cultures help the execution of information security policies and work out to the organization. Security culture covers social, cultural, and ethical scale to develop the security pertinent behavior of the organizational organs and keep it to be a subculture of organizational culture.
- **Privacy**: confidentiality of data that give access to only licensed users. Privacy considered the major concern to any organization that willing cloud computing because really cannot have completely control to the information that stored on cloud-based servers.

3.3. Perceived Security Benefits

This category comprises of the perceived cloud computing security features that affect cloud adoption decision making in the organizations which highlighted by organization industries and research studies. According to European Network and Information Security Agency (ENISA), the cloud security features are further elaborated below:

Table 1. The factors identified for cloud adoption

Category	Factors
Security risks	Insecure interfaces
	Share technology
	Account or service hijacking
	Malicious insiders
	Failure of Compliance with Regulations
	Data ownership
	Service and data integration
Social Factors	Trust
	Security Culture
	Privacy
Perceived Security Benefits	Smart Scalable security benefits
	Cutting edge Cloud security market
	Advanced security mechanism
	Standardized security interfaces
	Cloud security auditing
	SLAs audit enforcement
	Resource concentration

- **Smart scalable security benefits**: this is defined as the ability to extend the security features to multiple locations, edges networks, timeless of response and threat management. The list of cloud resources that can be rapidly scaled on demand already includes, e.g., storage, CPU time, memory, web service requests and virtual machine instances, and the level of granular control over resource consumption is increasing as technologies mature.
- **Cutting edge cloud security market**: Cloud providers such as Amazon, Google are considered the two largest hardware and software provider in the world. Therefore, the cloud costumer can benefit up to date high standard security techniques in order to secure their assets.
- **Advanced security mechanism**: cloud provider can provide centralized security as service patches and updates for the customer, which is more efficient than traditional organization security capability.
- **Standardized security interfaces**: security management free interfaces can ease the consumer ability to change from provider to other providers in a short period and reduced cost.
- **Cloud security auditing**: auditing in the cloud can be better organized, via pay as you go for auditing and gathering audit log requirements.
- **Service level agreement (SLAs) audit enforcement**: cloud customer can benefit set of audit manage requirements and the provider should comply with those audit demands stated in the service level agreements (SLAs).
- **Resource concentration**: pool of security resources can be harnessed by costumers including access control, comprehensive security policy, patch and data management and maintenance processes.

3. Methodology

An expert review is a simple technique that supports investigators to collect data from experts who have understanding of the subject regards to study. This method can be used in quantitative which regularly using closed questions, qualitative regularly using open-ended question or mixed methods (quantitative and qualitative) at different stages of the research. In this preliminary study, semi-structured interviews were used for collecting data from twelve IT and security experts who is working in different departments in government agencies by Saudi Arabia such as ministries, telecommunication agencies, state universities, research institutes, and education. The study population consists of a person who considered an expert if they had at least five years' experience of working on IT projects and two years' experience on security or cloud within a Saudi government agency.

The aim of the interviewing IT and security experts was to review the categories and its factors that were previously identified in the framework. A second goal was to determine other factors not mentioned in former studies. Five of the participants in this study were working in agencies that had already adopted cloud computing, while seven (59%) of them were not adopt cloud computing yet.]

4. Results And Discussions

As the information from closed ended questions is considered as quantitative data, the expert's questions were provided to twelve experts and they are asked to respond on the importance security factors to the adoption of cloud computing in Saudi Government Agencies. The responses to these questions were based on a five point Likert scale, with 5 denoting 'Very Important', 4 denoting 'Important', 3 denoting 'May Be Important', 2 denoting 'Not Important', and 1 denoting 'Not Relevant' as presented in Figure 1. SPSS was used to analyses the data. The one sample T-test was used to analyses as a statistical test and the results of the quantitative data.

