IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 27, 2019, accepted September 11, 2019, date of publication September 19, 2019, date of current version October 2, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2942424

Determining Factors Pertaining to Cloud Security Adoption Framework in Government Organizations: An Exploratory Study

MADINI O. ALASSAFI[1], RAYED ALGHAMDI[1], ABDULRAHMAN ALSHDADI[2], ABDULWAHID AL ABDULWAHID[3], AND SHEIKH TAHIR BAKHSH[1]

[1]Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589 , Saudi Arabia
[2]Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah 21577, Saudi Arabia
[3]Computer Science and Engineering Department, Jubail University College, Royal Commission for Jubail and Yanbu, Jubail Industrial 30031, Saudi Arabia

Corresponding author: Rayed AlGhamdi (raalghamdi8@kau.edu.sa)

This work was supported by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, under Grant DF-069-611-1441. The authors, therefore, gratefully acknowledge DSR technical and financial support.

ABSTRACT In wealthy developing countries like the Kingdom of Saudi Arabia (KSA), the adoption of cloud computing is progressing slowly compared to the developed countries. To accelerate the cloud computing adoption, this study takes place exploring and investigating the associated security factors with cloud computing that influence organisations' desire for adopting the services of cloud computing. This exploratory study has been conducted through two steps: (1) develop a framework based on security factors discussed in related studies and (2) validate the security factors' relationships within the developed security framework. In the validation study, an instrument was distributed to 217 IT experts in different Saudi government organisations. Correlation analysis is used to explore the relationship(s) among items and factors. The results suggested that the security factors were significantly correlated with each other. The internal consistency reliability analysis results were great. Worthy Cronbach's alpha results also indicated that the items used to measure each factor were independent measures, which are positivity correlated with one another. The key findings of the exploratory factor analysis revealed three main components named as security benefits, security risks, and security awareness. Overall, the implications of this exploratory study provide a significant contribution towards cloud adoption in Saudi organisations. The outcomes of this study will serve as valuable information for policymakers, practitioners, and researchers.

INDEX TERMS Cloud computing, adoption, security factors, Saudi government organisations.

I. INTRODUCTION

There have been traditionally six different stages of the development of computers as illustrated in Fig. 1 [1]. The first stage was mainframe computingwhen a number of users shared a CPU using a number of terminals. The second stage was personal computing (PC) when every user used their own stand-alone PC. While in stage three, personal computers are together in a local area network. The fourth stage was the Internet, a network of networks. In the fifth stage of computing movements, several high-performance computing resources collaborate for a particular purpose; this stage is grid computing. Cloud computing is considered the sixth stage, which is the development of computing resources on the Internet as services [2].

Cloud computing is a developing paradigm and involves the distribution of Internet-based IT services to its users as a utility service [3]. One of the biggest cloud computing advantage is that it dynamically allows the on-demand use of computing resources to many users in multiple locations at any time. Governments across the world are dynamiclly shifting to cloud computing in order to achieve higher efficiency. It must also be stated that cloud adoption is considered by organisations to be an IT solution that can be used to reduce costs and recognize the scalability of data capabilities [4]. Moreover, cloud adoption may satisfy an agencyneeds for IT to varying degrees, depending on the depth of adoption. It is clear that today's ever-growing computing environment is shifting towards cloud services. According to some cloud

The associate editor coordinating the review of this manuscript and approving it for publication was Kaitai Liang.

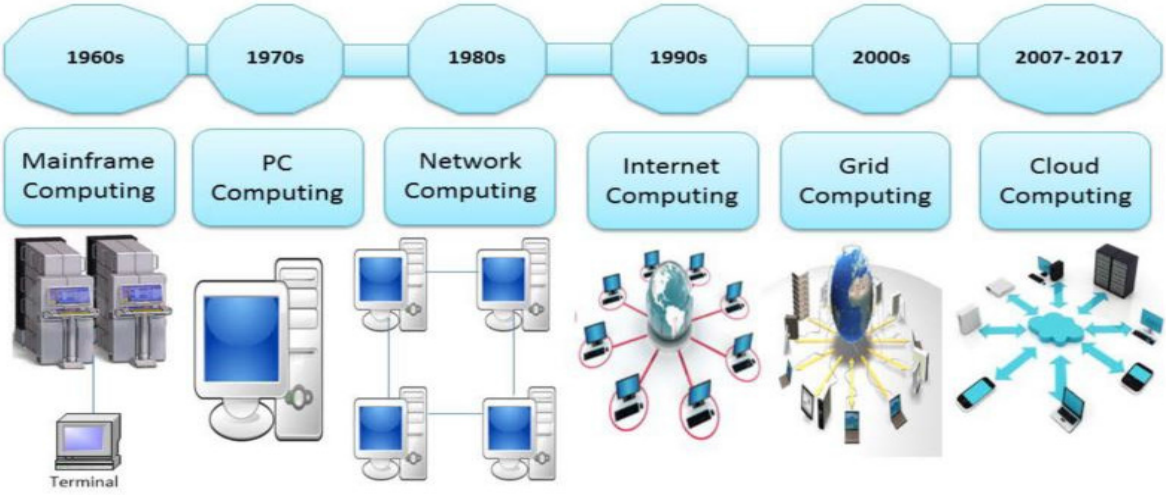

FIGURE 1. Computing paradigm developments (1960 - 2017).

adoption studies, the main appeals of using the cloud are falling IT costs as a result of collective productivity, availability, reliability, and flexibility, as well as reduced response times [5].

Despite the advantages of cloud computing, adopting and integrating its services with the existing traditional systems may raise several obstacles. These challenges may occur in different domains including legislation, management strategy, and technology aspects. Security related factors are the most significant challenge [6]. This main concern has hindered the adoption progress of the cloud computing services by government organisations worldwide. However, government organisations in developed countries have started to migrate to cloud services or in the process to set up cloud roadmap initiatives. By contrast, developing countries still relatively lagging behind [5], [7]. Therefore, a project to investigate the slowness of cloud computing adoption by government organisations in Saudi Arabia has taken place. The project has gone throgh several steps to develop a security factors framework. The current paper reports the exploration and confirmation of the security factors framework [3], [8]. The framework comprises three categorical domains: Security benefit factors, Security social factors, and Security risk factors.

II. LITERATURE REVIEW

In this section, existing related work and approaches to security in cloud computing will be discussed and summarized. When deciding whether to use cloud-based systems, the majority of Saudi government organisations place primary emphasis on their own custom needs [5]. Like other innovations, acceptance and use of cloud computing should be carefully studied. Adopting cloud computing services by organisations may be hindered due to the security issues. Security has been identified as the main challenge for organisations to adopt cloud computing in their organisations. It has been ranked in the top list concerning organizations to adopt such technology [9].

Zhou *et al.* [10] analyzed the hindrances that challenge users' decisions to use cloud computing systems. However, they encountered a lack of evidence related to the security risks and benefits tailored to the user side. Paquette *et al.* [11] tested the cloud adoption level, its usages by governments, and the tangible and intangible risks associated with the usages. With this said, however, the authors did not address security risks and benefits. The literature showed that security in cloud adoption in Saudi Arabia is limited, especially in government organisations. This work identified an important gap in the literature. The gap relates to security issues and their effects on the adoption of cloud computing. Hence, this study sought to investigate the security risks, as well as the security awareness and benefits factors influencing the cloud computing adoption by Saudi government organisations.

Che *et al.* [12] investigated the cloud computing security risks. However, this investigation focused on security strategies. Moreover, Sun *et al.* [13] placed emphasis on the issues of privacy, security and trust in cloud computing environments. The study guided the users to identify the all the perspective threats when using such technology. It failed, however, to provide an empirical evidence.

Along similar lines, both Alsanea and Barth [7] and Alkhater et al. [14] investigated the factors of management, technology and environment that affect cloud computing adoption in the Saudi Arabian environment. Nevertheless, they did not address the security risks or provide an in-depth analysis of said risks.

Furthermore, Subashini and Kavitha [15] suggested a few security elements related to cloud computing and its vital role as an integral part of the SaaS development and deployment process. However, the researchers failed to address the security risks, benefits and social related factors.

