The Impact of Cloud Computing on Network Security Risk for Organization Behaviours

Nagham Hamid[1,*], Nada Mahdi Kaitan[1], Sanaa Mohsen[1]

[1]College of Business Informatics, University of Information Technology and Communications, Baghdad, Iraq

Emails: nagham.finjan@uoitc.edu.iq; nadait.2016@uoitc.edu.iq; sanaa.muhsin@uoitc.edu.iq

Abstract

Cloud computing presents a new trend for IT and business services which typically involves self-service access over internet. Over these features, cloud computing has the advantages to enhance IT and business ways by offering cost efficiency, dynamically scalable, and flexibility. However, using cloud computing has raised the level of the network security risk due to the services are presented by a third party. In addition, to maintain the service availability and support data collections. Understanding these risks through cloud computing help the management to protect their system from security attacks. In this paper, the most serious and important risks and threats of the cloud computing are discussed. The main vulnerabilities is identifying with the literature related to the cloud-computing environment with possible solutions to overcome these threats and risks.

Keywords: Cloud computing; Security risk; Network security; Virtualization

1. Introduction

Cloud computing is received a rapidly increasing attention in both the industrial and academic fields. Cloud computing has been considered as one of the most top 10 recent technologies that has better influence on the successful of the organizations among these years based on study carried out by Gartner [1]. The key benefits of the cloud computing is summarized in enabling on-demand network access, ubiquitous, convenient, and able for configuration of computing resources. These resources include networks, storage, applications, servers, and services, which can be widely managed and released with minimal number of service provider interface. The main task of cloud computing is to provide a high level of security, net computing, quick process, and convenient data storage [2-7]. Taking in consideration that all the computing resources are visualized as services and would be delivered over the internet [3, 4]. As cloud, computing can be seen as a distribution architecture as well as a computational model. Moreover, cloud computing improves agility, availability, scalability, collaboration, adaption of fluctuations based on demand, cost reduction, and speed up development work [5-7].

The cloud is consisted of a number of computing models and concepts such as Web 2.0, virtualization, and service-orientated architecture (SOA). These models are relied on the Internet, which provides mutual business services online through common web browsers to fulfil the computing needs of users. In the same time, the data and software are saved on existing remotely servers [5]. In another words, the cloud can be represented as the mature of these concepts and technologies, which presents to a marketing term the maturity of the services provided [6]. Thought there are several advantages to implementing cloud computing, there are some important obstacles facing the adoption of cloud computing. These obstacles are mainly focused on the security issues, privacy, compliance, and legal matters [8, 9]. That is mostly because cloud computing can be defined as a new computing architecture. In that matter, a great adopts of how security level can be functional on network, application, data levels, and host [9]. While how the application and data security can be achieved in the cloud, computing is another issue to be investigated [10]. Generally, security matters relate to risk ranges such as lack of control, dependency on the internet, integration with internal security, and external data storage. Cloud has several features compared to the

DOI: https://doi.org/10.54216/JCIM.150121
Received: April 14, 2024 Revised: June 12, 2024 Accepted: August 10, 2024

common technologies, it can be summarized as large scale, and the resources are completely virtualized and distributed by the cloud providers [11]. In cloud computing, the security controls are similar to any IT environment security controls. However, since cloud-computing structure is employed the operational models, the different threats and risks could be presented to an organization compared to the common IT solutions.

Unluckily, implementing security controls into these solutions is usually supposed as making them more inflexible [4]. For an organization, the transferring of their critical data and applications from their central data networks is of great concerned. To overcome these concerns, cloud computing provides a solution that should ensure the privacy and security of the customer's applications and services are highly protected [12]. In this paper, a classification of network security issues of cloud computing is provided based on SPI model. The main vulnerabilities of this system are identified and the major risks and threats related to cloud computing are found and reviewed based on the recent literatures. A threat or risk is well known as a potential or unwanted attack that may cause to misuse of resources or information. The vulnerability term is defined as a fault inside the system, which allows an attack to be happened. Some surveys introduced cloud-computing security in general without taking in consideration the vulnerabilities and threats. In this survey, a list of vulnerabilities and threats are presented in related with cloud computing security level and which cloud resources and services are affected by these vulnerabilities and threats.

