SEMARAK ILMU PUBLISHING

Semarak International Journal of Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.my/index.php/sijaset/
ISSN: 3030-5314

Towards Cloud Computing Security Risks among the Young Generation

Maziah Mahmud[1,*], Noor Ilanie Nordin[1], Norlaila Md Nor[1], Nur Elini Jauhari[1], Wan Fairos Wan Yaacob[1], Jusoh Yaacob[2]

[1] School of Mathematical Sciences, College of Computing, Informatics and Media, Universiti Teknologi MARA Kelantan Branch, 18500 Machang, Kelantan, Malaysia
[2] Kolej Teknologi Darul Naim, Kelantan, Malaysia

ARTICLE INFO

Article history:
Received 15 January 2025
Received in revised form 15 February 2025
Accepted 15 March 2025
Available online 30 March 2025

Keywords:
Cloud security; security risk; cloud computing

ABSTRACT

Cloud security, privacy, integrity, and trust issues are some major security concerns leading to the widespread adoption of cloud computing. There are researches on the awareness and factors that influenced cloud computing among the young generation. However, the young generation needs to be aware of the security risk of using cloud computing. The purpose of this article is to explore the trust and risks among the young generation that affects cloud computing security risk. This article creates awareness of the use of cloud computing among the young generation. A simple random sampling method was implemented to select forty-eight students in Universiti Teknologi MARA Kelantan Branch, Kota Bharu Campus as respondents. The conclusion has been discussed that the providers and users of cloud services are responsible for ensuring a safe cloud environment.

1. Introduction

Cloud computing is a type of Internet-based computing that uses shared computing resources instead of local servers or personal devices to handle applications for storing and accessing data and programs over the Internet. Cloud computing has the potential to completely transform the way we use technology and is an emerging computing method in computer science today. It is a collection of resources and services provided by the network or internet that extends various computing techniques such as grid computing and distributed computing. The cloud helps its users by providing virtual resources over the internet [1,2]. An architectural strategy was proposed that consists of a cloud-enabled data model, monitoring infrastructure, and the construction of assessment mechanisms based on trust, risk, energy, and cost (TREC factors). The research discussed on how self-management, through decision-making procedures, might maximise the providers' business objectives [3].

* *Corresponding author.*
E-mail address: maziah740@uitm.edu.my

https://doi.org/10.37934/sijaset.5.1.1624

Nowadays, cloud computing is used in both industrial and academic fields. This technology allows users and businesses to access programs, storage, and application development platforms over the Internet and through the services offered by cloud service providers (CSPs) [4-7]. As the field of cloud computing expands, new techniques are evolving. This increase in the cloud computing environment also increases security challenges for cloud developers [8-11]. Cloud users store their data in the cloud, so the lack of security in the cloud can make users lose trust.

Potential vulnerabilities in the collaboration of cloud computing and logistics service providers can arise in relation to vital factors such as security and trust. Cloud security, privacy, integrity and trust issues are a few severe security concerns leading to the wide adoption of cloud computing, hence there are studies on Security Risk Assessment Model [12,13]. The risk factors affecting cloud computing security among small and medium-sized enterprises (SMEs) identify the risks involved in using cloud computing as it can affect the operations of the organizations also discussed in [14-16].

Meanwhile, the changing behaviour of society in general, and the younger generation, requires a new environment especially in higher institutions. There is research on the awareness and factors that influenced in cloud computing among the young generation [17-21]. However, the young generation, who regard technology as an essential part of their life, need to be aware of the security risk of using cloud computing.

This article aims to explore the risk and trust among the young generation that affects cloud computing security risk. Both risk and trust have been extensively studied in various contexts for many years [12]. Some interview questions have been conducted by [16] regarding the issues of how to protect the business from cyberattacks. In this article, the authors adapt and adopt the questionnaires from other articles and come out with five different variables of risk security. The variables that will be presented are Data Trustworthy, Security Architecture, Access Control, Contingency Planning and Security Monitoring. This article is organized as follows: Section 2 provides a cloud service and deployment model. Section 3 shows the variables of security risk and findings on the survey followed by results and discussion in Section 4. Finally, Section 5 represents the conclusion of this work.

