Journal of Information Technology Management

Print ISSN: 2008-5893

Online ISSN: 2423-5059

Factors Influencing the Security Framework in Cloud Computing: A Case Study of Infrastructure Communications Company

Mohammad Mehdi Minaee

Ph.D. Candidate, Department of Industrial Management, IT and Technology, Central Tehran Branch, Islamic Azad University, Tehran, Iran. E-mail: mehdi.minaee91@gmail.com

Mahmood Mohammadi*

*Corresponding author, Assistant prof., Department of Industrial Management, IT and Technology, Central Tehran Branch, Islamic Azad University, Tehran, Iran. E-mail: mahmoodmohammadi525@yahoo.com

Hasan Mehrmanesh

Assistant prof., Department of Industrial Management, IT and Technology, Central Tehran Branch, Islamic Azad University, Tehran, Iran. E-mail: has.mehrmanesh@iauctb.ac.ir

Abstract

Cloud computing technology could bring about cost-effectiveness, scalability, usage easiness, and flexibility against environmental changes. Despite several advantages of this technology, the acceptance and movement to the cloud computing environment occurs slowly, particularly in several organizations in developing countries. Cloud computing allows an individual to share distributed sources and services. This study aims to identify the optimal security framework in cloud computing, focusing on the Infrastructure Communications Company as a case study. The method used in this study is descriptive (non-test) and the correlative research scheme is PLS (partial least squares). The participants of the current study were selected among the Tehran Communication Infrastructure Company employees. Based on the Cochran formula and the research population which was 600, 234 were selected using the random sampling method. To measure the security framework in cloud computing, the questionnaires related to Joils and Opria (2017), Tari (2014), Qio and Gayi (2017), and Sing et al. (2016) were used. Findings indicate that the impacts of technological and technical factors, experienced human resources, financial resource provision and secure infrastructures on information technology security were significant (0.01). Moreover, information technology management and supporting regulations on security risk assessment have significant effects. The assessment of security risk has a significant effect on information security. Additionally, information security management and supporting regulations have a significant effect on Goal setting (0.01). Goal setting has a significant effect on environmental and physical security. Based on the results, the evaluated model of the research could explain 0.53 of information security management, 0.50 of security evaluation, 0.36 of goal setting, 0.55 of information security, and 0.35 of environmental security.

Keywords: Security framework, cloud computing, Communications Infrastructure Company

Journal of Information Technology Management, 2024, Vol. 16, Issue 2, pp. 206-222
Published by the University of Tehran, College of Management
doi: https://doi.org/ 10.22059/JITM.2024.303185.2534
Article Type: Research Paper
© Authors

Received: March 25, 2023
Received in revised form: July 16, 2023
Accepted: February 13, 2024
Published online: April 30, 2024

Introduction

Data and information technology play an important and remarkable role in organizations' lives, allowing theoreticians and managers to encourage organizations to take advantage of strategies related to these technologies for future learning of organizations (Khayer et al., 2020). Organizations may adopt this strategy primarily due to the advancements in modern technologies over the last two decades, facilitated by modern information systems. These advancements have accelerated productivity and economic development worldwide. In line with this trend, cloud computing is a modern paradigm that could provide the necessary infrastructure to help organizations execute applications as a proper service through Web Explorer (Chang, 2020). Nowadays, the role of data technology among modern organizations is so remarkable that several theoreticians, managers, and decision-makers recommend organizations adopt strategies related to these technologies for future orientations (Alam, 2020).

In recent years, cloud computing has surged in importance, introducing a virtual framework for resource sharing distributed across geographical locations. This allows organizations to access a shared pool of resources. The idea of a virtual framework such as a cloud is not considered proper for certain organizations, since organizations might imagine that others have access to their resources throughout a shared space. Organizations prefer to use their infrastructure resources, due to the sensitivity and importance of information or data. This is not only costly but also is considered an improper method to use resources. To increase cloud efficiency, the trust issue should be resolved so that an organization can use shared resources trustingly or offer services over this platform. Therefore, the user seeks high-quality and trustworthy resources, while the service provider seeks trustworthy users (Garg & Singh, 2017).

Although numerous advantages have been reported for using cloud computing, it comes along with several risks regarding its implementation, management, and usage. Besides the traditional calculation model in which users fully control data storage and calculations, it is necessary to delegate physical data management and machines to cloud computing service providers. Data storage and calculations could be endangered due to the lack of owners' control over data security. Thus, it is vital to deeply consider the security, confidentiality, and regulations following and hosting other risks before any activities in the field of cloud computing (Chaturvedi & Gupta, 2020). Therefore, cloud computing is not excluded from risks and its main one is security issues. Lack of security is one of the major obstacles hindering the extensive usage of cloud computing. Certain research and commercial organizations are reluctant to fully trust cloud computing for the transmission of digital assets to third-party service providers. In IT traditional infrastructure, digital assets are kept within the internal platform of organizations in which data and software processing, transmission, and management are carried out. Conversely, controls and managerial actions performed by cloud computing service providers are not transparent and clear for organizations. The existence of numerous users having no contact with organizations has intensified concerns. Users must trust cloud computing service providers; however, mutual trust might not exist. The mentioned reasons have intensified customers' doubts regarding digital assets in cloud computing, leading to reluctance and lack of tendency in cloud computing adoption (Pourmohamad, 2016).