Hence, this paper focuses on identify the security risks, vulnerability, mitigation control, and benefit of cloud computing on organizational behaviour. The guidelines and standards toward secure cloud computing is presented as a fundamental for the cloud computing development.

2. The Materials and Methods

To summarize the current existing vulnerabilities and threats related to the cloud computing security, a literature systematic reviews from [13-15] is carried out. In order to analyse the major security issues related to vulnerabilities and threats in these related existing literature for identifying the cloud computing security levels.

the question is focused on identifying the main issues in the cloud computing security with related to threats, risks, vulnerabilities, solutions and requirements of the network security of cloud computing. Hence, the question is addressed as follows: what is the threats and that are most significant in cloud computing security network? Therefore, the keywords are stated in that order to fulfil the question handling; cloud security, SPI security, cloud systems, cloud vulnerabilities, cloud threats, cloud recommendations, and delivery models security.

The selection of sources is defined in this research based on the following: Scholar Google, ACM digital Library, ScienceDirect, DBLP, and IEEE digital library. Once the list of sources is defined, the process and the criteria for study selection are described. The criteria of this research are based on the research question introduced in previous sub-section. Therefore, this research is contained topics related only to the security of the cloud computing including risks, vulnerabilities, and threats.

After determination of the research criteria and defined the sources, the obtained reviews are evaluated. The evaluated sources then are executed to obtain a set of 140 results. A set of 50 relevant studies are selected. Then, these 50 studies are again filtered to produce a set of relevant 16 studies, which can be found in [5, 6, 11, 15-26].

3. Results and Discussion

The results of the systematic analysis and cloud security issues are found in Table 1. As can be noticed from Table I, the risks and vulnerabilities are mostly focused on cloud computing security issues. The approaches in the systemic review are discussed in terms of classify, identify, and analyse in respect with the risks and vulnerabilities of the cloud computing. The reviewed systematic analyses are focused on the existing threads and risks in the cloud computing, offering a solution on how these threads can be avoided or recovered. The studies also showed a direct relationship between threats or vulnerability and possible mechanism and solutions to overcome these problems. Additionally, other security issues are discussed in this study such as trust, data security, security recommendations, and a possible mechanism to solve any of these threats and risks.

Three types of services level are introduced in the cloud model by [22, 27, and 28]. These are; Software as a service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS can be described as the capability of using the applications provided by the cloud users and running on the cloud infrastructure. The applications in SaaS can be accessed from several users using a simple or based web browser. PaaS is a platform that allows the consumer to deploy the applications onto the cloud infrastructure. This capability does not need any installing of tools or software on the client's local machines. IaaS is defined as the capability of allowing the customers to process their applications on networks, storage, and any other cloud resources. This allowed the users to run their

DOI: https://doi.org/10.54216/JCIM.150121
Received: April 14, 2024 Revised: June 12, 2024 Accepted: August 10, 2024

applications and software on the same cloud computing models. To analyse the security problems in cloud computing, an understanding of the relationship between the cloud models should be clarified. Generally, SaaS and PaaS are stacked on the top of IaaS model. Hence, any attack or threat in IaaS will be affected both SaaS and PaaS. However, PaaS provides an applications platform for SaaS, which effects the security risk between each model. In the same time, SaaS provider can barrow a development environment from PaaS provider, and PaaS can rent from IaaS an infrastructure. Therefore, each layer has its own security risk and threat. Leading to have or creates confusion on which service or model was responsible on the attack.

In SaaS providers, the users have application services like business applications, emails, CRM, ERP, SCM, and conferencing software [27]. In this model, the security control is less among the three basic levels. However, some security concerns might be raised in this cloud level as show in Figure 1. In PaaS providers, the software and hardware layers is handled based on the cloud deployment of the applications with no cost of purchase involved [21]. The security level in PaaS depends on the exciting web browser and server network. The application security level consists of two major software layers; the security of the applications for users, and the security of the platform. Thus, the providers are controlled the security of the platform and protect user applications. However, the most challenges that PaaS layer are described as follow; life cycle development, relationships between the third party, and security of the infrastructure as illustrated in Figure 2.

