International Journal of Information Science and Management
Vol. 21, No. 4, 2023, 165-187
DOI: https://doi.org/10.22034/ijism.2023.1977435.0 / DOR: https://dorl.net/dor/20.1001.1.20088302.2023.21.4.8.4

Original Research

The Information Richness Assessment of Information Security Awareness in Iranian Cloud Storage Users: Case Study of iCloud

Mahnam Zamani Kalajahi
M. A. student of Knowledge and Information Science, Shahid Beheshti University, Tehran, Iran.
m.zamanikalajahi@mail.sbu.ac.ir
ORCID iD: https://orcid.org/0000-0001-7719-4489

Solmaz Zardary
Associate Prof., Department of Knowledge and Information Science, University of Tabriz, Tabriz, Iran.
Corresponding Author: szardary@tabrizu.ac.ir
ORCID iD: https://orcid.org/0000-0002-7348-7820

Shima Mardi
M. A. student of Knowledge and Information Science, scientometrics, University of Tabriz, Tabriz, Iran.
mardishima56@gmail.com ORCID iD: https://orcid.org/0009_0003_3282_1233

Received: 03 Febrauary 2021
Accepted: 20 June 2022

Abstract

Cloud storage technology is attracting more attention due to the increasing implementation of technology in everyday life. The present study aims to assess Iranian iCloud users' richness of information security awareness at the three levels of knowledge, attitude, and behavior, based on six aspects required for adhering to information security policies. Accordingly, in this study, the self-reported data of 384 Iranian users of Apple products (IUAP) were investigated using a questionnaire designed by a researcher. Then, the data were analyzed using Microsoft Excel software. This research showed that the average information security awareness of IUAP is 3.22 out of 5, a slightly higher than average score using a quantitative approach and descriptive statistics,. Almost three-quarters of them use iCloud, mainly because of its easy access to information. It also assesses various aspects and examples of information security awareness and behaviors that indicate compliance with information security policies. Finally, the general knowledge of Iranian iCloud users about the components of information security awareness is estimated to be 73.83, which is relatively low and unsatisfactory, showing that more attention and training are needed. Moreover, this study prioritizes different components of information security awareness.

Keywords: Information Security Awareness, Information Security Management, iCloud, Cloud Security, Iran.

Introduction

Among the emerging technologies in the 21st century, there is a growing desire to use portable devices instead of PCs to access Internet services. Since such technologies usually do not have strong processing capabilities, the answer to this need lies in the concept of cloud computing. Cloud computing-based tools have attracted superior interest from a diverse range of individuals and organizations, and the inevitability of fundamental reliance on technology facilities due to the COVID pandemic has reinforced the acceleration of this trend (Prajapati &

Shah, 2020). Cloud services make information available, easier to access, and cheaper. As Deighton and Wakefield (2020) report, Cloud adoption is proliferating: 88% of UK organizations have already adopted its services, and 67% of users expect to increase their use of the cloud. Even these online services are cited as fundamental to modern societies' survival (Alsmadi & Prybutok, 2018). "cloud computing" was first coined by John McCarthy in the 1960s. Emphasizing the necessity of using this technology, he stated that cloud computing will eventually be recognized and organized as a universal need in the public arena (Von Solms & Von Solms, 2004). Today, the accuracy of his prediction is evident in many areas such as education, banking, health care, and the major electronic information sources such as large online encyclopedias. “Cloud computing is a distributed architecture that centralizes server resources on a scalable platform” to provide computing resources on demand (kaur & kaur, 2018). The word cloud in this term is a metaphor for a network or a sum of large networks like the Internet, where the user technically does not know what is going on behind the scenes and what happens next, as with the cloud. It means that the cloud hides its technical details from the users and creates a level of abstraction between these technical details and the users.

Cloud storage is a part of cloud computing technologies that cause alteration in information sharing and storage behavior. In simplified terms, cloud storage is defined as storing and accessing data and applications using the Internet instead of the physical memories embedded in computers. Some common services among cloud users are Mozy, NextCloud, iCloud, Google Drive, OneDrive, Dropbox, BigMIND, Cloud Me, Crash Plan, DriveBox, etc. “with various types of security confidentiality, integrity, and availability”(Prajapati & Shah, 2020). In this technology, a specific and limited space is dedicated to each user to store personalized data, simulating the function of a hard disk drive. The dedicated cloud storage space to each user varies based on employed software and applications, and users can hire or purchase additional storage space according to given contracts after getting initial mostly free-of-charge limited storage space.

Considering the attractiveness of cloud-based technologies and storage facilities, cloud storage raises privacy concerns because the data is hosted on an outside server, which means that the data in the cloud is vulnerable and breachable at any time. Cloud storage service providers could monitor and control data and communications between users of the services and the hosted cloud. Cloud storage service providers could legally or illegally monitor and manage data and communications between users of the services and the hosted cloud. Possible deliberate or accidental modification or deletion of data from inside or outside the cloud without users’ satisfaction, which means limited control, is a clear example of endangering security. This limited control over data can pose several security issues and threats, including data leakage, insecure interfaces, resource sharing, data availability, and internal attacks. For example, previous research has shown that 24.6% and 3.4% of threats leading to cloud outages are due to data loss or leakage and cloud-related malware, respectively (Jarno, Baharom & Shahpasand, 2017). Therefore, the security of data and communications has become a priority and important issue (McCormac, Zwaans, Parsons, Calic, Butavicius & Pattinson, 2017; kaur & kaur, 2018; AlAhmad, Kahtan, Alzoubi, Ali & Jaradat, 2021). The way users can deal with these security risks in addition to security management of cloud providers is related to the concept called “users information security awareness”. The information richness that users have about information security awareness is in the interest of protecting against the potential vulnerability of the cloud.

Users' richness to protect data and their information security awareness makes them responsibly understand the significance of potential risks and threats and take various measures accordingly (Kruger & Kearney, 2006; McCormac et al., 2017; McLeod & Dolezel, 2022). The main goal of information security awareness as a preventive measure is to reduce human error in security incidents. Users must weigh the benefits of cloud storage against its risks. Therefore, it is necessary to understand users' awareness, beliefs, and treat toward cloud storage technology and its security over time and to explore factors related to cloud storage security beaches that influence their usage behavior (Alsmadi & Prybutok, 2018). Thus, users’ information security awareness affects the prevention of loss events, exposure of stored data to malicious acts, and recovery and remediation of the consequences of a security incident or unauthorized activity as corrective controls. It is necessary to occasionally assess users' richness of information security awareness to reinforce the strengths and eliminate possible weaknesses.