The security issue is one of the most important factors in systems, particularly in cloud computing. In this regard, an organization should take serious action against security threats and their consequent risks. In this case, cloud computing is distinctive compared to traditional models due to the loss of direct control over assets and the probability of lack of potential management by cloud computing service providers, which is considered one of the main existing risks. This issue is the most essential security threat in hybrid and general cloud computing models as well as private models offered by a third-party company. In these cases, using cloud computing services involves responsibility transmission and partial control over information and the organization's systems to the external service provider. Organizations might have independence from a certain provider and face challenges regarding data transmission and service provision to another provider. Using cloud computing advantages creates new services hindering an organization's speed when a security accident happens (Qiu & Gai, 2017). The open and distributed structure of cloud computing has been converted into a considerable target for cyber-attacks of attackers. The old penetration detection and prevention systems are somehow inefficient to be implemented in cloud process environments, due to their openness and specific nature. The introduction of penetration detection and prevention systems and their performance and different classifications could be considered the latest achievement in terms of stabilization challenges identification in cloud computing (Pouryan Mameghani, 2016).

Given the fast growth and extensive usage of electronic data processes and electronic business on cable and wireless networks and the Internet as well as web-based applications, information security is considered an essential principle for society's economic welfare and safety.

The cloud computing service architecture comprises three interdependent layers: infrastructure, platform, and application. Various configuration errors that may occur in any layer by the user or service provider could make the entire service provider vulnerable. A cloud process system could be vulnerable to various threats such as those related to generality, confidentiality, and accessibility to virtual sources and infrastructures. Cloud services are available and easy for hackers when they present themselves as service customers. Lack of complete control over infrastructure is a big concern for cloud service customers. This fact indicates the role of penetration detection systems to protect the information assets of users in the cloud process (Qiu & Gai, 2017).

Given the mentioned issues and the numerous advantages of cloud computing, there are security and confidentiality issues that prevent from using cloud computing services by various organizations and the IT industry. Data confidentiality and privacy are considered as the main concerns of an organization to transmit its data to the cloud environment. Lack of trust in data protection and control loss over data are the other reasons for decreasing the trust level of cloud computing providers. Therefore, it is necessary to ensure data security and guarantee performance and behavior, cloud service providers should be trusted (Kanwal et al., 2013). The importance and necessity of recognizing the effective factors of cloud computing is that this concept offers various types of necessary hardware and software such as applications, storage, processes, and virtual servers on the web. Thus, the identification of its extension factors has clarified its application path and enhanced the trust of usage for users. As a result, it justifies the scalability and lack of need for extensive investment in expensive hardware and provides significant advantages for the organization (Mondal et al., 2020).

Therefore if the key element of trust does not exist, cloud computing will face numerous difficulties. In cloud computing, as a solution for increasing security, trust has gained considerable attention from researchers. As the administrator of the telecommunication network as well as the agent of the Ministry of Communication and Information Technology, the infrastructure communications company has the responsibility of providing the inter-province and international communication of telecommunication operators in the presence points and related networks. Given the mission of the mentioned company, data keeping security and controlling over data has essential importance. The present study examines and identifies the security framework in cloud computing using the quantity approach and consequently offers a model in this context. The main issue of the present study is: What is the security framework of cloud computing in infrastructure communications companies?

Theoretical framework

The concept of cloud computing has been defined by diverse methods by analyzer companies, academics, industries, and information technology companies. Table 1 presents the description of several cloud computing analyzer companies.

