Information Security Management Framework for Cloud Computing Environments

Manal M. Nasir [1,*], Salim M. Hebrisha[2]

[1]Gwinnett Technical College (GTC), Lawrenceville , GA, 30043, USA

[2]Libyan Iron and Steel Company (LISCO), Misrata, Libya

Emails: Mnasir@gwinnetttech.edu; salimhibrisha@gmail.com

Abstract

Cloud computing has become a popular paradigm for delivering computing resources and services over the internet. However, the adoption of cloud computing also brings new security challenges and risks, including data breaches, insider attacks, and unauthorized access. Therefore, it is critical to have a comprehensive information security management framework to address these challenges and ensure the security and privacy of cloud computing environments. This paper proposes a machine learning (ML) based information security management (ISM) framework for cloud computing environments that integrates best practices and standards from various domains, including cloud computing, information security, and risk management. The proposed framework includes residual recurrent network to effectively discriminate different patterns of cloud security attacks. The proposed framework emphasizes the importance of threat detection, security controls, and continuous monitoring and improvement. The framework is designed to be flexible and scalable, allowing organizations to tailor it to their specific needs and requirements.

Keywords: Information Security; Information Management; Cloud Computing; Machine Learning

1. Introduction

Cloud computing is a paradigm for delivering on-demand computing resources and services over the internet. It enables users to access and use a wide range of computing resources, including servers, storage, databases, applications, and services, without having to own or manage the underlying infrastructure. Cloud computing has become a popular option for organizations of all sizes, as it provides numerous benefits, such as cost savings, scalability, flexibility, and agility. Cloud computing also enables organizations to rapidly deploy new applications and services, collaborate and share resources across geographies, and leverage advanced technologies, such as artificial intelligence, machine learning, and the internet of things.

Cloud computing presents various security challenges and risks that organizations must address to protect their data and resources. Some of the key security issues of cloud computing include data breaches, insider threats, misconfiguration, compliance and regulatory challenges, and vendor lock-in. The shared responsibility model of cloud computing also adds complexity to security management, as organizations are responsible for securing their own data and applications in the cloud, while cloud providers are responsible for securing the underlying infrastructure. Cloud computing environments also create new attack surfaces, as attackers can exploit vulnerabilities in the cloud provider's infrastructure, shared resources, or weak user credentials to gain unauthorized access or steal sensitive information. Therefore, organizations must implement a comprehensive information security management framework that

Doi : https://doi.org/10.54216/JCIM.110102
Received: October 18, 2022 Revised: December 21, 2022 Accepted: January 06, 2023

addresses these challenges and includes measures such as risk assessment, access controls, encryption, monitoring, and incident response to ensure the security and privacy of cloud computing environments.

Information Security Management (ISM) is a systematic approach to managing the confidentiality, integrity, and availability of an organization's information assets. In the context of cloud computing, ISM becomes more complex due to the shared responsibility model and the dependence on third-party providers. ISM involves identifying and assessing risks, developing policies and procedures, implementing security controls, monitoring and measuring performance, and continuously improving the security posture of the organization. Effective ISM in cloud computing

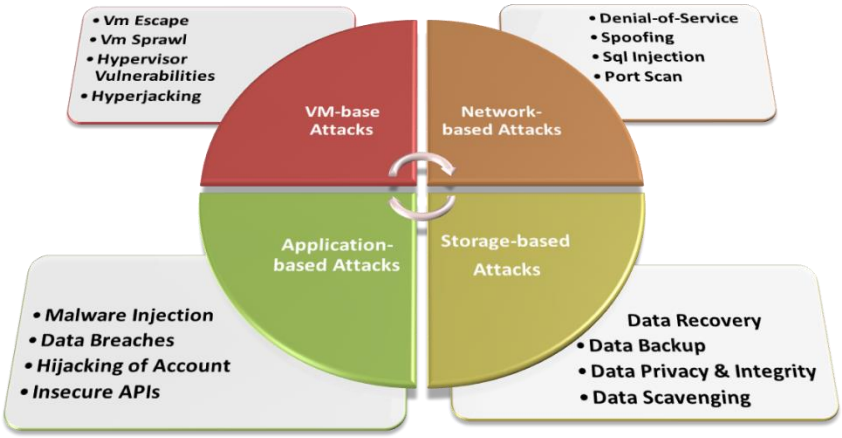

Figure 1: categories of cyber-attacks in cloud computing.

environments requires a comprehensive understanding of the organization's information assets, the cloud provider's security controls and certifications, and the legal and regulatory requirements applicable to the organization. ISM also involves building a culture of security awareness and training to ensure that employees, partners, and customers understand their roles and responsibilities in protecting the organization's information assets in the cloud.

