A Framework for Critical Security Factors that Influence the Decision of Cloud Adoption by Saudi Government Agencies

Madini O. Alassafi, Abdulrahman Alharthi, Robert J Walters and Gary B Wills
School of Electronics and Computer Science, University of Southampton, Southampton, UK
Faculty of Computing and Information Technology, Kind Abdul-Aziz University, Jeddah, Saudi Arabia
Southampton, United Kingdom {moa2g15, aaa2g14, rjw5, gbw}@soton.ac.uk

Abstract

Cloud computing technologies can play an essential role in public organisations and companies while it reduces the cost of using information technology services. It allows users to access the service anytime and anywhere, with paying for what they use. In developing countries, such as Saudi Arabia, the cloud computing is still not extensively adopted, compared to countries in the west. In order to encourage the adoption of cloud services, it is considerable to understand an important and particular complications regarding to cloud computing is the potential and perceived security risks and benefits posed by implementing such technology.

This paper investigates the critical security factors that influence the decision to adopt cloud computing by Saudi government agencies. A framework was proposed for three categories, Social Factors category, Cloud Security Risks Category and Perceived Cloud Security Benefits that includes well-known cloud security features. 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. An experiment study was conducted in five government agencies in Saudi Arabia by interview and questionnaire with experts in order to improve and confirm the framework. All the factors in the proposed framework were found to be statistically significant. An additional factor identified was Failure of client side encryption. Moreover, they suggested including this factor as a potential risk under Security Risk Factors Category. The initial framework was updated based on the expert reviews and questionnaires. The results were analysed via one-sample t-test with the data integrity analysed via Cronbach's alpha. The outcome indicated the majority of cloud security adoption framework categories were statistically significant. Potential future study directions and contributions are discussed.

Keywords: Saudi Government Agencies; Cloud Adoption; Cloud Security Risks; Cloud Security Benefits.

1 Introduction

Cloud computing is a term used to define distributed computing connected over a network to afford utility services to the end user (Buyya et al., 2009). Cloud computing is a way to deliver computing resources based on different technologies such as cluster computing, distributed systems and web based services (Mauch et al. 2013). In an economic recession, cloud computing technology services can play a considerable role in public organisations and private sector companies since they reduce the cost of using information technology (IT) services in addition to offering certain other features (Alsanea & Barth 2014). The main objective of cloud computing technology is to lower companies' IT costs and offers organisation the chance to take control over their data centres.

Several countries have begun to recognise the benefits of using cloud computing in government organisations (Bannerman 2010). While the adoption of cloud computing services can provide many advantages for government services, few European countries have developed governmental cloud strategy plans (Elena & Johnson 2015a). The security concerns related to the cloud hinder many organisations' attempts to adopt cloud services (Sabahi 2011). Such security concerns include physical security and simple access to facilities and equipment (Pearson 2013). Furthermore, the security element has the potential to influence the acceptance of cloud computing across most of the world. In KSA, the government has acknowledged the importance of cloud-based services and has started to lay out plans to establish government cloud services and other forms of cutting-edge technology such as smart cities and IoTs sensing. KSA government organisations spent approximately 4 billion GBP in 2010 and it is predicted that the total spending for the subsequent years might have increased by as much as 10.2% (Alsanea & Barth 2014). This indicates that, in KSA, there is a positive attitude toward adopting and implementing advanced technology. A number of studies have been conducted to investigate the influence of the social and management aspects that facilitate or pose challenges to cloud adoption in KSA (Alsanea & Barth 2014; Alharthi et al. 2017). Moreover, little is known about the security factors that influence cloud computing adoption services across the world (Elena & Johnson 2015a). According to ICorps Technologies, by 2020 it is expected that the value of the cloud computing market will exceed $270 billion. This forecast implies that the cloud computing industry is on the up, and that the number of cloud users around the world is increasing. The increase in the use of cloud computing technology is directly related to the various benefits it offers, such as low initial investment, lower maintenance cost, and very high computation power (Kumar 2010). It is clear that cloud adoption in KSA is influenced by security risks and benefits awareness; in light of this, and in order to understand the influence of security on cloud computing adoption, the present research will investigate the security risks, security social factors and security benefits associated with the adoption of cloud computing in Saudi government organisations.

1.1 Motivation

According to World Bank, World Development Indicators, 2013, the Kingdom of Saudi Arabia (KSA) is the 19th largest economy in the world and is driven by the exportation of crude oil. The KSA is pushing itself in order to achieve strong economic expansion and move away from its oil-based economy (Alshahrani & Alsadiq 2014). When it comes to expanding the economic opportunities in the KSA, information and communication technology (ICT) plays a very significant role in promoting the saudi governemnt's 2030 vision inititive, the aim of which is to diversify the country's economy income and technology (Alsanea & Barth 2014). With organisations around the world looking towards third party IT platforms such as mobile, big data, cloud computing, social media, etc. KSA has realised that mobility and cloud computing technology represents the future investment areas of ICT technology (Kumar 2010).

Cloud computing propagation becomes a worthy research topic as it qualifies corporations to scale up their transactions along value series activities. This activities can include and not limited to sales, manufacturing, customer service, distribution, information sharing and association with exchange partners (Vaquero et al. 2008). As organisations around the world are looking towards third party IT platforms like mobile, big data, cloud computing, social media, etc. Saudi Arabia has realized that mobility and cloud computing technologies are the future investment areas of ICT technologies (Alharthi, Madini O Alassafi, et al. 2016). With the increased number of cyber-ttacks on the KSA in the recent years, it is very important to understand the security cultures and prcatices existing in the governemt agencies before adopting cloud services. Hence, the the research aims was to:

- Help KSA government organisations to identify the security factors which could potentially influence their adoption of cloud computing.
- Fill the gaps in existing research related to the influence of security on the adoption of cloud computing in KSA government organisations. The KSA has a distinctive approach that emerges from its cultural context as a developing country in the Gulf region.

This study will meet its goals by answering the following reseach questions ans sub questions:
RQ. What is an appropriate framework for security factors on the adoption of cloud computing in the Saudi government context?

And the subquestions as the following.
Q1. What are the security risk factors in cloud computing adoption?

Q2. What are the security benefits factors in cloud computing adoption?

Q3: What are the security social factors in cloud computing adoption?

This paper is structured as follows: first, we review the state of art for adoption of cloud services in government agencies. Second, we review the literature review which contains an overview of cloud computing paradigm principles and critical review of the related work in the field of cloud adoption, cloud

adoption cases in different countries in general and in the KSA in particular. Moreover, shows overview of security in cloud computing, security principles, cloud security benefits and cloud security risk factors highlighted in the literature by different organisation industry standards. Third, we present our methodology which used in this study. Next, we present our empirical analysis of the results, and we conclude the study with a discussion of the results and future research directions.

2 Literature Review

By adopting cloud computing services, government agencies can deploy their application systems over a group of independently managed resources. However, the majority of such agencies rely on their own custom needs which must be considered if they decide to use cloud-based systems (Alharthi, Madini O. Alassafi, et al. 2016). As any contemporary innovation, cloud computing usage and user's acceptance need to be understood due to the fact that users are key players in promoting new innovations. As trending computing model, many industry white papers and academics researchers spent an efforts to define and illustrate the notion of cloud computing.

The best definition of cloud computing is perhaps that of The National Institute of Standards and Technology (NIST): '*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'.* NIST has defined the components of cloud computing with five essential features, three cloud service models, and four cloud deployment models. A conceptual view of cloud computing presented in Figure 1.