On the other hand, it is noteworthy that Apple Inc. products are currently used by various users worldwide. However, according to our primary studies, despite the importance of the information security challenges in iCloud (explained in the following sections) as a cloud service of Apple Inc., no research was found on iCloud users' information security awareness in Iran and abroad. Therefore, in addition to all the benefits and reasons to use the cloud in one form or another, it is important to consider the importance of security when moving to cloud platforms (Deighton & Wakefield, 2020), which is measured in this research on the use of Apple Inc.'s cloud service. The present study aims to address the security challenges faced by Iranian iCloud users and to assess their information richness in terms of information security awareness at the three levels of knowledge, attitude, and behavior, based on six different aspects required for information security compliance, to show that users can better cope with the probable threats to information security in the cloud if they are aware of the vulnerabilities of information security in the cloud. To this end, the results of this study will address the following specific objectives:

- Demographic characteristics of Iranian users of Apple Inc. products (IUAP), including age, gender, education level, and duration of likely use of the iCloud service ;
- IUAP familiarity with the basic concepts of information security in general and malware, hacking, and time intervals for changing iCloud passwords in particular;
- The usage rate of the iCloud service by IUAP, as well as the reasons for using or not using it and the main benefits of using iCloud from their point of view;
- Actions taken by IUAP to improve iCloud security on six different aspects required for information security compliance;
- IUAP awareness of information security measures embedded in iCloud at the three levels of knowledge, attitude, and behavior; and
- Assessing the information security richness from IUAP about iCloud information security awareness and prioritizing the components that require attention in this regard.

Users who do not adequately understand the significance of information security will not be able to protect their information and passwords in iCloud, and thus, they may lose their information privacy, some of which is irreparable. Then, it must be ensured that users are well justified and comply with what they must do to provide security policies and procedures. The results of this study give an accurate picture of the status and importance of information security for iCloud users.

Features, Advantages, and Disadvantages of Cloud Storage

Using portable devices such as flash drives or hard disks to store data and information increases the risk of data loss or damage, thus urging computer professionals to seek a more reliable method, which leads them to come up with some solutions, one of which is the concept of cloud storage. Cloud storage mitigates the need for advanced hard disks on the client (Talib, Clarke & Furnell, 2010). Cloud storage is a network-based model where data is stored on virtual servers. This service is usually offered by hosting companies that have large data centers. Private, public, hybrid, and community clouds are different deployment models for cloud-based technologies. Users who want this hosting can buy or hire storage space from these companies.

On the other hand, cloud storage providers are virtualizing their data sources according to users' needs for management by users. In practice, the data stored on a virtual server may be stored on several physical servers. Cloud service providers try to offer solutions for data storage, similar to public industries (like water, electricity, telecommunications, etc.). This means providing access to technology-based information resources over the Internet at the time of need and based on user demand is elastic and scalable, like that users pay for the electricity or water they consume. So, if a fee is charged to users for this type of service, users only pay for the amount of services they use from the cloud. This method of calculating costs is the "pay-as-you-go" method, which can help reduce capital costs but can also result in unexpected operating costs for unaware users.

In this regard, cloud storage services allow users to store, backup, and recover their ever-increasing amount of data and “provide a shared pool of resources for users to process and transfer their files seamlessly” at low cost (Prajapati & Shah, 2020). Perhaps in the public mind, one of the most essential features of these cloud storage services is the provision of backups copies of all required information such as images, videos, documents, audio files, etc. Users can upload this information to their accounts and access their data as needed by logging into their accounts from an Internet-connected device such as a phone, PC, or other devices. Hence, given the progress in recent years, these cloud computing-based storage services have become popular among users (Kruger & Kearney, 2006; Vurukonda & Rao, 2016; Prajapati & Shah, 2020; Deighton & Wakefield, 2020). The advantages of cloud storage services don’t confined to the aspects mentioned above and, among others, include utilization and efficiency improvements while device and location independence, diminished cost of using non-cloud technologies, scalability and elasticity in easy storage of data without the need to engineer for peak loads, and subsequently peak-load capacity boosting, faster execution of commands, optimal use of green technology, increased memory capacity for storage, agility, and easy portability of information at any time and anywhere, higher compatibility of the of stored documents, reliability of the data production process in such spaces, facilitation of teamwork, saving of time, and adaptability to consumer preferences (Vurukonda & Rao, 2016;). Generally, avoidance or minimization of up-front IT infrastructure costs is another benefit highlighted by cloud services advocates (Deighton & Wakefield, 2020).

On the other hand, it should be considered that all technologies have some drawbacks and limitations along with their benefits, and cloud storage has proven to be no exception. Although the advent of cloud storage has led to the advantages mentioned above, users are still indecisive about embracing cloud-based technologies, mainly due to a lack of confidence in some of the cloud issues such as reliability, lack of standards, regulations, and legal issues, and security of data hosted on an outside server (Vurukonda & Rao, 2016). As discussed earlier, the relative security of cloud storage is a controversial issue that privacy advocates criticize and could delay cloud storage acceptance. Some precautions have been taken on the part of service providers regarding the vulnerability of cloud security. It must be considered that often, at the beginning of the application to cloud storage services use, in an agreement on their privacy policies, which is left with negligence, stored data in case of need for law and order without authorization that provider cloud to share information with third parties. Thus, user misbehavior fuels this issue and unconsciously leads to penetrating the information assets in the cloud. Hence, users of cloud services often need to be aware of the legal and regulatory differences. Also, there are numerous legal cases in which software companies collude and misuse private information for their business interests and publishe this information publicly worldwide. Indeed, legal ownership of the data is challenged in cloud storage. As a result, although trust is necessary, it is not enough to offer sensitive or private information to a commercial company. As such, end users are responsible for protecting their information, which can be achieved by skills and awareness that users must acquire through their experiences of privacy issues in general and cyber information security issues in particular when submitting sensitive, confidential data to various clouds. Also, another solution used by professional users to deal with these risks is processed or stored data encryption in a cloud to prevent unauthorized access. Of course, this solution requires more relevant expertise and contradicts (Vurukonda & Rao, 2016) and challenges some of the benefits of this technology. Nevertheless, it should be noted that advocates of this technology believe that service providers have a strong incentive to maintain trust and, therefore, use a higher level of security.

Some of the disadvantages of cloud storage include the need for a permanent internet connection, inaccessibility of data in downtime, inadequate performance in poor connections or peak-load, the limited capability of applications in cloud spaces, reduced security of data stored therein, lack of continuous control over data processing, the possibility of cyber-attacks, lack of decisive regulations for the prosecution of offenders, and data transfer between clouds.

Therefore, it is worth mentioning that various essential security challenges and policies arise in cloud storage technologies. These challenges include unauthorized access, data leakage, sensitive information disclosure, privacy disclosure, confidentiality, reliability, and security as one the most important (Prajapati & Shah, 2020; Sehgal, Bhatt & Acken, 2020; Yang, Xiong & Ren, 2020). Given the security issues in the cloud storage, users' data should be protected against any cyber infiltration or misuse of cloud-stored information by cloud service providers. Dramatically number of security and data breaches per month in the cuple of recent years had a significant rising trend, as warned by Prajapati and Shah (2020). This issue influences the performance of cloud spaces, too. As a result, in some cases, we are urging cloud service providers to find a way to provide much security and higher performance together. To this end, some systems capable of automatically detecting suspicious operations along the cloud storage network have been proposed. These operations include unauthorized access, firewall bypass, preventing virus-infected data transfer, cyber-attacks, etc. (Kruger & Kearney, 2006).

iCloud and its Security Challenges

Among the abovementioned clouds, iCloud is a cloud storage service provided by Apple Inc., which was launched on October 12, 2011, and then introduced in 2014 at Apple's Worldwide Developers Conference (WWDC). This service aims to make a backup copy of the information stored on devices such as iPhone, iPad, or iPod. In other words, iCloud is a cloud service for Apple Inc. products, used for online storage, backing up, and synchronization of emails, contacts stored in various apps and devices, calendars, etc. (Kruger & Kearney, 2006). This cloud service seems to perform more optimally than a physical hard drive and offers an easy way to access the contents of all iCloud-enabled devices. It provides users instant access to music, applications, emails, and the latest files without the need for prior synchronization and management of information.