This paper proposes an ML-based ISM framework that integrates residual recurrent networks to effectively identify the main security threats against cloud computing environments. The framework aims to address the new security challenges and risks associated with the adoption of cloud computing and ensure the security and privacy of cloud computing environments. Extensive analysis of public case studies of security attacks validates the effectiveness, flexibility, and scalability of our framework, allowing organizations to tailor it to their specific needs and requirements.

2. Literature review

The literature on cloud computing and security challenges has grown rapidly in recent years, reflecting the increasing adoption of cloud computing and the growing concern about the security risks it presents. Many studies have focused on identifying and analyzing the key security challenges of cloud computing, such as data breaches, insider threats, misconfiguration, compliance and regulatory challenges, and vendor lock-in, as well as the potential impacts of these challenges on organizations. Research has also proposed various security frameworks and models to help organizations manage security in cloud computing environments. For example, the Cloud Security Alliance (CSA) has developed the Cloud Controls Matrix (CCM) and the Cloud Security Open API (CSOA) to provide guidance on security controls and compliance in cloud computing. Other frameworks, such as the NIST Cybersecurity Framework, ISO 27001, and COBIT, have been adapted to cloud computing environments to provide a systematic approach to security management. In addition, research has investigated various security technologies and solutions that can be used to enhance security in cloud computing environments, such as encryption, access controls, identity and authentication, intrusion detection and prevention, and secure data storage and backup. ML and AI techniques have also been explored to improve the detection and response to security threats in the cloud.

Doi : https://doi.org/10.54216/JCIM.110102
Received: October 18, 2022 Revised: December 21, 2022 Accepted: January 06, 2023

The literature on ISM solutions is extensive and diverse, reflecting the importance of effective information security in today's digital landscape. For example, Subramanian and Jeyaraj [4] provided an overview of the recent security challenges in cloud computing. They identified and analyzed the key security challenges of cloud computing, including data breaches, insider threats, compliance and regulatory challenges, misconfiguration, and vendor lock-in. They also discussed the potential impacts of these challenges on organizations and the factors that contribute to the complexity of security management in cloud computing environments. The various security solutions and approaches to address these challenges, such as access controls, encryption, intrusion detection and prevention, and incident response. Chenthara et al. [6] studied the security and privacy challenges of e-health solutions in cloud computing. They highlighted the importance of e-health solutions and the benefits they offer in terms of cost, accessibility, and patient care. However, they also identified the security and privacy risks associated with storing and processing sensitive health data in the cloud. They provided an overview of the key security and privacy challenges of e-health solutions in the cloud, including data breaches, insider threats, compliance and regulatory challenges, and data protection. They also discussed the role of cloud providers and the need for a shared responsibility model to ensure the security and privacy of e-health solutions. Hussein and Khalid [10] provided a comprehensive survey of the security challenges and solutions of cloud computing, including data breaches, denial of service attacks, insider threats, compliance and regulatory challenges, and cloud provider dependency. They also discussed the potential impacts of these challenges on organizations and the factors that contribute to the complexity of security management in cloud computing environments. Sun et al [11] surveyed the critical security issues in cloud computing by identifying and analyzing the key security issues of cloud computing, including data breaches, denial of service attacks, insider threats, compliance and regulatory challenges, and data protection. They also include various security solutions and approaches to address these challenges, such as access controls, encryption, intrusion detection and prevention, and incident response. They also discussed emerging security technologies and techniques, such as secure multi-party computation, homomorphic encryption, and blockchain, which have the potential to improve cloud security. Zaslavskaya et al. [22] discussed the features of ensuring information security when using cloud technologies in educational institutions based on the growing trend of cloud adoption in the education sector and the benefits it offers, such as scalability, accessibility, and cost-effectiveness. They also identified the security risks associated with storing and processing sensitive educational data in the cloud. In [25], the authors presented a comparative study of information security risk assessment models for cloud computing systems. They identified the importance of risk assessment in ensuring the security of cloud systems and highlight the lack of standardization and consensus in the selection of risk assessment models for cloud computing. They presented a comparative analysis of several risk assessment models, including the ISO 27005, the NIST 800-30, and the OCTAVE Allegro. The authors evaluate the models based on various criteria, such as their scope, methodology, and applicability to cloud computing environments. In [28], Ali et al. provided an overview of the benefits of cloud computing, such as cost savings, scalability, and accessibility, and highlighted the security risks associated with cloud adoption. They presented a comprehensive review of the existing security solutions and techniques for cloud computing, such as encryption, access control, and intrusion detection.