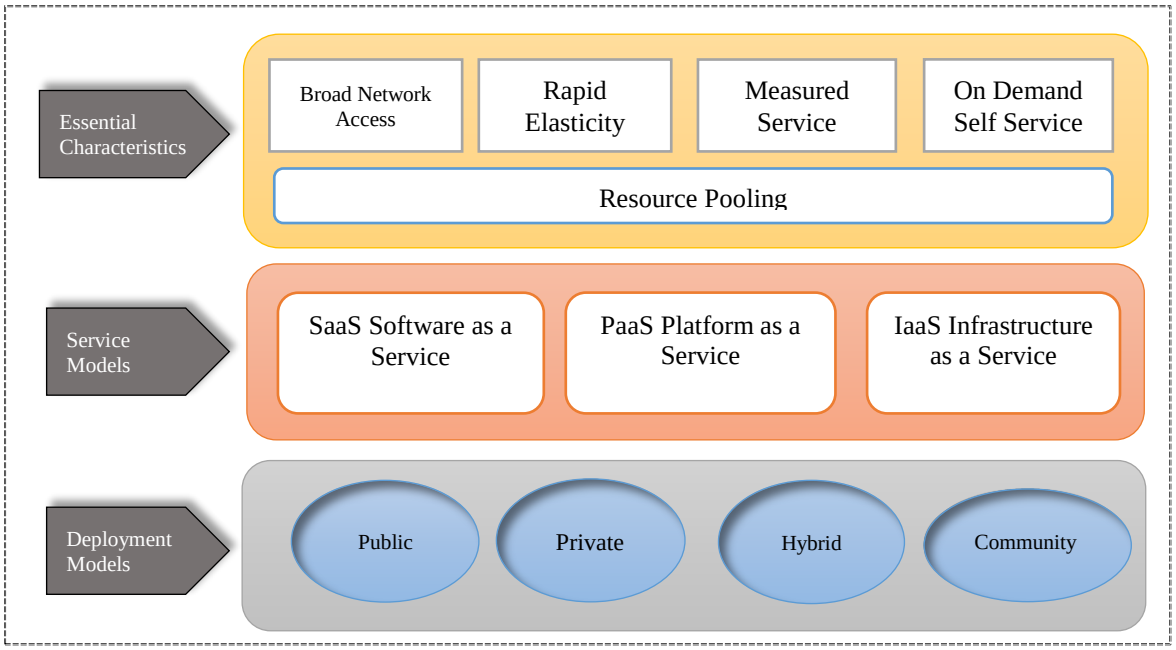

Figure 1: Conceptual view of cloud computing

This paper focuses on the perspective of security professionals. An organisation thinking of adopting cloud computing needs professionals with security skills because security management is most important in the

cloud (KPMG 2011). The full utilization of cloud based services depends on the security of personal information about the organisation and its employees, which is the biggest concern (Ahmed Albugmi, et al. 2016).

Security is defined by three principles: confidentiality, availability, and integrity (Cherdantseva & Hilton, 2013). These principles cover the wide span from a user's internet history of encrypted data to their access to it. Violation of any one of the principles can cause a serious harm to those affected by this breach (Cherdantseva & Hilton, 2013).

2.1 Review of Related Work

The majority of Saudi government agencies rely on their own custom needs which must be considered if they decide to use cloud-based systems (Alharthi, Madini O. Alassafi, et al. 2016). As with any innovation, cloud computing usage and user acceptance need to be understood because users are key players in promoting innovation. When it comes to adopting such technology these organisations hesitate to embrace it due to the security risks. Security has been identified as the major challenge organisations need to consider before adopting the cloud. Security is typically ranked as the top concern in cloud computing adoption (Bannerman 2010). Zhou et al. (2010) analysed the barriers users may encounter when they decided to adopt cloud computing systems, but lacked evidence of the security risks and benefits tailored to the user side. Paquette et al. (2010)examined the current level of adoption and use by government and the risks – tangible and intangible – associated with its use, without addressing security risks and benefits.

Che et al. (2011) highlighted the security risks of cloud computing, but only investigated security strategies. Sun et al. (2011) emphasized the major security, privacy and trust issues in current cloud computing environments and helped users identify the tangible and intangible threats related to them, but it did not provide empirical investigation.

Both Alkhater et al. (2014) and Alsanea & Barth (2014) investigated the managerial, technological and environmental factors influencing cloud adoption in Saudi Arabia. However, they did not address the security risks or provide deep analysis of them. Subashini & Kavitha (2011) suggested a few security elements and the vital role as an integral part of the SaaS development and deployment process, but did not address the security risks and benefits.

2.2 Risks and Benefits of Cloud Adoption in Government Agencies

Several governments are starting to shift to cloud computing as a resource of rising efficiency (Badger et al., 2011). Despite all the benefits of cloud adoption, some risks have hindered its adoption by governments, as listed below.

- Time Risk: time to recognise where it can be used, tome to comply with data protection, time to explore and time to implement cloud computing, and time to understand and comply with service level agreements (Elena & Johnson 2015a).

- Performance Risk: consumers want confidence and transparency in the cloud performance, since the service it offers is dynamic, which meets their performance needs and holds operating costs low (NIST, 2012).
- Social or Reputational Risk: Social risk is very high because of the possibility of damage to the organisation and loss of reputation in leaking data and potential unavailability of the cloud services (Chang et al. 2015).
- Financial Risk: including costs of reputational damage. Financial risk is important because cloud services need to demonstrate integrity and performance before money is spent (Gentzoglanis 2011).
- Security Risks: most studies show that security is most important when adopting cloud computing services by government agencies (Bannerman 2010; Elena & Johnson 2015b; Alassafi et al. 2017).

According to Cloud Security Alliance (2013), the definition of security is 'The set of control-based technologies and policies designed to follow regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use'.

Therefore, several challenges are associated with the adoption of cloud computing that need to be addressed (Sen 2013). Prior to the adoption of cloud services, every organisation should be ready and aware of the multiple dimensionality of security risks and benefits (Fumei Weng 2014). The top security risks associated with cloud computing are: Insecure interfaces, Shared technology, Account or service hijacking, Malicious insiders, Failure of compliance with regulations, Data ownership, Service and data integration, and Data leakage (Babu et al. 2010; Catteddu & Hogben 2009; Mell & Grance 2011).

However, the top security benefits of cloud computing are (ENISA, 2009):

- Security and the benefits of scale
- Security as a market differentiator
- More timely and effective and efficient updates and defaults
- Rapid, smart scaling of resources
- Standardised interfaces for managed security services
- Audit and evidence-gathering
- Audit and SLAs force better risk management
- Benefits of resource concentration

2.3 The Status of Cloud Adoption

In 2011, the UK government announced cloud Strategy Plans that endorse the adoption of the cloud paradigm to enhance their IT services in term of cost efficiency, interoperability, and flexibility (Elena & Johnson 2015a). These strategies will employ private and community deployment models. The USA has embraced cloud services in their government agencies, to consolidate and promote public electronic services.

The Chinese government has yet to engage in national cloud computing. However, it has recognised the benefits of cloud computing and started the process of cloud implantation with IBM to develop regional

cloud services infrastructure (Alsanea & Barth 2014). In Australia, the government started to transfer the vast majority of their systems' data to the cloud (Taskforce 2010).

The Thai government are planning for the government cloud to add Software as a Service, and has previously developed a national platform for cloud-based and email services. It considers that such consolidation will increase service assistance for government organisations, while concurrently cutting down their IT costs significantly (Wyld 2010).

In Saudi Arabia, the government has acknowledged the importance of cloud-based services and has plans to establish government cloud services, and other new technologies such as smart cities and Internet of Things sensing (Madini O. Alassafi et al. 2016). Moreover, Saudi ICT infrastructure in government agencies, such as the Ministry of the Interior and Higher Education, have started to invest in the cloud in order to scale up their IT services for their stakeholders and standardise their means of communication (Alharthi, Madini O. Alassafi, et al. 2016; Alharthi et al. 2015).

2.4 The Proposed Framework

The following framework is proposed based on desk research and it was further elaborated in previous research paper (Alassafi et al. 2016). The framework consists of three categories, as now described.

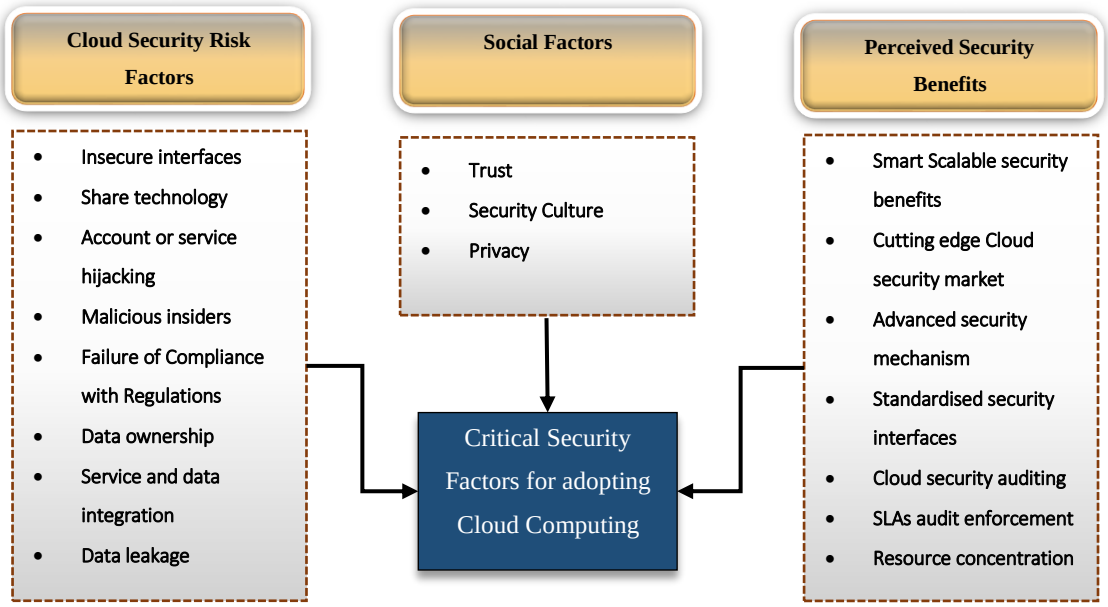

Figure 2, Proposed Cloud Security Framework

2.4.1 Cloud security risk factors:

- **Insecure interfaces and application programming interfaces (APIs).** Consumers manage and interact with cloud services through interfaces and APIs. Providers have to guarantee that security is inserted and considered in their service models. However, users must be aware of security risks in their use (Cloud Security Alliance 2013).