TABLE 1. Summary of the reviewed related work.

Study	Type of Contribution	Security	Saudi Context	Evaluation
[7]	TOE Model	NO	Yes	This study only examined a range of factors affecting cloud computing adoption by governments in general. It failed to consider the security risks.
[10]	Identified factors	NO	NO	This study explored the security and privacy concerns resulting from a certain degree of cloud computing use.
[11]	Identified factors	NO	NO	This study identified different issues which arise when government organisations utilise cloud computing.
[12]	Identified factors	Yes	NO	This study proposed strategies and security models that can be utilised to address existing security issues.
[13]	Identified factors	NO	NO	The security risk classification was not considered.
[14]	Identified factors by using models	NO	Yes	This study investigated factors that impact on orgnaisation's decision. The security risks and benefits classifications were not considered.
[15]	Identified factors	NO	NO	This study conducted an investigation into cloud computing security issues linked to the cloud computing service delivery model (SPI model). The sole focus was on the SaaS model, and so the risks were not addressed.
[16]	Identified factors	NO	NO	This study offered a framework to evaluate the costs of using IT infrastructure in the cloud but did not reflect the feature of security.
[17]	Combined TOE framework and TAM model	NO	NO	This study combined the TOE framework and the TAM model to identify organisational, technological and environmental factors that have a direct influence on cloud computing adoption. It failed to consider the security factors.
[18]	Proposed extended UTAUT model	NO	Yes	This study revelaed that performance expectancy, trust and facilitating conditions influence users' intention to use cloud computing. This study did not focus on government organisations, while other security factors were also missing.
[19]	Developed a framework	NO	Yes	This study identified challenges and applications in Saudi SMEs. However, identification of the security factors based on an in-depth analysis were not found.

Klems *et al.* [16] suggested a framework with which to evaluate the cost risks of utilizing IT infrastructure based the cloud. They associated it with predictable IT methods, like a grid computing service or the cost of setting up in-house IT infrastructure. They considered the costs in their framework as indirect and direct costs.

IT infrastructure resources are a sample of direct costs, while an indirect cost is suffered due to failure to come across business aims and nominate training courses with the new technology. However, their work was in the development stage, and consequently the outcomes are not provided. In addition, their study did not consider the aspect of security as part of the cloud implementation framework.

Gangwar *et al.* [17] combined the TOE framework and the TAM model to identify organizational, technological and environmental factors that have a direct influence on cloud computing adoption at the organization level. However, this study did not include any factors related to security.

Alharbi [18] proposed an extended UTAUT model to investigate the factors that influence users' intention to employ cloud services. Adding trust factor seemed the major extension of the UTAUT. There are other security factors that were not covered in this study. Furthermore, the study did not studied the intention to employ cloud services at government organisations level.

Alturki [19] proposed a conceptual framework for Small and Medium Enterprises (SMEs) to adopt and use cloud computing systems. The framework included the identification of challenges and applications in the Saudi Arabian environment. However, this research failed to provide in-depth analysis that lead to identify the security factors.

After reviewing the previous studies, it is clear, to the best knowledge of the researcher, that no formal studies have examined the security factors that influence the Saudi government organisations to adopt cloud computing systems. The current study therefore contributes in narroeing this gap. An investigation and in-depth analysis is carried out to explore how government organisations in Saudi Arabia are influenced to adopt cloud computing. The investigation covers studying the security risks, social aspects, and benefits factors. It begins with a review of the literature, the purpose of which is to paint a comprehensive picture of cloud adoption security-related factors in the global context. Following this, the synthesized factors based on the literature survey are confirmed by conducting interviews and surveys with security experts and specialists working in government organisations in KSA. The summaries and reviews of the work related to this research are presented in Table I.

As consequence, the following research questions are going to be answered:

RQ: What is a suitable instrument with which to evaluate security factors in the cloud adoption framework and how can the instrument be validated?

RQ: What are the relationship(s) among the security factors identified from applying the exploratory factor analysis technique?

III. METHODOLOGY

This research involved two stages of model building: an exploratory stage, and a confirmatory stage. During the exploratory stage, Exploratory Factor Analysis (EFA) was applied in order to propose an initial model, while Confirmatory Factor Analysis (using Structural Equation Modelling) was used to validate and confirm the initial model in the confirmatory stage.

EFA is a data-driven approach that is used as a technique for relationships identifications among variables [20]. It is usually employed to discover a possible underlying factor structure of observed factors set. Subsequently, the procedures of factor analysis can be applied through the following processes [21]–[23]:

- Identifying objectives of factor analysis.
- Designing a factor analysis.
- Identifying assumptions in factor analysis.
- Deriving factors and assessing overall fit.
- Interpreting the factors.
- Validating factor analysis.

The factor analysis technique seeks to determine the substantial constructs or sets which is assumed to underlie the original variables [22]. Factor analysis is conducted to identify the dimensions and significance of variables. It summarizes the relationships between datasets and groups these variables accordingly. Moreover, factor analysis is also employed to minimize large sets of variables into smaller sets of underlying variables, which are referred to as a factor or category. Reference [22] summarized the main purpose of using factor analysis, as can be seen below:

- To identify underlying dimensions called factors, which describe the correlations among sets of variables.
- To assess factors which influence responses to observed variables.
- To achieve data reduction and scale development.

EFA is vital when it comes to defining underlying constructs for a set of measured variables. Another alternative in terms of identifying the appropriateness of the data for factor analysis is to examine the strength of inter-correlations among the variables. Factor analysis should not proceed with variables that correlate very highly with other variables [24]. There are certain issues which must be taken into consideration when defining the appropriateness of the data: the sample size, data screening, and the strength of the relationships between the variables (Kaiser-Meyer-Olkin (KMO) measure), interpretation correlation, factor extraction, factor rotation, and the analysis of the factors.

During the exploratory stage, exploratory factor analysis was used to examine the factors, propose the hypotheses, and build and confirm the initial model. This stage was followed by Confirmatory Factor Analysis (CFA) to evaluate the extent to which the model fits the data. This was achieved by using Structural Equation Modelling.

In factor analysis, 'factor extraction' involves defining the lowest number of factors (or categories) that can explain the interrelations of all the sets of variables. There are various approaches which can be used to extract the factors, e.g. Principal Component Analysis (PCA), principal axis factoring, and maximum likelihood factoring [22], [23].

In this research, during the first stage of model building, no prior relationship was assumed, and the model was built from scratch. As such, it was decided that principal component analysis (PCA) was more appropriate to use than factor analysis, in which relationships are assumed [25].

In addition, among the advantages of PCA is the fact that it determines the total variance and can provide an explanation for the maximum portion of the overall variance characterized in the original set of variables in SPSS [15], [27].

Therefore, to conclude how many factors (or components) are extracted, eigenvalues (Kaiser's criterion) and scree plot are two information sets that can be referred to [28].

Both methods were considered in this research, and the analysis process comprised of two stages: a preliminary stage and a final stage. In the preliminary stage, only factors (or components) with eigenvalues above 1 were extracted. The scree plot test from this preliminary stage was used to decide on the correct number of factors (or components) to extract. Following this, in the final stage, the whole analysis was rerun with the chosen number of factors (or components) from the preliminary stage.

A. INSTRUMENT DEVELOPMENT AND VALIDATION

A survey instrument was used for collecting data. The more attention paid to the development of the research instrument, the easier it is to ensure that the research is valid [11], [29], [30]. The literature was reviewed in order to develop the survey statements. These statements related to security factors that affect government organisations to adopt cloud computing. The survey aims to collect data in order to evaluate the security cloud adoption factors [3]. The main part of the survey consists of twenty constructs. Each construct is measured using a number of measurment items, a total of 67 items. These items test the extent to which the respondents agree with the effect of the security-related factors. They were evaluated using a five-point Likert scale ranging from 1 (strongly agree) to 5 (strongly disagree). Table II illustrates the model constructs, measurement items, and the sources from which these items were derived.