Based on the aforementioned discussions, the prevalence of cloud storage on the one hand and the functionality of iCloud, on the other hand, have led to various challenges for users, including the security of information stored thereon, especially private information. For example, on 31 August 2014, over 100 personal photos of celebrities were stolen from iCloud and leaked online by an anonymous hacker. The main challenge of iCloud security is that the data owner has no full and conscious control over the data, which in turn causes various complicated issues and prevents users from the optimal use of iCloud (Kruger & Kearney, 2006). However, Apple is trying to increase the security of iCloud information by adopting policies such as access control, data encryption, and server authentication by service providers to address the challenges (Talib et al., 2010). On the other hand, it should be borne in mind that information security should not be considered solely by service providers, that is, users and their awareness of the concepts of information security and management also play an essential role in increasing security. So, raising iCloud users' information security awareness helps better protect and manage information security (Von Solms & Von Solms, 2004).

Literature Review

With the ever-increasing use of various technologies in daily life, the interactions between people and information sources in the technological environment have led to information security challenges and increased the potential for security breaches. (Tolah, Furnell & Papadaki, 2021). Therefore, the risks to information security in general and cloud storage security in particular have been considered in academic literature and research. Numerous studies have addressed information security globally, but studies on the role of user awareness in managing this security are limited, particularly concerning the use of cloud computing technology. In addition to studies on various technical aspects of this issue, for which there is ample evidence, some studies have discussed various aspects of information security awareness, including organizational awareness, the work environment, the home environment, and individual characteristics focused on user behavior toward technology. The following are related to the subject of research worldwide.

Kruger and Kearney (2006) designed a pilot model for assessing and measuring information security awareness at the organizational level for an international mining company. They argued that such models are valuable asset for organizations in controlling and guiding strategic goals to establish information security. Based on the proposed model, the authors considered three levels of knowledge, attitude, and behavior to measure the richness of individuals' information security awareness. These included issues like adhering to policies, keeping passwords secret, reporting security threats to relevant administrators, etc. If used properly, these strategies can improve individuals' information security awareness in workplaces, which will also make them enthusiastically seek information security in home environments.

Makarevich, Mashkina and Sentsova (2013) proposed a method for evaluating the possibility of information security risks in cloud computing systems. Considering the research goal, they proposed fuzzy cognitive maps and artificial neural networks (ANNs) to address the information security risks in the cloud storage. Using this approach, the possibility of a threat or the acceptable level of risk is investigated to strengthen the protection mechanisms against unwanted security risks and instantly provide an appropriate logical response to attacks.

In line with these studies, various researchers have also considered the influences of personal characteristics and aspects on information security. Khan, Alghathbar, Nabi and Khan (2011) explored information security awareness tools and techniques according to psychological theories and models while Tsohou, Karyda and Koklakis (2015) focused on security decision-making and concluded that cultural and cognitive biases affect information security awareness and related behaviors. Based on their findings, they offered some recommendations on how to improve security information awareness programs.

Vurukonda and Rao (2016) studied the issues related to cloud data storage and presented possible solutions to the problems in the cloud. They classified cloud security challenges in three categories: 1. Data storage issues; 2. Identity management and access control; and 3. Contractual and legal issues.

Prajapati and Shah (2020) in literature review of Cloud storage services point out researches about several approaches including Convergent Encryption (CE), Proof of Ownership (PoW), Provable Data Possession (PDP), Proof of Retrievability (POR), secure keyword search, DupLESS, Proof of Storage with Deduplication (PoSD), Dekey, Message-Locked Encryption, Attribute-Based Encryption (ABE) and Identity-Based Encryption (IBE) to address client’s security concerns. Also they compare cloud service providers’ facilities of AWS, Azure, Cloud, Oracle, IBM, and Alibaba in different aspects of critical security control services to protect the confidentiality and integrity of data and suggest some of them based on provided prioritization. This research’s main focus is reviewing various scientific findings to mitigate storage overhead and save upload bandwidth to use secure deduplication data techniques in cloud storage. Finally, these researchers provide potential directions and ideas for improvements in secure deduplication cloud storage techniques.

As per Sehgal, Bhatt and Acken (2020) Data Movement, Loss of Control, Uncertain Performance, Identity Authentication and Unauthorized Access, Data Theft, Denial of Service Attacks, Data Integrity, Invasion of Privacy and Activity Monitoring, Web Threat Models: HTML, Rendering Content, Remote Scripting, Cookies, Frames and frame busting; Web Application Security: Injection, Broken Authentication and Session Management, Cross-Site Scripting (XSS), Insecure Direct Object References, Security Misconfiguration, Sensitive Data Exposure, Missing Function Level Access Control, Cross-Site Request Forgery (CSRF), Using Components with Known Vulnerabilities, Un-validated Redirects and Forwards are different serious dimensions of cloud storage risks. With this all-encompassing warning, they encourage vendors to follow interoperability standards in their edge-based devices to reach the evolution of the edge computing domain with IoT-based solutions. They detected the issues, as mentioned earlier, of user-data privacy and legal jurisdiction as a lag in this fast evolution.

Tolah et al. (2021) proposed two factors to elevate influential information security culture in organizations in protecting their information assets against security breaches. Based on their research, dimensions include those factors that influence security culture (top management, security policy, security education and training, security risk analysis and assessment, and ethical conduct), those that reflect security culture (security awareness, security ownership, and security compliance), and factors of organizational behavior (job satisfaction; personality traits). This study showed a significant relationship between personality traits and security culture. AA framework has been provided based on results as a tool for assessing and improving organizational security culture management.

Of course, the issues related to security information in cloud storage have also been studied in domestic research in Iran. In a study entitled “A framework for the role of human factors in Information Systems Security", Elahi, Taheri and Hasanzadeh (2009) pointed out information systems security as a critical issue organizations worldwide face. The authors proposed a model based on "human" factors emphasizing “behavioral information security”. This model is based on the notion that users and human factors are generally the weakest and most vulnerable elements in the security models for information systems. They concluded that no information system or organization can establish security or even claim to have one such fully. However, there are specific exercises that managers can employ to optimize their security support and efficacy. Finally, the theoretical model proposed in this study is claimed to assist managers in focusing their efforts on potentially decisive areas in information security.

By examining Postbank employees' information security awareness, Jahangiri (2011) provided a conceptual framework for evaluating the richness of users' information security awareness and educating them on it. This study assessed users' information security awareness at three levels: knowledge, attitude, and behavior. To this end, survey methods and a questionnaire were employed to collect data. The findings indicated that (1) information security training is of utmost significance, and (2) to enhance training effectiveness, in the security awareness program, it is necessary to consider employees' occupation, academic discipline, and job credit.