- **Shared technology risk.** IaaS is constructed on shared infrastructure that has frequently not been designed with multi-tenant architecture in mind, such as CPU caches and GPUs.
- **Account or service hijacking.** According to the CSA, service traffic hijacking was recognised as the third highest security risk. It is regularly operated with stolen identifications and current defence is the two factor authentication technique.
- **Malicious insiders.** Current or previous operators from the provider authorise access to an organisation's system and thus have access to potentially sensitive data. It is important for government organisations to verify what providers are doing to identify and protect against malicious insiders.
- **Failure to Comply with regulations.** Government agencies should be aware of regulations before adopting the cloud even when compliance takes place through a service provider. There are no government regulations or directions that can support the organisation after a data breach.
- **Data ownership (governance) and accountability.** Government agencies need to carefully think about this risk and mitigate it since the organisation must defend the data it owns.
- **Service and data integration/protection.** Every organisation must be sure its own data is protected moving between the end user and the cloud data centre because unsecured data is more liable to interception in transmission.
- **Data leakage.** This reflects a weakness in security access rights to more domains and a weakness of physical transport systems for cloud data and backups.

2.4.2 Social Factors

- **Trust.** This consists of trusting the service itself and its provider to supply a level of authentication, confidentiality, and integrity of the service and of the stored data.
- **Security Culture.** Security culture means that information security must be a normal part of daily activities for all employees. It helps in the execution of information security policies, and covers social, cultural, and ethical training to develop the pertinent security behaviour.
- **Privacy.** Privacy is confidentiality of data that allows access to only designated users. It is a major concern since users cannot have complete control of information stored on cloud-based servers.

2.4.3 Perceived Security Benefits

- **Smart scalable security benefits.** This is the ability to extend the security features to multiple locations, to the edges of networks, timeless of response and to manage threats. The list of cloud resources that can be rapidly scaled on demand already includes storage, CPU time, memory, web service requests and virtual machine instances, and the level of granular control over resource consumption is improving as technologies mature.
- **Cutting edge cloud security market.** Cloud providers Amazon and Google are considered the largest hardware and software providers in the world. The cloud user can thus benefit from up-to-date high standard security techniques.

- **Advanced security mechanism.** Cloud providers can provide centralised security with service patches and updates for government agencies, which is more efficient than traditional organisational security.
- **Standardised security interfaces.** Interfaces free of security management can ease the time and cost of user to change from one provider to another.
- **Cloud security auditing.** Auditing in the cloud can be better organised, pay as you go for auditing, and gathering audit log requirements.
- **SLAs audit enforcement.** Service level agreements allow cloud users to set audit manage requirements that the provider should comply with.
- **Resource concentration**. The pool of security resources can be harnessed by users including access control, comprehensive security policy, patch and data management and maintenance processes.

3 Research Methods

A mixed method approach was used, grouping quantitative and qualitative methods. The results were validated through triangulation (Kaplan & Duchon 1988). This involved comparing data discovered from the review of literature, an expert review and a questionnaire survey. The triangulation was applied to each method individually (M. Morse 1991). Data was first collected from relevant literature to build an initial framework, shown in Figure 3. Then, interviews were conducted with experts to review that initial framework. Open-ended questions were used to explain the reasons behind the experts' answers for the closed questions, and to help in suggesting new factors that were not in the current framework. The third phase was the distribution of an online questionnaire to IT and security experts in different Saudi government agencies who were experienced in this field.

The qualitative data is regularly grouped using an open-ended question. In this method, the investigators can gain more information about the current situation, human attitudes, opinions and decisions (Creswell 2003). This research method used when there is a developed theory needs to be confirmed (Connolly 2011).

However, the quantitative method aims to explain human opinions, attitudes, actions and decisions. The qualitative method regularly uses close-ended questions, where the participant has to choose from specific selections and the participants are not allowed to describe their answers (Creswell 2003).

In order to improve and confirm the critical security factors that influencing the cloud adoption in Saudi government agencies a simultaneous methodological triangulation was implemented. It involved joining and comparing data discovered from a detailed literature review, an expert review and a questionnaire survey as illustrated in Figure 3. The triangulation is implemented in three phases since each method should be applied individually (Driscoll et al. 2007).

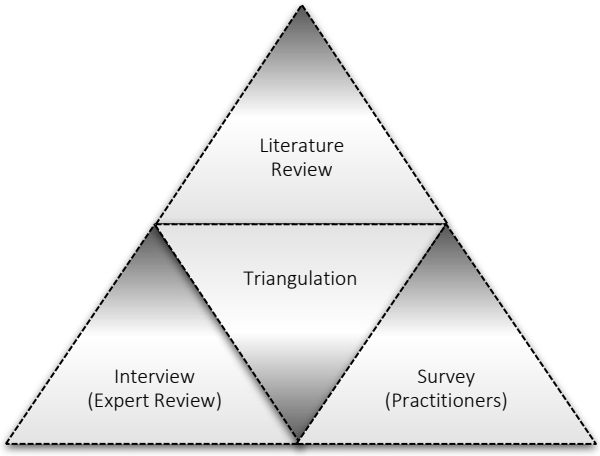

Figure 3, Methodological Triangulation Validation Method to confirm the framework

First phase, data was collected from secondary research by reviewing related literature to build the proposed framework. The second phase, interviews were conducted with experts to review the framework and confirm it. This phase included both open-ended and closed-ended questions. The open-ended questions were used identify and to explain the reasons behind experts' answers for the closed-ended questions, and to help in suggesting new factors that did not to be in the current framework. The third phase is distributing online questionnaire to IT and security experts who have experienced of this field in different Saudi government agencies, including closed-ended questions, to confirm the critical security factors as shown in Figure 4.

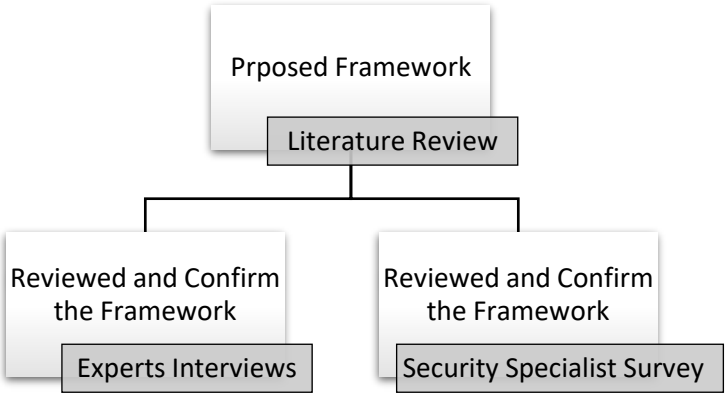

Figure 4, Simultaneous Research Methodology

3.1 Expert interviews design and analysis

12 security experts were interviewed from IT projects in different departments of Saudi government agencies such as ministries, telecommunication agencies, state universities, research institutes, and education. The interviews were conducted in Riyadh, Jeddah and Madinah. A person was 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.

A five-point Likert Scale was used for the 18 closed questions to explore the current factors in the framework. A pilot session to test the interview questions was carried out with five people; three were IT security experts from security group and two were computer science researchers.

There is no agreed number of experts for an interview in a content validity study, according to (Grant & Davis 1997) and Guest et al. 2006 suggest that saturation is usually reached within 12 interviews.