2. Cloud Computing

2.1 Cloud Service Model

Cloud computing offers Cloud Service Model which divided into three parts as shown in Figure 1:

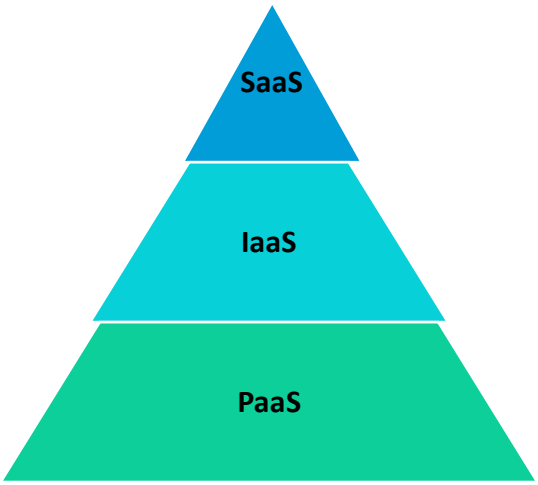

Fig. 1. Cloud Service Model that contains SaaS, IaaS and PaaS

2.1.1 SaaS (Software as a service)

SaaS is a software delivery model that delivers a single application to multiple users. The SaaS service is fully controlled by the CSP, so the customer has minimal control over security since the executing platform is outside of the user's network.

2.1.2 IaaS (Infrastructure as a Service)

IaaS provides virtualized computing resources over the internet. IaaS offers greater user control compared to SaaS, but less than that of IaaS.

2.1.3 PaaS (Platform as a Service)

PaaS provides all the infrastructure to create and manage customer applications. Compared to IaaS and SaaS, it offers the customer maximum control over security as the execution platform resides in the user's network.

2.2 Cloud Deployment model

The cloud deployment model is categorized into four sub models as shown in Figure 2.

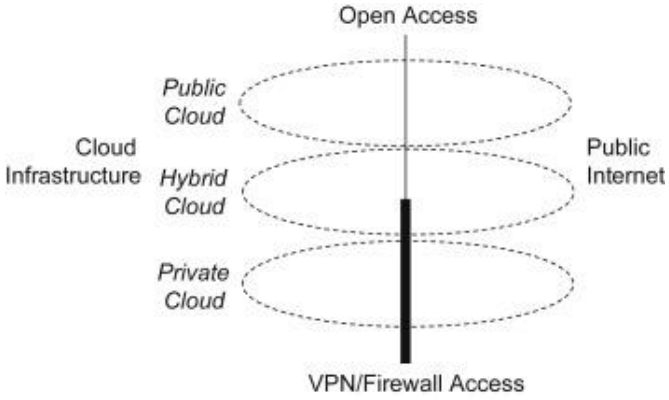

Fig. 2. Cloud Deployment Model [22]

2.2.1 Public Cloud

A cloud model is a set of resources provided by a cloud service provider. This service is provided to the user or large business enterprises. The server is located on CSP side, so the security part is also managed by CSP. Users remain unaware of the file location used by CSP, the geographical location of the server and how data is stored within the server. Thus, organization compromises with security which indeed is a major concern.

2.2.2 Private Cloud

Resources related to the cloud are provided to an organization or a company by CSP. Ownership of the cloud is with a single organization or CSP. The private cloud solves the security issue of the public cloud because the cloud is managed by that organization only, but it introduces problems related to storage management, maintenance and keeping track of capacity.

2.2.3 Community Cloud

A community cloud serves common functions and purposes such as security, policies, mission, regulatory compliance, etc. which are needed by multiple organizations. Cloud is managed by an organization or third party. The main drawback of the community cloud is data gets spared to multiple organizations [6] so data security and data privacy are compromised.