Table 1

Definitions of cloud computing by selected analytics companies (Joyce & Opera, 2017)

Source	Definition
Gartner	**Gartner** defines public **cloud computing** as a style of **computing** where scalable and elastic IT-enabled capabilities are provided as a service to external customers using Internet technologies
IDC	An emerging IT development, deployment and delivery model, enabling real-time delivery of products, services, and solutions over the Internet.
NIST	**cloud computing** is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable **computing** resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management
Merrill Lynch	the idea of delivering personal (e.g., email, word processing, presentations.) and business productivity applications (e.g., sales force automation, customer service, accounting) from centralized servers" the idea of delivering personal (e.g., email, word processing, presentations.) and business productivity applications (e.g., sales force automation, customer service, accounting) centralized Server The idea of delivering personal (email, word processing, presentations)and business productivity applications (Sales force automation, customer services accounting)from centralized serves
Group 451	**Cloud computing** describes a service model that combines a general organizing principle for IT delivery, infrastructure components, an architectural approach, and an economic model–basically, a confluence of grid **computing**, virtualization, utility **computing**, hosting, and software as a service (SaaS)

All those definitions have a common characteristic: All these definitions intend to describe and define cloud computing from the perspective of the final user. They also emphasize how the final user might experience it. According to these definitions, the main characteristic of cloud computing is the provision of the information technology infrastructure and applications as a service and scalability. The definition of the cloud process has been discussed in scientific society. Similar to commercial press, different opinions regarding the definition and characteristics of cloud computing exist. Compared to commercial press definitions, the definitions are scientific literature that not only consists of the end user's perspective but also deals with architectural aspects. For example, Berkely Rad laboratory defines the cloud process as such:

Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. The hardware and software of a data center is called a cloud. When this cloud is offered to the public using cost payment and usage, it is called a public cloud. Sold service is instrumental processing. The term "private cloud" refers to internal data centers of a business or organization which is not available to the public.

Definitions offered in the “cloud definitions” section indicate that cloud processing consists of different information technology capabilities such as infrastructure, platforms, and software. Since the information technology resources delivery or capabilities are considered as an important specific service of cloud processing, the three cloud processing architectures are:

1) Infrastructure as a service (IaaS)

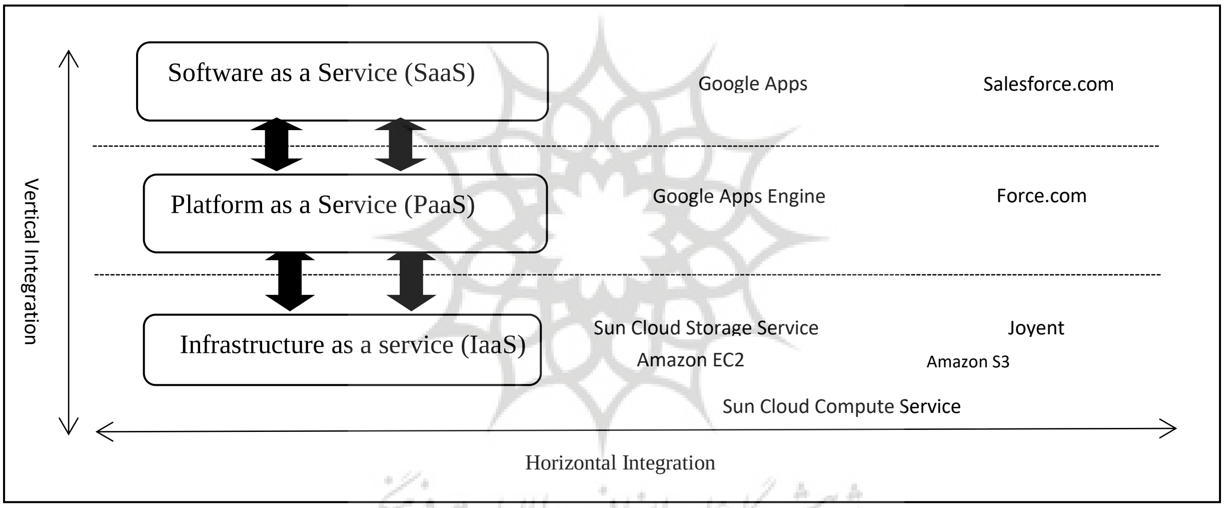
2) Platform as a Service (PaaS)

3) Software as a Service (SaaS)

In the figure below three cloud processing layers and their interconnections are seen.

Figure1

Three cloud processing layers: IaaS, PaaS, and SaaS (Sing et al., 2016)


Software as a Service (SaaS)
Google Apps
Salesforce.com
Platform as a Service (PaaS)
Google Apps Engine
Force.com
Infrastructure as a service (IaaS)
Sun Cloud Storage Service
Joyent
Amazon EC2
Amazon S3
Sun Cloud Compute Service
Vertical Integration
Horizontal Integration

Cloud computing has been investigated in several researches. Each investigation deals with the concept of cloud computing from a certain angle. Table 2 examines the related theories and perspectives.