This study was used a semi-structured interview to designing the interview, which included both open and closed questions. Therefore, the two main purposes of these interviews were:

- *To review the factors identified in the literature review based study conducted previously in order to improve the framework.*
- *To identify additional factors from the context of Saudi government agencies and have not been mentioned previously in the literature.*

3.2 IT questionnaire design and analysis

The self-administered online questionnaire was sent to 32 different experienced IT staff from IT and security departments in the Saudi government agencies such as ministries, telecommunication agencies, state universities, research institutes, and educations, in different locations around the Saudi Arabia. A pilot survey was conducted with five IT security practitioners drawn from the IT Division in the Ministry of Education, from a security group, and from computer science researchers.

When calculating the minimum acceptable sample size, two types of error are considered (Tessmer 2009). Type1 or α errors occur when rejecting a true null hypothesis and type2 or β errors occur when a false null hypothesis is not rejected. The likelihood of these errors occurring can be reduced by increasing the sample size. By convention, α is set to 0.05 for a 95% confidence and (1–β) is set to 0.9 or 10% for missing an association(Banerjee 2009)The effect size refers to the magnitude of the association between the predictor and outcome variables. Cohen (1988) defines three different effect sizes: small (d=0.2), medium (d=0.5) and large (d=0.8). In exploratory studies, effect size is usually set at large. In this study G* Power software was used to calculate the minimum sample size which was 23. The calculation was performed for a t-test to find the difference in mean from constant.

4 Study Results and Discussion

This section provides the results of the mixed methods used. In order to refine and confirm the proposed critical factors in the security cloud adoption framework and the main aim of the interviews and questionnaires were to examine the factors of the framework as well as the reliability of the framework constructs and items.

4.1 Results of the Expert

This section presents the results of the interviews with IT and security experts. The interviews included qualitative and quantitative methods which are open ended question and closed ended questions. The data was collected using semi-structured interviews from 12 security experts in Saudi Arabia government

agencies. The aim of this task was to review the critical security factors identified by the literature review and explore other factors that are not mentioned in previous studies. The experts were asked to rate their attitude to each of the proposed factors. The raw responses to these questions are presented in Figure 5, and 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'.

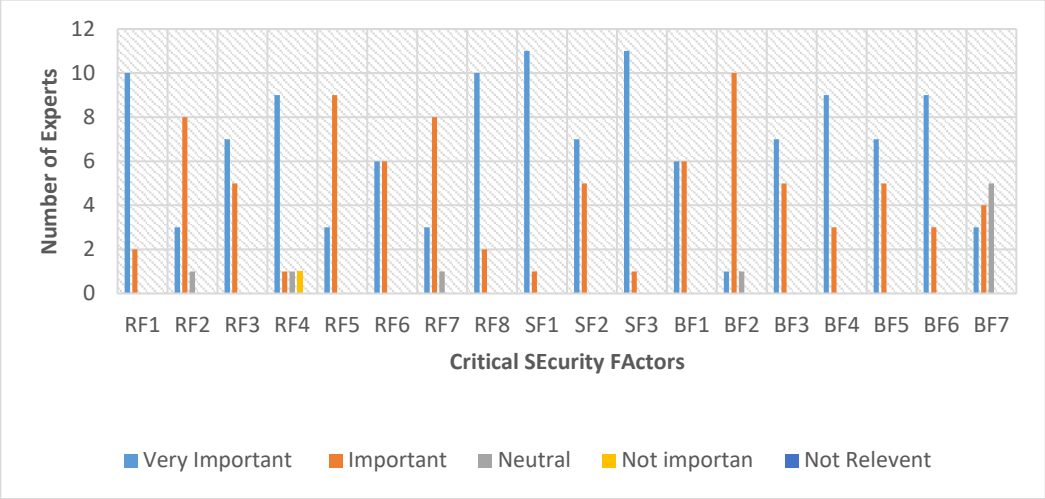

Figure 5, Rating by Expert of each factor

The interviews were asked for their attitude about all the proposed factors using quantitative method. The aim of the questions was to evaluate the importance of the proposed security factors to adopt cloud services in Saudi government agencies, from the experts' point of view. The experts' responses were collected and entered by SPSS software. The data was analysed by using the one sample t-test. The result of the test is illustrated in Table 1.

Table 1, One sample T- test of experts interviews

Category	Ref	Item	Mean	Sig (2-Tailed) P-value	Results
Security Risk Factors	RF1	Insecure interfaces	4.83	<.001	Statically Significant
	RF2	Share technology	4.17	<.001	Statically Significant
	RF3	Account hijacking	4.58	<.001	Statically Significant
	RF4	Malicious insiders	4.50	<.001	Statically Significant
	RF5	Failure of Compliance with Regulations	4.25	<.001	Statically Significant
	RF6	Data ownership	4.50	<.001	Statically Significant
	RF7	Service and data integration	4.17	<.001	Statically Significant
	RF8	Data leakage	4.83	<.001	Statically Significant
Social Factors	SF1	Trust	4.92	<.001	Statically Significant
	SF2	Security Culture	4.58	<.001	Statically Significant
	SF3	Privacy	4.92	<.001	Statically Significant
Perceived Security Benefits	BF1	Smart Scalable security benefits	4.50	<.001	Statically Significant
	BF2	Cutting edge security market	4.00	<.001	Statically Significant
	BF3	Advanced security mechanism	4.58	<.001	Statically Significant
	BF4	Standardised security interfaces	4.75	<.001	Statically Significant
	BF5	Cloud security auditing	4.58	<.001	Statically Significant

	BF6	SLA audit enforcement	4.75	<.001	Statically Significant
	BF7	Resource concentration	3.25	<0.082	Statically NOT Significant

Regarding on the experts' opinion, the results 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 0.05.

- Resource concentration factor: (0.082 > 0.05).

While the result shows that the Resource concentration factor has no significant impact on organisation decision, the findings from previous studies pointed that this factor has a major influence on the decision to adopt cloud computing (Catteddu & Hogben 2009). Consequently, the Resource concentration factor will be kept in the proposed framework. The justification of not removing this factors is that, several studies have found that the 'Resource concentration factor' is one of the importance factors that influence the use of online services and the adoption of new technology (Tei & Gurgen 2014; Catteddu & Hogben 2009).

On other hand, the purpose of the qualitative open-ended expert interview questions is to get deep analysis and review to identify other factors relating to adoption of cloud services in Saudi Arabia government agencies. Nvivo software was used for analysing and coding expert's response. Their opinions were analysed and coded to produce the following results. The interviews were asked to answer open ended question about the framework with three categories which are Security risk factors, Social and Security Benefits factors. All agreed that most of these factors that mentioned in the framework are important and it affects the decision to adopt cloud services. Their opinions were analysed and coded to produce the finding. A key points of the expert's insights are provided as followed:

Expert B: *"I agree that most of the factors in the framework are potential variables that hindered some organisation to using cloud services and there are some other factors influencing to adopt cloud services such as: Encryption and Sophisticated Authentication Techniques".* And

"We should consider these factors which are Encryption and Sophisticated Authentication Techniques as security risks when we thinking to adopt cloud services because there are some reasons behind using this services such as Consolidated Services, Collaboration and Sharing and Reduce Total Cost of Ownership".

Another interesting point stated by **Expert B:**

"There are some challenges that faced my agency and other organisations in Saudi Arabia since using this technology. I advised that, it is important to ensuring the proper rising of the cloud based implementation to satisfy the organization needs and security breaches caused by social trends".

Some of the experts agreed that it is necessary for any government to attempt cloud technology before implementing it. This will help them to understand the way technology works and if it meets their needs.

Expert F: *"I agreed all security risk factors, social and benefits factors that mentioned in your framework are essential when any government agencies making decision to adopting cloud computing in their agencies and I recommend any agencies to be aware of prepare data for client side encryption before and after using cloud services".* And he suggested other points:

"Exclusive allocation of the cloud resources should consider it as security risks when adopting cloud".

"There are three challenges faced my organisation while we using cloud services, you may consider them as importance which are: Setting up cloud infrastructure, Training for using the cloud and adopting classical applications for the cloud".

Expert L: *"I think we need to try the cloud services before adopting it, that we call it a test phase".*

Another interesting point from **Expert L**:

"As social Users awareness when using cloud platforms is important to avoid shadow IT data leakage and man from the inside attack".

"As security risk, Security transparency, the providers should alert the consumers with the security control updates or policies that applied to their data. Moreover, transparency when incident occurred, cloud provider should not cover any security incident happened to their assets and they should share lessons learned from each with the costumers to ensure well-protected cloud environment".

"We should consider cloud multi-geographical infrastructures as security benefits because it plays important benefits for the consumers especially when natural catastrophes happened".

Expert G: *"Cloud service is more appropriate for government or even private sector that depend on IT technology. Hence, the organisation needs to consider the nature of its business and its requirements before adopting cloud service"*

"As my experience I greed totally with this framework and these factors that should we consider it as essential when any government agencies making decision to adopt cloud services".

