Accredited Ranking SINTA 2
Decree of the Director General of Higher Education, Research, and Technology, No. 158/E/KPT/2021
Validity period from Volume 5 Number 2 of 2021 to Volume 10 Number 1 of 2026

Published online on: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 6 No. x (2022) 1028-1036 ISSN Media Electronic: 2580-0760

Faux Insider Hazard Investigation on Non-Public Cloud Computing by Using ADAM's Technique

Dwi Kurnia Wibowo[1], Ahmad Luthfi[2], Yudi Prayudi[3], Erika Ramadhani[4], Muhamad Maulana[5]
[1,2,3,4,5]Department of Informatics, Faculty of Industrial Technology, Indonesian Islamic University
[1]dwikurniawibowo@gmail.com*, [2]ahmad.luthfi@uii.ac.id, [3]prayudi@uii.ac.id, [4]erika@uii.ac.id, [5]vanmoeljr8@gmail.com

Abstract

Cloud computing is a service system mechanism that businesses and organizations use to perform computerized and integrated transactions over computer networks. The service system must, of course, be matched with a certain amount of security. It is applied to forecast the probability of cybercrime. A Cloud Service Provider (CSP) often offers cloud-based services with a basic level of security. Typically, CSPs are set up to offer their services on the open internet. Data security-focused organizations strive to shield their systems from a wide range of attackers. One of the alternatives is to construct a private cloud computing system. The issue is the potential for Man in the Cloud (MITC) assaults, which compromise and modify identities and are identified in cloud systems as phony insider threats. Based on the ISO 27032 standard research, the goal of this work is to undertake a threat analysis of MITC attack methodologies against private cloud computing services. With regards to risks to cloud services in a private cloud computing environment, it is intended that reporting and documenting the study' findings would lead to suggestions for more research and cybersecurity management procedures.

Keywords: Cloud, MITC, Forensics, ADAM, Analysis.

1. Introduction

Companies use service system techniques known as cloud-based services to conduct automated and integrated transactions across a computer network. The concept of cloud computing dates back to the 1950s. The mainframe Time-Sharing idea, which is still relevant in the current industrial 4.0 age, defines this generation. Cloud service providers (CSPs) typically set up their systems so that their services may be accessible over the open internet. Cloud service providers provide three types of services: Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS) [1]–[4].

In cloud computing, there are four different deployment models, which are as follows: Private cloud (internal), when the cloud infrastructure is made exclusively available for use by a single company that caters to a sizable user base. Community cloud: A type of cloud computing environment wherein a certain group of customer communities from cooperating organizations have exclusive access to the cloud infrastructure. Cloud infrastructure that is made available to the broader public for open use in the public cloud. A company, academic institution, government agency, or a combination of these entities may own, manage, and run it. A hybrid cloud's cloud architecture is made up of two or more distinct cloud infrastructures (private, community, and public), each of which is unique from the others but is connected to the others through standard or proprietary technologies that provide data and application exchange [1], [5].

Businesses that place a high priority on data security need a system that is secure from various cyberattacks. Alternative solutions like private cloud computing models are a possibility. In an effort to protect information security, especially for business and user and consumer data, a private cloud has been developed. Private cloud computing strategies in an effort to foresee potential dangers of all types. Threats made and at businesses organizations are a serious issue for and governmental agencies. Attacks that are carried out either purposefully or inadvertently against cloud systems are threats. Threats are often divided into two groups: Exider Threats, or assaults on the system by outsiders with certain goals and objectives An insider threat is an attack that targets the system from within with a specific goal [6]–[9].

Accepted: 25-11-2022 | Received in revised: 14-12-2022 | Published: 29-12-2022

The Man in the Cloud assault scenario is an imagination one to talk about because it falls under the category of an external danger, yet is widely believed to be an insider threat. To properly comprehend identity engineering, which hackers exploit to pose as system insiders, further in-depth study is needed. The purpose of the inquiry is to determine whether it is feasible to assess the threat that the Man in the Cloud case poses. The validation's results will be useful in categorizing the threats that are faced. The inquiry and validation process uses the ADAM (The Advance Data Acquisition Model) method. The ADAM approach was selected since it was created from a number of earlier methods that were based on earlier investigations. It is suggested to utilize the ADAM method while performing a series of investigations utilizing digital evidence up to the reporting stage of the investigation's conclusions since the phases are more thorough than those of other approaches [1], [10], [11].

One issue that frequently arises is ignorance of the threat posed by cybercrime. This is a result of a lack of knowledge about cyber security procedures. To provide the best company security protection, socio-technical management processes must still be developed in order to maximize technical and non-technical security measures. Because humans continue to be the weakest link in corporate security, substantial research over the past ten years has demonstrated this. Because of this, human error or conduct is the cause of the majority of cyberattacks [12], [13].

An insider threat is a dangerous risk posed by people working for a firm, and it typically involves intentional fraud, the theft of confidential or sensitive information for commercial gain, or the disruption of computer systems. The external threat, on the other hand, involves the same activity but is carried out by people who are not affiliated with the organization. Technical threats that take the shape of assaults on cloud services are extremely diverse and use a variety of attack techniques. Attacking strategies include Man in the Cloud. A brand-new attack method called Man in the Cloud was first observed in cloud services in 2015. (MITC). This MITC attack is distinct from the common Man in the Browser (MITB) and Man in the Middle (MITM) attacks [10], [14]–[18].