After finalizing the designing of the survey, reliability and validity tests were conducted. Conducting reliability and validity tests are critical to get accurate results [32], [42]. These tests were conducted using pre-test and content validity techniques. In the present research, validity was tested beforehand and afterward of the data collection, and reliability was evaluated at the time of data collection.

B. INSTRUMENT PRE-TEST

Three computer science academics and four IT security experts pre-tested the instrument. The provided feedback was sought to verify content validity. The purpose of the pre-testing is to satisfy the requirement of clarity and

TABLE 2. The model constructs and measurement items.

Construct	Code	Number of Items	Sources
Insecure Interfaces	II	3 items	[29], [31], [32]
Shared Technology	ST	3 items	[29], [31], [33]
Account or Service Hijacking	AH	4 items	[11], [29], [32]
Malicious Insiders Risks	MI	3 items	[29], [31], [32]
Failure to Comply with Regulations	CR	4 items	[29], [34], [35]
Data Ownership	DO	5 items	[29], [31], [32]
Service and Data Integration	SDI	3 items	[29], [34], [35]
Data Leakage	DL	4 items	[11], [29], [32]
Failure of Client-side Encryption	CSE	3 items	Authors contribution through Experts' review
Trust	TR	3 items	[11], [36], [37], [38]
Security Culture	SC	3 items	Authors contribution through Experts' review
Privacy	PR	3 items	[39], [40], [41]
Smart Scalable Security Benefits	SS	4 items	[29], [34]
Cutting-edge Cloud Security Marketing	CE	3 items	[29], [33]
Advance Security Mechanism	AS	3 items	[29], [33]. [32]
Standardised Security Interfaces	SSI	4 items	[29], [33]
Cloud Security Auditing	CS	3 items	[29], [33], [32]
Service Level Agreement (SLA) Audit Enforcement	SLA	3 items	[29], [34]
Resource Concentration	RC	3 items	[29], [33]
Decision to Adopt the Cloud	DAC	4 items	Authors contribution through Experts' review
Total: 20 Constructs		67 Items	

understandability [32], [41]. The pre-test aimed to ensure that (1) measurement items are applicable and sufficient in examining the under-investigation concept, (2) questions' wording, response format, guidelines, instrument size, and layout are suitable, and (3) the survey structure is easy to read and understandable.

The participants of the pre-test provided a number of comments, and the questions were edited according to the said comments. The changes made to the original survey instrument included: selecting a sufficient items number to represent a factor, adopting player-suitable terms, and using a layout that is easy to read and distribute during the experiment. The pre-test demonstrated that the survey design is suitable to investigate the study topic.

C. CONTENT VALIDITY OF THE INSTRUMENT

Content validity is to ensure how perfectly the instrument demonstrates the measurement items. This kind of validity depends on the understanding of specialists, and on the specific content filed [43]. Reference [35] recommended that using statements which have been validated in the literature is essential if they are available. However, in this research, the statements from the literature were adopted and improved to suit the existing research objectives. Two recommended steps of content validity were used in order to validate the instrument's content: (1) the development and (2) the judgment quantification [45]. The development stage starts with measuring the aim of the instrument and identifying the full content scope. This stage can be achieved through the use of a literature review and by consulting the views of experts. The second stage is judgment quantification, which comprises two conceptions: the content of all items displayed is valid, and the content of the developed instrument is valid for the research objective. Reference [45] recommended that a minimum number of five experts ought to be used; however, this number may depend on the availability of such experts.

Seven experts were requested to assess the content of the instrument. A printed copy of the questionnaire, as well as a brief background of the research, was sent to them. Some changes in the measurement items were recommended to improve the survey. For further enhancement of the content validity, the experts were asked separately to comment and give feedback. The first step of judgment quantification involved a two-hour meeting with three researchers. Each expert answered the questions and responded to each statement. Following this, the instrument new version was ready to be shown to the next four security experts. In the following judgment quantification step, it was managed using the same procedure; this involved an online face-to-face Skype video meeting with Saudi security experts. The modifications to the questions were improved. Overall, 67 measurement items were reformulated.

The validation process aimed to explore the relationship between all factors and items. The improved instrument version was distributed to a number of participants, and their responses were analyzed to establish the instrument's reliability. Statisticians have stated that a sample size of 30 is adequate, as this is the value put forth in the Central Limit Theorem [26]. A total of 30 security experts participated in the research. The goal was for the respondents to state that the survey is clear and understandable.

D. DATA COLLECTION AND ANALYSIS

The selected survey respondents to the questionnaire were the IT and security experts who work in Saudi government organisations. These experts were deemed particularly suitable

given their ability to gauge the existing conditions of information technology in their organisations. All the selected participants work in different IT departments with a minimum of two years of experience in the security or cloud fields in their organisations. These organisations include the Saudi Food and Drug Authority, the Ministry of Education, the Ministry of Health, the Ministry of Labor Saudi, the Saudi Interior, and King Abdul-Aziz University.

With regard to the selection of respondents, the questionnaire was distributed online in two ways. Invitations were first sent by email to experts and certain specialists who met the requirements. Second, the link to the questionnaire was shared on Twitter and Facebook with the Saudi experts' security groups. For some organisations, authorisation had to be obtained in person at first to identify the person in charge and email him/her the participation link. The identified number of participants who had the ability to access the participation link was 226; Six cases were found Incomplete and three others were randomly answered. Therefore, the total number of the valid responses was 217.

After collecting the responses, they were made ready for analysis. SPSS software was utilised to analyse the quantitative data, while Vivo software helped the researcher to analyse the interview findings. Exploratory and confirmatory factor analyses were conducted. This results to develop a model. The initial step of factor analysis together with various statistical techniques is to address the research questions. The common goal of the factor analysis technique is to identify and summarize the information derived from a number of variables in newer multi-dimensions or various factors with a low level of information. Factor analysis is conducted to identify the dimensions and variables significance. It summarizes the relationships between datasets and groups these variables accordingly. Moreover, factor analysis is also employed to minimise large sets of variables into smaller sets of underlying variables, which are referred to as a factor or category.

IV. RESULT

The demographic profile was collected using five questions. Demographic analysis of the respondents and their organisations is presented in Table III. All respondents have involved in IT/security projects. Seventy percent of the participants have used cloud computing services at their organisation. However, almost 37% of the respondents mentioned that their organisations to some extent adopt cloud computing services at present. When requesting further informtion for the type of adopted services, they mention using services such as the google forms, docs and sheets, and Dropbox. These types of services are called as IaaS (Infrastructure as a Service) and SaaS (Software as a Service) [1], [15], [33]. The vast majority (84%) of the respondents agreed that security issues significantly affected the decision of cloud computing adoption by their organisations. The respondents' level of experience in the IT/security project field is as follows. Twenty-eight percent (28%) have had 6–10 years' experience, 36% of participants have had 3–5 years' experience, 18% of the respondent have had more than 10 years' experience, and the rest (18%) have had 2 years' experience. The results of the demographic analysis showed that more than 60% of organisations used the cloud, but more than 84% of them have concern about security, which strongly affected their decisions to adopt the cloud computing services.

TABLE 3. The demographic data of the participants' responses.

Item	Answers	Frequency	Percentage
Involved working in IT/security projects in a Saudi organisation	Yes	215	100%
	No	0	0%
Used cloud services at the organisation	Yes	151	70%
	No	64	30%
Could services adoption by the organisation	Yes	80	37%
	No	135	63%
Do you think security affects your organisation's decision to adopt the cloud?	Yes	181	84.%
	No	34	16%
Years of experience in the IT/security field	2 years	38	18%
	3–5 Years	77	36%
	6–10 Years	61	28%
	10+ years	39	18%

A. THREATS TO VALIDITY

The proposed system has considered various factors that affect the adaption of cloud computing in an organization. The impact of cause-and-effect relationship needs to be validated for whether the changes in the independent variables caused the observed changes in the dependent variable. Such a study is called as internal validity. Also, whether the results of this study could be generalized for other organizations is studied under the umbrella of external validity. Both internal and external validity are part of threats to validity.