In the life cycle development, the prospective of the developers is facing a complexity from the application development. Where, the applications could be built a speed secure host in the same cloud [12, 23]. If the speed changes at each application, the cloud will be affected in both security and the System Development Life Cycle (SDLC) [23]. Hence, in PaaS the developer should be frequently upgraded the applications to ensure speed and security of their application development. Nevertheless, the developers should always be careful that any changes in PaaS applications could affect the security of the PaaS applications. As the PaaS offers a third party web services such as mashups [30], this could inherit a security risk and threat in the services applications of users.

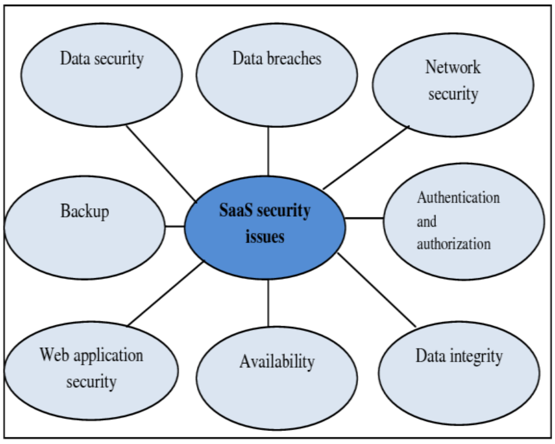

Figure 1. The general SaaS security threats and issues.

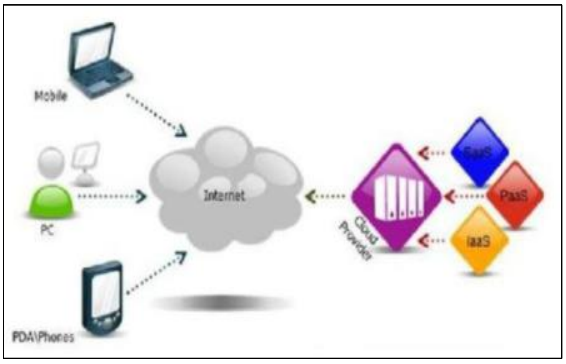

Figure 2. PaaS security levels.

Table 1: The subjects that have been analyzed.

Subjects/References	[22]	[24]	[25]	[26]	[27]
Vulnerabilities		√			√

DOI: https://doi.org/10.54216/JCIM.150121
Received: April 14, 2024 Revised: June 12, 2024 Accepted: August 10, 2024

Threats	√	√	√	√	√
Mechanisms/Recommendations		√	√	√	√
Security Standards		√		√	
Data Security	√	√	√	√	√
Trust	√		√	√	√
Security Requirements	√			√	√
SaaS, PaaS, IaaS Security		√		√	

That means the users should depend on the security of the web hosted development and the third-party applications and services. In PaaS infrastructure, the users generally do not have the ability to access the infrastructure layer [21]. Therefore, the PaaS providers are responsible on the applications services as well as the security of the infrastructure [21]. As a conclusion, there is a less literature on security issues in PaaS level as well as SaaS level. SaaS delivers software over the web, while PaaS delivers development tools for creating SaaS applications. However, both PaaS and SaaS use multi- architecture so multiple security issue may rise. As well-known both SaaS and PaaS provide data processing and transferring. Thus, it is the provider responsibility to secure these data exchanging in the cloud.

The user in IaaS level is accepted to access software and resources with full management and editing [19]. IaaS offers several resources such as networks, servers, storage, and system virtualization. This resource can be accessed through internet. With respect to PaaS and SaaS, IaaS allows user to control the security and manage the threats in better way. Taking in consideration that there is no hole appears inside the virtual machine. In such case, the providers are responsible the software security inside their virtual machine. Despite these features of IaaS level, the cloud providers control the resources. Hence, more efforts should be taken to secure the cloud systems and services.

These apps are generally presented Online by way of an internet browser [26, 27]. Nevertheless, weaknesses in web browsers have a higher possibility of generating threats for any SaaS applications. Opponents tend to use the internet web browsers to compromise user’s computer systems and put malicious software in order to retrieve a sensitive data. For instance, 10 security threats are discussed by the Open Web Application Security Project (OWASP) for enhancement of the security internet applications as shown in Figure 3. These security threats are classified as apply defence in depth, using a positive security, fail securely, run with least privilege, obscurity to avoid security, simplify security as possible, detect intrusions, no trust in infrastructure, no trust in services, and building secure defaults [28].