A field called digital forensics was created to gather and examine data from computer systems, networks, wireless communications, and storage devices in a way that may be used as evidence in court [19]. Four distinct phases make up the digital forensics process: Collection of artifacts that are deemed to have potential worth, including digital proof and supporting documentation. Dependable, thorough, accurate, and provable preservation of original objects. Using artifact screening analysis, valuable artifacts are either removed or added. A presentation where the investigation's supporting evidence is displayed. The two main types of digital forensics—static digital / "write block" and "live forensics" are the result of forensics ability to construct and capture complicated circumstances. Analysis of static data, such as that found on hard disks retrieved by conventional formal acquisition processes, is the focus of static forensics. Live forensics refers to the analysis of system memory and other relevant data while the system under study is still in use [10], [19]–[22].

The technical control phases of the cyber security framework are described by internationally recognized standards. There are many companies that use ISO/IEC 27001 information security controls on their systems and follow solid cyber security procedures. If the firm complies with ISO 27001, the process of putting technical controls in place for cyber security is considerably simpler. The ISO 27032 standard offers technical measures for cyber security defense against social engineering assaults. Malicious software, hacking (malware) [4]–[7], [23], [24].

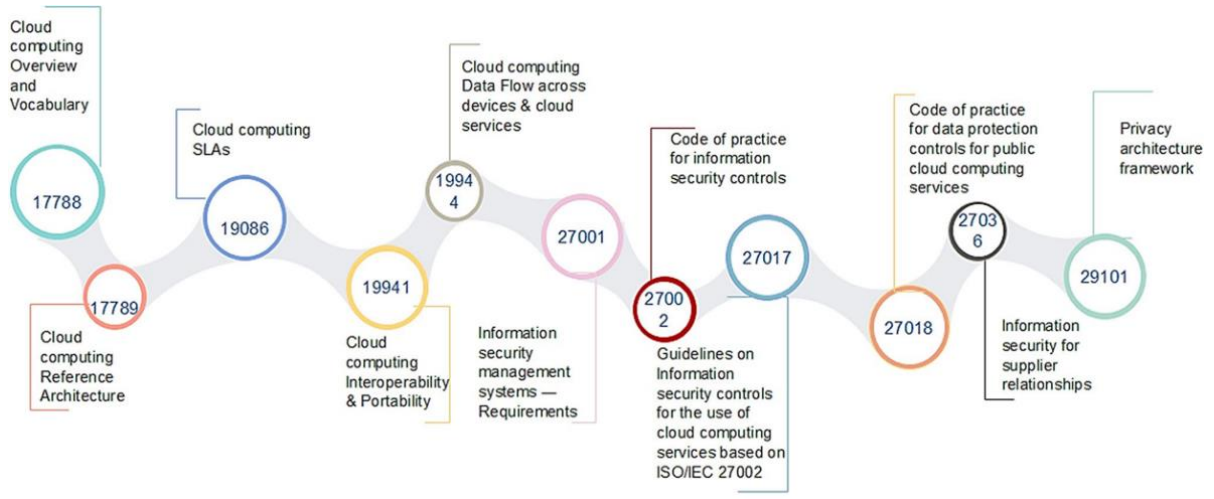

Figure 1. ISO Cloud Computing Standards [2]

DOI: https://doi.org/10.29207/resti.v6i6.4714

Secure coding is one of the technical safeguards that must be in place to protect the data that products collect online. Network monitoring and response: To guarantee that network services continue to be dependable, secure, and available, controls must be in place. The quality of network service shouldn't be compromised by cyberspace. To ensure that servers are safely accessible from the internet and protected from unauthorized access and harmful material, controls at the server level are required. Application-level security measures Put measures in place to stop unauthorized data tampering, issues with transaction recording, and handling errors. Controls must be in place to guard against known exploits and attacks on end-user infrastructure across the company [25], [26].

It is exciting to do a thorough study of cloud services in relation to threats posed by Man in the Cloud (MITC) attack tactics based on the fundamental concerns mentioned, studies from related research, as well as speculations from earlier studies. MITC's handling and how it differs from other attack methods will be explained. Describe the types of MITC attacks that utilize actors from outside parties who construct identities if the cloud service is private [5], [10], [17], [27]–[29].

2. Research Methods

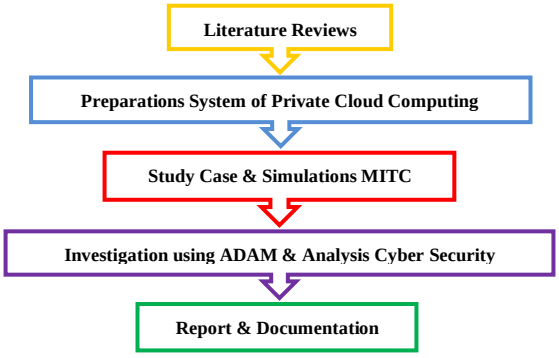

Figure 2. Research Process Flow

The focus of the research to be conducted is decided using a number of research characteristics. The study's variables include describe on Table 1.

Table 1. Variable Indicator of Research

Independent Variable	Dependent Variable
• Cloud Computing	• Private Cloud Computing Scheme
• Threat	• Man in the Cloud attack tecqhnique
• Investigation	• Acquisition with ADAM Method
• Security	• Standard Cyber Security Analysis
	• Cyber Security Framework Analysis

The next stage is to decide on the method of doing research after creating a mind map and outlining how forensics and security disciplines relate to cloud services. This process is a sequence of actions that will be taken and turned into a methodology for conducting research. One of this study's contributions is the suggested technique. To implement the case scenarios and simulations in this study, private cloud computing services that were drawn from instances that happened in the Tasikmalaya City Diskominfo environment were employed. The identities and locations were masked as "XYZ Organization" to safeguard privacy. The private cloud service infrastructure system's names and services have been modified for the field's conditions. Using the ADAM method to gather information and the cyber security framework to analyze it. During the investigation and analysis phases of the cyber security process, the results of the two procedures will be analyzed and confirmed for the kind of danger.