The impact among independent variables has been studied using correlation analysis. The strength of relationship among various factors is described in Table VII. Among various threats to internal validity, authors considered: Selection, Experimental Mortality and Instrumentation Validity. One important factor, selection of subjects or participants in the survey was taken care, by choosing people with adequate expertise in the area of research. Another factor, experimental mortality, when applied to our study stands good as all those who participated in the survey completed the survey completely.

Among the threats to external validity, authors considered the Population Validity. With focus on Saudi Arabia, the study is restricted to organizations in Saudi Arabia. All the participants involved in the study are from Saudi Arabia and have strong correlation to the problem concerned.

1) INSTRUMENT VALIDITY

The validity of a measurement model is gauged based on the requirements of three validity types: content, convergent, and discriminant validities.

TABLE 4. Content validity ratio among items of the instrument.

Construct	items	Significant Items	CVR					
			item 1	item 2	item 3	item 4	item 5	Average
II	3 items	3 items	0.7	1.00	1.00	-	-	0.90
ST	3 items	3 items	0.7	1.00	0.7	-	-	0.81
AH	4 items	3 items	0.7	1.00	0.7	0.4	-	0.71
MI	3 items	3 items	0.7	0.7	0.7	-	-	0.71
CR	4 items	3 items	1.00	1.00	0.7	0.1	-	0.90
DO	5 items	4 items	0.7	1.00	1.00	1.00	0.1	0.77
SDI	3 items	3 items	0.7	0.7	0.7	-	-	0.71
DL	4 items	3 items	1.00	1.00	1.00	0.4	-	0.86
CSE	3 items	3 items	0.7	1.00	0.7	-	-	0.81
TR	3 items	3 items	0.7	0.7	1.00	-	-	0.81
SC	3 items	3 items	1.00	1.00	0.7	-	-	0.90
PR	3 items	3 items	0.7	0.7	0.7	-	-	0.71
SS	4 items	3 items	1.00	0.7	0.7	0.1	0.4	0.64
CE	3 items	3 items	0.7	0.7	1.00	-	-	0.81
AS	3 items	3 items	1.00	1.00	0.7	-	-	0.90
SSI	4 items	3 items	1.00	0.7	0.7	0.1	-	0.64
CS	3 items	3 items	0.7	0.7	1.00	-	-	0.90
SLA	3 items	3 items	1.00	0.7	0.7	-	-	0.81
RC	3 items	3 items	0.7	0.7	0.7	-	-	0.71
DAC	4 items	4 items	0.7	1.00	0.7	1.00	-	0.86
Total	67	62						

To assess the content validity, the content validity ratio (CVR) was utilised. CVR is a quantitative method used to establish the validity of the content. With the quantitative content validity method, confidence is kept in selecting the most significant and accurate content in an instrument, which is measured using the CVR [46]. The thoughts of the seven experts who participated in the judgment quantification was deployed at this stage. The statistical significance level for each factor was also assessed as recommended by reference [47]. In this way, the experts are demanded to identify whether an item is essential for operating a concept in a set of items. The items deemed 'Essential' by the experts were calculated, as presented in Table IV. The evaluation criteria of the items/scale were as follows:

- **Essential:** The question is necessary to define the security factors in cloud computing adoption. It must be involved and, if not involved, would affect the factors negatively.
- **Useful but not essential:**The question may be valuable but NOT necessary to define the factors in cloud computing adoption.
- **Not Necessary:**The question is NOT obligatory in terms of defining the cloud computing adoption security factors. It does NOT need to be involved, and if involved, would NOT affect the factors.

Consequently, the experts' responses were gathered, and the items which the experts deemed 'Essential' were calculated using CVR formula in Equation1:

$$CVR = (N_e - N/2)/(N/2) \quad (1)$$

where *Ne* is the experts' number that deemed the item to be 'essential', and *N* is the total participated experts' number.

To consider CVR significant, the agreement level among experts had to be more than 50%. It provides some guarantee of content validity [31], [46]. The results showed that, 62 out of 67 items were found statistically significant at the range of more than 0.50. The items which were found insignificant (with a CVR value lower than 0.50) were removed. Consequently, this CVR identified that the security items of the cloud computing adoption framework had acceptable content validity, thus meaning that the items are capable of measuring the model being studied [46].

After completing the previous step for the content validity, the second convergent validity need to be achieved. Thirty (30) security experts were called for participation in this research. Slight modifications to the instrument final version were made upon receiving the feedback. To achieve the convergent validity, factor loadings must be significant from the statistical point of view and the value must be 0.5 or more. The top value is 0.7, as the square of consistent factor loading signifies how much variation in an item is clarified by the latent factor. Moreover, the Average Variance Extracted (AVE) could also prove this validity, as presented in Table V. AVE is one of the collective approaches used for assessing convergent validity. It proved that all the 62 observed items satisfied convergent validity test.

The third validity type is discriminant valid it. Table V illustrates the discriminant validity results. Discriminant validity happens when the measurement model does not have redundant items. The other requirement for discriminant validity is that the correlation between constructs should be lower than 0.85 [48]. Other than that, the square root of AVE for the construct must be bigger than the correlation concerning the corresponding constructs. Table VI clearly shows that the values of the AVE square-root of every latent

TABLE 5. The analysis of convergent validity.

Components	Constructs	Observed Items	Estimate	Error Variance	Squared Correlations
SB	TR	TR1,TR2,TR3	.790	0.108	0.623
	CR	CR1,CR2,CR3	.827	0.091	0.683
	CE	CE1,CE2,CE3	.859	0.115	0.737
	AS	AS1,AS2,AS3	.898	0.07	0.806
	CS	CS1,CS2,CS3	.886	0.091	0.784
	SLA	SLA1,SLA2,SLA3	.932	0.046	0.868
	SSI	SSI1,SSI2,SSI3	.900	0.07	0.811
	RC	RC1,RC2,RC3	.892	0.084	0.796
	SS	SS1,SS2,SS3, SS4	.941	0.053	0.821
SR	CSE	CSE1,CSE2CSE3	.870	0.072	0.756
	MI	MI1,MI2,MI3	.658	0.055	0.434
	SDI	SDI1,SDI2,SDI3	.832	0.044	0.692
	DO	DO1,DO2,DO3	.841	0.057	0.708
	II	II1,II2,II3	.609	0.082	0.371
	ST	ST1,ST2,ST3	.694	0.061	0.481
	SC	SC1,SC2,SC3	.723	0.094	0.522
SA	PR	PR1,PR2,PR3	.715	0.09	0.511
	AH	AH1,AH2,AH3	.753	0.064	0.567
	DL	DL2,DL2,DL3	.538	0.094	0.289
	DAC	DAC1,DAC2,DAC3,DAC4	.640	0.038	.648
$AVE = \frac{\sum_{i=1}^{n} L_i^2}{n}$		**SB AVE**	**SR AVE**	**SA AVE**	
		0.73	**0.57**	**0.55**	
** Value > 0.5					
Notes: (SR) Security Risks, (SB) Security Benefits, (SA) Security Awareness					

TABLE 6. Analysis of the discriminant validity.

	CR	AVE	MSV	Max R(H)	SR	SB	SA
SR	0.900	0.567	0.445	0.918	**0.753**		
SB	0.961	0.736	0.373	0.979	0.611	**0.848**	
SA	0.733	0.555	0.445	0.981	0.667	0.433	**0.696**

Discriminant Validity: Compare the squared correlations and AVE scores for each of the pairwise constructs
Notes: SR Security Risks, SB Security Benefits, SA Security Awareness

construct was greater than the correlation between these constructs. Therefore, the results presented acceptable confirmation regarding the latent constructs' discriminant validity.

B. CORRELATION ANALYSIS

Correlation analysis is used to understand the relationship between factors and can be used to define the strengths and direction of a linear relationship between two variables. Moreover, correlations analysis displays the value of the correlation coefficient. This can be ranged from -1 to $+1$, and the sign delivers the direction of the relationship; all produce a statistic that ranges from -1.00, indicating a perfect negative correlation, to $+1$, indicating a good positive correlation. A value of 0 specifies no correlation at all. Reference [48] alluded to the strength of the coefficient correlation value. In this study, Pearson's correlation coefficient method was used, and the guidelines below were followed in the correlation analysis.