2.2.4 Hybrid Cloud

A hybrid cloud is a mixture of more than two cloud models i.e. public, private or community. All models remain unique entities but bond with some standards and policies. Hybrid cloud offers cost and scale effective services as compared to public cloud but on other hand, compromises data security when data migrate from public cloud to private cloud or vice versa.

3. Cloud Security Risk

The survey was conducted among students of Universiti Teknologi MARA Kelantan Branch, Kota Bharu Campus. A validated administered survey was used in this study. The survey consisted of six sections which were demographics profiles (Section A), Data Trustworthy (Section B), Security Architecture (Section C), Access Control (Section D), Contingency Planning (Section E) and Security Monitoring (Section F). The survey was transformed into Google Form to ease the data collection process. All Section B through Section F ratings involved using a total of 5 points as ratings. Respondents were asked to rate their assessment by giving a simple general rating from 1 to 5, e.g.: 1 equal to strongly disagree and 5 representing strongly agree. Table 1 shows the reliability test result to validate questionnaire items. All items in Section B until Section F gives a value of Cronbach's Alpha more than 0.6. Therefore, all the variables are reliable and consistent with the study.

Table 1
Result of Reliability Test

Section	Variable	Number of Items	Cronbach's Alpha
B	Data Trustworthy	6	0.851
C	Security Architecture	7	0.916
D	Access Control	6	0.949
E	Contingency Planning	6	0.850
F	Security Monitoring	5	0.923

3.1 Data Trustworthy

Section B starts with Data Trustworthy on cloud computing. Data trust is believing that your organization's data is in good health and available for use. The item asked as follows:

D1 : Password-protected screen savers that activate automatically.
D2 : File integrity monitoring software on servers.
D3 : Passwords with at least 10 characters that have complexity requirements and are changed every 90 days.
D4 : Passwords are never stored in clear text.
D5 : Sets account lockout feature.
D6 : Prohibits split tunnelling.

Table 2 below shows the mean for Data Trustworthy configuration. Overall, the mean for each item in section B is above 3 which indicates that the majority of respondents agree with the statement given to improve the data trustworthy configuration.

Table 2
Data Trustworthy on Cloud Computing

	D1	D2	D3	D4	D5	D6
Mean	4.21	3.92	3.21	3.85	3.96	3.77
Median	4.00	4.00	3.50	4.00	4.00	4.00
Std. Deviation	.849	.794	1.202	.989	.824	.857
Variance	.722	.631	1.445	.978	.679	.734

3.2 Security Architecture

With today's technology, an organization must have a Security Architecture in place to protect critical information. This significantly minimizes the risk of an attacker successfully compromising a company's systems. The item asked as follows:

S1 : Network firewall protection.
S2 : Web application firewall protection.
S3 : Host firewall protection.
S4 : Provides network redundancy.
S5 : Uses enterprise virus protection on all systems.
S6 : Restrict access to data from others.
S7 : Manage and secure access points on its wireless network.

Among the numerous benefits of Security Architecture is its ability to translate each unique requirement into practical strategies and create a risk-free environment for an organization while adhering to the latest security standards and business requirements. Table 3 shows that respondents are aware of security protection which involve firewall protection and password.

Table 3
Security Architecture on Cloud Computing

	S1	S2	S3	S4	S5	S6	S7
Mean	3.98	3.98	4.04	4.04	4.04	3.98	3.92
Median	4.00	4.00	4.00	4.00	4.00	4.00	4.00
Std. Deviation	.699	.838	.824	.743	.922	.812	.942
Variance	.489	.702	.679	.551	.849	.659	.887

3.3 Access Control

Access control is a critical component of security that decides who has access to certain data, apps, and resources and under what conditions. The item asked as follows:

A1 : Policy to protect client information against unauthorised access.
A2 : Policy that prohibits sharing of individual accounts and passwords.
A3 : Policy that implements the need-to-know and separation-of-duties principles.
A4 : Multi-factor authentication in order to access client resources.

A5 : Provides customer support with escalation procedures.