Table 2

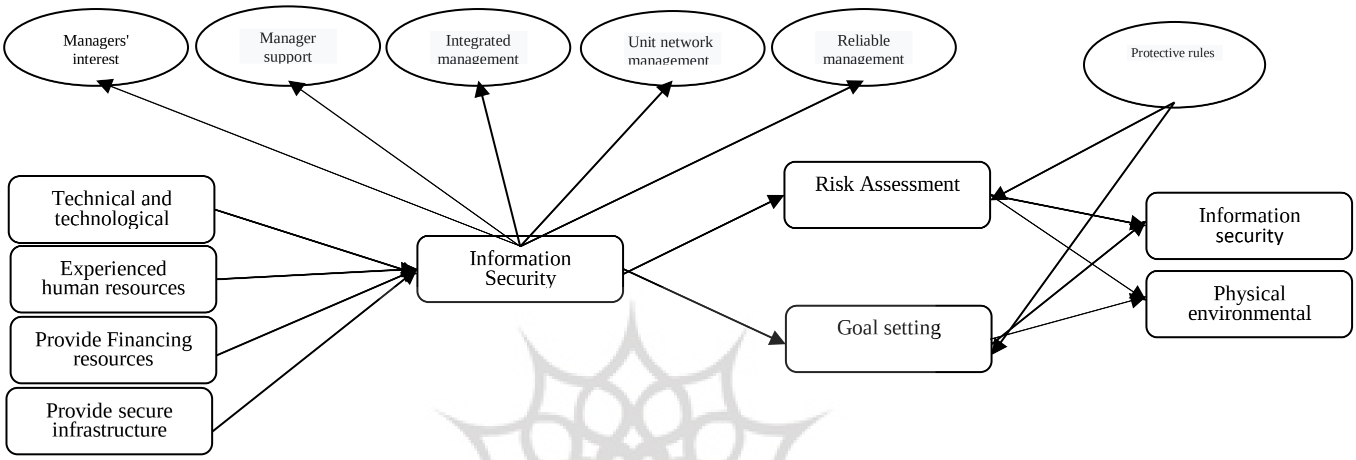
Cloud Computing Views and Theories

Row	Theoretician	Indices
1	Salehi (2017)	Equity return, data security, integrity, process structure, individual access to information
2	Dargazi Khojin (2016)	Security maintenance, data security, privacy
3	Abayi Khorasani (2016)	Cost-effective, uncomplicated, higher information security, confidentiality, using modern technology
4	Joils & Opria (2017)	Security enhancement, encrypting, Integrity
5	Qiu & Guy (2017)	Implementation, security, privacy maintaining
6	Jair et al. (2020)	Information security, easiness, high speed, high efficiency
7	Chang (2020)	Environmental security, timesaving, privacy control
8	Chatoridi & Gopta (2020)	Cost saving, information security, integrity, updated

Based on the theoretical framework and research background and interviews with experts, the conceptual model is designed based on Joils and Epria (2017), Tari (2014) Giu and Gai (2017) and Sing et al. (2016).

Figure 2

Security framework in cloud computing



Methodology

The present study is a descriptive survey. The statistical sample for Tehran Infrastructure Communications Company, which employs 600 individuals, was chosen using random sampling. Three buildings in Tehran, including Central, Imam Khomeini Square, and Enghelab Square, were selected based on the random sampling method. Each member of the statistical population was assigned a number from 1 to the end and recorded on similar small cards.

Subsequently, all the cards were placed in a box, and one card was randomly selected each time after shaking the box. The number on the selected card was recorded, and this process continued until the desired number of sample units was obtained. According to the Cochran formula, a sample of 234 employees from Tehran Infrastructure Communication Company was selected.

In this study, 234 employees meeting the entry criteria were selected following the university's permission, which was then submitted to Tehran Infrastructure Communication Company. Upon arrival, a questionnaire was distributed among the employees of the Infrastructure Communication Company. To assess the security framework in cloud computing, a questionnaire comprising 42 questions was utilized, sourced from Joils and Epria (2017), Tari (2014), Qiu and Gai (2017), and Singh et al. (2016). This questionnaire covered various aspects including information security management, risk assessment, support regulations, technical and technological factors, skilled human resources, target selection, financial resource allocation, secure infrastructure provision, and variables related to information security and the physical environment.

The questionnaire questions were graded based on a Likert 5-point scale (Very low, low, moderate, high, and very high).

The reliability and validity of the questionnaire were reported in Joils and Epria (2017), Tari (2014), Qiu and Gai (2017), and Singh et al. (2016) in an acceptable manner. Table 3 provides factor loads, ρc, and AVE of variables, indicating the validity of constructs. Findings related to confirmatory factor analysis are presented in Table 3.