The correlation matrix, Table VII, displays the strength of the relationship among factors in this section. As an example, Correlation of Insecure Interfaces (II) is statistically significant and correlated with Shared Technology (ST), $r(30) = .646$ and Service and data integration (SDI) $r(30) = .467$, (both $p<0.01$).

C. FACTOR EXTRACTION SUMMARIZING VARIABLES

This section describes the results of the factor extraction in EFA. It includes the theoretical aspects related to factor extraction, including its uses and options. As such, in this analysis, principal component analysis (PCA) was deemed more appropriate for use than factor analysis. This is because, with the latter, relationships are assumed appropriate to sums up most of the variance of original information in a lower limit number of factors predictions. To define the number of components that should be extracted, two methods were used in this analysis: Kaiser's criterion (using eigenvalues > 1) and scree plot investigation.

1) THE FIRST METHOD, KAISER'S CRITERIO

The first method, Kaiser's criterion was put forth by Guttman and amended by Kaiser; it considers factors with an eigenvalue greater than 1.00 as common factors. The eigenvalue of a factor signifies the total variance amount described by

TABLE 7. Correlation matrix among security factors.

Inter-Item Correlation Matrix																				
Construct	**II**	**ST**	**AH**	**IMI**	**CR**	**DO**	**SDI**	**DL**	**CSE**	**TR**	**SC**	**IPR**	**SS**	**CE**	**AS**	**SSI**	**SC**	**SLA**	**RC**	**DAC**
II	1	.646	.160	.348	.228	.076	.467	.216	.135	-.054	.067	.272	.020	.011	.171	-.146	0.249	0.064	0.053	.552**
ST		1	.335	.296	.435*	.200	.446*	.186	.433*	.083	.119	.355	.081	.168	.169	.063	-.152	.054	.104	.411*
AH			1	.189	.214	.630**	.484**	.493**	.706**	.419*	.479**	.571**	.395*	.329	.420*	.441*	.259	.346	.299	.319*
IMI				1	.112	.212	.366*	.234	.190	-.068	-.049	.216	.095	.000	.144	.086	-.142	-.123	-.049	.576**
CR					1	.425*	.464**	.402*	.398*	.425*	.188	.290	.527**	.306	.590**	.430*	.313	.414*	.270	.587**
DO						1	.510**	.648**	.505**	.358	.470**	.384*	.426*	.217	.376*	.348	.273	.296	.192	.494*
SDI							1	.540**	.506**	.213	.420*	.517**	.365*	.371*	.377*	.334	.169	.213	.199	.527**
DL								1	.259	.595**	.491**	.552**	.427*	.187	.609**	.462*	.213	.487**	.306	.678**
CSE									1	.405*	.307	.280	.428*	.346	.319	.428*	.139	.359	.335	.598**
TR										1	.281	.251	.497**	.339	.662**	.679**	.267	.728**	.568**	.301*
CS											1	.212	.349	.347	.390*	.497**	.448*	.467**	.308	.431*
IPR												1	.129	.049	.746**	.252	.113	.193	.105	.493*
SS													1	.592**	.494**	.753**	.654**	.790**	.793**	.701**
CE														1	1	.615**	.609**	.534**	.494**	.490**
AS																.781**	.456*	.741**	.572**	.468**
SSI																1	.569**	.847**	.726**	.515**
CS																	1	.578**	.510**	.460*
SLA																		1	.860**	.553**
RC																			1	.551**
DAC																				1
**. Correlation is significant at the 0.01 level (2 Tailed).																				
*. Correlation is significant at the 0.05 level (2-tailed).																				

that factor. Table VIII shows the initial eigenvalues from the factor analysis [24].

The Eigenvalues Total column shows the eigenvalue for each component. The Eigenvalues percentage of Variance column shows how much variance each factor explains, while the Eigenvalues Cumulative percentage column shows the variance amount accounted for by all previous factors added together. As demonstrated in Table VIII, components 1, 2 and 3 had eigenvalues greater than 1. Therefore, as per Kaiser's criterion, they were extracted.

2) THE SECOND METHOD, INVESTIGATION OF THE SCREE PLOT

The second method represents another way to define the number of factors which should be extracted from the final solution. This is a plot of the eigenvalues connected with each of the factors extracted, against each factor. In this method, visual inspection is performed, during which there is a careful examination of the intersection point between virtual vertical lines; this point connects the factors with another virtual horizontal line (in which the factors should be leveling out), thus connecting the remaining factors.

The factors to be extracted should lie to the left of this intersection point. When sample size is more than 200 to 250 participants, the scree plot offers a properly reliable criterion for factor selection [26]. Moreover, the scree plot technique from this preliminary is utilised to decide on the correct number of factors (or components) to be extracted. Many recommend retaining only components above the point, as presented in Fig. 2. It can be seen that there are three components to the left of the intersection point between the virtual vertical

TABLE 8. Eigenvalues and total of explained variance.

Component	Eigenvalues		
	Total	**% of Variance**	**Cumulative %**
1	**9.802**	**51.588**	**51.588**
2	**2.391**	**12.585**	**64.173**
3	**1.310**	**6.892**	**71.065**
4	.998	5.254	76.319
5	.859	4.516	80.835
6	.858	4.396	81.133
7	.680	3.581	84.415
8	.556	2.928	87.344
9	.521	2.742	90.085
10	.398	2.094	92.179
11	.311	1.639	93.818
12	.295	1.551	95.369
13	.180	.947	96.316
14	.160	.842	97.158
15	.136	.715	97.872
16	.107	.566	98.438
17	.098	.514	98.952
18	.081	.428	99.380
19	.067	.353	99.732
20	.051	.268	100.000

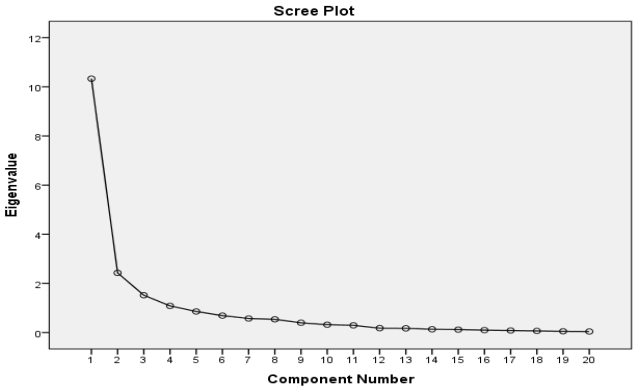

FIGURE 2. Factor extraction applied scree plot.

and horizontal lines. This suggests that the three components should be extracted. It should be noted that the results from the scree plot inspection are now always in line with Kaiser's criterion. Fortunately, this was the case in the present analysis, and thus there is more confidence in the results.

3) FACTOR ROTATION IMPROVING INTERPRETATION OF FACTORS

The results of the factor rotation are presented in this section. Factor rotation is a process used to examine the factor axes and thus gain a simpler and more significant solution [22] As suggested by Reference [25], both orthogonal and oblique rotations were used in this analysis, with the aim of finding the most interpretable solution. In addition, given the differences between the total eigenvalues of components 3, 4 and 5, as shown in Fig. 2.

The decision was taken to rerun the analysis for each of these components while rotating them once obliquely and again orthogonally. This means that a total of six runs were conducted. The solutions provided by using orthogonal rotation do not differ significantly from those provided by using oblique rotation, which is aligned with the literature [25]. However, these combinations made it possible to find the most interpretable solution, as orthogonal rotation was used, with three components extracted.

This solution was also found to support the theoretical framework suggested in the present research. In other words, although considered a form of exploratory analysis, EFA served as a validation tool for the framework. Table IX provides a summary of commonalities for all security factors and their correlated indicator.

The factor loading results showed that all variables had a loading value of 0.5 and above, thus indicating a good loading. A good loading, with the 200-sample size, needs to be more than 0.36 [23]. The next section presents the factor analysis results that were conducted after the factor extraction and rotation.

4) EXPLORATORY FACTOR ANALYSIS (EFA)

In this research, there were three considerations for assessing the suitability of data for EFA: the size of the sample,

TABLE 9. Factor loading (communalities) using orthogonal rotation.