In a study entitled “Information technology risk management in cloud computing”, Kazempourian Mamghani and Mirahmadi (2016) argued that cloud computing offers unlimited computing power, good scalability, on-demand capacities etc., while challenging security, privacy, legal issues, and so on, on the other hand. The authors proposed some solutions for cloud users to minimize the risks and vulnerabilities of cloud computing systems. As such, they introduced two new categories for information security risks in cloud computing.

Moreover, Ghasemi, Kiumarsi and Zamani Dehkordi (2017) examined the secure storage and transmission of messages in cloud-based networks. Given its cost-effectiveness, they argued that the cloud computing network has become an ideal platform for using service-oriented architecture. Yet the most critical challenge of this technology is its security, which has made managers of some organizations distrust it. Also, they examined security approaches to data storage and transmission in the cloud space. Furthermore, the properties of cloud computing, its challenges, data storage and transmission security in private cloud spaces, access level determination methods, data encryption, and the use of server authentication were discussed.

Accordingly, Zeinali Khosroshahi, Babaei and Ghasemi (2018) studied the security challenges of cloud computing and argued that owing to the high level of user access and the sharing of a significant amount of information, this technology often faces a plethora of security issues. To this end, the latest security advancements in cloud-based networks were reviewed, and it was cited that intrusion detection and prevention systems were the most crucial security operations because infiltrations and intrusions severely undermine the cloud platform. Therefore, the researchers concluded that providing methods and models for creating and maintaining security in cloud-based systems is necessary.

In general, according to research backgrounds, it is found that despite the recent emergence of data security and privacy protection studies and focusing on concepts related to cloud computing technology, information security is still a highly sought-after subject, and still lack of systematic surveys is felt about cloud storage systems by various above mentioned national and international researchers (e.g Yang et al., 2020, Zhang, Xu & Shen 2020, etc.). Also, in many of these works of literature, most reasons for inefficient information security in information technology are attributed to human factors.

Materials and Methods

The present study is applied research in which data were collected using a researcher-made questionnaire designed based on the literature review and awareness assessment provided by Kruger and Kearney (2006). Accordingly, users' information security awareness was measured in six categories of ‘basic familiarity with information security concepts’, ‘information attacks including malware, hacking, etc.’, ‘community engineering’, ‘backup security’, ‘data transfer and protection’, ‘password’, ‘adherence to security policies of the cloud service provider’ at three levels of knowledge (what people know), attitude (how people feel about security issues), and behavior (what people do in this regard). Values gained from awareness assessment indicate users' information security awareness in these three levels and their sum. Values below 59 mean unsatisfactory awareness, 60-79 mean further examination of awareness and more education of users are required, and 80-100 mean satisfactory awareness. In addition to the reliability and convergent validity of the questionnaire, the difference between a variable’s indicators and other variables’ research indicators should be compared to evaluate the divergent validity. It is calculated by comparing the AVE’s square of each variable with the correlation coefficients between the first-order variables. To do so, a matrix is formed whose main diameter values are the square root of the AVE coefficients of each variable, and the lower values of the main diameter are the correlation coefficients between each variable and other variables (Hair, Ringle & Sarstedt, 2011). These values are shown in Table 1.

Table 1
Divergent Validity Results

Concepts	perceived usage of iCloud	information security richness
perceived usage of iCloud	0.808	
information security richness	0.543	0.744

As shown in Table 1, all AVE square values for each variable are greater than correlation coefficients between first-order variables. As a result, the questionnaire enjoys excellent divergent validity. The statistical population included IUAP in different age groups, genders, and educational levels. Participation in this study was voluntary, and questionnaires were submitted to the statistical population online and in hard copy. Due to the infinity of the statistical population, there is no determined volume of its number. Following Krejcie Morgan's table and assuming it has more than 10,000 users, the sample size was estimated to be 384, and samples were randomly selected. In addition, the collected data were analyzed using descriptive statistics such as percentage, mean, and frequency using Microsoft Excel software. In addition to the validation of the questionnaires by the experts who have done similar studies, Cronbach’s alpha coefficient has been used to assess the reliability of the questionnaire and ensure the internal consistency of the measurement tool.

A Likert scale has been used (1 (disagree to 5, totally agree) to measure each question. The use of SPSSwin19 and SmartPLS 3 has also analyzed the data. After that, the main research hypothesis was examind based on the information security richness effectiveness that correlated with the perceived use of iCloud. Structural Equation Modeling (SEM) has also been used. It should be noted that the least allowable value for Cronbach's alpha is 0.7 (Hair, Ringle & Sarstedt, 2011). The present research is reliable since Cronbach's alpha value calculated for each variable was above 0.7.

Results

In this section, the collected data, including demographic information IUAP's knowledge of information security issues, are categorized and presented in general and iCloud. These results are divided into different parts; firstly the demographic information regarding gender, age, education levels, and familiarity with information security concepts. Second, the usage rate of the iCloud service by Iranian Apple Inc. product users and their experiences of using/not using it. The third part was the knowledge section to evaluate Iranian iCloud users' security knowledge and awareness levels. It includes knowledge, attitude, behavior scores and ranking priorities of components requiring attention. Finally, the correlation examined between information security richness effectiveness and the perceived use of iCloud. According to the findings, Table 2 shows the classification of IUAP in terms of age group:

Table 2
Age Frequency Distribution of IUAP

	Age group	Frequency	Percentage
1	Less than 10 years	1	0.26
2	11- 20 years	56	14.58
3	21- 30 years	231	60.16
4	31-40 years	70	18.23
5	41-50 years	20	5.21
6	More than 50 years	5	1.30
7	N/A	1	0.26
Total		384	100

As shown in Table 2, most IUAPs are aged between 21 and 30. However, these products rarely have an audience under the age of 10. Table 3 shows the classification of them by gender.

Table 3
Gender Frequency Distribution of IUAP

	Gender	Frequency	Percentage
1	Female	206	53.65
2	Male	168	43.75
3	N/A	10	2.60
Total		384	100

Regarding the genders of IUAP, 54% (n=206) are females, and 44% (n=168) are men. The classification of them at the educational level is presented in Table 4.

Table 4
Frequency Distribution of IUAP's Levels of Education

	Level of education	Frequency	Percentage
1	High school diploma and lower	43	11.2
2	B.A or B.S	225	58.59
3	M.A or M.S	86	22.4
4	Ph.D and higher	27	7.03
5	N/A	3	0.78
Total		384	100

Table 3 reveals that most IUAP have a bachelor's degree, followed by a master's degree, high school diploma and lower, and a Ph.D. and higher. Then, IUAP's familiarity with the basic information security concepts was investigated. Table 5 shows their frequency distribution regarding the level of familiarity with the basic security concepts.

Table 5
Frequency Distribution of IUAP's Levels of Familiarity with the Concepts of Information Security

	Level of familiarity	Frequency	Percentage
1	Very low	43	11.2
2	Low	49	12.77
3	Moderate	126	32.81
4	High	107	27.86
5	Very high	58	15.10
6	N/A	1	0.26
Total		384	100

As seen in Table 4, 23% of respondents self-reported having low or very low familiarity with information security concepts. IUAP’s average familiarity with information security concepts was obtained at 3.22 out of 5, a slightly above median value. As a result, it seems they should be moderately familiar with the concepts of information security. The various aspects of information security and the level of IUAP awareness were studied after a general survey. The findings on IUAP’s familiarity with malware, as one of the principles of richness in awareness levels, are presented in Table 6.