Table 3

Findings of confirmatory factor analysis

Variables	A	Factor loads on structures											
		Pc	AVE	Environmental and physical security	Information security	Protective rules	Security targeting	Risk Assessment Information system security	Information Security Management	Provide secure infrastructure	Provide Financing resources	Experienced human resources	Technical and technological factors
Technical and technological factors	.85	.80	.57										
Q1													.87
Q2													.89
Q3													.91
Q4													.88
Experienced human resources	.89	.82	.56										
Q5												.64	
Q6												.63	
Q7												.68	
Q8												.71	
Q9												.77	
Q10												.78	
Provide Financing resources	.85	.80	.55										
Q11											.46		
Q12											.84		
Q13											.83		
Q14											.85		
Provide secure infrastructure	.83	.81	.51										
Q15										.75			
Q16										.71			
Q17										.68			
Q18										.78			
Q19										.79			
Q20										.75			

Information Security Management	.90	.87	.60										
Q21									.44				
Q22									.79				
Q23									.84				
Q24									.84				
Q25									.75				
Risk Assessment Information system security	.87	.85	.52										
Q26								.71					
Q27								.74					
Q28								.71					
Q29								.77					
Security targeting	.89	.85	.53										
Q30							.81						
Q31							.81						
Q32							.82						
Q33							.85						
Q34							.88						
Protective rules	.91	.88	.54										
Q35						.86							
Q36						.89							
Q37						.88							
Information Security Management	.88	.86	.51										
Q38					.84								
Q39					.85								
Q40					.87								
Environmental and physical security	.89	.85	.52										
Q41				.91									
Q42				.90									

Note: All operating loads at the alpha level of 0.01 are significant.

Table 3 presents the fitting indices for each of the research constructs. In this table, the acceptable and estimated values for each construct can be observed. The results indicate that all constructs including technological and technical factors, experienced human resources, financial resource provision, secure infrastructure provision, information security management, information systems security risk assessment, target selection in line with security, supporting rules, and information and physical environmental security have acceptable fitting indices.

To examine the relationships among research variables, structural equations were employed. Hypotheses in this research were analyzed using partial least squares (PLS) via Smart-PLS software. PLS is a useful tool for examining complex models containing latent variables.

Results

Table 3 presents the results related to the second-factor examination. Based on the provided tables, all measures have the highest factor loadings on their respective constructs, and the least distance between factor loadings related to their constructs is 0.1, indicating that the research constructs have appropriate validity.

In Table 4, the results related to the correlation examination and the validity of the second factor are reported.

Table 4

Correlation matrix and mean square of the extracted variance

Variables	1	2	3	4	5	6	7	8	9	10
Technical and technological factors	.77									
Experienced human resources	.29**	.79								
Provide Financing resources	.31**	.33**	.79							
Provide secure infrastructure	.40**	.35**	.30**	.77						
Information Security Management	.36**	.40**	.34**	.38**	.78					
Risk Assessment Information system security	.28**	.32**	٠.41**	.36**	.47**	.77				
Security targeting	.34**	.30**	.33**	.37**	.32**	.41**	.78			
Protective rules	.32**	.35**	.42**	.39**	.32**	.39**	.43**	.77		
Information Security Management	.31**	.32**	.45**	.37**	.42**	.29**	.31**	.29**	.79	
Environmental and physical security	.28**	.34**	.32**	.43**	.33**	.35**	.37**	.41**	.51**	.78

**p<0.01

Based on Table 4, the variance extracted mean square of all research variables exceeds their correlation with other variables, supporting the divergent validity of the second factor of variables. Additionally, numbers below the correlation matrix diameter were examined to assess the relationship between variables, with significant correlation coefficients observed among all variables.

To evaluate the predictability of the proposed conceptual model, structural equations methodology was employed, utilizing the PLS method for model estimation. Hypothesis testing and examination of the research structure were conducted through path coefficients (factor loadings) and R2 values. The Bootstrap method was utilized to calculate T-values, indicating the significance of path coefficients. These coefficients were used to determine the contribution of each predictor variable to explaining the variance of the measured variable. R2 values represent the explained variance of the measured variable by predictor variables. Moreover, the Stone-Geisser coefficient was employed to assess the prediction ability of dependent variables from independent variables. A positive coefficient value indicates prediction ability (Vinzi et al., 2010). Figure 3 illustrates the tested model of relationships among research variables.