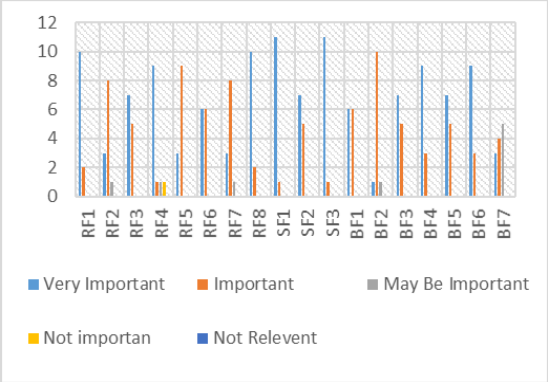

Figure 1. Experts of each factor

The descriptive and frequency analyses were used to understand the responses regarding the eighteenth factors of the framework. These factors under three categories:

- **Security Risk Factors**

Table 2 presents the frequency of security risk factors. There are eight factors of security risk that affect the adoption of cloud computing in Saudi government agencies. Of the 12 respondents, 83% stated that 'Insecure Interface' is a 'very important' type of security risk which affects the adoption of cloud computing, while the other 17% of respondents feel that it is 'important'. The second factor of Security risk is Share Technology. Approximately 67% of the respondents feel that this is 'important', while 25% of respondents see it as 'very important', and 8% of participants state that it may not be among the important security risk factors in terms of affecting the adoption of cloud computing. With regard to the Account and Service Hijacking factor of security risk, 58% of the participants see it as 'very important', and 42% of participants state that it is an 'important' factor of security risk. In terms of the fourth factor, namely Malicious Insiders, nearly 75% of the 12 experts conclude that it is 'very important', while 25% of participants see it as 'important', 'may be important' and 'not important' respectively in terms of its effect on the adoption of cloud computing in Saudi government agencies. With regard to the 'Failure of compliance with regulations' factor, most (75%) of the participants feel that it is 'important' and the others (25%) rate it as 'very important'. The sixth factor, "Data Ownership", is deemed by 50% of the experts to be 'very important', while the other 50% of the 12 participants see it as 'important'. 67% of the respondents state that the 'Data and Service Integration' factor is an 'important' element of security risk, while 25% of the participants see it as 'very important' and 8% as 'may be important'. Most (83%) of the participants conclude that the 'Data leakage' factor is a 'very important' element of security risk when it comes to the adoption of cloud computing in Saudi government agencies.

Table 2. Security Risk Factors Frequency

Factors	Frequency (Percentage)					
	Very Important	Important	May Be Important	Not Important	Not Relevant	Total
Insecure interfaces	83%	17%	0%	0%	0%	12
Share technology	25%	67%	8%	0%	0%	12
Account or service hijacking	58%	42%	0%	0%	0%	12
Malicious insiders	75%	8%	8%	8%	0%	12
Failure of Compliance with regulations	25%	75%	0%	0%	0%	12
Data ownership	50%	50%	0%	0%	0%	12
Service and data integration	25%	67%	8%	0%	0%	12
Data leakage	83%	17%	0%	0%	0%	12

- **Social Factors**

The expert questionnaire addressed the importance of social factors in relation to the adoption of the cloud service in Saudi government agencies. The responses to these questions were based on a five-point Likert-type scale, with 5 denoting 'Very Important', 4 denoting 'Important', 3 denoting 'May Be Important', 2 denoting 'Not Important', and 1 denoting 'Not Relevant**. Table 3,** presents the frequency of social factors in terms of their influence on the adoption of the cloud service in Saudi government agencies. A total of three social factors were included in the questionnaire. Of the 12 participants, 83% find that trust is a 'very important' social factor when it comes to the adoption of the cloud service in Saudi government agencies, while 17% of the respondents rate it as 'important'. In terms of the 'Security culture' factor, 58% of participants state that it is 'very important', and 42% of the participants find that it is an 'important' social factor which influences the adoption of the cloud service in Saudi government agencies. The last social factor is 'Privacy'. Most (92%) of the participants regard this as a 'very important' social factor when it comes to the adoption of the cloud service in Saudi government agencies.