3. Methodology

The research approach adopted in the paper is primarily based on a systematic review and comprehensive analysis of the literature presented in the previous section. The research approach of our work is focused on collecting security traffic data, preparing the data for training, and building an ML model to enhance the effectiveness of the ISM in the cloud.

The first step in successful research on ISM involves collecting a large dataset of security traffic in cloud computing environments, as a case study for evaluating the proposed framework. This usually involves gathering data from various sources, such as network logs and system event data, to provide a comprehensive view of the security threats and attacks that occur in cloud computing environments. The data collection process may have also involved defining specific criteria for selecting data, such as data that is relevant to a particular type of cloud computing environment or data that is representative of different types of attacks. However, with the availability of public representative datasets, our research approach replaces the data collection step by using CIC-IoT-Datase. The CIC-IoT Dataset is a publicly available dataset containing network traffic data from IoT devices. It is the latest version of the CIC IoT Dataset series, which is maintained by the Canadian Institute for Cybersecurity (CIC) at the University of New Brunswick. The dataset was created by capturing network traffic from a variety of IoT devices in a controlled lab environment, as well as from real-world IoT networks. The captured traffic was then labeled and filtered to remove irrelevant traffic, such as noise or background traffic. The dataset contains a total of 6 scenarios, each representing a different IoT network

Doi : https://doi.org/10.54216/JCIM.110102
Received: October 18, 2022 Revised: December 21, 2022 Accepted: January 06, 2023

environment. The scenarios include Power, Idle, Interactions, Scenarios, Active, and Attacks. The class distribution of the dataset is given in Table 1.

Table 1: Distribution of samples in CIC-IoT-Dataset.

	CAMERA	HOME AUTOMATION	AUDIO
# samples	191175	19557	18774
# samples (resampled)	20175	19557	18774

The summary statistics of the dataset are given in Table 2.

Table 2: Descriptive Statistics of CIC-IoT-Dataset2022.

	count	**mean**	**std**	**min**	**25%**	**50%**	**75%**	**max**
port_class_src	229506	2.166702	0.68169	0	2	2	3	3
port_class_dst	229506	2.01813	0.634339	0	2	2	2	3
pck_size	229506	640.248634	573.434117	0	32	408	1096	1480
ip_dst_new	2.30E+05	2.15E+09	1.04E+09	0.00E+00	1.15E+09	2.21E+09	3.23E+09	4.29E+09
ethernet_frame_size	229506	674.290507	573.388214	42	66	442	1130	1514
ttl	229506	81.704034	56.14046	0	64	64	64	255
total_length	229506	660.207511	573.48095	0	52	428	1116	1500
protocol	229506	13.354095	5.221833	0	6	17	17	17
source_port	229506	32220.87109	22236.08284	0	11159	36720	52399	65130
dest_port	229506	25636.60286	21374.55356	0	6285	20296	47277	65130
...	...	...	...	...	...	...	...	...
average	229506	640.917114	410.292419	0	268.149994	638.806244	988	1480
skew_e	229506	0.037188	1.147916	-4.129483	-0.385853	0	0.612859	4.129483
kurt_e	229506	-0.713068	2.843665	-3	-1.966667	-1.5	-0.563972	15.052631

Doi : https://doi.org/10.54216/JCIM.110102
Received: October 18, 2022 Revised: December 21, 2022 Accepted: January 06, 2023

var_e	229506	160108.5313	159310.25	0	2134.055542	138649.9531	267321.5781	532900
q3_e	229506	875.082581	505.801727	0	366.5	1040	1324	1480
q1_e	229506	414.757812	511.009186	0	32	76	1026.75	1480
iqr_e	229506	460.324707	504.007721	0	0	258.5	888.5	1460
epoch_timestamp	2.30E+05	1.63E+09	2.28E+05	1.63E+09	1.63E+09	1.63E+09	1.63E+09	1.63E+09
inter_arrival_time	229506	0.047167	0.459032	0	0	0.000619	0.009246	30.345287
time_since_previously_displayed_frame	229506	12.402766	9.699078	0	3.58985	10.688952	19.609797	93.283325