Loaded Factors/ Components No	Variables	Code	Initial	Extraction
1	Failure to Comply with Regulations	CR	1.000	0.664
1	Trust	TR	1.000	0.632
1	Smart Scalable Security Benefits	SS	1.000	0.903
1	Cutting-edge Cloud Security Market	CE	1.000	0.802
1	Advanced Security Mechanism	AS	1.000	0.829
1	Standardised Security Interfaces	SSI	1.000	0.872
1	Cloud Security Auditing	CS	1.000	0.815
1	SLA Audit Enforcement	SLA	1.000	0.878
1	Resource Concentration	RC	1.000	0.829
1	Decision to Adopt the Cloud	DAC	1.000	0.862
2	Insecure Interfaces	II	1.000	0.505
2	Shared Technology	ST	1.000	0.602
2	Malicious Insiders	MI	1.000	0.595
2	Data Ownership	DO	1.000	0.710
2	Service and Data Integration	SDI	1.000	0.751
2	Failure of Client-side Encryption	CSE	1.000	0.770
2	Security Culture	SC	1.000	0.564
3	Account or Service Hijacking	AH	1.000	0.612
3	Data Leakage	DL	1.000	0.644
3	Privacy	PR	1.000	0.827
Extraction Methods: Principal Component Analysis				

TABLE 10. KMO test result.

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		**0.881**
Bartlett's Test of Sphericity	Approx. Chi-Square	4128.125
	Df	171
	Sig.	0.001

the relationships strength among the variables (using KMO), and the data screening. A sample size assessment must be conducted before running EFA, while KMO and data screening can be checked after running the analysis. Factor analysis helps to find the underlying factors that summarize a group of items. However, it is the researchers' role to interpret and label these factors. In order to select the items for this study, experts were requested to rate the significance of each item in the instrument.

One of the statistical measures that can identify the suitability of data is Kaiser-Meyer-Olkin (KMO). It uses a metric that ranges from 0 to 1. If the value is more than 0.5, then the correlations between the variables are acceptable and can be used to conduct factor analysis. A minimum KMO value for good factor analysis is 0.6 [25]. The KMO value for the sample collected in the current research is 0.881, which suggests that the factor analysis was suitable for this dataset, as demonstrated in Table X.

D. DATA SCREENING

It has been recommended to screen data prior using any statistical technique [25], [44]. One of the considerations in

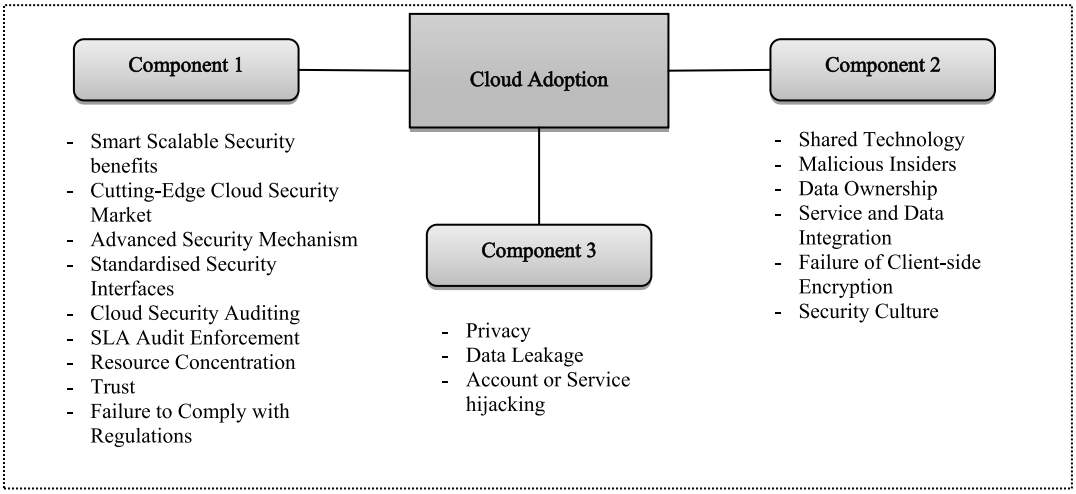

FIGURE 3. Components and constructs retrieved from the instrument.

data screening is checking for and handling missing variables. Fortunately, there were no missing variables in this analysis, and therefore no handling was needed. Another consideration, which is specific to EFA, is that variables should be reasonably correlated with each other. This can be checked by investigating the correlations. Fortunately, the correlation matrix showed that there were many correlations among variables which exceeded 0.3, thus suggesting that the dataset was suitable for EFA [23].

Principle Component Analysis (PCA) was used in the factor analysis. When it comes to choosing the number of components which should be extracted, different approaches exist. Two common approaches were considered in this research: Kaiser's criterion and scree plot inspection. In this study, 62 items relate to security in cloud computing adoption were inspected by practitioners working in different departments of Saudi government organisations. This solution was also found to support the theoretical framework suggested in the present research. In other words, although considered a form of exploratory analysis, EFA served as a validation tool for the framework. The factor loading results showed that all variables had a loading value of 0.5 and above, thus indicating a good loading; for 200 sample size of, the loading value should be more than 0.36 [25].

V. DISCUSSION

This section provides a discussion of the exploratory factor analysis findings of the exploratory factor analysis methods in the previous section. During the analysis, requesting only the factors that were introduced to the next level have values of 0.4 and higher for the factor loadings provided a significant value at the 0.01 level for each loading in the factor analysis. This significance value of the factor loading shows the essence of that component to the factor. Fig. 3 shows demonstrate the constructs retrieved from the instrument. In terms of identifying the factors or components, SPSS does not supplement the identifying or meaning of each factor or component.; in fact, SPSS only determines the grouping of variables. Therefore, it is up to the researcher to recognize the content of the loadings and their meaning regarding in alignment with the research goals.

In this factor analysis, the loaded factors were organized under three components. the components were clustered based on the questionnaire responses. In addition, it was still necessary to interpret the meanings of all the extracted components. The meanings of the components loaded on the factors are discussed as follows.

A. THE FIRST COMPONENT

The first component was loaded by nine indicators and showed the importance of security benefits in cloud computing, as agreed upon by the security experts in the government organisations. The highest loadings clarified the importance of the Smart Scalable Security Benefits factor in cloud computing adoption, which had a loaded value of 0.903. This factor is defined as the ability for extending security benefits. This was followed by the resource consideration factor, with a loading value of 0.829, which also shows the importance of security benefits in cloud computing when it comes to access control, comprehensive security policy, patch, and data management, and maintain processes.

The other indicators with high loading included Standardised security interfaces, Service Level Agreement (SLA) audit enforcement, Cloud security auditing, advanced security mechanisms, and Cutting-edge security market. This component was thought to refer to Cloud Adoption Security Benefits. Only two factors, namely Failure to Comply with Regulations, and Trust initially belonged to a different group but were regrouped after being rotated to this first component.

B. THE SECOND COMPONENT

The second component was loaded by eight indicators, and the result from the factor analysis revealed the importance of

cloud security risks when implementing the cloud adoption. The highest loading showed the importance of the decision to adopt the cloud factor, with a loading value of 0.862; this was followed by the client-side encryption factor, with a loading value of 0.770. Moreover, the Malicious Insiders factor had a high loading value of 0.595, thus indicating that all organisations must be sure that their own data is protected; this also shows the importance of these factors when deciding to adopt the cloud services.

This component also included Ownership of Data, Technology Sharing, Service and Data Integration, Insecure Interfaces and Security Cultures. Only one factor, namely security culture, belonged to a different component after the rotation. All these loadings are important when adopting cloud services and are best described as Cloud Adoption Security Risks.

C. THE THIRD COMPONENT

The three loadings described the fear of leaking data and the privacy of the organisation information; this fear related to the notion that, when personal information is accessed by third-party organisations, this may raise privacy concerns and affect the decision to adopt the cloud. The highest loading in this component was the privacy factor, with a loading value of 0.827; this was followed by the account hijacking factor, with a loading value of 0.612, and the data leakage factor, with a loading value of 0.644. These loadings are best described as Cloud Adoption Security Awareness.