Table 3. Social Factors frequency

Factors	Frequency (Percentage)					
	Very Important	Important	May Be Important	Not Important	Not Relevant	Total
Trust	92%	8%	0%	0%	0%	12
Security Culture	58%	42%	0%	0%	0%	12
Privacy	92%	8%	0%	0%	0%	12

- **Perceived Benefit Factors**

The expert questionnaire was also implemented in order to gauge, according to the 12 experts, the importance of security benefits in relation to the

decision to adopt cloud services in Saudi government agencies. The responses to these questions were based on a five-point Likert-type scale, with 5 denoting 'Very Important', 4 denoting 'Important', 3 denoting 'May Be Important', 2 denoting 'Not Important', and 1 denoting 'Not Relevant. Table 4 represents the frequency of security benefits for the decision to adopt cloud services in Saudi government agencies. Of the 12 participants, 50% see the 'Smart Scalable Security' factor as a 'very important' and beneficial factor, while 50% view it as an 'important' security benefit when it comes to the decision to adopt cloud services in Saudi government agencies.

In relation to the 'Cutting Edge Cloud' security market, most (84%) of the participants feel that this is 'important' and the other 16% of participants see it as 'very important' and 'may be important' in terms of security benefits.

The third perceived benefit factor is 'Advanced security mechanism'. Of the 12 respondents, 58% regard it as 'very important', and 42% feel it is 'important' when it comes to decisions to adopt cloud services in Saudi government agencies. With regard to the 'Standardised security interfaces' factor, 75% of participants rate it as 'very important', and 25% of participants feel that it is 'important' in terms of affecting the decision to adopt cloud services in Saudi government agencies.

In terms of the fifth benefit factor, which is "Cloud security auditing", 58% of the 12 respondents see it as 'very important', while 42% of participants view it as 'important'.

In reference to the 'Service level agreement audit enforcement' factor, most (75%) of the participants rate it as 'very important' and the others (25%) feel it is 'important' in relation to decisions to adopt cloud services in Saudi government agencies. Among the 12 participants, 25% people regard 'Resource concentration' as 'very important', while 33% of respondents feel it is 'important' and 42% of respondents agree that it 'may be important' for decisions to adopt cloud services in Saudi government agencies.

The results of the closed ended questions to interviews demonstrated in the **Error! Reference source not found.**. The interviews were asked for their approach for the proposed framework using quantitative method. The objective of the questions was to evaluate the importance of the proposed security factors to adopt cloud services in Saudi government agencies, from the experts' interviews point of view. The experts' responses were collected and entered by SPSS software to analyses the data statistically.

The One Sample T-test was used to analyses as a statistical test and the results of the quantitative data. This test supports in comparing the mean of a population (μ) with a hypothesized value (μ0).

Table 4. Perceived Benefit Factors Frequency

Factors	Frequency (Percentage)					
	Very Important	Important	May Be Important	Not Important	Not Relevant	Total
Smart Scalable security benefits	50%	50%	0%	0%	0%	12
Cutting edge security market	8%	84%	8%	0%	0%	12
Advanced security mechanism	58%	42%	0%	0%	0%	12
Standardized security interfaces	75%	25%	0%	0%	0%	12
Cloud security auditing	58%	42%	0%	0%	0%	12
SLA audit enforcement	75%	25%	0%	0%	0%	12
Resource concentration	25%	33%	42%	0%	0%	12

In this study Bonferroni correction was applied for controlling the false positive finding by dividing alpha (α= 0.05) by the number of factors involved in the questionnaire.

$$P\text{-}value = (\alpha/n)$$
$$(\alpha/n) = 0.05/18$$
$$= 0.0027$$

The hypothesized mean (μ0) = 3, which indicates Maybe Important on the five point Likert-type scales. The test value was defined as 3 on the five-point Likert scale for security factor, which ranged from 5 (Very Important) to 1 (Not Relevant).

The statistical significant level alpha is α = 0.05. The null hypothesis (H0) is rejected if the probability (p-value) of question is > 0.0027. The factor is statistically significant if the p-value < 0.0027, otherwise, the factor is not statistically significant.

Regarding on the experts' opinion, the results in the above table showed that mean of all proposed factors are garter than the defined value, which is 3. Moreover, the inferential analysis of responses to these questions shows that the factors are statistically significantly important except one factor of security benefits category which is the 'Resource concentration factor' where the p-value greater than 0.0027.

- Resource concentration factor: (0.082 > 0.0027).

However, the result shows that the Resource concentration factor has no significant impact on organization decision, the findings from previous studies said that this factor has an importance to influence the adoption of cloud computing [19]. Therefore, the resource concentration factor will be kept in the proposed framework. The defense of not take away this factors is that, some studies have found that the 'Resource concentration factor' is one of the significance factors that impact the use of online services and the adoption of new technology [19], [20].