3. Results and Analysis

By using the Man in the Cloud simulation and case scenario, the investigation procedure for the stage of cyber security analysis is carried out (MITC). Digital evidence is gathered during the investigating process. Analyses carried out with the ADAM Method (Initial Planning, On-site Planning, Digital Data Acquisition). The NIST Cyber Security Framework's Steps and ISO 27032 Cyber Security Guidelines were then used to examine the examination of the Man in the Cloud (MITC) attack scenarios and simulations as a danger to cloud systems on XYZ Organization. Data Acquisition: Digital Tables 4 and 5 provide descriptions of the phases the study reached and the outcomes. As a result, it is easy to locate the error that is dangerous.

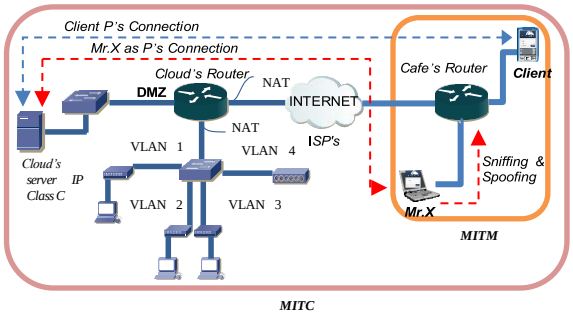

Figure 3. Man in the Cloud (MITC) Case Scenarios

The ADAM's method approach is then used for investigation after the simulation has gone well. Investigations were conducted to find digital proof in the cloud server and router logs. Once the data has been collected, packet tracking is done on the access log on the cloud server as well as the network traffic log on the cloud router. Figure 5, Figure 6 and Figure 7 all provide descriptions of these stages.

DOI: https://doi.org/10.29207/resti.v6i6.4714

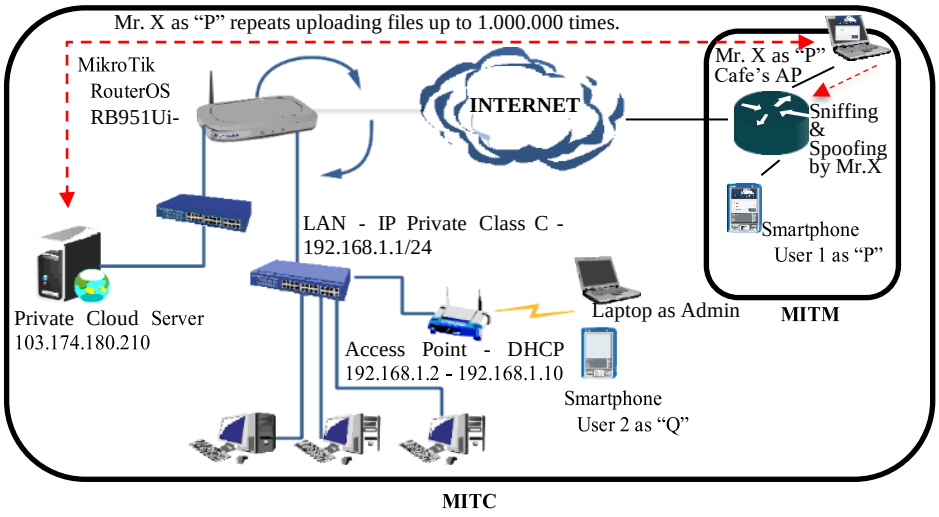

Figure 4. Man in the Cloud (MITC) Case Simulation

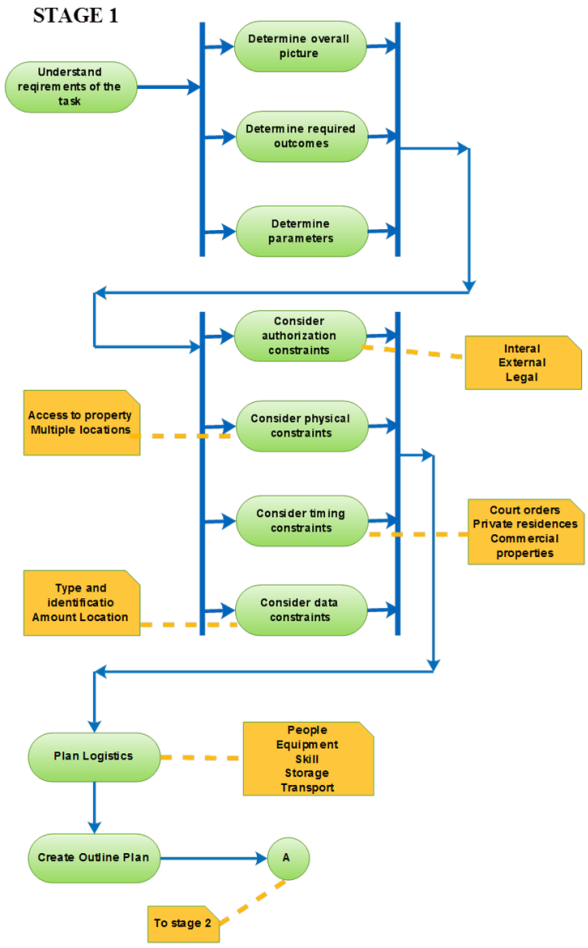

Figure 5. ADAM Stage 1 Initial Planning [30]

Several findings were attained and are summarized in Table 2 based on Figure 5, which illustrates the steps of the Stage 1 Initial Planning inquiry. The outcomes of the Stage 1 Initial Planning inquiry process flow using the ADAM Method are explained. The results obtained are the output of the analysis before conducting technical investigations in the field or in other words, Stage 1 for Initial Planning is the details of the investigation preparation stage. The preparation starts with case abstraction to planning equipment requirements.