Several systematic analysing for security Vulnerabilities inside the cloud computing have been addressed based on the provided cloud services as summarized in Table II. The evaluation of the risks and threats in Table 2 cover SPI cloud services that influences the Vulnerabilities in the cloud. Particularly, threats-based technology are primarily analysed. However, Vulnerabilities related to the business found to be additionally tricky. These threats in the business on the cloud can be summarized as follows; the practice of poorly screening and hiring of the employee, lack of checking client background, and poorly lake of education protection.

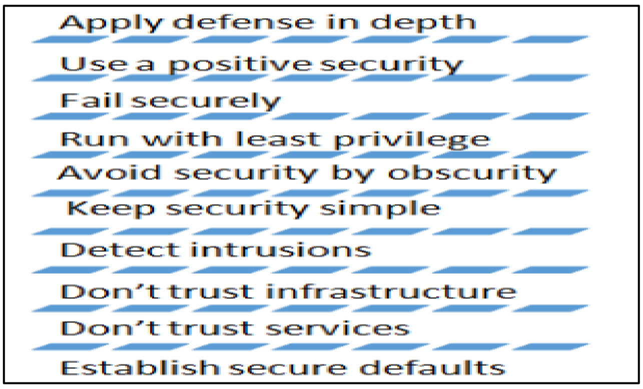

Figure 3. OWASP Security threats and levels.

In the lack of employee hiring and screening, several cloud services are not performed screening for their employees or providers. In this case, cloud admins have limited access to the provided cloud information about the employees. In the other hand, most of the cloud providers not able to do checking on their client’s background or history. In which way, any client can easily create account on cloud without history check. This enables attackers

DOI: https://doi.org/10.54216/JCIM.150121
Received: April 14, 2024 Revised: June 12, 2024 Accepted: August 10, 2024

to put any malicious software without being detected in the cloud service. These accounts can be registered with simple legitimate emails and bankcards. Additionally, the lake of education in the security of the cloud services playing a main role in weak the whole services and allowed the attacks to be increased. Especially, in business that communicates other organizations, suppliers, third party, and end users within the cloud.

Table 3 illustrates the most threats that could be faced the cloud services. It can be noticed that the most threats come from the attackers are from the low level of the cloud services, and most effectively stolen the data or taking control of the cloud infrastructure. In this case, most of threats are targeting the information of the users more than the structural cloud. Table 4 shows the relation between the vulnerabilities and threats, which describes how the threats can cause several vulnerabilities to compromise the product.

Table 2: Vulnerabilities in cloud computing

Vulnerabilities	Description	level
V01(resources)	Inaccurate modeling usage	SPI
V02 (data related)	Unrestricted allocation	SPI
V03 (Insecure Appl.) interfaces)	Weak credential	SPI
V04 (virtual machine)	Possible covert channel	SPI
V05 (virtual image)	Uncontrolled virtual machine	SPI
V06 (hypervisors)	Complex code	SPI
V07 (virtual network)	Sharing of virtual networks	SPI

Table 3: Threats in cloud computing

Threats	Description	Level
T01 (account) risk)	Attacker access user profiles	SPI
T02 (data leakage)	Attacker recover data	SPI
T03 (denial of service)	the system cannot satisfy any request	SPI
T04 (VM scape)	to take control of the infrastructure	SPI
T05 (VM hopping)	VM is able to gain access to another VM	SPI
T06 (VM creation)	Malicious VM creation	SPI
T07 (VM migration)	Insecure VM migration	SPI

Table 4: Threats and vulnerabilities relationship

Vulner.	Threats	Description	Possible solutions
V01	T01	Use user profile account	Identity and Access
V02	T02	Data cannot be removed	Dynamic credential
V03	T03	Side channel	Digital Signatures
V04	T04	An attacker can request more computational resources	limited computational resources scanners
V05	T05	command injection	Web application
V06	T06	most virtual machines monitor	Mirage
V07	T07	Sniffing and spoofing virtual networks	network modes: "bridged" and "routed

4. Conclusion

Cloud computing is important in providing a well services to the business companies and users. However, cloud computing suffers from various risks and threats that effects the protection of the confidential information of the

DOI: https://doi.org/10.54216/JCIM.150121
Received: April 14, 2024 Revised: June 12, 2024 Accepted: August 10, 2024

provider or user. Understanding what threats and vulnerabilities in the cloud computing gives a big help to the businesses to shift toward using of the cloud. Several solutions have been proposed to resolve the security threats in the cloud computing models. By dividing cloud computing model into three layers; SaaS, PaaS, and IaaS. As a result, it have been found that storage, virtualization, and network servers are the most critical area to be security hacked. However, different challenges occurred considering protection of the user information as well as company profile. Most of vulnerabilities come from the lake of checking client background, and poorly lake of education protection. Therefore, further investigation should be done in a scheme to find the optimal solution or suggestion to resolve these threats and vulnerabilities.