Table 6
IUAP’s Levels of Familiarity with the Concepts of Malware Frequencies

	Level of familiarity	Frequency	Percentage
1	Very low	133	34.64
2	Low	80	20.84
3	Moderate	74	19.27
4	High	62	16.14
5	Very high	34	8.85
6	N/A	1	0.26
Total		384	100

Table 6 indicates that more than half of 384 IUAP have low or very low familiarity with the concept of malware, although 8.85% had very high familiarity with the concept. The IUAPs' average awareness of the concept of malware was calculated to be 2.4 of 5, indicating a low level of awareness. Another aspect of familiarity with information security is the awareness of the concept of hacking and examples of getting it, the results presented in Table 7.

Table 7
Frequencies of IUAP's Levels of Familiarity with the Concepts of Hacking

	Level of familiarity	Frequency	Percentage
1	Very low	32	8.33
2	Low	54	14.07
3	Moderate	89	23.18
4	High	139	36.20
5	Very high	70	18.22
Total		384	100

As shown in Table 7, it can be concluded that most IUAP self-reported being highly familiar with the concept of hacking, and only 8.33% (n=23) self-reported being unfamiliar with the concept. Accordingly, IUAP's average awareness of the concept of hacking was 3.4 of 5, which is an above-median value. Then, participants were asked about their usage of iCloud, the cloud storage service by Apple Inc. The results are listed in Table 8.

Table 8
Frequencies of IUAP's Usage Rate of the iCloud Service

	Usage rate	Frequency	Percentage
1	Very low	100	26.04
2	Low	48	12.5
3	Moderate	37	9.64
4	High	57	14.85
5	Very high	140	36.45
6	N/A	2	0.52
Total		384	100

As shown in Table 8, most use IUAP apply this service frequently. However, a quarter of the statistical population had minimal experience using this service, and only about 10% of IUAP used this service moderately. IUAP, who did not seek the benefits of this service, cited the reasons listed in Table 9 as their main reasons.

Table 9
Frequencies of Reasons Cited by IUAP for Not Using the iCloud Service

	Reason for not using iCloud	Frequency	Percentage
1	Not efficient on slow Internet connections	17	6.1
2	Technical difficulties while operating	14	5.01
3	Better or alternative services	18	6.45
4	High costs (financial/ non-financial) of using iCloud	30	10.75
5	Getting out of reach of cloud provider	18	6.45

6	Requiring a permanent Internet connection	33	11.85
7	Inefficiency	23	8.25
8	Low security of this space	13	4.65
9	Lack of familiarity with iCloud	85	30.46
10	Applied restrictions and filters	28	10.03
Total		279	100

Table 9 reveals that the most prevalent reason for not using iCloud was unfamiliarity with iCloud (frequency= 85, 30.46%), while the least pervasive reason was the low security of this space (frequency= 85, 4.65%). Other reasons for not using iCloud are almost scored similarly. The following section discusses only the findings on Iranian iCloud users. Of course, it should be explained that only 228 from the statistical sample were using iCloud.Considering that iCloud was introduced worldwide in 2011, IUAP’s length of experience using this technology is presented in Table 10.

Table 10
IUAPs' Lengths of Experience of the iCloud Service

	Length of experience	Frequency	Percentage
1	Less than 1 year	39	17.10
2	1-2 year	57	25
3	3-4 years	64	28.1
4	5-6 years	45	19.73
5	7-8 years	22	9.64
6	More than 8 years	0	0
7	N/A	1	0.43
Total		228	100

Table 10 shows that respondents have reported different lengths of experience using the iCloud service. The most extended period of familiarity and use is between 3 to 4 years (frequency= 64, 28.1%), while the shortest is reported to be 7 to 8 years (frequency= 22, 9.64%). Table 11 points out why IUAP is considering using iCloud as a cloud service.

Table 11
Reasons Cited by Iranian Apple Product Users for Using the iCloud Service

	Reasons for using iCloud	Frequency	Percentage
1	No particular reason	30	7.47
2	Will be used in the future	15	3.74
3	To generate content	19	4.72
4	Proper security of this space	105	26.11
5	Easy access to stored data in this cloud	123	30.59
6	To allocate high volumes of space for storage	80	19.90
7	Solely due to being the default space in a device	30	7.47
Total		402	100

As seen in Table 11, it can be concluded that the IUAPs' main reason for using iCloud is the easy access to information stored in this space (frequency=123, 30.59%), followed by the proper security of iCloud space (frequency=105, 26%), and the allocation of high volumes of space for storage (frequency=80, 20%). In this regard, IUAP also reported the benefits of using iCloud, listed in Table 12.

Table 12
The Averages of the Most Important Benefits of Using iCloud

	Component	Average
1	Easy storage of data	3.72
2	Providing backups of data	3.82
3	High server capabilities	3.51
4	Efficiency increment	3.27
5	Software as a service	3.26
6	Saving costs and time	3.15
7	Saving costs of applications	2.94
8	Dynamism and portability	3.65
9	Facilitating teamwork and collaboration	3.12
10	Extensibility	3.27

Table 12 indicates that among the advantages of using iCloud space, providing backups, easy data storage, and easy portability components receive the highest rankings respectively. This is while IUAP paid less attention to saving software costs in using iCloud space. Based on previous findings on the widespread use of iCloud by IUAP, researchers considered their awareness of various aspects of information security embedded in Apple Inc.'s service. Table 13 shows the results obtained for this issue.

Table 13
Frequency of IUAPs' Awareness of Security Aspects Embedded in iCloud

	Security aspects	Frequency	Percentage
1	Not aware	66	30.55
2	Identity management and authorization	89	41.20
3	Access control	61	28.25
4	Other aspects	0	0
Total		216	100

According to the frequencies in Table 13, Iranian iCloud users know the security aspect of identity management using the service. This type of security includes the confirmation of an IUAP's authenticity when he/she logs in. Also, about 28% of IUAP noticed that content access of IUAP is checked when using iCloud. However, nearly one-third of iCloud users still did not realize that these items are embedded to protect users' information in iCloud. Another aspect that needs to be addressed to improve information security is the constant change of accounts' passwords. Table 14 summarizes the time interval between password changes by IUAP.

Table 14
The Frequency of Time Intervals of Changing Password

	Duration	Frequency	Percentage
1	Every 6 month	12	5.35
2	Every 8 month	7	3.15

3	Every one year	18	8.03
4	When the need arises without a prior schedule	86	38.39
5	Never change	100	44.64
6	N/A	1	0.44
Total		224	100

According to Table 14, although the constant and occasional change of password in the cloud is necessary to improve overall information security, about 45% of users never change their passwords, and about 38% of them change their passwords only when they feel the need and threat without any predetermined schedule.

The various measures that IUAP is expected to take to comply with multiple aspects of information security are discussed below. The results are presented in Table 15.