Table 2. Investigation Results Based on Stage 1 Initial Planning

No.	STAGE 1 - Understand Requirement of the Task	Results
1.	• Determine overall picture • Determine required outcomes • Determine parameter	• Understand the system architecture of the Private Cloud Computing Service and the threat mechanisms that occur • Determine the results to be obtained in the form of digital evidence of the identity of users who access the cloud server through a cloud router • Determine data acquisition techniques with live forensics
2.	• Consider authorization constraints • Consider physical constraints • Consider timing constraints • Consider data constraints	• The investigation was carried out on a simulation of the Private Cloud Computing Service system • Prepare for investigation support hardware needs • Investigations are carried out with live forensics before the threat activity ends to obtain the expected digital evidence • Digital evidence is captured because the data is easily changed or lost
3.	• Plan Logistics • Create Outline plan	• Preparations made regarding hardware, software and licensing requirements

DOI: https://doi.org/10.29207/resti.v6i6.4714

	• The investigation was carried out independently

STAGE 2

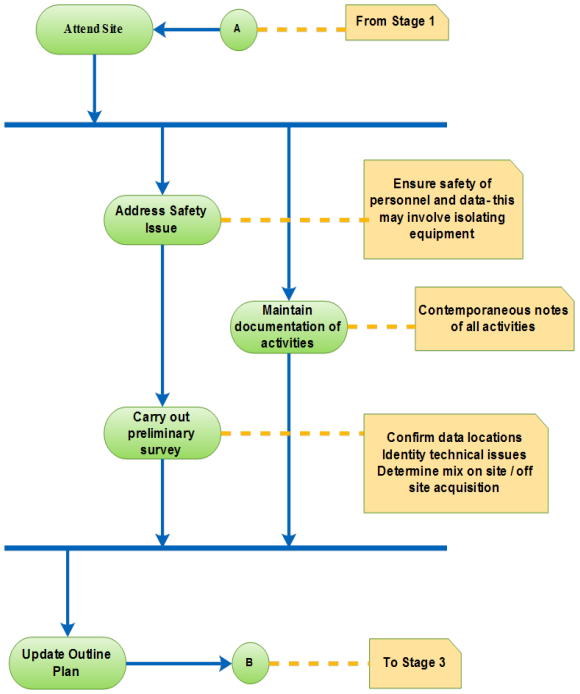

Figure 6. ADAM Stage 2 The Onsite Plan [30]

Based on Figure 6 described for Stage 2 of The Onsite Plan, the results obtained are described in Table 3.

Table 3. Investigation Results Based on Stage 2 The Onsite Plan

No.	STAGE 2 - The Onsite Plan	Results
1.	• Attend Site	• Private laboratory for simulations and case scenarios
2.	• Address Safety Issue	• Do not give permission to unauthorized parties to enter the laboratory
3.	• Maintain Documentation of Activities	• Documentation is not distributed without permission
4.	• Carry Out Preliminary Survey	• The survey was conducted by taking into account the provisions and limitations of Stage 1 Initial Planning
5.	• Update Outline Plan	• Investigations are carried out independently and using equipment in a private laboratory

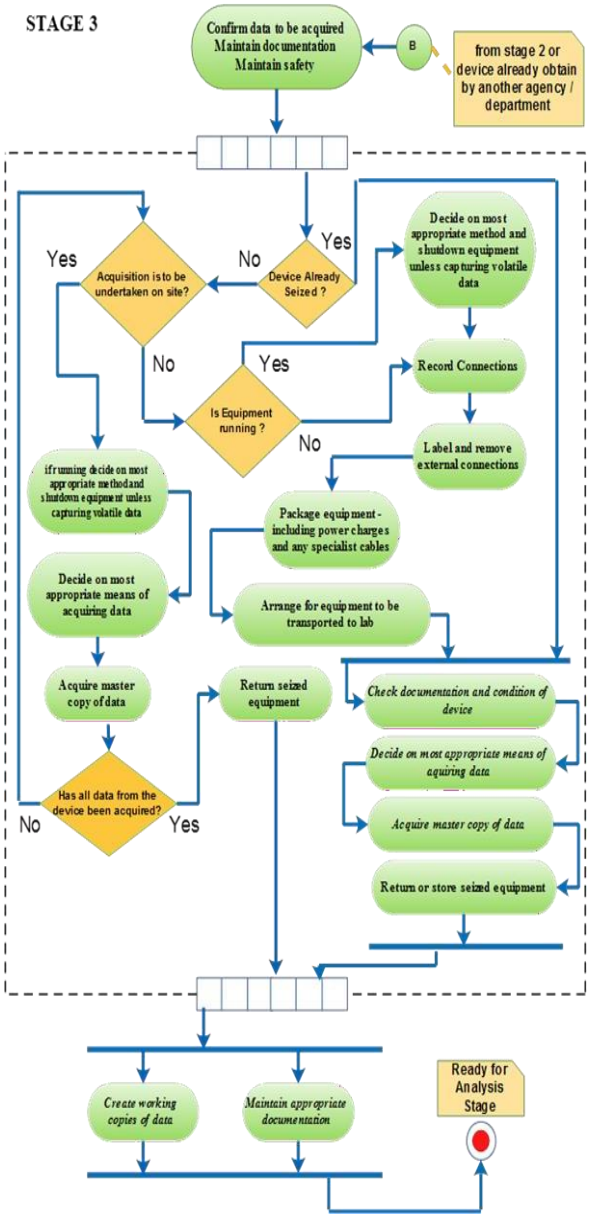

Figure 7. ADAM Stage 3 Acquisitions [30]