Figure 3

Tested research model in standard mode

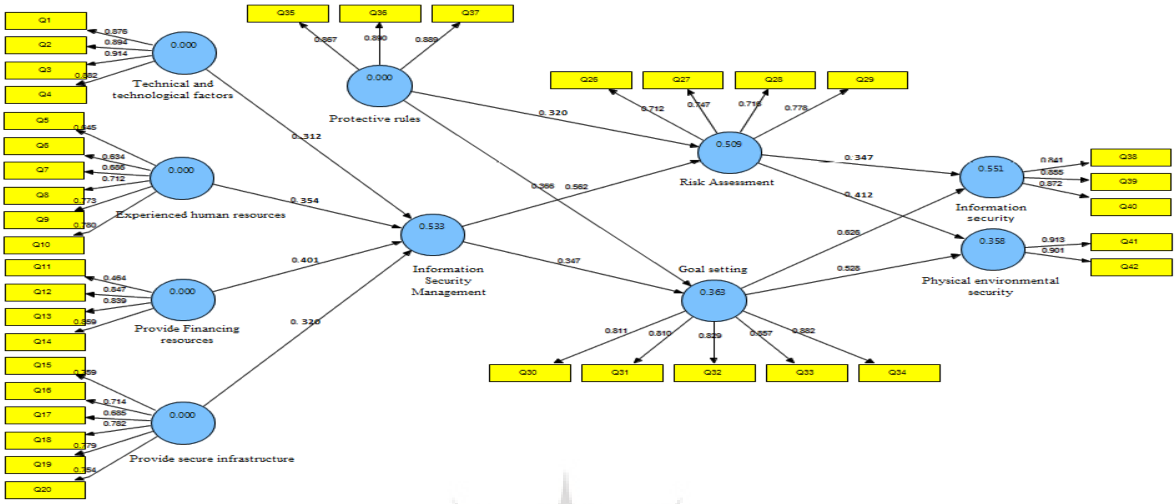


Figure 4

Tested research model in a significant way

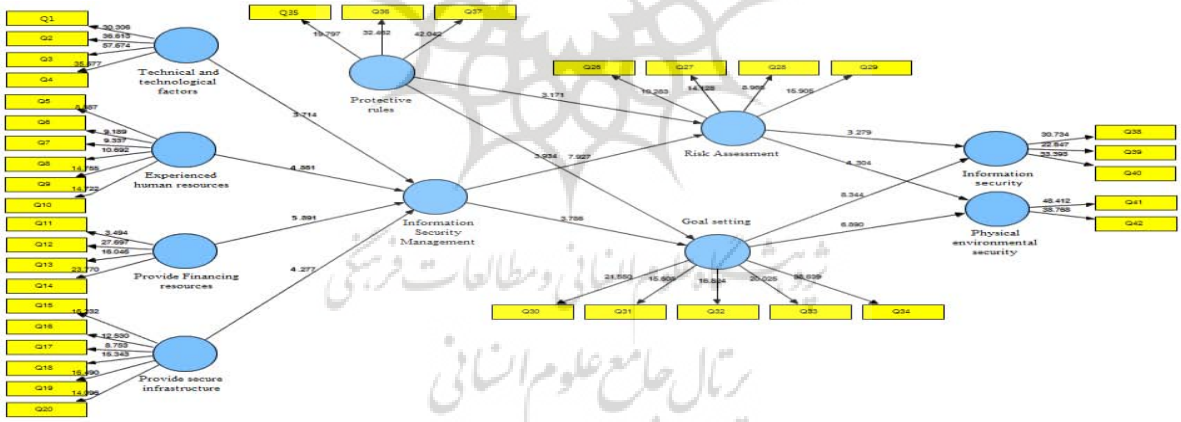


Figure 4 shows the T coefficients of research paths. T coefficients between +-1.96 to +-2.38 are significant at 0.5 and T coefficients above +- 2.58 are significant at 0.01. Moreover, in Table 4 the estimated quantity of path coefficient and explained variance of the research model have been reported.

Path coefficient explains the existence of linear relation as well as the intensity and orientation of this relation between two latent variables. It is the regression coefficient in standard form we can see in simpler regression models (simple and multiple). The path coefficients are between -1 to +1. If it is equal to 0 implies the lack of linear relation between two latent variables.

Table 5

Route coefficients

Direction	Route coefficient
1-Technical and technological factors on information security management	.444
2-Experienced human resources on information security management	.452
3-Provide funding for information security management	.394
4-Provide secure infrastructure for information security management	.646
5-Information security management on security risk assessment	.414
6-Protective laws on security risk assessment	.398
7- Information security management on targeting	.630
8-Protective laws on targeting	.391
9-Evaluate security risk over information security	.306
10-Targeting environmental and physical security	.537
11-Evaluate security risk over information security	.434
12-Targeting environmental and physical security	.412

According to Table 5, the impact of technical and technological factors, experienced human resources, financial resource provision, and secure infrastructure provision on information security management is significant (0.01)

Information security management and supporting rules also have a significant effect on security risk evaluation. Security risk evaluation has a significant effect on information security. Moreover, the effect of information security management and supporting rules on target selection is significant (0.01). Additionally, target selection has a significant effect on physical and environmental security. Based on the results, the research model can explain 0.36 of target selection, 0.55 of information security, and 0.35 of environmental security variance.

Table 6 shows the sharing credit and redundancy. As can be seen in the table, all the values regarding redundancy and sharing credit are positive, showing the proper and acceptable quality of the research model.