Following the above analysis, the dataset is resampled and then prepared for training by performing various pre-processing tasks. This includes data cleaning to remove any irrelevant or inaccurate data and feature selection to identify the most relevant features for our framework model. Since the data values lie in different ranges, we apply min-max normalization to scale down the values to the same range.

$$y_{in} = \frac{x_{in} - min(x_{in})}{max(x_{in}) - min(x_{in})} \quad (1)$$

Since the data becomes ready for training, we start discussing the building of our ML model. In the ISM framework, residual LSTM is proposed to detect cloud threats. The residual LSTM is developed as an extension to the standard Long short-term memory (LSTM) model, which combines residual linking between different layers of the network. The inclusion of residual connections can facilitate the flow of gradient, which addresses the issue of vanishing gradients, which can occur during the training process. The residual LSTM model uses skip connections to allow the input to bypass one or more layers in the network, enabling the network to learn from the residual of the input and the output of the layer. The typical design of LSTM is composed of forgetting gate f_t, input gate i_t, and output gate o_t.

$$f_t = sigmoid\left(W_f h_{t-1} + V_f x_t + b_f\right) \quad (2)$$
$$i_t = sigmoid(W_i h_{t-1} + V_i x_t + b_i) \quad (3)$$
$$\tilde{c}_t = tanh(W_{\tilde{c}} h_{t-1} + V_{\tilde{c}} x_t + b_{\tilde{c}}) \quad (4)$$
$$o_t = sigmoid(W_o[h_{t-1}, x_t] + b_o) \quad (5)$$
$$r_t = o_t \times \tanh(c_t) \quad (6)$$
$$h_t = W_p \cdot r_t \quad (7)$$

where x_t and h_t represents the input and hidden state, respectively. c_t designate the cell state. To include residual connectivity in our design, we update our computation as follows.

$$r_t = \tanh(c_t) \quad (8)$$
$$m_t = W_p \cdot r_t \quad (9)$$
$$h_t = o_t \cdot (m_t + W_h x_t) \quad (10)$$

In the context of threat detection, the residual LSTM is trained on a labeled dataset of security traffic to learn the patterns of normal and malicious network behavior. Once trained, the model is used to classify incoming traffic as either normal or malicious. The output of the model is a probability score, which can be used to make a decision on whether to allow or block incoming traffic.

The hyperparameters of our model are given in Table 3.

Doi : https://doi.org/10.54216/JCIM.110102
Received: October 18, 2022 Revised: December 21, 2022 Accepted: January 06, 2023

Table 3: Hyperparameters of our LSTM.

Hyperparameter	Description
Number of Layers	3
Hidden Units	20
Dropout	0.3
Learning Rate	0.0006
Batch Size	32
Epochs	60
Activation Function	ReLU
Loss Function	Cross-entropy
Optimizer	Adam

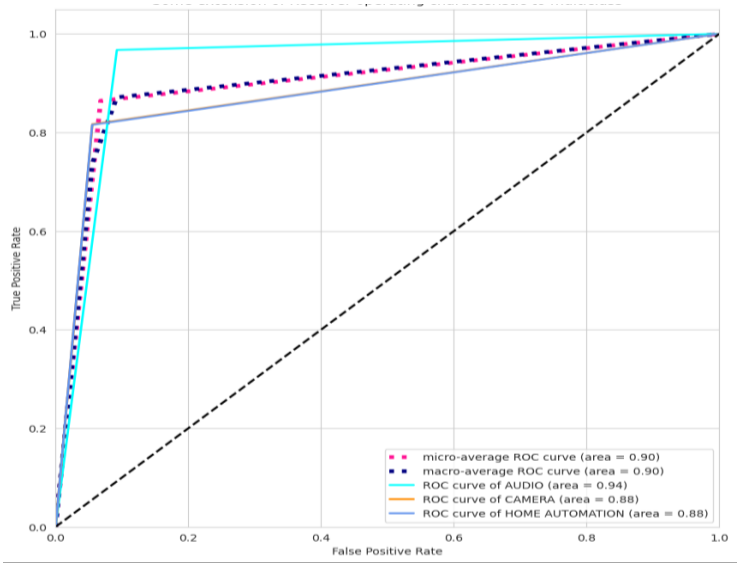

Figure 2: Visualization of the results of ROC analysis for the proposed ISM framework.