Based on Figure 7 described for ADAM Stage 3 Acquisitions, the results are described in Table 4. In Table 4 it is explained for the results of the acquisition of digital evidence for evidence that has been confiscated. In Stage 3, it is the investigator's choice to be able to cut the process chain according to the condition of the device. If the device has not been confiscated then the process must be carried out from the confiscation of the device first. If the device has been confiscated, you can immediately proceed to the data acquisition stage on the device.

DOI: https://doi.org/10.29207/resti.v6i6.4714

Table 4. Investigation Results Based on Stage 3 Acquisitions for Secured Evidence Flow

No.	STAGE 3 – Confirm data to be acquired, Maintain, Documentation, Maintain Safety	Results
1.	Device Seized	• Check documentation and condition device • Documentation is maintained and the condition of the device in the form of cloud servers and cloud routers is still alive
2.		• Device on most appropriate means of acquiring data • The state of the device is still in a state of receiving threats from Mr. X.
3.		• Acquire master copy of data • Monitoring and capturing data traffic packets when Mr. X performs a file upload loop
4.		• Return and store seized equipment • After investigating the cloud server and cloud router, the device is secured from access by unauthorized parties
5.	• Create working copies of data	• Capturing on the cloud server for registered users on the system, access level, user device identity, Mr.X device identity • Capturing on the cloud router for the MAC Address of the user's device registered on the system, the identity of the user's device, the MAC Address of the Mr.X device on the system, the identity of the Mr.X device • Capturing on network monitoring tools for Mr.X data packet traffic when looping file uploads
6.	• Maintain appropriate documentation	• Mapping for registered users, access levels, user device identification, Mr. X device identification and Mr. X status analysis on the Private Cloud Computing Service

The findings of the ADAM Method inquiry are in the form of digital traces, and a validation process is then carried out to demonstrate that the culprit is an outsider who enters the system using a login and password of a registered user. Figure 8 provide descriptions of the resulting screenshots of the user data that was entered into the system. After keeping an eye on the cloud router for logged-in, users, keep an eye on it for threats. Then it is explained how the cloud server monitors for threats such as looping upload files 1.000.000 times. Figure 9 and Figure 10 show how monitoring is done from the cloud router side when the loop upload file occurs to determine who is looping file uploads and track data information in the form of device name and MAC addresses.