Based on the eigenvalue rules through exploratory factor analysis, three components were extracted and retained for additional investigation. After the rotation was implemented, the factors that were loaded on these three components were interpreted and the meanings of the three components were defined. Two indicators of the total variance showed that it could belong to the first and third components. However, it was decided that it should be grouped in the first component because the factor loading was strongly explained in the first component. The analysis of the factors made it possible to summarize that a structure for data gained from the instrument was recognized; 62 items conducted and were gathered into 20 constructs.

VI. CONCLUSION

The biggest advantages of cloud computing are that it dynamically allows on-demand to use of computing resources to multiple users in multiple locations at any time. In addition, the users are entitled to make payment only for the services that they need. The aim of the current research is to investigate and develop a security cloud model by exploring several security factors relevant to cloud computing. The significant security factors related to various organisation and technology aspects were revealed. An in-depth exploration of these aspects led to identifying security factors that influence Saudi organisation to accept and use cloud computing services. The findings were based on the response of 217 of IT specialists and security experts in different departments of the Saudi government organisations. The collected data was analyzed through Exploratory Factor Analysis (EFA) to propose an initial model since no prior models exist in the literature. The presence of correlation among different variables involved justified the selection of EFA. The study provided the results of the data analysis conducted for the instrument design and validation process. The development process and the validation process of the instrument were presented, and the instrument was given consideration in order to define the accuracy of the outcomes that the researchers were attempting to measure. Based on the security cloud computing adoption framework, twenty factors have been explored, and sixty-two measurement items have been developed for more consideration. Thus, this research validates a model associated with the important factors that contribute to adopt/not adopt cloud computing in the Saudi government organisation context. The findings pertaining to the security factors in the framework were all derived from statements made by the experts and IT security specialists in the questionnaire. All experts agreed that security is the top priority in an organisation. If an organisation does not ensure that proper security is in place, then the services will not be reliable or acceptable to the users. The results of tests exposed that the instrument delivered an influence measurement of the developed variables. The outcomes presented that the factors had a direct influence on an organization's decision to adopt the cloud. In summation, it is supposed that the outcomes of this research can help decision makers, cloud providers and researchers in formulating reputable strategies which will encourage the adoption of cloud computing. The outcomes of this study can also enhance the above-mentioned parties' awareness and considerate of why some government organisations are implementing the cloud, while some are not.

REFERENCES

[1] L.-J. Zhang and Q. Zhou, "CCOA: Cloud computing open architecture," in *Proc. IEEE Int. Conf. Web Services*, Jul. 2009, pp. 607–616. doi: 10.1109/ICWS.2009.144.

[2] I. K. Azeemi, M. Lewis, and T. Tryfonas, "Migrating to the cloud: Lessons and limitations of 'Traditional' is success models," *Procedia Comput. Sci.*, vol. 16, pp. 737–746, Jan. 2013. doi: 10.1016/j.procs.2013.01.077.

[3] M. O. Alassafi, A. Alharthi, R. J. Walters, and G. B. Wills, "A framework for critical security factors that influence the decision of cloud adoption by Saudi government agencies," *Telematics Informat.*, vol. 34, no. 7, pp. 996–1010, Nov. 2017. doi: 10.1016/j.tele.2017.04.010.

[4] 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," *Telematics Inform.*, vol. 34, no. 2, pp. 664–678, May 2017. doi: 10.1016/j.tele.2016.10.008.

[5] A. Alharthi, F. Yahya, R. J. Walters, and G. Wills, "An overview of cloud services adoption challenges in higher education institutions," in *Proc. 2nd Int. Conf. Workshop Emerg. Softw. Service*, May 2015, pp. 102–109. doi: 10.5220/0005529701020109.

[6] M. O. Alassafi, H. F. Atlam, A. A. Alshdadi, A. I. Alzahrani, R. A. AlGhamdi, and S. M. Buhari, "A validation of security determinants model for cloud adoption in Saudi organisations' context," *Int. J. Inf. Technol.*, pp. 1–11, Aug. 2019. doi: 10.1007/s41870-019-00360-4.

[7] 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. Services*, vol. 3, pp. 1–16, Dec. 2014.

[8] M. Alassafi, A. Alharthi, A. Alenezi, R. Walters, and G. Wills, "Investigating the security factors in cloud computing adoption: Towards developing an integrated framework," *J. Internet Technol. Secured Trans. (JITST)*, vol. 5, no. 2, pp. 486–494, Jun. 2016.

[9] P. L. Bannerman, "Cloud computing adoption risks: State of play," in *Proc. IEEE 17th Asia–Pacific Softw. Eng. Conf. Cloud Workshop*, New York, NY, USA, 2010, pp. 10–16.

[10] M. Zhou, Y. Mu, W. Susilo, M. H. Au, and J. Yan, "Privacy-preserved access control for cloud computing," in *Proc. IEEE 10th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Nov. 2011, pp. 83–90.

[11] S. Paquette, P. T. Jaeger, and S. C. Wilson, "Identifying the security risks associated with governmental use of cloud computing," *Government Inf. Quart.*, vol. 27, no. 3, pp. 245–253, Jul. 2010. doi: 10.1016/j.giq.2010.01.002.

[12] J. Che, Y. Duan, T. Zhang, and J. Fan, "Study on the security models and strategies of cloud computing," in *Proc. Int. Conf. Power Electron. Eng. Appl.* vol. 23, 2011, pp. 586–593. doi: 10.1016/j.proeng.2011.11.2551.

[13] D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and analyzing security, privacy and trust issues in cloud computing environments," *Procedia Eng.*, vol. 15, pp. 2852–2856, Jan. 2011.

[14] N. Alkhater, G. Wills, and R. Walters, "Factors influencing an organisation's intention to adopt cloud computing in saudi arabia," in *Proc. IEEE 6th Int. Conf. Cloud Comput. Technol. Sci.*, Dec. 2015, pp. 1040–1044.

[15] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, Jan. 2011. doi: 10.1016/j.jnca.2010.07.006.

[16] M. Klems, A. Lenk, J. Nimis, S. Tai, and T. Sandholm, "What's inside the Cloud? An architectural map of the Cloud landscape," *IEEE Workshop Softw. Eng. Challenges Cloud Comput.*, May 2009, pp. 23–31.

[17] H. Gangwar, H. Date, and R. Ramaswamy, "Understanding determinants of cloud computing adoption using an integrated TAM-TOE model," *J. Enterprise Inf. Manage.*, vol. 28, pp. 107–130, Feb. 2015. doi: 10.1108/JEIM-08-2013-0065.

[18] S. T. Alharbi, "Trust and acceptance of cloud computing: A revised UTAUT model," in *Proc. Int. Conf. Comput. Sci. Comput. Intell., CSCI*, Mar. 2017, pp. 131–134. doi: 10.1109/CSCI.2014.107.

[19] S. M. Alturki, "Analysis and identification of cloud usage in private and public sector in saudi arabia," *Int. J. Comput. Appl.*, vol. 162, no. 4, pp. 17–21, 2017. doi: 10.5120/ijca2017913270.

[20] B. M. Byrne, *Structural Equation Modeling With AMOS: Basic Concepts, Applications, and Programming* Abingdon, U.K.: Routledge, 2016. doi: 10.4324/9781410600219.

[21] D. Child, *The Essentials of Factor Analysis*. London, U.K.: Cassell Educational, 1990.

[22] J. F. Hair, R. E. Anderson, R. L. Tatham, and W. C. Black, *Multivariate Data Analysis*, 7th ed. Upper Saddle River, NJ, USA: Prentice-Hall. doi: 10.1016/j.ijpharm.2011.02.019.

[23] D. D. Suhr, "Exploratory or confirmatory factor analysis," in *Proc. SAS Users Group Int. Conf.* Cary, NC, USA: SAS Institute, Inc., 2006, pp. 1–17.

[24] D. Child, *The Essentials of Factor Analysis*, 3rd ed. New York, NY, USA: Continuum International Publishing, 2006.