Table 15

Various Measures IUAP Takes to Improve the Information Security of iCloud

	Component	Yes		no	
		Frequency	Percentage	Frequency	Percentage
1	Other persons not having access to the iCloud accounts of users	24	10.66	201	89.33
2	Storing the backups of the information in iCloud	155	69.19	69	30.80
3	Storing information in a space other than the device connected to iCloud	83	50.92	80	49.07
4	Making sure the information is virus-free	50	22.32	174	77.67
5	Using uppercase letters for iCloud passwords	193	86.16	31	13.83
6	Using numerals for iCloud passwords	206	92.37	17	7.62
7	Using non-letter and non-numeric characters such as (, / *) for iCloud passwords	85	38.63	135	61.36
8	Familiarity with software bugs in iCloud	64	28.95	157	71.04
9	Configuring the access of apps to the iCloud space	140	62.78	83	37.21
10	Reporting from iCloud after using it	64	28.95	157	71.04
11	Familiarity with ways to recover data in the case of data loss	128	57.39	95	42.60

According to Table 15, Iranian iCloud users have the highest information richness of awareness of using numerals for iCloud passwords (92%), followed by not having access to iCloud accounts to others (90%), and using uppercase letters for iCloud passwords (86%). The least prevalencet measures these users take in this regard are ensuring that the information is virus-free (77%), being familiar with the software bugs in iCloud, and reporting from iCloud after using it (both 71%).

Finally, the information richness of Iranian users' iCloud information security awareness was assessed based on the adapted tool described in the methodology section, shown in Table 16. In this table, values indicate IUAPs' information security awareness.

Table 16
Richness of iCloud Users' Information Security Awareness

	knowledge	attitude	behavior	Awareness of each component	Priorities of components requiring attention
Basic familiarity with the concepts of information security	96.57	68.58	94.09	86.41	6
Information attacks include malware, hacks, and more	86.37	63	58.29	69.22	2
Community engineering	83.15	64.22	76.34	74.57	3
Security of data backups, transfer, and protection	39.35	55.14	33.58	42.69	1
Password	89.39	74.85	92.41	85.55	5
Adherence to the security policies of the cloud service provider	93.45	73.26	86.84	84.52	4
	Awareness at the level of knowledge = 81.38	Awareness at the level of attitude = 66.51	Awareness at the level of behavior = 73.59	Overall awareness of the components = 73.83	

Finally, the SEM with the partial Least Squares approach was used to evaluate the model fitness and analyze the data. Therefore, the model fitness was assessed using reliability, convergent validity, and divergent validity criteria. Cronbach’s alpha and combined reliability were used to evaluate the model’s reliability. Also, the questionnaire’s validity was assessed using convergent and divergent validity. The Average Variance Extracted (AVE) was used to evaluate the convergent validity. The results for these criteria are presented in Table 17.

Table 17
Statistics of the Model Fitness Evaluation

Concepts	indexes	factor load	T statistics	CR	AVE
information security richness	Q1	.781	21.025	.832	.555
	Q2	.704	13.581		
	Q3	.639	9.21		
	Q4	.698	14.585		
	Q5	.701	13.297		
perceived use of iCloud	Q6	.783	20.433	.852	.656
	Q7	.781	22.973		
	Q8	.759	16.45		
	Q9	.645	9.725		
	Q10	.674	10.711		

	Q11	.774	4.26		
	Q12	.812	2.444		
	Q13	.652	9.17		
	Q14	.895	3.51		
	Q15	.793	4.466		

As seen in Table 17, all combined reliability values of the research constructs are above 0.7. Also, the AVE values for the constructs are above 0.5, indicating the research model's acceptable reliability and convergent validity.

Structural Model Fitting

The most basic indicators for the structural model are its path coefficients and significance. The outputs and test results are shown in Table 18. It should be noted that for evaluating the significance of the correlations, the t-statistic values should be considered. The standard value above the absolute value of 1.96 indicates the significance of the relationship.

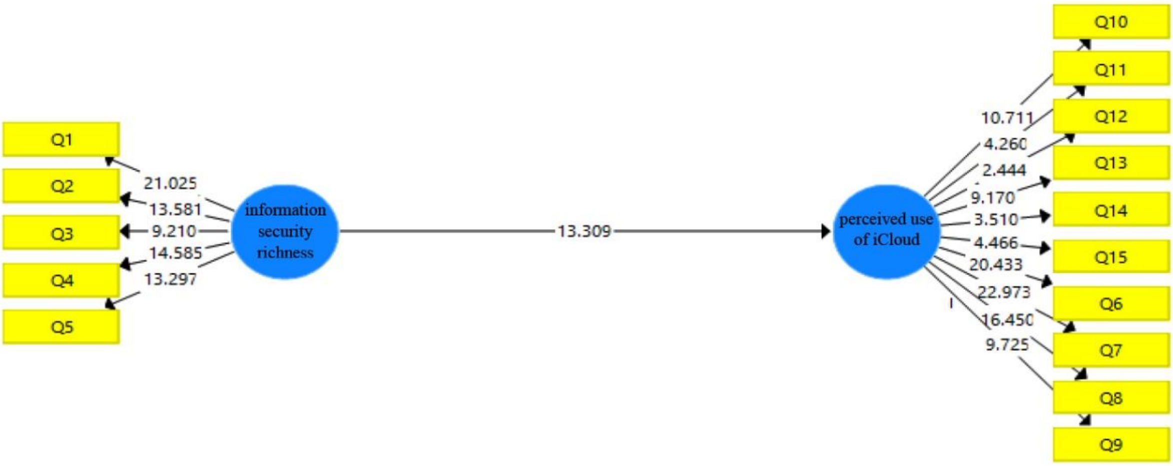

Figure 1: The Significance Level Of The Research Model

As it is shown in Figure 1, The path coefficient of the research variables has been above 1.96, so the research hypothesis is significant and approved. The significance test results show t statistic=13.309, proving the significant relationship between variables. The coefficient of determination (R^2), effect size (f^2), and measurement criterion value (Q^2) are the other criteria used to connect the SEM’s measurement and structural sections, which are equal to 0.595, 0.418, and 0.256, respectively, in analyzing the results of effects on endogenous variables and structural model quality values. The three values of 0.19, 0.33, and 0.67 have been proposed as the standard values for weak, medium, and strong values of coefficient of determination (Chin, 1998), and 0.02, 0.15, and 0.35 have been proposed for weak, medium, and strong values of effect size and measurement criterion value (Henseler, Ringle & Sinkovics, 2009). The values obtained indicate the acceptability of the fitness of the structural model.

Evaluation of the General Model

In addition to the criteria mentioned above for the evaluation of the measurement model and the structural model, a criterion named goodness-of-fit (GoF) index proposed by Tenenhaus, Amato and Esposito Vinzi, (2004) is also used for the overall evaluation of the model (equation 1). This criterion considers both the measurement and structural models at the same time. In fact, by using this criterion, the researchers controlled the fitness of the general section after evaluating the fitness of the model's measurement and structural sections. Fornell and Larcker (1981) have proposed the three values of 0.01, 0.25, and 0.36 as the weak, medium, and strong values for this criterion.

Equation 1:

$$GOF = \sqrt{\overline{Com} \quad \times \quad \overline{R^2}} = \sqrt{0/256 \times 0/595} = 0/390281$$

Regarding the criterion values for the general model evaluation, the obtained value of 0.390 indicates a strong fitness of the model.