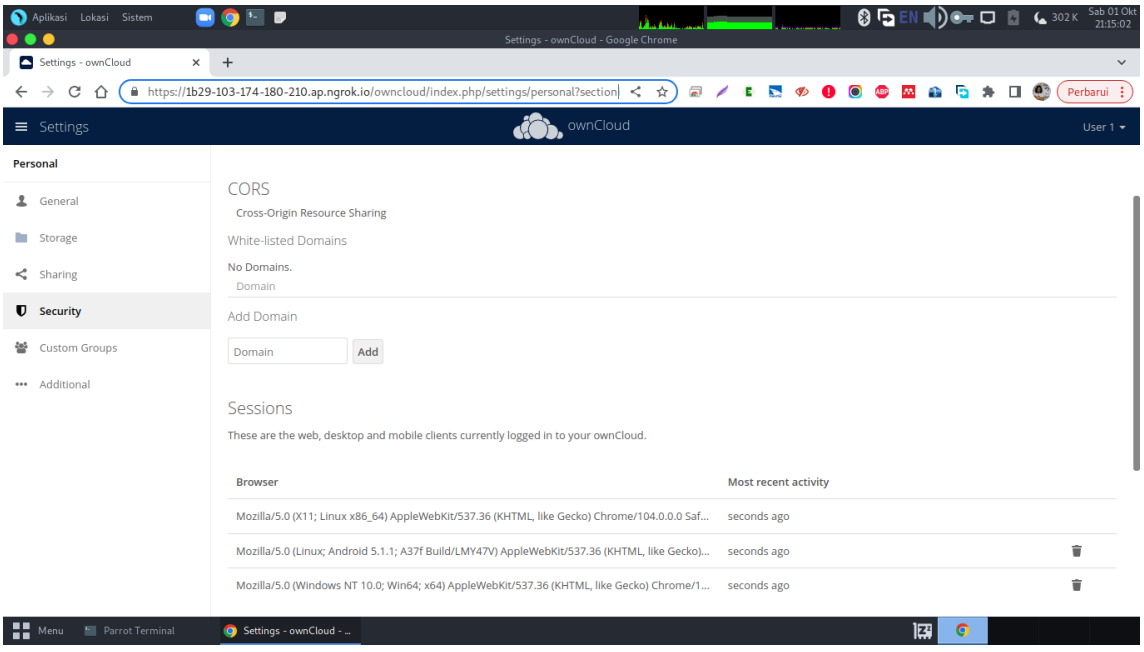

Figure 8. User 1 Registered and User 1 Unregistered

DOI: https://doi.org/10.29207/resti.v6i6.4714

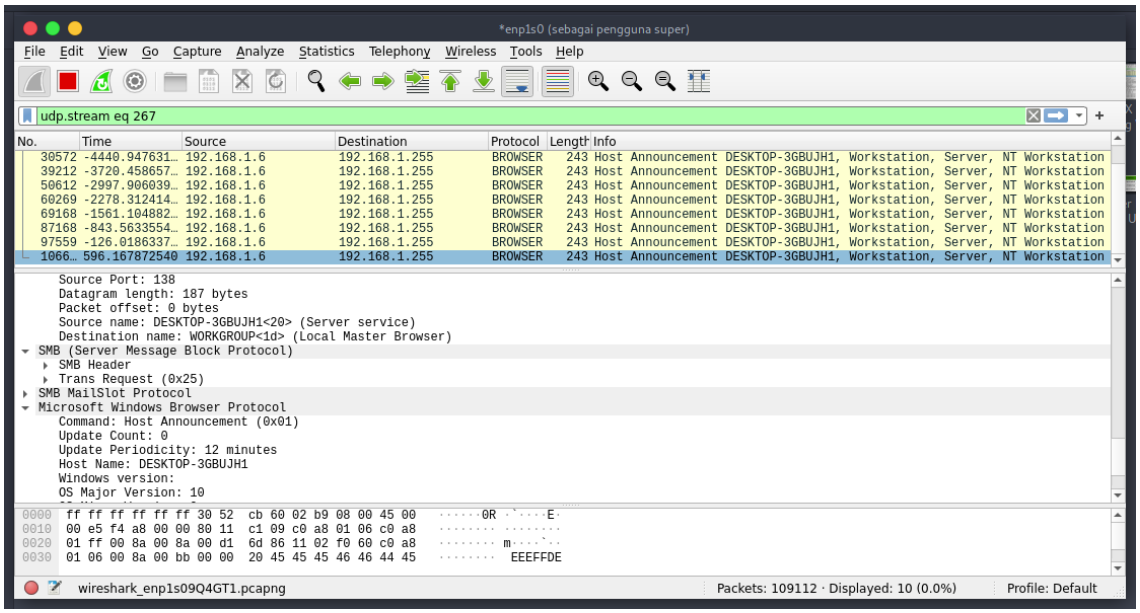

Figure 9. Log traffic threat monitoring on cloud router

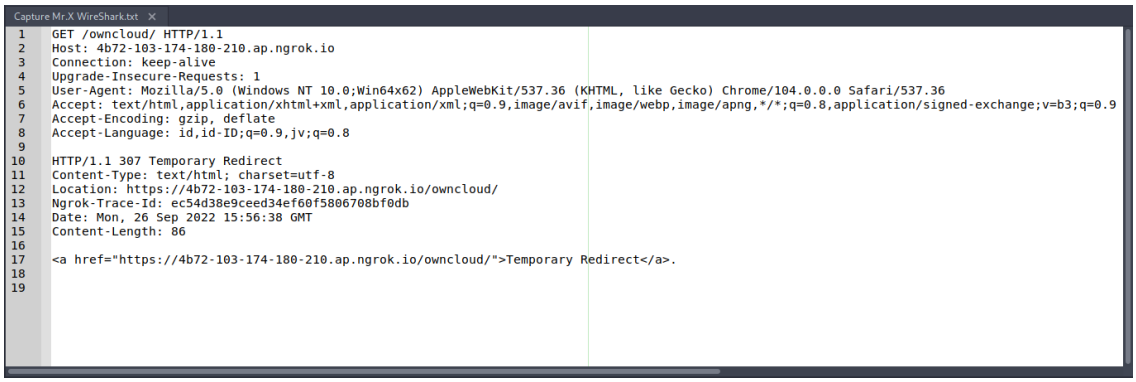

Figure 10. Log of Mr. X threat capturing on cloud router

The steps used to gather the data are shown in Figure 5, Figure 6, and Figure 7, and the results are summarized and explained in Table 5. The steps outlined in Figure 8, Figure 9, and Figure 10 were used to gather the data, which is then summarized and discussed in Table 6.

Table 5. Registered Cloud Users

Cloud Username	Device			MAC Address	Access Level
	Type	Name	Series		
Thesis DKW	Laptop	HP	Notebook 15	74:C1:7D:98:2F:4B	Admin
User 1	Smartphone	OPPO	A37f Build/LMy47V	CC:B0:DA:7A:CF:61	User
User 2	Smartphone	Samsung	SM-J730G	C0:87:EB:07:A4:53	User

Table 6. Threat Detection from Cloud Users

Cloud Username	Device			MAC Address	MAC Address and Device
	Type	Name	Series		
Thesis DKW	Laptop	HP	Notebook 15	74:C1:7D:98:2F:4B	Recognized
User 1	Smartphone	OPPO	A37f Build/LMy47V	CC:B0:DA:7A:CF:61	Recognized
User 2	Smartphone	Samsung	SM-J730G	C0:87:EB:07:A4:53	Recognized
User 1	Laptop	DESKTOP-3GBUJH1	Lenovo Ideapad G30	30:52:CB:60:02:B9	Unrecognized

DOI: https://doi.org/10.29207/resti.v6i6.4714

Based on the analysis in Table 5 and Table 6, Mr. X was detected accessing the cloud server using the identity as User 1. However, the server admin did not recognize the identity of the device used. Mr.X activities of looping file uploads 1.000.000 times is a threat because it has the potential to burden and damage the cloud server hardware components. Although theoretically carried out by individuals outside the business in order to be verified as phony insider threats, threats that employ registered user access fall under the category of insider threats. An analysis of the dangers that have materialized is done based on the findings of the case simulations, investigations, and validations that have been conducted. In order to determine how to respond to 5W+1H inquiries on threats that happened, a system security analysis was done. The examination was carried out from the viewpoint of information security, which encompasses Availability, Confidentiality, and Integrity (CIA). The NIST Cyber Security Framework's Steps and the ISO 27032 Cyber Security Guidelines were used to improve the study before a comparison was conducted. Table 7 presents and explains the analysis' findings in more detail.