Results illustrated in Table 4 show that the respondents are aware of the policy and procedures for Access Control. Access Control rules safeguard digital places in the same way that keys and pre-approved guest lists secure physical locations. To put it another way, they let the right people in while keeping the wrong people out.

Table 4
Access Control on Cloud Computing

	A1	A2	A3	A4	A5
Mean	4.21	4.17	3.98	4.04	4.02
Median	4.00	4.00	4.00	4.00	4.00
Std. Deviation	.713	.694	.863	.849	.863
Variance	.509	.482	.744	.722	.744

3.4 Contingency Planning

A contingency plan is created when there is a risk that an emergency might occur and something needs to be done to prevent or minimize the damage. A contingency plan usually includes a list of actions that are intended to be taken in the event of a disaster. The item asked as follows:

P1 : Written contingency plan for mission critical computing operations.
P2 : Updates the contingency plan.
P3 : Written backup procedures and processes.
P4 : Tests the integrity of backup media.
P5 : Stores backup media in a secure manner and controls access.
P6 : Maintains a documented and tested disaster recovery plan.

The findings demonstrated in Table 5 show that there are respondents who are not aware or ready for an uncertain situation where they are supposed to have a plan to resolve the situation. A contingency plan can also be made when there is uncertainty about the future and what will happen. This could involve planning different outcomes of different scenarios so that someone is prepared no matter what happens.

Table 5
Contingency Planning on Cloud Computing

	P1	P2	P3	P4	P5	P6
Mean	3.88	3.79	4.02	3.92	4.10	4.13
Median	4.00	4.00	4.00	4.00	4.00	4.00
Std. Deviation	.789	.651	.812	.895	.778	.672
Variance	.622	.424	.659	.801	.606	.452

3.5 Security Monitoring

The security monitoring service could keep an eye on almost every aspect of the customer's systems and networks. They analyze network traffic and look for abnormalities. The item asked as follows:

M1 : Reviews system logs for failed logins, or failed access attempts.
M2 : Reviews and remove dormant accounts on systems.
M3 : Reviews network and firewall logs.
M4 : Reviews wireless access logs.
M5 : Performs scanning for rogue access points.

Based on the result in Table 6, respondents are aware that security monitoring is the method of analyzing indicators of potential security threats, followed by appropriate actions to solve them.

Table 6
Security Monitoring on Cloud Computing

	M1	M2	M3	M4	M5
Mean	3.94	3.94	3.96	3.98	4.19
Median	4.00	4.00	4.00	4.00	4.00
Std. Deviation	.836	.783	.771	.785	.673
Variance	.698	.613	.594	.617	.453

4. Result and Discussion

A self-administrated questionnaire was used as an instrument tool to collect the data that contains 6 sections in this study. The data was gathered by creating an online questionnaire and receiving forty-eight responses from Universiti Teknologi MARA Kelantan Branch, Kota Bharu Campus degree students. The inclusion criteria of the population are undergraduate students from Universiti Teknologi MARA Kelantan Branch, Kota Bharu Campus. The exclusion criteria are the respondents from part 7 which is the intern students. The data were analyzed using Statistical Package of Social Sciences (SPSS) software version 22 (IBM Inc., USA).

Descriptive analysis for Section B, C, D, E and F has been made with respondents completing the survey for this study. This study creates an overall analysis of trust and risk among the young generation about trustworthiness towards cloud computing security risk. Fig. 3 below gives the overall overview based on the security risk component. It shows that the respondents had low awareness of data trustworthiness but has aware of security monitoring on cloud computing.