Table 6

Explained variance, subscription validity, and variability

Research variables		Q^2 (CV-Redundancy)	CV- Communality
1.	Technical and technological factors	-	0.635
2.	Experienced human resources	-	0.547
3.	Providing financial resources	-	0.545
4.	Providing safe infrastructure	-	0.601
5.	Information security management	0.630	0.574
6.	Security risk assessment	0.527	0.638
7.	Targeting in order to ensure security	0.654	0.507
8.	Protective laws	-	0.604
9.	Information security	0.517	0.567
10.	Environmental and physical security	0.592	0.577

Finally, the PLS method was used to indicate the credit of the model's findings credits. There are methods to examine the model credit in PLS. These methods called cross-validation include CV-communality and CV-redundancy. The CV-Communality index evaluates each block's measurement. CV-Redundancy, which is also called Q2 Stone-Geiser, measures the quality of the structural model for each endogenous block. The positive values of these indices indicate the proper and acceptable quality of measurement and structural model. As can be seen in Table 5, the positive values of CV-Communality and CV-Redundancy for all variables in the current study indicate the proper and acceptable structural and measurement quality.

In addition to the above-mentioned indices, the general explanation index in PLS is GOF (goodness of Fit). It can be generally used for credit examination or PLS pattern quality. This index has the same function as the Laserl model indices and is between zero and one. Values close to one indicate proper quality. This index examines the predictability of the entire model and whether the tested model was successful in predicting endogenous latent variables. In the present study, the explanation index (GOF) is 0.47 showing a proper explanation of the tested model.

Conclusion

The present study aims to examine the effective factors in the security framework in cloud computing using structural equations. The results show that the suggested model explains well the data and could explain 0.53, 0.50, 0.36, 0.55, and 0.35 of information security management, security risk, target selection, information security, and environmental security respectively. Research findings indicate that information security management, technological and technical factors, experienced human resources, and financial resource provisions have significant effects on secure infrastructure provision. Results show that information security management has a significant effect on risk assessment and target selection. Research findings risk assessment: supporting rules and target selection have an impact on information security and environmental security. Research findings regarding the effective factors of security framework on cloud computing are in line with Salehi (2017), Tari (2014), Joils and Epria (2017), Qiu and Gai (2017), and Chatoridi and Gopta (2020).

In a research Salehi (2017) deals with the "cloud computing accepting model" and its findings show that the most important factor in the cost dimension is equity return, in the security dimension is medical devices information security, in the integration dimension is integration with patients caring process structure, in access dimension is the extent to which individuals have access to patients information, in organization culture is staff special education, in infrastructure dimension is information contact link between hospital and service provider. Moreover, the major problem in accepting cloud computing is the lack of sufficient knowledge in the field of cloud computing and thereby resistance against its acceptance.

In addition, Tari (2014) deals with security in cloud computing. This research considers security issues and relevant security solutions. Though its main focus is on cloud computing security, it does not point out future trends. The current research has considerable differences with relevant research in terms of extension and generality of cloud computing security. It has also an emphasis on existing security solutions in the literature review.

In a study, Joils and Epria (2017) deal with “Security issues identification in cloud computing”. In addition to dealing with security gaps of cloud computing in small and big systems, they have offered a framework to enhance cloud computing security, in which they have focused on encrypting and integration. Moreover, Qiu and Gai (2017) examine mobile cloud computing: models, implementation, and security. In this research, cloud computing in mobile systems has been studied and issues related to security, confidentiality, threats as well as privacy techniques in mobile devices have been provided.

Chatoridi and Gopta (2020) conclude that using cloud computing technology in an organization leads to information security enhancement, saves time and costs, and has a positive impact on the organization’s productivity.

To explain the research findings, it can be mentioned that stored sensitive data of customers and organizations have been established in a cloud, particularly a “public cloud which is a common environment between customers and other organizations’ data”. Therefore, certain tools to control access and safe storage of data should be considered. Whether in the stored, transmission, or usage status of data security, data storage and accessibility should be controlled. In computer networks, certain standards and protocols must be used to transfer data, specifically the “encrypting keys as the data transmission license”. This method is normally used in the cloud including the infrastructure environment as a service and platform. As a result, the security of a system using encrypting depends on proper control of central keys and key management components. Recently, the management of encrypting key management occurs in the consumer part of the cloud. Key generation and storage are usually performed outside the cloud using hardware security modules.

Information, systems, networks, and supporting procedures are among the major assets of an organization. Confidentiality, generality, accuracy, and accessibility could have several impacts on profitability, efficiency, law-abiding, and the organization’s operational horizon. Organizations, their information systems, and communication networks have been increasingly attacked in terms of security.