ROC analysis is applied in our experiments to evaluate the performance of our ML-based ISM framework for cloud computing environments, as shown in Figure 2. As shown, we can plot the ROC curve by varying the decision threshold of the classifier and computing the true positive rate (TPR) and false positive rate (FPR) for each threshold. The ROC curve is a graphical representation of the relationship between TPR and FPR, and it provides a way to evaluate the performance of the classifier across all possible decision thresholds. The classification performance reaches its maximum level in the AUDIO class while maintaining similar performance on attacks on Home Automation and Camera class.

A confusion matrix is used in our experiments to assess the performance of the ISM framework in detecting security threats for cloud computing environments, as shown in Figure 3. By analyzing the confusion matrix for our ISM framework, we can calculate the classification performance of our ML-based model in detecting different types of security threats in cloud computing environments and identify areas where the model may need improvement (i.e., Automation and Camera). These insights can be used to refine the model and improve its performance.

Doi : https://doi.org/10.54216/JCIM.110102
Received: October 18, 2022 Revised: December 21, 2022 Accepted: January 06, 2023

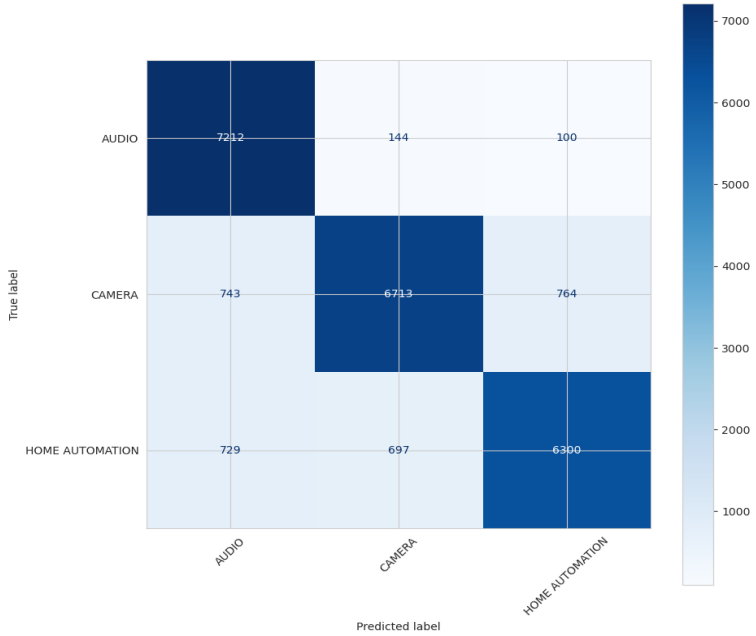

Figure 3: Visualization of the results of confusion matrix for the proposed ISM framework.

4. Conclusion

In this work, we present an ML-based ISM framework for cloud computing environments to address the unique security challenges of cloud adoption. In particular, a residual recurrent network is applied to empower the ISM frameworks to automatedly identify different attacks in cloud domains. The paper contributes to the understanding of information security management in cloud computing environments and provides a practical framework for organizations to secure their cloud systems. The framework can serve as a guide for security practitioners and researchers in the field, and its adoption can help organizations to enhance the security of their cloud systems and protect their sensitive information assets.

References

[1] Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A comprehensive survey on security in cloud computing. *Procedia Computer Science*, *110*, 465-472.

[2] Mahboob, T., Zahid, M., & Ahmad, G. (2016, August). Adopting information security techniques for cloud computing—a survey. In *2016 1st International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)* (pp. 7-11). IEEE.

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

[4] Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. *Computers & Electrical Engineering*, *71*, 28-42.

[5] Song, H. H. (2020). Testing and evaluation system for cloud computing information security products. *Procedia Computer Science*, *166*, 84-87.

[6] Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-health solutions in cloud computing. *IEEE access*, *7*, 74361-74382.

[7] Tariq, M. I. (2019). Agent based information security framework for hybrid cloud computing. *KSII Transactions on Internet and Information Systems (TIIS)*, *13*(1), 406-434.