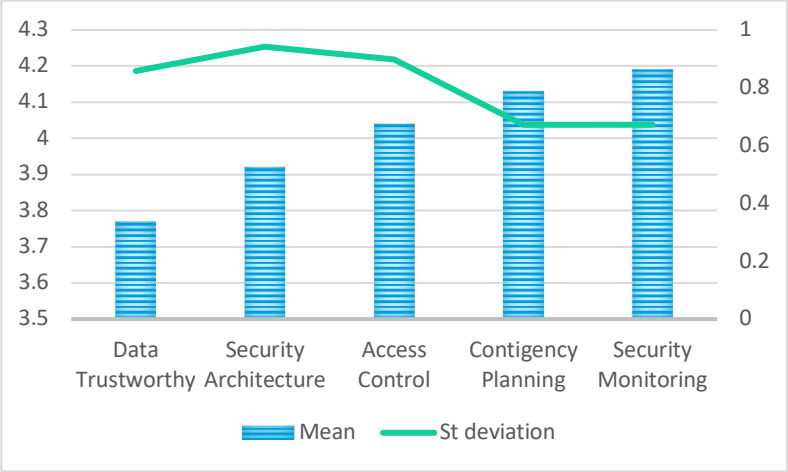

Fig. 3. Mean and standard deviation value for security risk component

5. Conclusion

In summary, this article enables CSPs to learn about their performance against security risks to make their service better especially in targeting the young generation. Although, a higher level of trust in cloud technologies from the side of enterprises and a cost effective and reliable productivity from the side of CSPs. Hence, they can identify, analyzes and evaluates security risks affecting cloud computing adoption. This research creates the perspective level of the security risk of cloud computing to avoid the risk of the data being stolen or hacked and build a peaceful cloud environment. Since this article only analyzes the trust and risk among the young generation, it is recommended that future studies get the security risk ranking which can improve the performance of CSPs.

Acknowledgement
Special gratitude to our group members for stimulating, suggestions and encouragement on this project. Furthermore, we would like to acknowledge with much appreciation to UiTM for providing the research Geran Dalaman (600-TNCPI 5/3/DDN (03)(008/2020)). We would like to extend our sincere thanks to all respondents who participated in this project.

References

[1] Ullah, Israr, Shakeel Ahmad, Faisal Mehmood, and DoHyeun Kim. "Cloud based IoT network virtualization for supporting dynamic connectivity among connected devices." *Electronics* 8, no. 7 (2019): 742. https://doi.org/10.3390/electronics8070742

[2] Angiuoli, Samuel V., Malcolm Matalka, Aaron Gussman, Kevin Galens, Mahesh Vangala, David R. Riley, Cesar Arze, James R. White, Owen White, and W. Florian Fricke. "CloVR: a virtual machine for automated and portable sequence analysis from the desktop using cloud computing." *BMC bioinformatics* 12 (2011): 1-15. https://doi.org/10.1186/1471-2105-12-356

[3] Kiran, Mariam, Gregory Katsaros, Jordi Guitart, and Juan Luis Prieto. "Methodology for information management and data assessment in cloud environments." *International Journal of Grid and High Performance Computing (IJGHPC)* 6, no. 4 (2014): 46-71. https://doi.org/10.4018/IJGHPC.2014100104

[4] Singh, Parminder, Avinash Kaur, Pooja Gupta, Sukhpal Singh Gill, and Kiran Jyoti. "RHAS: robust hybrid auto-scaling for web applications in cloud computing." *Cluster Computing* 24, no. 2 (2021): 717-737. https://doi.org/10.1007/s10586-020-03148-5

[5] Reddy, P. Muthi, Ansaf Ahmed, S. H. Manjula, and K. R. Venugopal. "Resource allocation in the cloud for video-on-demand applications using multiple cloud service providers." *Cluster Computing* 22 (2019): 223-239. https://doi.org/10.1007/s10586-018-2847-y

[6] Chahal, Rajanpreet Kaur, and Sarbjeet Singh. "Fuzzy rule-based expert system for determining trustworthiness of cloud service providers." *International Journal of Fuzzy Systems* 19 (2017): 338-354. https://doi.org/10.1007/s40815-016-0149-1

[7] Cayirci, Erdal, Alexandr Garaga, Anderson Santana de Oliveira, and Yves Roudier. "A risk assessment model for selecting cloud service providers." *Journal of Cloud Computing* 5, no. 1 (2016): 14. https://doi.org/10.1186/s13677-016-0064-x