Table 7. Security Analysis Of XYZ Organization Cloud System

NIST Cyber Security Framework's Steps		**ISO 27032 Cyber Security Standard Guidelines**	
• Priority Scope	√	• Cyber Security Governance	√
• Orient	-	• Risk Assesment and Threatment	-
• Create a Current Profile	√	• Information Aset Management	-
• Conduct a risk assesment	-	• Impement Secure Coding	√
• Create a Target Profile	√	• Network Monitoring Respon	-
• Determine Analyse and Priority Gaps	-	• Server Level Control	√
		• Aplication Level Control	√
		• Workstation Level Control	-
		• Cyber Insident : Information Sharing	-
		• Cyber Insident Handling	-

4. Conclusion

Threats to cloud computing platforms are common. Another extra element is necessary to verify that users that use the private cloud computing system are actual registered users. Since private cloud computing systems shouldn't be accessible to anybody outside of the firm, this is vital. Information security needs to be improved by system administrators and users alike. To maintain data integrity in the system, information security awareness is a necessity. The 2FA user-side access method can be improved in terms of security. As a result, only users who have registered with the cloud server are able to access it. The level of security awareness of cloud system accounts can be observed, and the degree of loss aversion on the part of the user can also be tested, to conduct further research.

Reference

[1] N. Widiyasono, I. Riadi, and A. Luthfi, "Investigation on the services of private cloud computing by using ADAM Method," *International Journal of Electrical and Computer Engineering*, vol. 6, no. 5, pp. 2387–2395, 2016, doi: 10.11591/ijece.v6i5.11527.

[2] N. Tissir, S. el Kafhali, and N. Aboutabit, "Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal," *Journal of Reliable Intelligent Environments*, vol. 7, no. 2. Springer Science and Business Media Deutschland GmbH, pp. 69–84, Jun. 01, 2021. doi: 10.1007/s40860-020-00115-0.

[3] P. Sharma, D. Arora, and T. Sakthivel, "Enhanced Forensic Process for Improving Mobile Cloud Traceability in Cloud-Based Mobile Applications," in *Procedia Computer Science*, 2020, vol. 167, pp. 907–917. doi: 10.1016/j.procs.2020.03.390.

[4] M. I. Tariq and V. Santarcangelo, "Analysis of ISO 27001:2013 controls effectiveneb for cloud computing," in *ICISSP 2016 - Proceedings of the 2nd International Conference on Information Systems Security and Privacy*, 2016, pp. 201–208. doi: 10.5220/0005648702010208.

[5] A. Alshammari, S. Alhaidari, A. Alharbi, and M. Zohdy, "Security Threats and Challenges in Cloud Computing," in *Proceedings - 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017 and 3rd IEEE International Conference of Scalable and Smart Cloud, SSC 2017*, Jul. 2017, pp. 46–51. doi: 10.1109/CSCloud.2017.59.

[6] A. Harilal, F. Toffalini, J. Castellanos, J. Guarnizo, I. Homoliak, and M. Ochoa, "TWOS: A dataset of malicious insider threat behavior based on a gamified competition," in *MIST 2017 - Proceedings of the 2017 International Workshop on Managing Insider Security Threats, co-located with CCS 2017*, Oct. 2017, vol. 2017-January, pp. 45–56. doi: 10.1145/3139923.3139929.

[7] D. C. Le and A. N. Zincir-Heywood, "Evaluating insider threat detection workflow using supervised and unsupervised learning," in *Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops, SPW 2018*, Aug. 2018, pp. 270–275. doi: 10.1109/SPW.2018.00043.

[8] F. Liu, X. Jiang, Y. Wen, X. Xing, D. Zhang, and D. Meng, "Log2vec: A heterogeneous graph embedding based approach for detecting cyber threats within enterprise," in *Proceedings of the ACM Conference on Computer and Communications Security*, Nov. 2019, pp. 1777–1794. doi: 10.1145/3319535.3363224.

[9] P. Moriano, J. Pendleton, S. Rich, and L. J. Camp, "Insider threat event detection in user-system interactions," in *MIST 2017 - Proceedings of the 2017 International Workshop on Managing Insider Security Threats, co-located with CCS 2017*, Oct. 2017, vol. 2017-January, pp. 1–12. doi: 10.1145/3139923.3139928.

[10] X. Liang, S. Shetty, L. Zhang, C. Kamhoua, and K. Kwiat, "Man in the Cloud (MITC) Defender: SGX-Based User Credential Protection for Synchronization Applications in Cloud Computing Platform," in *IEEE International Conference on Cloud Computing, CLOUD*, Sep. 2017, vol. 2017-June, pp. 302–309. doi: 10.1109/CLOUD.2017.46.

[11] Triawan Adi Cahyanto, M. A. Rizal, Ari Eko Wardoyo, Taufiq Timur Warisaji, and Daryanto, "Live Forensic to Identify the Digital Evidence on the Desktop-based WhatsApp," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 6, no. 2, pp. 213–219, Apr. 2022, doi: 10.29207/resti.v6i2.3849.