"Many environmental and technical changes have been going on the IT environment which need to be settled down first. The IT environment is not ready yet for cloud computing (readiness)".

Expert D: *"An organisation needs to know its need to be on the cutting edge of technology. I consider the important thing to recognise who is your corporation. We are a Saudi food and drug authority, so we are not an IT company, and may not have a high willing to be on the cutting edge technologically".*

Another interesting point from **Expert D**:

"Other factors should be considering as security risks if using cloud practically in governments such as data access authorization mechanism and use of client side encryption".

"The best things behind using cloud computing in my organisation are Ease of Access and Team Work".

"As security risk factor should prepare data encryption and use encryption when using cloud services"

Experts B, C, D and F:

The social factor aspects are also an important that should be taken into consideration. Culture is defined as the "beliefs, values, habits, rules and communication forms of some of people in a community" (Alharbi et al. 2015). Those experts specified that while cloud technology influence reduce the number of jobs in system of government, it delivers an opportunity for jobs in the country that hosts the services, where the need in this country is to create job for community and increase the economy. The analysis exposes that social has an influence on the adoption decision.

Expert E: *"In my opinion other important factors need to be considered as security risks when an organisation adopting cloud services such as identifying the current Vulnerabilities in the organisation and*

compare it to the cloud vulnerabilities and Supply Attacks including all factors that mentioned in your framework".

"We start using cloud and the reason behind that: it is better agile paradigm to perform the electronics workloads, it is helps collaborations, speed and gives better engagement".

Another interesting point from **Expert E**:

"The service quality, access to data and downtime and accessibility are some of challenging that we faced when we adopt the cloud".

Both quantitative and qualitative results confirmed that all factors in the framework affect to adopt cloud computing services.

4.2 Results of the Questionnaires

This section provides the results of the survey. The quantitative data was using an online questionnaire. All of the respondents are currently working in different departments in Saudi government agencies and have at least two years' experience in security and cloud filed. The aim of the survey was to confirm the proposed framework. The closed-ended questions were proposed to refine the factors in the framework. The closed-ended questions in this section were involved fifty-one items, where two to four were stated about each factor. A five-point Likert Scale (strongly agree, agree, neutral, disagree, strongly disagree) was used. The measure of questionnaire responses was the same as that for the responses to the closed-ended questions in the interviews. As the information from closed ended question is considered as quantitative data, the experts' responses were collected and entered by SPSS software to analyse the data statistically. The One Sample T-test was used to analyse as a statistical test the results of the quantitative data. This test helps in comparing the mean of a population (μ) with a hypothesised value ($\mu 0$). The hypothesised mean ($\mu 0$) = 3, which indicates Neutral on the five point Likert-type scales. The hypotheses for testing each factor are as follows:

- H0: If the mean rating of the proposed factor is >= 3, accept the null hypothesis, that the factor is significant, and it affects the cloud adoption decision.
- H1: If the mean rating of the proposed factor is < 3, accept the alternative hypothesis, that the factor is not significant, and it does not affect the cloud adoption decision.

The test value was defined as 3 on the five-point Likert scale for security factor, which ranged from 5 (strongly agree) to 1 (disagree). The statistical significant level alpha is $\alpha = 0.05$. The null hypothesis (H0) is rejected if the probability (p-value) of question is $> \alpha = 0.05$. The factor is statistically significant if the p-value < 0.05, otherwise, the factor is not statistically significant. **Table 2**, shows the analysis results of questionnaire for each factors. From the questionnaire results, it can be seen that the attitude of all categories and its factors are all significant in affecting to adopt cloud computing. All the results of the items show a mean > 3 and p-value < 0.05, so H0 is accepted and the H1 is rejected.

Table 2, one sample T-test of Questionnaire Results

Category	Variable	Items	Mean	Sig (2-tailed) P-value	Results
Security Risk Factors	1. Insecure Interfaces	II1	4.50	<0.001	Statically Significant
		II2	4.53	<0.001	Statically Significant
		II3	4.53	<0.001	Statically Significant
	2. Share Technology	ST1	4.59	<0.001	Statically Significant
		ST2	3.75	<0.05	Statically Not Significant
	3. Account or Service Hijacking	AH1	4.13	<0.001	Statically Significant
		AH2	3.91	<0.001	Statically Significant
		AH3	3.88	<0.001	Statically Significant
	4. Malicious Insiders	MI1	4.22	<0.001	Statically Significant
		MI2	4.56	<0.001	Statically Significant
		MI3	4.66	<0.001	Statically Significant
	5. Failure of Compliance with Regulations	CR1	3.91	<0.001	Statically Significant
		CR2	4.16	<0.001	Statically Significant
		CR3	4.06	<0.001	Statically Significant
		CR4	4.53	<0.001	Statically Significant
	6. Data Ownership	DO1	4.47	<0.001	Statically Significant
		DO2	4.22	<0.001	Statically Significant
		DO3	4.03	<0.001	Statically Significant
	7. Service and Data Integration	SDI1	4.56	<0.001	Statically Significant
		SDI2	4.09	<0.001	Statically Significant
		SDI3	4.19	<0.001	Statically Significant
	8. Data Leakage	DL1	4.25	<0.001	Statically Significant
		DL2	3.97	<0.001	Statically Significant
		DL3	4.06	<0.001	Statically Significant
Social Factors	1. Trust	TR1	4.00	<0.001	Statically Significant
		TR2	4.41	<0.001	Statically Significant
		TR3	3.44	0.070	Statically Not Significant
	2. Security Culture	SC1	4.19	<0.001	Statically Significant
		SC2	4.19	<0.001	Statically Significant
		SC3	4.25	<0.001	Statically Significant
	3. Privacy	PR1)	4.50	<0.001	Statically Significant
		PR2	4.25	<0.001	Statically Significant
		PR3	3.41	0.079	Statically Not Significant
Perceived security Benefits	1. Smart Scalable security benefits	SS1	4.16	<0.001	Statically Significant
		SS2	4.09	<0.001	Statically Significant
		SS3	4.16	<0.001	Statically Significant
		SS4	4.00	<0.001	Statically Significant
	2. Cutting edge security market	CE1	4.31	<0.001	Statically Significant
		CE2	4.31	<0.001	Statically Significant
	3. Advanced security mechanism	AS1	4.19	<0.001	Statically Significant
		AS2	4.34	<0.001	Statically Significant
		AS3	4.34	<0.001	Statically Significant
	4. Standardised security interfaces	SSI1	4.16	<0.001	Statically Significant
		SSI2	4.34	<0.001	Statically Significant
		SSI3	4.41	<0.001	Statically Significant
	5. Cloud security auditing	CS1	4.19	<0.001	Statically Significant
		CS2	4.06	<0.001	Statically Significant
	6. SLA audit enforcement	SLA1	4.03	<0.001	Statically Significant
		SLA2	4.25	<0.001	Statically Significant
	7. Resource concentration	RC1	4.00	<0.001	Statically Significant
		RC2	3.97	<0.001	Statically Significant

4.3 Reliability

It is mostly acknowledged that when a concept has been operationally well-defined, in that a measure of it has been proposed, the ensuing measurement device should be both reliable and valid. reliability of the experts' statements was tested using Cronbach's Alpha Coefficient, (Connolly 2011). If the reliability score is less than 0.6, it is considered poor, moderate if it is around 0.6, good if around 0.7 and very good at 0.8 or above. Figure 6, presents the mean average of items and reliability results of questionnaire for each factor. SPSS software was used to carry out the Cronbach's Alpha test. The overall reliability test of factors, Cronbach's alpha, was 0.756, showing that the results of items in Table 3, are reliable.