[8] Zhang, Ning. "An overview of advantages and security challenges of cloud computing." *Int J Comput Sci Mob Comput* 10, no. 1 (2021): 76-85. https://doi.org/10.47760/ijcsmc.2020.v09i12.010

[9] Li, Wenjuan, Weizhi Meng, Zhiqiang Liu, and Man-Ho Au. "Towards blockchain-based software-defined networking: security challenges and solutions." *IEICE Transactions on Information and Systems* 103, no. 2 (2020): 196-203. https://doi.org/10.1587/transinf.2019INI0002

[10] Sardar, Ruhma, and Tayyaba Anees. "Web of things: security challenges and mechanisms." *Ieee Access* 9 (2021): 31695-31711. https://doi.org/10.1109/ACCESS.2021.3057655

[11] Subramanian, Nalini, and Andrews Jeyaraj. "Recent security challenges in cloud computing." *Computers & Electrical Engineering* 71 (2018): 28-42. https://doi.org/10.1016/j.compeleceng.2018.06.006

[12] Cayirci, Erdal, and Anderson Santana De Oliveira. "Modelling trust and risk for cloud services." *Journal of Cloud Computing* 7 (2018): 1-16. https://doi.org/10.1186/s13677-018-0114-7

[13] Youssef, A. "A Delphi-Based security risk assessment model for cloud computing in enterprises." *Journal of Theoretical and Applied Information Technology* 98, no. 1 (2020): 151-162.
[14] Levin, Avner, Paul Goodrick, and Daria Ilkina. "Securing cyberspace: A comparative review of strategies worldwide." In *The 2014 IT Canadian Conference*. 2013.
[15] Henson, Richard, and D. Sutcliffe. "An insurance-based approach to improving SME Cyber Security." (2017): 171-186.
[16] Cook, Kimberly Diane. "Effective cyber security strategies for small businesses." PhD diss., Walden University, 2017.
[17] Mahmud, Maziah, Nor Hazreeni Hamzah, Shamsunarnie Mohamed Zukri, Wan Fairos Wan Yaacob, and Jusoh Yacob. "Factors Influenced the Cloud Computing Adoption in Teaching and Learning Process." *International Journal of Academic Research in Business & Social Science* 9, no. 13 (2019): 284-290. https://doi.org/10.6007/IJARBSS/v9-i13/6475
[18] Hamzah, Nor Hazreeni, Maziah Mahmud, Shamsunarnie Mohamed Zukri, Wan Fairos Wan Yaacob, and Jusoh Yacob. "The Awareness and Challenges of Cloud Computing Adoption on Tertiary Education in Malaysia." In *Journal of Physics: Conference Series*, vol. 892, no. 1, p. 012014. IOP Publishing, 2017. https://doi.org/10.1088/1742-6596/892/1/012014
[19] Simm, Will, Gordon Blair, Richard Bassett, Faiza Samreen, and Paul Young. "Models in the cloud: Exploring next generation environmental software systems." In *Environmental Software Systems. Data Science in Action: 13th IFIP WG 5.11 International Symposium, ISESS 2020, Wageningen, The Netherlands, February 5–7, 2020, Proceedings 13*, pp. 216-227. Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-39815-6_21
[20] Rogelj, Valerija, Alenka Temeljotov Salaj, and David Bogataj. "Digital transformation of community health and social services for ageing cohorts." *IFAC-PapersOnLine* 54, no. 13 (2021): 756-761. https://doi.org/10.1016/j.ifacol.2021.10.543
[21] Klimova, Blanka, and Petra Maresova. "Cloud computing and e-learning and their benefits for the institutions of higher learning." In *2016 IEEE Conference on e-Learning, e-Management and e-Services (IC3e)*, pp. 75-78. IEEE, 2016. https://doi.org/10.1109/IC3e.2016.8009043
[22] Amoroso, Edward G. "Cloud Security." *Elsevier EBooks*, (2017): 923–930. https://doi.org/10.1016/B978-0-12-803843-7.00064-8