Research Hypothesis Testing

The researchers can investigate and test hypotheses after evaluating the fitness of the measurement, structural, and general models. Therefore, the effects of independent and dependent variables were analyzed using the SEM in two cases of significant numbers to check the hypotheses and standard estimation to check the intensity of the influence of the variables on each other. The results are shown in Table 18.

Table 18
Results of Hypothesis Testing

structural path	Significant value	Path coefficient	Result
direct effects			
the information security richness→ Perceived use of iCloud storage	13.309	0.543	confirmed

As Table 18 shows, the results of hypothesis testing indicate that the correlations between the variables are significant, and as a result, the main hypothesis of the research is approved.

Discussion

In recent years, everyone utilizing technology has learned about the many benefits of using the cloud. Nevertheless, with the rapid development of information technology, information security and access have significantly been considered. As a result, with the widespread use of cloud storage worldwide, which is one of the state-of-the-art models for distributing and providing IT services, its security due to new vulnerabilities with the possibility of widespread cyberattacks has become one of the most important and thought-provoking challenges. The present study sought to investigate how much Iranian iCloud users are familiar with the concepts of information security and how they protect their information against intrusion and hacking at a time when new technologies such as smartphones, computers, etc., have affected all aspects of human life. In other words, the present study assessed the Iranian iCloud users' awareness of information security and management concepts. In the present study, which aimed to investigate the effects of information security richness on the use of perceived iCloud storage, the research hypotheses were formulated by studying the theoretical foundations and the research background. The results indicated that the richness of information security significantly and positively affects perceived cloud storage (with an effect size of 54.3%). According to Table 2 (demographic information of participants), Apple products are more popular among younger users aged between 20 and 30 in Iran. About 80 percent of the participants had a bachelor's degree or higher. The reason for that could be the user interface, successive creativity and innovations, appearance, color, design, quality, and technologies employed by Apple have made Apple products more desirable to the younger generation. Consistent with these findings, Zandvakili, Salehi and Rashidi (2012) acknowledged that this is natural and predictable considering Apple's credibility in science and technology and its half-century history.

The company has attracted many users annually by introducing new and up-to-date products, most of whom are youth (Motahari, Rouhani & Zare Rawasan, 2014). About the usage of iCloud by IUAP, participants stated several reasons for not using iCloud, the most important of which were unfamiliarity with iCloud (30%) and the high financial and non-financial costs of using iCloud. On the contrary, due to the easy use of information stored in iCloud with no temporal and spatial restrictions, Apple could encourage about one-third of users to keep their information in iCloud. Some people use it for no particular reason or simply because this possibility is built into Apple products. Most IUAP had 2-4 years experience of using iCloud. Therefore, it is necessary to consider these users' richness and identify the weaknesses and strengths of their information security awareness to take the measures required to remove the obstacles and improve the strengths.

In particular, collecting and analyzing data on IUAP s' information security awareness revealed that most respondents were moderately familiar with these concepts. More than half of the respondents reported that their familiarity with malware as a concept of information security was low or very low while they self-reported being well acquainted with the concept of hacking. These findings indicate that although users are familiar with general information security issues due to living in the information era, they are less familiar with its subcomponents and practical examples, warned Jarno et al. (2017) findings. In this regard, users should be familiar with the various dimensions of information security and enhance their awareness. This finding is the case that Prajapati and Shah’s (2020) result emphasizes cyber threats as one of the global risks in today's world.

On the other hand, users knew that iCloud designers had implemented the necessary security measures in this software to have awareness in knowledge level. However, 30% of IUAP had no information about these measures and their examples, which means to have awareness at the behavior level. The findings revealed that in Iran, when transferring information to iCloud, most users trust the company's brand and reputation and thus easily store their information in iCloud. Although trust in this company may be justified given its credit, iCloud is not immune to cyberattacks and data security issues, as its history proves. Also, McLeod and Dolezel (2022) found that data breaches are more likely when users are lax with security measures and do not follow security-related policies. So, users are urged to employ this space with more caution and take some measures to strengthen information security. As is often the case, people's information is easily hacked using various tricks and possible bugs in software. According to the findings, about 71% of participants were unfamiliar with software bugs.

According to Table 15, it is found that IUAP mainly uses the mandatory security measures embedded by iCloud designers, including uppercase letters in the account encryption (86%) and the combination of numerals and characters in the passwords (92%) (Awareness at the level of behavior). Related to these findings, Tolah et al. (2021) emphasize that a culture promoting secure human behavior through knowledge, values, and assumptions works better than merely factory's mandatory security measures, which is classified at the lowest level of awareness as awareness at the level of behavior. The only measures taken in this regard by Iranian users using iCloud were not giving access to their user accounts to others (about 90% of users), backing up information, and storing a copy of it in a space other than iCloud. These can be instances of information security awareness at the level of behavior. However, 77% of IUAP were unsure whether their information in iCloud was virus-free, which poses a potential risk to both the user and other iCloud users. Even in this regard, most IUAP did not change their account passwords intermittently; it is considered an essential and effective step in preserving information security, and only 35% of them changed their password without a particular schedule when they felt the need.

Conclusion

In conclusion, it seems that in Iran, despite people's interest in using information technology and smartphones, they have not been offered the desired training for acquiring the necessary skills in information security. Information security-related skills are one of the most essential factors for living in the information and technology age without damage. In this study, despite the high attractiveness of Apple products to the Iranian us IUAP, their general knowledge of all components of information security management in iCloud was estimated to be 73.83, which means further examination of awareness and more education of IUAP are required a need for higher levels of attention and training. Contrary to these findings, Tolah et al. (2021) observed an acceptable level of security awareness and knowledge in their research. In this perspective, they prescribe security risk analysis and assessment to help people "understand potential damage to security. It helps to increase awareness and knowledge, which improves the level of security culture".

The findings suggested that the dynamic process of information security awareness should first start with the security of data backups, transfer, and protection. It seems that alleviating users' unawareness of various aspects of information security, including (1) security of information backups, transmission, and protection, (2) being aware of information attacks, including malware, viruses, and hacks, and (3) social engineering, are of critical importance and considered three top priorities in this regard. To this end, attaining the required skills to prevent information loss greatly increases the likelihood of protecting information from attacks and malicious intrusion by hackers. Yet, this would not be possible without the cooperation of the educational organizations of the country and the application of appropriate fundamental programs on information security in general. In this regard, Tolah et al. (2021) required organizations "to use understandable guidelines to develop a culture of security awareness, which utilises various approaches to improve comprehension".

On the other hand, it is necessary for IUAP to increase their level of knowledge and to become familiar with the skills and measures required for preserving their information. Keeping up to date with the latest security measures and policies prepared by Apple Inc. as a cloud service provider will increase the optimal use of the facilities. Moreover, suppose such service companies particularly consider Iranian users and provide relevant educational content and related warning points personalized with Iranian users in iCloud and in Persian language to them. In that case, Iranian users can better recognize the need for adopting information security measures. It is suggested that future researchers who seek to study subjects related to the present study conduct this research on other communities and social classes. Also, it is recommended to perform the current analysis at different periods. Studies at different periods may lead to different results since the conditions are rapidly changing, and probably, these changes would affect the results. Finally, evaluating other effective aspects of information security richness on the use of perceived cloud storage is suggested regarding the importance of information security richness.