[12] M. Malatji, A. Marnewick, and S. von Solms, "Validation of a socio-technical management process for optimising cybersecurity practices," *Comput Secur*, vol. 95, Aug. 2020, doi: 10.1016/j.cose.2020.101846.

DOI: https://doi.org/10.29207/resti.v6i6.4714

[13]M. Malatji, S. von Solms, and A. Marnewick, "Socio-technical systems cybersecurity framework," *Information and Computer Security*, vol. 27, no. 2, pp. 233–272, May 2019, doi: 10.1108/ICS-03-2018-0031.

[14]S. Yuan and X. Wu, "Deep learning for insider threat detection: Review, challenges and opportunities," *Computers and Security*, vol. 104. Elsevier Ltd, May 01, 2021. doi: 10.1016/j.cose.2021.102221.

[15]F. Yuan, Y. Cao, Y. Shang, Y. Liu, J. Tan, and B. Fang, "Insider threat detection with deep neural network," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2018, vol. 10860 LNCS, pp. 43–54. doi: 10.1007/978-3-319-93698-7_4.

[16]S. H. Mohtasebi, A. Dehghantanha, and K. K. R. Choo, "Cloud Storage Forensics: Analysis of Data Remnants on SpiderOak, JustCloud, and pCloud," in *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*, Elsevier Inc., 2017, pp. 205–246. doi: 10.1016/B978-0-12-805303-4.00013-7.

[17]C. Y. Cheng, E. Colbert, and H. Liu, "Experimental study on the detectability of man-in-the-middle attacks for cloud applications," in *Proceedings - 2019 3rd IEEE International Conference on Cloud and Fog Computing Technologies and Applications, Cloud Summit 2019*, Aug. 2019, pp. 52–57. doi: 10.1109/CloudSummit47114.2019.00015.

[18]T. Sianturi and Kalamullah Ramli, "A Security Framework for Secure Host-to-Host Environments," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 6, no. 3, pp. 380–386, Jun. 2022, doi: 10.29207/resti.v6i3.4018.

[19]A. Ghorbel, M. Ghorbel, and M. Jmaiel, "Privacy in cloud computing environments: a survey and research challenges," *Journal of Supercomputing*, vol. 73, no. 6, pp. 2763–2800, Jun. 2017, doi: 10.1007/s11227-016-1953-y.

[20]Z. A. Al-Sharif, M. I. Al-Saleh, L. M. Alawneh, Y. I. Jararweh, and B. Gupta, "Live forensics of software attacks on cyber–physical systems," *Future Generation Computer Systems*, vol. 108, pp. 1217–1229, Jul. 2020, doi: 10.1016/j.future.2018.07.028.

[21]N. Y. Ahn and D. H. Lee, "Forensics and Anti-Forensics of a NAND Flash Memory: From a Copy-Back Program Perspective," *IEEE Access*, vol. 9. Institute of Electrical and Electronics Engineers Inc., pp. 14130–14137, 2021. doi: 10.1109/ACCESS.2021.3052353.

[22]Bita Parga Zen, Anggi Zafia, and Iwan Nofi Yono Putro, "Network Security Analysis Simulation at the GCS in the UCAV to support the Indonesian Defense Area," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 6, no. 5, pp. 824–831, Nov. 2022, doi: 10.29207/resti.v6i5.4412.

[23]R. R, I. Riadi, and Y. Prayudi, "A Maturity Level Framework for Measurement of Information Security Performance," *Int J Comput Appl*, vol. 141, no. 8, pp. 1–6, May 2016, doi: 10.5120/ijca2016907930.

[24]T. Rashid, I. Agrafiotis, and J. R. C. Nurse, "A new take on detecting insider threats: Exploring the use of Hidden Markov Models," in *MIST 2016 - Proceedings of the International Workshop on Managing Insider Security Threats, co-located with CCS 2016*, Oct. 2016, pp. 47–56. doi: 10.1145/2995959.2995964.

[25]B. Krumay, E. W. N. Bernroider, and R. Walser, "Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2018, vol. 11252 LNCS, pp. 369–384. doi: 10.1007/978-3-030-03638-6_23.

[26]S. Alneyadi, E. Sithirasenan, and V. Muthukkumarasamy, "A survey on data leakage prevention systems," *Journal of Network and Computer Applications*, vol. 62, pp. 137–152, Feb. 2016, doi: 10.1016/j.jnca.2016.01.008.

[27]R. von Solms and J. van Niekerk, "From information security to cyber security," *Comput Secur*, vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.

[28]M. Alim, I. Riadi, and Y. Prayudi, "Live Forensics Method for Analysis Denial of Service (DOS) Attack on Routerboard," *Int J Comput Appl*, vol. 180, no. 35, pp. 23–30, Apr. 2018, doi: 10.5120/ijca2018916879.

[29]H. Ernita, Y. Ruldeviyani, D. Nurul Maftuhah, and R. Mulyadi, "Strategy to Improve Employee Security Awareness at Information Technology Directorate Bank XYZ," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 6, no. 4, pp. 577–584, Aug. 2022, doi: 10.29207/resti.v6i4.4170.

[30]R. Adams, V. Hobbs, and G. Mann, "The Advanced Data Acquisition Model (Adam): A Process Model for Digital Forensic Practice," *Journal of Digital Forensics, Security and Law*, 2013, doi: 10.15394/jdfsl.2013.1154

.

DOI: https://doi.org/10.29207/resti.v6i6.4714