Table 3, Reliability Statistics of Questionnaire

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.756	.786	51

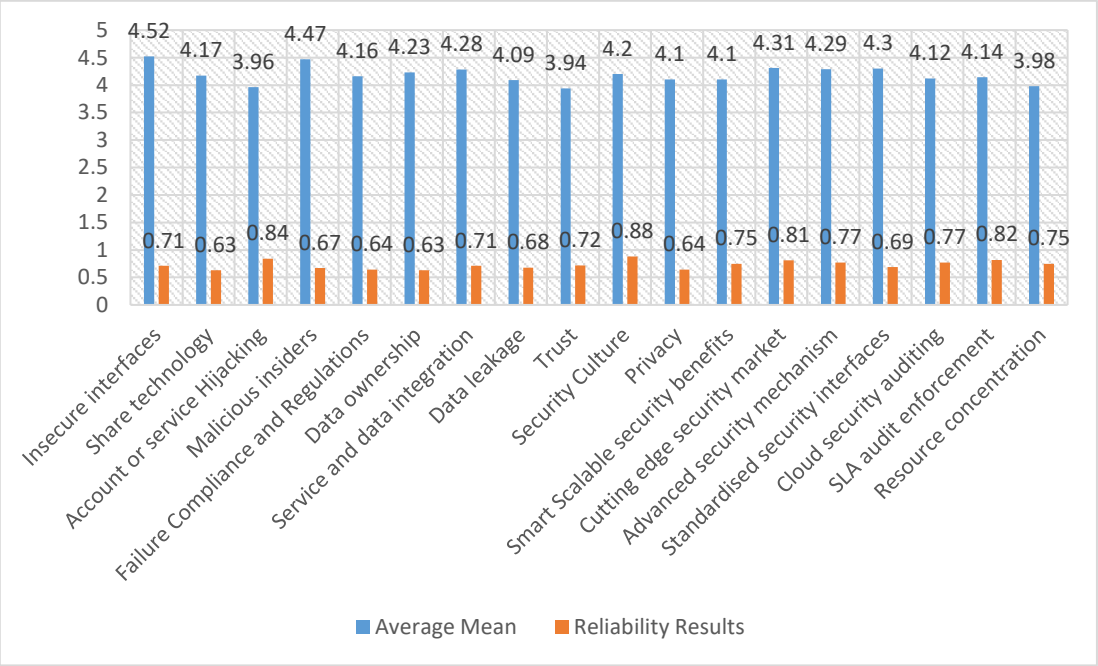

Figure 6, Mean and Reliability Chart of the Questionnaire

4.4 Discussion

This section presents the overall finding of the interviews and questionnaire conducted with experts of security and IT experts in different government agencies in Saudi Arabia. Hence, the finding regarding the factors in the framework from the experts' opinions and IT security specialist questionnaire. All experts are agreed that security is the top priority factor in the organization. If the organization does not ensure proper security, the services will not be reliable and acceptable to the users of the cloud computing. For the attitude

of categories and its factors, the expert indicate that they 'Strongly agree' that it has impact to adopt cloud services in Saudi government agencies. Furthermore, the statistical results of the experts' interviews also presented a strong significant, the means of these factors were between 3.2 and 4.9. In The questionnaire, the results give an indication that the social attitudes and its associate items have an effect on government agencies intention to adopt cloud computing. Moving to security risk factors category, the following factors are statistically confirmed *(Insecure interfaces, Share technology, Account or service hijacking, malicious insiders, Failure of compliance with regulations, Data ownership, Service and data integration and Data leakage).* The results of the interviews show that among 12 experts agreed these factors are either important or very important to the adoption of cloud in Saudi Government Agencies and it has high impact on stakeholders' behaviour to adopting cloud services. The means in the quantitative analysis of the interviews in this category were between 4.7 and 4.8 which is very high impact. Furthermore, the statistical results of the questionnaire to the security risk factors shows that all items are statistically significant except only one item belongs to Share Technology factor, which is (ST2), respectively is statistically not significant. Consequently, this item will be removed since their p-value > 0.05.

The quantitative analysis of interviews specifies that social factors category and its factors are essential to any government agencies making decision of adopting cloud. In the expert review, it is noticeable that *security culture, trust and privacy* are very important factor, as none of the experts disagreed that "these factors essential to help organisations to using cloud services", and all the experts selected the "Very important" and "important" choice, with mean from 4.6 to 4.9. While in the questionnaire responses, all the social category factors with its items are deemed important. However, two items belong to Trust and Privacy factors, which are (TR3) and (PR3), respectively are statistically not significant. Consequently, these items will be removed since their p-value > 0.05.

Finally, cloud computing service provides a number of benefits to the users from the expert's point of view this study. This study shows that the perceived security benefits category (*Smart Scalable security benefits, Cutting edge security market, advanced security mechanism, Standardised security interfaces, Cloud security auditing, SLA audit enforcement and Resource concentration),* all factors are crucial with mean range of 3.25 to 4.75 for the quantitative results of interviews, excepting the resource concentration factor with mean 3.25 Not statically significant as the value less than the test-value set for the analysis. Whereas the questionnaire results of the same category indicate statistical significant of all the category factors and it is sub-items with mean ranged between 3.97 and 4.41. The participants agreed that the security features of the cloud is an important element to be considered when the adopting cloud.

Despite the difference of the results Resource concentration factor in the questionnaire and the interview conducted, this factor will be kept in the proposed framework. The justification of not removing this factors is that several studies in the literature have stated the importance of this factor to influence the use of cloud services and the adoption of new technology (Tei & Gurgen 2014; Catteddu & Hogben 2009). In summary, the results show that 'there is a positive attitude towards adopting cloud services in Saudi Arabian

government agencies: 75 % of participants stated that their agencies expect to adopt cloud services in the near future'.

For additional factor, the experts were asked if they suggest of other factors, which are not included in the proposed security adoption framework and can have influence on the adoption of the cloud. Experts were recommending additional factor is importance when adopting cloud as following:

- Failure of Client side encryption.

It deemed to be important upcoming factor as five of the experts suggested to be added to the framework, is "Failure of Client side encryption". They pointed out this factor as it has beneficial effect on stakeholder's attitude towards using cloud services. Therefore, this factor becomes under the security risks category in the framework. Figure 7 shows the validated factors in this framework after editing according to the results of the experts' interviews and the questionnaire.

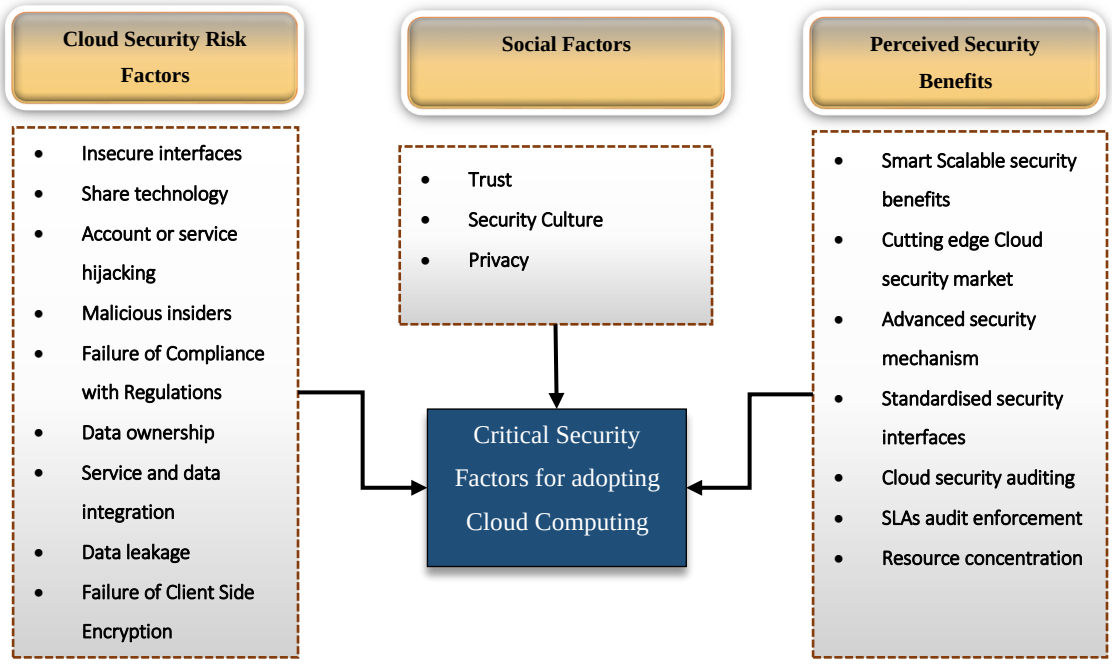

Figure 7, Confirmed the Framework

4.5 Conclusions

Semi-structured interviews were used to review the factors identified previously in literature review and to explore others factors that were unspecified in previous studies. Experts were interviewed and a questionnaire was distributed to examine the factors. Both quantitative and qualitative methods were used to ensure the validity of the results. The confirmation of critical security factors for cloud adoption in Saudi government agencies in this proposed framework was a first step in our attempt to investigate the potential factors enabling them to adopt cloud in Saudi Arabia. We aim to utilise the confirmed these factors from the preliminary study to survey a larger sample of IT experts and decision makers at government in several agencies in Saudi Arabia. The importance and impact of each component in our proposed framework will

be analysed and their significance in the model validated through a test of the proposed potential factors using Structure Equation Modelling (SEM). The framework can also be used in future studies on cloud computing adoption in other areas in the Middle East region with different government agencies. The results from the full study will also contribute to the literature on cloud computing through empirical evidence from the study results and provide a potential of success rate of cloud computing adoption project which can help the decision making process whether to adopt or not. The results from the proposed study will also give IT practitioners and cloud services provider's appreciated experimental data that can be influence in engagement and marketing cloud computing projects.