[25] B. G. Tabachnick and L. S. Fidell, *Using Multivariate Statistics*, 6th ed. New York, NY, USA: Harper Row, 2012. doi: 10.1037/022267.

[26] A. Field, *Discovering Statistics Using IBM SPSS Statistics*. London, U.K.: SAGE, 2017. doi: 10.1016/B978-012691360-6/50012-4.

[27] J. Pallant, *SPSS Survival Manual*. New York, NY, USA: McGraw-Hill, 2013.

[28] J. C. Nunnally, *Psychometric Theory*. New York, NY, USA: McGraw-Hill: 1978.

[29] *The Notorious Nine. Cloud Computing Top Threats in 2013 CSA*, Cloud Secur. Alliance, CSA Global Staff, Seattle, WA, USA, 2013, pp. 1–14. [Online]. Available: http://www.cloudsecurityalliance.org/topthreats

[30] D. R. Cooper and P. S. Schindler, *Business Research Methods*. New York, NY, USA: McGraw-hill, 2003, p. 38.

[31] S. B. Chebrolu, V. Bansal, and P. Telang, *Top 10 Cloud Risks That Will Keep You Awake at Night*. San Jose, CA, USA: CSICO, 2010, pp. 1–35. [Online]. Available: https://www.owasp.org/images/4/47/Cloud-Top10-Security-Risks.pdf

[32] G. Elena and W. C. Johnson, "Laypeople's and experts, risk perception cloud computing services," *Int. J. Cloud Comput., Services Archit.*, vol. 1, no. 2, pp. 1–19, 2015. doi: 10.5121/ijccsa.2015.5401.

[33] M. Dupré and U. Sporn, "Method for providing and billing for functionalities of a wireless identification module WIM in mobile communication terminals," U.S. Patent 7 492 878 B2, Feb. 17, 2009.

[34] D. Catteddu and G. Hogben, "Cloud computing benefits, benefits, risks and recommendations for information security (ENISA)," *ENISA Comput. Rep.*, vol. 1, no. 2, pp. 2009–2013, 2009. doi: 10.1007/978-3-642-16120-9_9.

[35] J. W. Rittinghouse and J. F. Ransome, *Cloud Computing: Implementation, Management, and Security*. Boca Raton, FL, USA: CRC Press, 2017.

[36] M. Alshehri, S. Drew, T. Alhussain, and R. Alghamdi, "The impact of trust on E-government services acceptance: A study of users' perceptions by applying UTAUT model," *Int. J. Technol. Diffusion (IJTD)*, vol. 3, no. 2, pp. 50–61, 2012.

[37] K. M. Khan and Q. Malluhi, "Establishing trust in cloud computing," *IT Prof.*, vol. 12, no. 5, pp. 20–27, Sep./Oct. 2010. doi: 10.1109/MITP.2010.128.

[38] R. A. Alghamdi, "Diffusion of adoption of online retailing in Saudi Arabia," Ph.D. dissertation, School Inf. Commun. Technol., Griffith Univ., Brisbane, QLD, Australia, 2012.

[39] T. Alhussain, R. AlGhamdi, S. Alkhalaf, and O. Alfarraj, "Users' perceptions of mobile phone security: A survey study in the kingdom of saudi arabia," *Int. J. Comput. Theory Eng.*, vol. 5, no. 5, p. 793, Oct. 2013.

[40] M. S. Featherman and P. A. Pavlou, "Predicting e-services adoption: A perceived risk facets perspective," *Int. J. Hum.-Comput. Stud.*, vol. 59, no. 4, pp. 451–474, Oct. 2003. doi: 10.1016/S1071-5819(03)00111-3.

[41] J. Sen, "Security and privacy issues in cloud computing," in *Cloud Technology: Concepts, Methodologies, Tools, and Applications*, I. Management Association, Ed. Hershey, PA, USA: IGI Global, 2015, pp. 1585–1630. doi: 10.4018/978-1-4666-6539-2.ch074.

[42] B. Kaplan and D. Duchon, "Combining qualitative and quantitative methods in information systems research: A case study," *MIS Quart.*, vol. 12, no. 4, pp. 571–586, Dec. 1988. doi: 10.2307/249133.

[43] L. J. Cronbach and R. J. Shavelson, "My current thoughts on coefficient alpha and successor procedures," *Educ. Psychol. Meas.*, vol. 64, no. 3, pp. 391–418, Jun. 2004. doi: 10.1177/0013164404266386.

[44] D. Straub, M. Boudreau, and D. Gefen, "Validation guidelines for IS positivist research," *Commun. Assoc. Inf. Syst.*, vol. 13, no. 1, p. 24, Mar. 2004. doi: 10.2307/249422.

[45] M. R. Lynn, "Determination and quantification of content validity," *Nursing Res.*, vol. 35, no. 6, pp. 382–385, Nov. 1986. doi: 10.1097/00006199-198611000-00017.

[46] C. Ayre and A. J. Scally, "Critical values for Lawshe's content validity ratio: Revisiting the original methods of calculation," *Meas. Eval. Counseling Develop.*, vol. 47, no. 1, pp. 79–86, 2014. doi: 10.1177/0748175613513808.

[47] C. H. Lawshe, "A quantitative approach to content validity," *Personnel Psychol.*, vol. 28, no. 4, pp. 563–575, Dec. 1975. doi: 10.1111/j.1744-6570.1975.tb01393.x.

[48] R. B. Kline, *Principles and Practice of Structural Equation Modeling*, 4th ed. New York, NY, USA: Guilford Press, 2016.

MADINI O. ALASSAFI received the B.S. degree in computer science from King Abdulaziz University, Saudi Arabia, in 2006, the M.S. degree in computer science from California Lutheran University, USA, in 2013, and the Ph.D. degree in security cloud computing from the University of Southampton, Southampton, U.K., in April 2018. He is currently an Assistant Professor with the Information Technology Department, Faculty of Computing and Information Technology, King Abdulaziz University. He has published numerous conference papers, journal articles, and two book chapters. His research interests include cloud computing and security and the Internet of Things (IoT) security issues, especially cloud security adoption, risks, cloud migration project management, and cloud of things security threats.

RAYED ALGHAMDI received the B.S. degree in computer science from Jeddah Teachers' College, Saudi Arabia, in 2003, and the M.S. and Ph.D. degrees in information and communication technology from the School of Information and Communication Technology, Griffith University, Brisbane, Australia, in 2008 and 2014, respectively. He is currently an Assistant Professor with the Faculty of Computing and Information Technology, King Abdulaziz University (KAU), where he serves as a Consultant for teaching and learning development. His research interests include diffusion and technology adoption and information technology education.

ABDULRAHMAN ALSHDADI received the B.S. degree in computer science from Taif University, Saudi Arabia, in 2008, the M.S. degree in information technology from the School of Computer Science, Nottngham University, U.K., in 2010, and the Ph.D. degree in cloud computing from the University of Southampton, Southampton, U.K., in February 2018. He is currently an Assistant Professor with the Information Technology Department, Faculty of Computing and Information Technology, University of Jeddah. He has published numerous conference papers, journal articles, and one book chapter. His research interests include cloud computing migration projects and Security, the Internet of Things (IoT) security issues, and data science for deep learning topics.

ABDULWAHID AL ABDULWAHID received the B.Sc. degree in computer information systems from King Faisal University, Saudi Arabia, in 2003, and the M.Sc. degree in management of information technology from Nottingham University, U.K., in 2010, and the Ph.D. degree in cyber-security from the Centre for Security, Communications and Network Research, Plymouth University, U.K. He is currently an Assistant Professor of cyber-security with the Computer Science and Engineering Department, Jubail University College, Saudi Arabia. He is also the College Dean of student affairs. He has published a number of peer-reviewed publications at credible journals and conferences. His research interests include user authentication, biometrics, and cloud security and privacy. He is a Professional Member of the ACM.

SHEIKH TAHIR BAKHSH received the Ph.D. degree in computer networks from Universiti Teknologi PETRONAS, Malaysia, in 2012. He is currently an Associate Professor with the Faculty of Computing and Information Technology, King Abdulaziz University. His research interests include cyber-security, the Internet of Things (IoT), fog computing, and wireless networks.