Moreover, the resource concentration is considered as pool of security resources that can be harnessed by costumers including access control, comprehensive security policy, patch and data management and maintenance processes.

Table 5. One sample T- test of expert's interviews

Category	*Factors*	*Ref*	*Mean*	*P-Value*
Security Risk Factors	Insecure interfaces	RF1	4.83	<.001 •1
	Share technology	RF2	4.17	<.001 •
	Account hijacking	RF3	4.58	<.001 •
	Malicious insiders	RF4	4.50	<.001 •
	Failure of Compliance with regulations	RF5	4.25	<.001 •
	Data ownership	RF6	4.50	<.001 •
	Service and data integration	RF7	4.17	<.001 •
	Data leakage	RF8	4.83	<.001 •
Social Factors	Trust	SF1	4.92	<.001 •
	Security Culture	SF2	4.58	<.001 •
	Privacy	SF3	4.92	<.001 •
Perceived Security Benefits	Smart Scalable benefits	BF1	4.50	<.001 •
	Cutting edge security market	BF2	4.00	<.001 •
	Advanced security mechanism	BF3	4.58	<.001 •
	Standardized security interfaces	BF4	4.75	<.001 •
	Cloud security auditing	BF5	4.58	<.001 •
	SLA audit enforcement	BF6	4.75	<.001 •
	Resource concentration	BF7	3.25	<0.082 ••

• P-value $\leqslant$ 0.05.
•• P-value > 0.05.

Table 6. Confirmation of the framework

Category	Factors	Confirmation
Security risks	Insecure interfaces	Confirmed
	Share technology	Confirmed
	Account or service hijacking	Confirmed
	Malicious insiders	Confirmed
	Failure of Compliance with Regulations	Confirmed
	Data ownership	Confirmed
	Service and data integration	Confirmed
Social Factors	Trust	Confirmed
	Security Culture	Confirmed
	Privacy	Confirmed
Perceived Security Benefits	Smart Scalable security benefits	Confirmed
	Cutting edge Cloud security market	Confirmed
	Advanced security mechanism	Confirmed
	Standardized security interfaces	Confirmed
	Cloud security auditing	Confirmed
	SLAs audit enforcement	Confirmed
	Resource concentration	Confirmed

Table 6 shows the confirmation of each factor in the framework after the results according to the expert's interviews.

The results of the interviews show that among 12 experts agreed these factors are important when adopting the cloud computing in Saudi Government Agencies and it has high power on stakeholders' behavior to adopting cloud services.

5. Conclusion

Cloud computing is the developing paradigm of distributing IT services to consumers as a utility service over the Internet. The great benefit of cloud computing is that the cloud offers resources to multiple users at any time in a dynamic way and according to users' needs. In addition, users only pay for the services that they need. However, regardless of the fact that the cloud offers some benefits for enterprises from flexibility to decreasing cost, moving an existing system to the cloud is not an easy task for the reason that there are a number of variant challenges in different domains such as legislations, technology, and management challenges. One of the most noticed challenges that face any government agency is security.

To investigate the latter issue of cloud security, the study was focused on the security factors that affect government agencies decision to adopt the cloud. This study was aimed to construct a framework to investigate the cloud security risks and the cloud security features that influence Cloud Computing adoption in Saudi Arabia.

Expert's interviews method was admitted for this study in order to confirm the security factors in the framework that identified by the literature review.

In this preliminary study, semi-structured interviews were used for collecting data from twelve IT and security experts who was working in different departments in government agencies by Saudi Arabia such as ministries, telecommunication agencies, state universities, research institutes, and education. The study population consists of a person who considered an expert if they had at least five years' experience of working on IT projects and two years' experience on security or cloud within a Saudi government agency.

The finding showed that all the proposed factors in the framework were statistically significant, except one factors under perceived cloud security benefits category were not statically significant. The future work of this study will be aimed to confirm the framework and identified other factors not mentioned in these factors from the preliminary study by applying the triangulation methods with IT and security experts and decision makers in Saudi government agencies.

6. References

[1] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Futur. Gener. Comput. Syst. J., vol. 25, no. JUNE, p. 17, 2009.