References

Ahmed Albugmi; Madini O Alassafi; Robert Walters; Gary Wills, 2016. Data Security in Cloud Computing. *Fifth International Conferance on FGCT IEEE*, 2(1), pp.1–169.

Alassafi, M.O. et al., 2016. Investigating the Security Factors in Cloud Computing Adoption: Towards Developing an Integrated Framework. *Journal of Internet Technology and Secured Transactions (JITST)*, 5(2), pp.486–494.

Alassafi, M.O. et al., 2017. Security in Organisations: Governance, Risks and Vulnerabilities in Moving to the Cloud. In *Enterprise Security , Springer*. pp. 241–258.

Alharbi, F., Atkins, A. & Stanier, C., 2015. Strategic Framework for Cloud Computing Decision-Making in Healthcare Sector in Saudi Arabia. *The Seventh International Conference on eHealth, Telemedicine, and Social Medicine*, 1(c), pp.138–144.

Alharthi, A., Alassafi, M.O., et al., 2016. An exploratory study for investigating the critical success factors for cloud migration in the Saudi Arabian higher education context. *Telematics and Informatics*, 34(2), pp.664–678. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0736585316303471.

Alharthi, A. et al., 2015. An Overview of Cloud Services Adoption Challenges in Higher Education Institutions. *Proceeding of the 2nd international conference workshop on emerging software as a services*, 1, pp.102–109.

Alharthi, A. et al., 2017. Critical Success Factors for Cloud Migration in Higher Education Institutions: A Conceptual Framework. *International Journal of Intelligent Computing Research (IJICR)*, 8(1), pp.817–825.

Alharthi, A., Alassafi, M.O., et al., 2016. Towards a framework to enable the migration process to eduactional clouds in Saudi higher education. *i-Society Conferance IEEE Advance Technology for Humanity*, (1), pp.1–4.

Alkhater, N., Wills, G. & Walters, R., 2014. Factors Influencing an Organisation's Intention to Adopt Cloud Computing in Saudi Arabia. *IEEE 6th International Conference on Cloud Computing Technology and Science*, pp.1040–1044.

Alsanea, M. & Barth, J., 2014. Factors Affecting the Adoption of Cloud Computing in the Government Sector : A Case Study of Saudi Arabia. *International Journal of Cloud Computing and Services*, 1, pp.1–16.

Alshahrani, S. a. & Alsadiq, A.J., 2014. Economic Growth and Government Spending in Saudi Arabia: an Empirical Investigation. *International Monetary Fund*, 14(3), p.1.

Babu, S. et al., 2010. Cisco: Top 10 Cloud Risks That Will Keep You Awake at Night. *CSICO*, pp.1–35. Available at: https://www.owasp.org/images/4/47/Cloud-Top10-Security-Risks.pdf.

Banerjee, A., 2009. Hypothesis testing, type I and type II errors. *Industrial psychiatry journal*, 1(Jul), p.127.

Bannerman, P., 2010. Cloud computing adoption risks: state of play. *Asia Pacific Software Engineering Conference Cloud Workshop*, 3(September), pp.0–2.

Buyya, R. et al., 2009. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems Journal*, 25(JUNE), p.17.

Catteddu, D. & Hogben, G., 2009. Cloud Computing Benefits, Benefits, risks and recommendations for information security. *ENISA Computing Report*, 72(1), pp.2009–2013. Available at: http://www.springerlink.com/index/R357K80TP72R7121.pdf.

Chang, V., Kuo, Y.-H. & Ramachandran, M., 2015. Cloud Computing Adoption Framework–a security framework for business clouds. *Future Generation Computer Systems*, 57, pp.24–41. Available at: http://www.sciencedirect.com/science/article/pii/S0167739X15003118.

Che, J. et al., 2011. Study on the security models and strategies of cloud computing. *international Conference on Power Electronics and Engineering Application*, 23, pp.586–593. Available at: http://dx.doi.org/10.1016/j.proeng.2011.11.2551.

Cherdantseva, Y. & Hilton, J., 2013. A Reference Model of Information Assurance & Security. *International Conference on Availability, Reliability and Security*, pp.546–555. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6657288.

Cloud Security Alliance, 2013. The Notorious Nine. Cloud Computing Top Threats in 2013. *CSA Global Staff*, pp.1–14. Available at: http://www.cloudsecurityalliance.org.

Connolly, P., 2011. Quantitative Data Analysis using SPSS. *An International for Health and Social Science*, pp.1–283.

Creswell, J.W., 2003. Research design Qualitative quantitative and mixed methods approaches. *SAGE Publications International Educational and Professional Publisher*, pp.3–26.

Deloitte, 2010. Information Security Briefing Cloud Computing. , (March), pp.1–71.

Driscoll, D.L., Salib, P. & Rupert, D.J., 2007. Merging Qualitative and Quantitative Data in Mixed Methods Research : How To and Why Not. *Ecological and Environmental Anthropology*, 3(1), pp.18–28.

Elena, G. & Johnson, C.W., 2015a. Factors influancing Risk Acceptance of Cloud Computing Sertvices in the UK. *International Journal on Cloud Computing: Services and Architecture (IJCCSA)*, 5(2).

Elena, G. & Johnson, C.W., 2015b. Laypeople's and experts risk perception of cloud computing services. *International Journal on Cloud Computing: Services and Architecture (IJCCSA)*, 5(4), pp.1–19.

Fumei Weng, M.-C.H., 2014. Competition and Challenge on Adopting Cloud ERP. *International Journal of Innovation, Management and Technology*, 5(4), pp.309–313.

Gentzoglanis, A., 2011. Risk , Financial Modeling and Cloud Computing : A New Approach. *International Conference on Software and Computer Applications*, 9, pp.147–151.

Grant, J.S. & Davis, L.L., 1997. Selection and use of content experts for instrument development. *Research in Nursing & Health*, 20(3), pp.269–274.

Guest, G., Bunce, A. & Johnson, L., 2006. How Many Interviews Are Enough ? An Experiment with Data Saturation and Variability. *Family Health International*, 18(1), pp.59–82.

Kaplan, B. & Duchon, D., 1988. Combining Qualitative and Quantitative Information Systems. *International Conference on information Systems*, 12(4), pp.571–586.

KPMG, 2011. The Cloud: Changing the Business Ecosystem. *Kpmg International*, pp.1–102.

Kumar, K., 2010. Cloud Computing for Mobile Users: Can Offloading Computation Save Energy? *IEEE Computer Society*, 43(4), pp.51–56.

M. Morse, J., 1991. Approaches to qualitative- quantitative methodological triangulation. *Nurssing Research*, 40(1), pp.120 – 123.

Madini O. Alassafi et al., 2016. Security Risk factors that influence Cloud Computing Adoption in Saudi Arabia Government Agencies. *i-Society Conferance IEEE Advance Technology for Humanity*, 1, pp.1–4.

Mauch, V., Kunze, M. & Hillenbrand, M., 2013. High performance cloud computing. *Future Generation Computer Systems*, 29(6), pp.1408–1416. Available at:

http://www.sciencedirect.com/science/article/pii/S0167739X12000647 [Accessed April 30, 2015].

Mell, P. & Grance, T., 2011. The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. *Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg,*, 145, p.7. Available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Paquette, S., Jaeger, P.T. & Wilson, S.C., 2010. Identifying the security risks associated with governmental use of cloud computing. *Elsevier Journal*, 27(3), pp.245–253. Available at: http://www.sciencedirect.com/science/article/pii/S0740624X10000225 [Accessed November 26, 2014].

Pearson, S., 2013. Privacy, Security and Trust in Cloud Computing. *Springer London*, pp.3–42.

Sabahi, F., 2011. Cloud computing security threats and responses. *2011 IEEE 3rd International Conference on Communication Software and Networks*, pp.245–249.

Sen, J., 2013. Security and Privacy Issues in Cloud Computing. *Architectures and Protocols for Secure Information Technology*, (iv), p.42.

Shirley Radack, 2012. Cloud Computing: A Review Of Features, Benefits, And Risks, And Recommendations For Secure, Efficient Implementations. *NIST Special Publication (SP) 800-146*, (June).

Subashini, S. & Kavitha, V., 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), pp.1–11. Available at: http://www.sciencedirect.com/science/article/pii/S1084804510001281 [Accessed July 12, 2014].