Funding: “This research received no external funding”

Conflicts of Interest: “The authors declare no conflict of interest.”

References

[1] Ahmed, O. (2024). Enhancing Intrusion Detection in Wireless Sensor Networks through Machine Learning Techniques and Context Awareness Integration. International Journal of Mathematics, Statistics, and Computer Science, 2, 244–258. https://doi.org/10.59543/ijmscs.v2i.10377

[2] A. E. Youssef and A. M. Mostafa, "Critical Decision-Making on Cloud Computing Adoption in Organizations Based on Augmented Force Field Analysis," in IEEE Access, vol. 7, pp. 167229-167239, 2019.

[3] M. Skafi, M. M. Yunis and A. Zekri, "Factors Influencing SMEs’ Adoption of Cloud Computing Services in Lebanon: An Empirical Analysis Using TOE and Contextual Theory," in IEEE Access, vol. 8, pp. 79169-79181, 2020.

[4] Z. Wen, J. Cała, P. Watson and A. Romanovsky, "Cost Effective, Reliable and Secure Workflow Deployment over Federated Clouds," in IEEE Transactions on Services Computing, vol. 10, no. 6, pp. 929-941, 1 Nov.-Dec. 2017.

[5] A. Rezgui, N. Davis, Z. Malik, B. Medjahed and H. S. Soliman, "CloudFinder: A System for Processing Big Data Workloads on Volunteered Federated Clouds," in IEEE Transactions on Big Data, vol. 6, no. 2, pp. 347-358, 1 June 2020.

[6] P. Jamshidi, A. Ahmad and C. Pahl, "Cloud Migration Research: A Systematic Review," in IEEE Transactions on Cloud Computing, vol. 1, no. 2, pp. 142-157, July-December 2013.

[7] S. Gupta and S. C. Misra, "Moderating Effect of Compliance, Network, and Security on the Critical Success Factors in the Implementation of Cloud ERP," in IEEE Transactions on Cloud Computing, vol. 4, no. 4, pp. 440-451, 1 Oct.-Dec. 2016.

[8] Z. Feng, D. K. W. Chiu, R. Peng, P. Gong, K. He and Y. Huang, "Facilitating Cloud Process Family Co-Evolution by Reusable Process Plug-in: An Open-source Prototype," in IEEE Transactions on Services Computing, vol. 10, no. 6, pp. 854-867, 1 Nov.-Dec. 2017.

[9] H. Cai, B. Xu, L. Jiang and A. V. Vasilakos, "IoT-Based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges," in IEEE Internet of Things Journal, vol. 4, no. 1, pp. 75-87, Feb. 2017.

[10] S. Mubeen, S. A. Asadollah, A. V. Papadopoulos, M. Ashjaei, H. Pei-Breivold and M. Behnam, "Management of Service Level Agreements for Cloud Services in IoT: A Systematic Mapping Study," in IEEE Access, vol. 6, pp. 30184-30207, 2018.

[11] S. Sobati Moghadam and A. Fayoumi, "Toward Securing Cloud-Based Data Analytics: A Discussion on Current Solutions and Open Issues," in IEEE Access, vol. 7, pp. 45632-45650, 2019.

[12] A. Abbas and S. U. Khan, "A Review on the State-of-the-Art Privacy-Preserving Approaches in the e-Health Clouds," in IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 4, pp. 1431-1441, July 2014.

[13] M. Ficco and F. Palmieri, "Introducing Fraudulent Energy Consumption in Cloud Infrastructures: A New Generation of Denial-of-Service Attacks," in IEEE Systems Journal, vol. 11, no. 2, pp. 460-470, June 2017.

[14] Q. N. Naveed, M. R. N. Mohamed Qureshi, A. Shaikh, A. O. Alsayed, S. Sanober and K. Mohiuddin, "Evaluating and Ranking Cloud-Based E-Learning Critical Success Factors (CSFs) Using Combinatorial Approach," in IEEE Access, vol. 7, pp. 157145-157157, 2019.