Limitations

The researchers always face limitations in their studies, some of which even pose at the beginning of the research. In general, any work of research has its limits. Some of the present research's limitations are noted in the following:

- A questionnaire has been used to collect the data in the present study. As a result, some participants may have refused to provide an accurate answer or provided a solution with lower accuracy. Their answers can also be affected by some specific conditions.
- Regarding the sample population, the results may vary for other populations. Thus, a 100% generalizability may not apply to the present research. Also, it has been conducted in a specific period, and thus, the results may not be the same for other periods.

References

AlAhmad, A. S., Kahtan, H., Alzoubi, Y. I., Ali, O. & Jaradat, A. (2021). Mobile cloud computing models security issues: A systematic review. *Journal of Network and Computer Applications*, 190. 103152. https://doi.org/10.1016/j.jnca.2021.103152

Alsmadi, D., & Prybutok, V. (2018). Sharing and storage behavior via cloud computing: Security and privacy in research and practice. *Computers in Human Behavior*, 85, 218-226. https://doi.org/10.1016/j.chb.2018.04.003

Chin, W. W. (1998). The partial least squares approach for structural equation modeling. In G. A. Marcoulides (Ed.), *Modern methods for business research* (pp. 295–336). Lawrence Erlbaum Associates Publishers.

Deighton, T. & Wakefield, M. (2020). Keep security top of mind when moving into the cloud. *Network Security*, 2020(6), 17-19. https://doi.org/10.1016/s1353-4858(20)30069-6

Elahi, Sh., Taheri, M. & Hassanzadeh, A. (2009). A framework for the role of human factors in information systems security. *Journal of Management Research in Iran*, 13 (2), 1-22. Retrieved from https://mri.modares.ac.ir/article_186_ae391fb02bfd0cd274bc728f56e2842e.pdf?lang=en [in Persian]

Fornell, C. & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of Marketing Research*;18(3), 382-388. https://doi.org/10.1177/002224378101800313

Ghasemi, S., Kiumarsi, F. & Zamani Dehkordi, B. (2017) Review of secure data storage and transmission in cloud-based networks. in *National Conference on Vision 2041 and Technological Advances in Electrical Engineering, Computer and Information Technology*, Shiraz: Iran Modern Education Development Center (Metana). [in Persian]

Hair, J. F., Ringle, C. M. & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, 19(2), 139-152. https://doi.org/10.2753/MTP1069-6679190202

Henseler, J., Ringle, C.M. & Sinkovics, R.R. (2009), The use of partial least squares path modeling in international marketing, Sinkovics, R.R. and Ghauri, P.N. (Ed.) *New Challenges to International Marketing* (Advances in International Marketing, Vol. 20), Emerald Group Publishing Limited, Bingley, pp. 277-319. https://doi.org/10.1108/S1474-7979(2009)0000020014

Jahangiri, N. (2011). A conceptual framework for assessing the richness and awareness of users information security (Case study: Post Bank), Master Thesis in Information Technology Management, Faculty of Engineering, Payame Noor University, Central Branch, Tehran. [in Persian]

Jarno, A. D. B., Baharom, S. B. & Shahpasand, M. (2017). Cloud testing: Requirements, tools and challenges. *Journal Of Applied Technology And Innovation*, 1(2), 79-93. Retrieved from https://dif7uuh3zqcps.cloudfront.net/wp-content/uploads/sites/11/2018/07/17035751/2017_Issue2_Paper8.pdf

kaur, A. & kaur, R. (2018). Cloud computing: A focus on security issues in cloud computing region. *International Journal of Advanced Research in Computer Science*, 9(2), 267-269. https://doi.org/10.26483/ijarcs.v9i2.5556

Kazempourian Mamghani, S. & Mirahmadi, J. (2016) Information technology risk management in cloud computing. in *3rd International Conference on Research in Engineering, Science and Technology*. [in Persian]

Khan, B., Alghathbar, K. S., Nabi, S. I. & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, *5*(26), 10862-10868. https://doi.org/10.5897/AJBM11.067

Kruger, H. A. & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25(4), 289-296. https://doi.org/10.1016/j.cose.2006.02.008

Makarevich, O., Mashkina, I. & Sentsova, A. (2013, November). The method of the information security risk assessment in cloud computing systems. In *Proceedings of the 6th International Conference on Security of Information and Networks* (pp. 446-447).

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, 69, 151-156. https://doi.org/10.1016/j.chb.2016.11.065

McLeod, A. & Dolezel, D. (2022). Information security policy non-compliance: Can capitulation theory explain user behaviors?. *Computers & Security*, 112, 102526. https://doi.org/10.1016/j.cose.2021.102526

Motahari, F., Rouhani, S. & Zare Rawasan, A. (2014). Introduction of cloud computing: Security and threats. in *1st National Conference on Researches of Computer Engineering*, Tehran: Farzin Center for Sustainable Development of Science and Technology. [in Persian]

Prajapati, P. & Shah, P. (2020). A review on secure data deduplication: Cloud storage security issue. *Journal of King Saud University-Computer and Information Sciences*, 34(7), 3996-4007. https://doi.org/10.1016/j.jksuci.2020.10.021

Vurukonda, N. & Rao, B. T. (2016). A study on data storage security issues in cloud computing. *Procedia Computer Science*, 92,128-135. https://doi.org/10.1016/j.procs.2016.07.335

Sehgal, N. K., Bhatt, P. C. P. & Acken, J. M. (2020). Future trends in cloud computing. In *Cloud Computing with Security* (pp. 235-259). Springer, Cham.

Talib, S., Clarke, N. L., & Furnell, S. M. (2010, February). An analysis of information security awareness within home and work environments. In *2010 International Conference on Availability, Reliability and Security* (pp. 196-203). IEEE.

Tenenhaus, M., Amato, S. & Esposito Vinzi, V. (2004, June). A global goodness-of-fit index for PLS structural equation modelling. In *Proceedings of the XLII SIS scientific meeting* (Vol. 1, No. 2, pp. 739-742).

Tolah, A., Furnell, S. M. & Papadaki, M. (2021). An Empirical Analysis of the Information Security Culture Key Factors Framework. *Computers & Security*, 108. 102354. https://doi.org/10.1016/j.cose.2021.102354

Tsohou, A., Karyda, M. & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security*, 52, 128-141. https://doi.org/10.1016/j.cose.2015.04.006

Von Solms, B. & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & security*, 23(5), 371-376. https://doi.org/10.1016/j.cose.2004.05.002

Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. *IEEE Access*, 8, 131723-131740. https://doi.org/1109/ACCESS.2020.3009876

Zandvakili, M., Salehi, S. & Rashidi, A. (2012). Conceptual expression of brand and its essence in marketing communication development; Case Study: Apple's Brand. *Journal of Visual and Applied Arts*, 5(9), 71-91. https://doi.org/10.30480/vaa.2012.261 [in Persian]

Zeinali Khosroshahi, A., Babaei, Sh. & Ghasemi, E. (2018) Review of security challenges in cloud computing. in *13th Conference on Recent Research in Science and Technology*, Kerman: Aseman Mehvaran Company. [in Persian]

Zhang, Y., Xu, C. & Shen, X. S. (2020). Summary and future research directions. In *Data Security in Cloud Storage* (pp. 167-171). Springer, Singapore.