[2] P. Bannerman, "Cloud computing adoption risks: state of play," Asia Pacific Softw. Eng. Conf. Cloud Work., vol. 3, no. September, pp. 0–2, 2010.

[3] G. Elena and C. W. Johnson, "Factors influancing Risk Acceptance of Cloud Computing Sertvices in the UK," Int. J. Cloud Comput. Serv. Archit., vol. 5, no. 2, 2015.

[4] M. Alsanea and J. Barth, "Factors Affecting the Adoption of Cloud Computing in the Government Sector : A Case Study of Saudi Arabia," Int. J. Cloud Comput. Serv., vol. 1, pp. 1–16, 2014.

[5] K. Kumar, "Cloud Computing for Mobile Users: Can Offloading Computation Save Energy?," IEEE Comput. Soc., vol. 43, no. 4, pp. 51–56, 2010.

[6] F. Alharbi, A. Atkins, and C. Stanier, "Strategic Framework for Cloud Computing Decision-Making in Healthcare Sector in Saudi Arabia," Seventh Int. Conf. eHealth, Telemedicine, Soc. Med., vol. 1, no. c, pp. 138–144, 2015.

[7] M. Miller, "Cloud Computing : Web-Based Applications That Change the Way You Work and Collaborate Online," Que Publ., pp. 1–29, 2009.

[8] L. Badger, D. Bernstein, R. Bohn, and Vaulx, "US Government Cloud Computing Technology Roadmap," Nist Spec. Publ., vol. II, p. 85, 2011.

[9] A. Alharthi, M. O. Alassafi, R. J. Walters, and G. B. Wills, "An exploratory study for investigating the critical success factors for cloud migration in the Saudi Arabian higher education context," Telemat. Informatics, vol. 34, no. 2, pp. 664–678, 2016.

[10] P. Mell and T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology," Comput. Secur. Div. Inf. Technol. Lab. Natl. Inst. Stand. Technol. Gaithersburg, vol. 145, p. 7, 2011.

[11] Ahmed Albugmi; Madini O Alassafi; Robert Walters; Gary Wills, "Data Security in Cloud Computing," Fifth Int. Conferance FGCT IEEE, vol. 2, no. 1, pp. 1–169, 2016.

[12] A. Alharthi, F. Yahya, R. J. Walters, and G. B. Wills, "An Overview of Cloud Services Adoption Challenges in Higher Education Institutions," Proceeding 2nd Int. Conf. Work. Emerg. Softw. as a Serv., vol. 1, pp. 102–109, 2015.

[13] A. F. Michael Armbrust, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, 2010.

[14] M. G. Avram, "Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective," 7th Int. Conf. Interdiscip. Eng. (INTER-ENG 2013) Advantages, vol. 12, pp. 529–534, 2014.

[15] L. Schubert, K. Jeffery, and B. Neidecker-Lutz, "The Future of Cloud Computing. Opportunities for European Cloud Computing Beyond 2010," Eur. Comm. Cloud Expert Gr., p. 66, 2010.

[16] A. Chandra and J. Weissman, "Nebulas : Using Distributed Voluntary Resources to Build Clouds," Proc. 2009 Conf. Hot Top. Cloud Comput., vol. 1, p. 2, 2009.

[17] D. C. Wyld and Robert Maurin, "Moving to the Cloud : An Introduction to Cloud Computing in Government E-Government Series Moving to the Cloud : An Introduction to Cloud Computing in Government," p. 82, 2009.

[18] Madini O. Alassafi, A. Alharthi, R. J. Walters, and G. B. Wills, "Security Risk factors that influence Cloud Computing Adoption in Saudi Arabia Government Agencies," i-Society Conferance IEEE Adv. Technol. Humanit., vol. 1, pp. 1–4, 2016.

[19]D. Catteddu and G. Hogben, "Cloud Computing Benefits, Benefits, risks and recommendations for information security," ENISA Comput. Rep., vol. 72, no. 1, pp. 2009–2013, 2009.

[20] K. Tei and L. Gurgen, "ClouT : Cloud of things for empowering the citizen clout in smart cities," 2014 IEEE World Forum Internet Things, WF-IoT 2014, pp. 369–370, 2014.