[8] Ding, L., Wang, Z., Wang, X., & Wu, D. (2020). Security information transmission algorithms for IoT based on cloud computing. *Computer Communications*, *155*, 32-39.

[9] Sun, X. (2018, May). Critical security issues in cloud computing: a survey. In *2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High*

Doi : https://doi.org/10.54216/JCIM.110102
Received: October 18, 2022 Revised: December 21, 2022 Accepted: January 06, 2023

Performance and Smart Computing,(HPSC) and IEEE International Conference on Intelligent Data and Security (IDS) (pp. 216-221). IEEE.

[10] Hussein, N. H., & Khalid, A. (2016). A survey of cloud computing security challenges and solutions. *International Journal of Computer Science and Information Security*, *14*(1), 52.

[11] Alsharif, M., & Rawat, D. B. (2021). Study of machine learning for cloud assisted iot security as a service. *Sensors*, *21*(4), 1034.

[12] Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. *arXiv preprint arXiv:1609.01107*.

[13] Alhenaki, L., Alwatban, A., Alamri, B., & Alarifi, N. (2019, May). A survey on the security of cloud computing. In *2019 2nd international conference on computer applications & information security (ICCAIS)* (pp. 1-7). IEEE.

[14] Puthal, D., Sahoo, B. P., Mishra, S., & Swain, S. (2015, January). Cloud computing features, issues, and challenges: a big picture. In *2015 International Conference on Computational Intelligence and Networks* (pp. 116-123). IEEE.

[15] Jakimoski, K. (2016). Security techniques for data protection in cloud computing. *International Journal of Grid and Distributed Computing*, *9*(1), 49-56.

[16] Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. *Procedia Computer Science*, *125*, 691-697.

[17] Singh, A., & Malhotra, M. (2015). Security concerns at various levels of cloud computing paradigm: A review. *International journal of computer networks and applications*, *2*(2), 41-45.

[18] Aljumah, A., & Ahanger, T. A. (2020). Cyber security threats, challenges and defence mechanisms in cloud computing. *IET Communications*, *14*(7), 1185-1191.

[19] Tsaregorodtsev, A. V., Kravets, O. J., Choporov, O. N., & Zelenina, A. N. (2018). INFORMATION SECURITY RISK ESTIMATION FOR CLOUD INFRASTRUCTURE. *International Journal on Information Technologies & Security*, *10*(4).

[20] Markandey, A., Dhamdhere, P., & Gajmal, Y. (2018, September). Data access security in cloud computing: A review. In *2018 International Conference on Computing, Power and Communication Technologies (GUCON)* (pp. 633-636). IEEE.

[21] Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015, November). An investigation on cyber security threats and security models. In *2015 IEEE 2nd international conference on cyber security and cloud computing* (pp. 307-311). IEEE.

[22] Zaslavskaya, O. Y., Zaslavskiy, A. A., Bolnokin, V. E., & Kravets, O. J. (2018). Features of Ensuring Information Security when Using Cloud Technologies in Educational Institutions. *International Journal on Information Technologies & Security*, *10*(3).

[23] Rao, R. V., & Selvamani, K. (2015). Data security challenges and its solutions in cloud computing. *Procedia Computer Science*, *48*, 204-209.

[24] Vacca, J. R. (Ed.). (2016). *Cloud computing security: foundations and challenges*. CRC press.

[25] Jouini, M., & Rabai, L. B. A. (2016). Comparative study of information security risk assessment models for cloud computing systems. *Procedia Computer Science*, *83*, 1084-1089.

[26] Chou, D. C. (2015). Cloud computing: A value creation model. *Computer Standards & Interfaces*, *38*, 72-77.

[27] Amin, Z., Singh, H., & Sethi, N. (2015). Review on fault tolerance techniques in cloud computing. *International Journal of Computer Applications*, *116*(18), 11-17.

[28] Ali, O., Shrestha, A., Osmanaj, V., & Muhammed, S. (2021). Cloud computing technology adoption: an evaluation of key factors in local governments. Information Technology & People, 34(2), 666-703.

[29] Rahman, A. U., Khan, F. G., & Jadoon, W. (2016). Energy efficiency techniques in cloud computing. *International Journal of Computer Science and Information Security (IJCSIS)*, *14*(6).

Doi : https://doi.org/10.54216/JCIM.110102
Received: October 18, 2022 Revised: December 21, 2022 Accepted: January 06, 2023