These invasions are so extensive that could affect the system through individuals' abuse of computer systems, espionage, vandalism, and even flood and fire. It is necessary to define and establish a particular management framework to create, maintain, and control information security within an organization's activity domain. To define and acknowledge the security policymaking, security roles reference, and inter-section security cooperation must be defined and guided by the senior management.

Based on the research findings, it is suggested that employees and individuals dealing with this technology within an organization would be educated and shed light on its challenges. Enlightening could be performed in various forms such as holding educational courses before initiation of cloud computing within the organization to increase the individuals' knowledge level and its users, provision of operational instructions for the system's users, recruiting experts within an organization for emergency cases and situations in which troubleshooting is needed.

Conflict of interest

The authors declare no potential conflict of interest regarding the publication of this work. In addition, the ethical issues including plagiarism, informed consent, misconduct, data fabrication and, or falsification, double publication and, or submission, and redundancy have been completely witnessed by the authors.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Alam, T. (2020). Cloud computing and its role in information technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 1(2), 108-115.

Chang, V. I. (2020). A proposed framework for cloud computing adoption. In Sustainable Business: Concepts, Methodologies, Tools, and Applications (pp. 978-1003). IGI Global.

Chang, V., Kuo, Y. H., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. Future Generation Computer Systems, 57, 24-41.

Chaturvedi, C., & Gupta, B. B. (2020). Cloud computing security: Taxonomy of issues, challenges, case studies, and solutions. In Handbook of Research on Intrusion Detection Systems (pp. 306-325). IGI Global.

Dargazi Khojin, M. G. (2015). Introduction of a new method for data protection against data attacks in mobile cloud computing. Tehran Payam-e Noor University. (Original work published in Persian)

Delgado, V. (2010). Exploring the limits of cloud computing. Master of Science Thesis, Stockholm, Sweden.

Ebayi Khorasani, F. (2016). Introduction of a method to enhance information security in cloud computing. Shahab Danesh Superior Education Institute-Computer and Electronic Faculty. (Original work published in Persian)

Erl, T., Cope, R., & Naserpour, A. (2015). Cloud computing design patterns. Prentice Hall Press.

Garg, K., & Singh, J. (2017). A Proposed Technique for Cloud Computing Security. In Innovations in Computer Science and Engineering (pp. 89-95). Springer, Singapore.

Juels, A., Oprea, A., & Bowers, K. D. (2017). Security Issues for Cloud Computing. Meta, 4(5).

Kanwal, A., Masood, R., Ghazia, U. E., Shibli, M. A., & Abbasi, A. G. (2013, August). Assessment criteria for trust models in cloud computing. In Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing (pp. 254-261). IEEE.

Khayer, A., Talukder, M. S., Bao, Y., & Hossain, M. N. (2020). Cloud computing adoption and its impact on SMEs' performance for cloud supported operations: A dual-stage analytical approach. Technology in Society, 60, 101225.

Mondal, A., Paul, S., Goswami, R. T., & Nath, S. (2020, January). Cloud computing security issues & challenges: A Review. In 2020 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-5). IEEE.

PourMohamad, R. (2016). Introduction an access control model based on dynamic trust in cloud computing environment. Master's Thesis, Tabriz University. (Original work published in Persian)

Pourya Mameghani, K. (2015). Quality control model for information technology security threats in cloud computing. Shahed University, Engineering and Technical Faculty. (Original work published in Persian)

Qiu, M., & Gai, K. (2017). Mobile cloud computing: Models, implementation, and security. Chapman and Hall/CRC.

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. Information and Software Technology, 58, 44-57.

Rittinghouse, J. W., & Ransome, J. F. (2017). Cloud computing: Implementation, management, and security. CRC Press.

Salehi, A. (2017). Introduction of cloud computing acceptation model in Tehran hospitals. Tarbiat Modares University, Faculty of Accounting and Management. (Original work published in Persian)

Shoeibi, D. (2016). Introduction of a distributed penetration detection system to enhance security in cloud computing. Kerman Industrial and Technological Graduate Education, Privilege Sciences and Technologies University. (Original work published in Persian)

Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D. (2015). Twenty security considerations for cloud-supported Internet of Things. IEEE Internet of Things Journal, 3(3), 269-284.

Tsugawa, M., Matsunaga, A., & Fortes, J. A. (2014). Cloud computing security: What changes with software-defined networking? In Secure Cloud Computing (pp. 77-93). Springer New York.

Bibliographic information of this paper for citing:

Minaee, Mohammad Mehdi; Mohammadi, Mahmood & Mehrmanesh, Hasan (2024). Factors Influencing the Security Framework in Cloud Computing: A Case Study of Infrastructure Communications Company. *Journal of Information Technology Management*, 16 (2), 206-222. https://doi.org/10.22059/JITM.2024.303185.2534