Sun, D. et al., 2011. Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments. *Procedia Engineering Elsevier Journal*, 15, pp.2852–2856. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1877705811020388.

Taskforce, G., 2010. Engage: Getting on with Government 2.0. *Government 20 Taskforce*, pp.1–136. Available at: http://www.citeulike.org/user/cobi/article/6863079.

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

Tessmer, M., 2009. Hypothesis testing, type I and type II erro. *Industrial Psychiatry Journal*, 1, pp.127–131.

Vaquero, L.M. et al., 2008. A break in the clouds. *ACM SIGCOMM Computer Communication Review*, 39(1), p.50.

Wyld, D.C., 2010. The Cloudy Future Of Government IT: Cloud Computing and The Public Sector Around The World. *International Journal of Web & Semantic Technology*, 1(1).

Zhou, M. et al., 2010. Security and Privacy in Cloud Computing: A Survey. *Sixth International Conference on Semantics, Knowledge and Grids*, 1(1), pp.105–112.

Appendix:

- **Experts Frequencies**

RF1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	4	2	16.7	16.7	16.7
	5	10	83.3	83.3	100.0
	Total	12	100.0	100.0	

RF2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	1	8.3	8.3	8.3
	4	8	66.7	66.7	75.0
	5	3	25.0	25.0	100.0
	Total	12	100.0	100.0	

RF3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	4	5	41.7	41.7	41.7
	5	7	58.3	58.3	100.0
	Total	12	100.0	100.0	

RF4

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	1	8.3	8.3	8.3
	3	1	8.3	8.3	16.7
	4	1	8.3	8.3	25.0
	5	9	75.0	75.0	100.0
	Total	12	100.0	100.0	

RF5

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	4	9	75.0	75.0	75.0
	5	3	25.0	25.0	100.0
	Total	12	100.0	100.0	

RF6

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	4	6	50.0	50.0	50.0
	5	6	50.0	50.0	100.0
	Total	12	100.0	100.0	

RF7

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	1	8.3	8.3	8.3
	4	8	66.7	66.7	75.0
	5	3	25.0	25.0	100.0
	Total	12	100.0	100.0	

- **One-Sample Test of Experts with Test Value = 3**

	Test Value = 3					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
RF1	16.316	11	.001	1.833	1.59	2.08
RF2	7.000	11	.001	1.167	.80	1.53
RF3	10.652	11	.001	1.583	1.26	1.91
RF4	5.196	11	.001	1.500	.86	2.14
RF5	9.574	11	.001	1.250	.96	1.54
RF6	9.950	11	.001	1.500	1.17	1.83
RF7	7.000	11	.001	1.167	.80	1.53
RF8	16.316	11	.001	1.833	1.59	2.08
SF1	23.000	11	.001	1.917	1.73	2.10
SF2	10.652	11	.001	1.583	1.26	1.91

SF3	23.000	11	.001	1.917	1.73	2.10
BF1	9.950	11	.001	1.500	1.17	1.83
BF2	8.124	11	.001	1.000	.73	1.27
BF3	10.652	11	.001	1.583	1.26	1.91
BF4	13.404	11	.001	1.750	1.46	2.04
BF5	10.652	11	.001	1.583	1.26	1.91
BF6	13.404	11	.001	1.750	1.46	2.04
BF7	1.915	11	.082	.250	-.04	.54

- **Frequency Table of Questionnaire**

II1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	3.1	3.1	3.1
	3	1	3.1	3.1	6.3
	4	10	31.3	31.3	37.5
	5	20	62.5	62.5	100.0
	Total	32	100.0	100.0	

II2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	2	6.3	6.3	6.3
	4	11	34.4	34.4	40.6
	5	19	59.4	59.4	100.0
	Total	32	100.0	100.0	

II3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	2	6.3	6.3	6.3
	4	11	34.4	34.4	40.6
	5	19	59.4	59.4	100.0
	Total	32	100.0	100.0	

ST1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	1	3.1	3.1	3.1
	4	11	34.4	34.4	37.5
	5	20	62.5	62.5	100.0
	Total	32	100.0	100.0	

ST2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	5	15.6	15.6	15.6
	3	5	15.6	15.6	31.3
	4	10	31.3	31.3	62.5
	5	12	37.5	37.5	100.0
	Total	32	100.0	100.0	

AH1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	6.3	6.3	6.3
	3	6	18.8	18.8	25.0
	4	8	25.0	25.0	50.0
	5	16	50.0	50.0	100.0
	Total	32	100.0	100.0	

AH2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	4	12.5	12.5	12.5
	3	3	9.4	9.4	21.9
	4	13	40.6	40.6	62.5
	5	12	37.5	37.5	100.0
	Total	32	100.0	100.0	

AH3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	4	12.5	12.5	12.5
	3	5	15.6	15.6	28.1
	4	10	31.3	31.3	59.4
	5	13	40.6	40.6	100.0
	Total	32	100.0	100.0	

MI1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	6.3	6.3	6.3
	3	3	9.4	9.4	15.6
	4	11	34.4	34.4	50.0
	5	16	50.0	50.0	100.0
	Total	32	100.0	100.0	

MI2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	2	6.3	6.3	6.3
	4	10	31.3	31.3	37.5
	5	20	62.5	62.5	100.0
	Total	32	100.0	100.0	

MI3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	4	11	34.4	34.4	34.4
	5	21	65.6	65.6	100.0
	Total	32	100.0	100.0	

- **One –Sample Test of the Questionnaire**

	Test Value = 3					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
II1	10.072	31	.001	1.500	1.20	1.80
II2	13.940	31	.001	1.531	1.31	1.76
II3	13.940	31	.001	1.531	1.31	1.76
ST1	16.102	31	.001	1.594	1.39	1.80
ST2	3.050	31	.005	.750	.25	1.25
AH1	5.638	31	.001	1.125	.72	1.53
AH2	4.008	31	.001	.906	.45	1.37
AH3	3.768	31	.001	.875	.40	1.35
MI1	6.445	31	.001	1.219	.83	1.60
MI2	14.281	31	.001	1.563	1.34	1.79
MI3	19.416	31	.001	1.656	1.48	1.83
CR1	4.473	31	.001	.906	.49	1.32
CR2	6.416	31	.001	1.156	.79	1.52
CR3	5.171	31	.001	1.063	.64	1.48
CR4	13.940	31	.001	1.531	1.31	1.76
DO1	13.371	31	.001	1.469	1.24	1.69
DO2	6.445	31	.001	1.219	.83	1.60
DO3	4.844	31	.001	1.031	.60	1.47
SDI1	15.661	31	.001	1.563	1.36	1.77
SDI2	5.536	31	.001	1.094	.69	1.50
SDI3	6.731	31	.001	1.188	.83	1.55
DL1	7.721	31	.001	1.250	.92	1.58
DL2	5.018	31	.001	.969	.58	1.36

DL3	5.438	31	.001	1.063	.66	1.46
TR1	4.980	31	.001	1.000	.59	1.41
TR2	12.938	31	.001	1.406	1.18	1.63
TR3	1.877	31	.070	.438	-.04	.91
SC1	6.731	31	.001	1.188	.83	1.55
SC2	7.215	31	.001	1.188	.85	1.52
SC3	7.440	31	.001	1.250	.91	1.59
PR1	11.811	31	.001	1.500	1.24	1.76
PR2	6.960	31	.001	1.250	.88	1.62
PR3	1.815	31	.079	.406	-.05	.86
SS1	11.392	31	.001	1.156	.95	1.36
SS2	9.659	31	.001	1.094	.86	1.32
SS3	9.658	31	.001	1.156	.91	1.40
SS4	5.568	31	.001	1.000	.63	1.37
CE1	10.718	31	.001	1.313	1.06	1.56
CE2	12.535	31	.001	1.313	1.10	1.53
AS1	9.105	31	.001	1.188	.92	1.45
AS2	13.939	31	.001	1.344	1.15	1.54
AS3	12.636	31	.001	1.344	1.13	1.56
SSI1	7.400	31	.001	1.156	.84	1.47
SSI2	10.849	31	.001	1.344	1.09	1.60
SSI3	12.938	31	.001	1.406	1.18	1.63
CS1	9.698	31	.001	1.188	.94	1.44
CS2	8.399	31	.001	1.063	.80	1.32
SLA1	8.395	31	.001	1.031	.78	1.28
SLA2	8.036	31	.001	1.250	.93	1.57
RC1	7.874	31	.001	1.000	.74	1.26
RC2	7.407	31	.001	.969	.70	1.24