[15] E. Z. Milian, M. d. M. Spinola, R. F. Goncalves and A. L. Fleury, "Assessing Challenges, Obstacles and Benefits of Adopting Cloud Computing: Study of an Academic Control System," in IEEE Latin America Transactions, vol. 13, no. 7, pp. 2301-2307, July 2015.

DOI: https://doi.org/10.54216/JCIM.150121
Received: April 14, 2024 Revised: June 12, 2024 Accepted: August 10, 2024

[16] Y. A. M. Qasem, R. Abdullah, Y. Y. Jusoh, R. Atan and S. Asadi, "Cloud Computing Adoption in Higher Education Institutions: A Systematic Review," in IEEE Access, vol. 7, pp. 63722-63744, 2019.

[17] J. L. Rice, V. V. Phoha and P. Robinson, "Using Mussel-Inspired Self-Organization and Account Proxies to Obfuscate Workload Ownership and Placement in Clouds," in IEEE Transactions on Information Forensics and Security, vol. 8, no. 6, pp. 963-972, June 2013.

[18] M. Berekmeri, D. Serrano, S. Bouchenak, N. Marchand and B. Robu, "Feedback Autonomic Provisioning for Guaranteeing Performance in MapReduce Systems," in IEEE Transactions on Cloud Computing, vol. 6, no. 4, pp. 1004-1016, 1 Oct.-Dec. 2018.

[19] P. Hofmann and D. Woods, "Cloud Computing: The Limits of Public Clouds for Business Applications," in IEEE Internet Computing, vol. 14, no. 6, pp. 90-93, Nov.-Dec. 2010.

[20] J. N. Khasnabish, M. F. Mithani and S. Rao, "Tier-Centric Resource Allocation in Multi-Tier Cloud Systems," in IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 576-589, 1 July-Sept. 2017.

[21] E. Bauer, "Cloud Automation and Economic Efficiency," in IEEE Cloud Computing, vol. 5, no. 2, pp. 26-32, Mar./Apr. 2018.

[22] A. Samba, "Logical Data Models for Cloud Computing Architectures," in IT Professional, vol. 14, no. 1, pp. 19-26, Jan.-Feb. 2012.

[23] M. Skafi, M. M. Yunis and A. Zekri, "Factors Influencing SMEs’ Adoption of Cloud Computing Services in Lebanon: An Empirical Analysis Using TOE and Contextual Theory," in IEEE Access, vol. 8, pp. 79169-79181, 2020.

[24] L. Sangavarapu, S. Mishra, A. Williams and G. R. Gangadharan, "The Indian Banking Community Cloud," in IT Professional, vol. 16, no. 6, pp. 25-32, Nov.-Dec. 2014.

[25] A. M. Sebastian and J. J. Kizhakkethottam, "A review on cloud security threats and solutions," 2015 International Conference on Soft-Computing and Networks Security (ICSNS), Coimbatore, India, 2015, pp. 1-4.

[26] M. Ficco and F. Palmieri, "Introducing Fraudulent Energy Consumption in Cloud Infrastructures: A New Generation of Denial-of-Service Attacks," in IEEE Systems Journal, vol. 11, no. 2, pp. 460-470, June 2017.

[27] Ryoo, S. Rizvi, W. Aiken and J. Kissell, "Cloud Security Auditing: Challenges and Emerging Approaches," in IEEE Security & Privacy, vol. 12, no. 6, pp. 68-74, Nov.-Dec. 2014.

[28] J. Ryoo, S. Rizvi, W. Aiken and J. Kissell, "Cloud Security Auditing: Challenges and Emerging Approaches," in IEEE Security & Privacy, vol. 12, no. 6, pp. 68-74, Nov.-Dec. 2014.

[29] M. Irfan, M. Usman, Y. Zhuang and S. Fong, "A Critical Review of Security Threats in Cloud Computing," 2015 3rd International Symposium on Computational and Business Intelligence (ISCBI), Bali, Indonesia, 2015, pp. 105-111.

DOI: https://doi.org/10.54216/JCIM.150121
Received: April 14, 2024 Revised: June 12, 2024 Accepted: August 10, 2024