Investigation Of Fake Insider Threats On Private Cloud Computing Services

Dwi Kurnia Wibowo[1*], Ahmad Luthfi[2], Nur Widiyasono[3]

[1,2] Department of Informatics, Faculty of Industrial Technology, Universitas Islam Indonesia, Sleman, Yogyakarta, Indonesia.
[3] Department of Informatics, Faculty of Engineering, Universitas Siliwangi, Kota Tasikmalaya, Jawa Barat, Indonesia.
[*]Corresponding Author:
Email: ahmad.luthfi@uii.co.id

Abstract.
Cloud-based services are service system mechanisms used by companies or organizations in conducting computerized and integrated transactions in a computer network. A service system must of course be balanced with a level of security. This is used to anticipate cyber crimes that have the potential to occur. Cloud-based services themselves are usually offered by a Cloud Service Provider (CSP). CSPs are generally configured so that they are accessible on the public internet for their services. Companies that prioritize data security want a system that is safe from a series of cyber crimes. Private cloud computing scheme is a solution that can be implemented as an alternative. The problem that occurs is the possibility of MITC (Man in the Cloud) attacks that infiltrate and manipulate identities so that they are detected as fake insider threats on cloud systems. This thesis aims to carry out threat analysis with the Man in the Cloud attack technique on private cloud computing services based on a study of the ISO 27032 standard. Reports and documentation of the results of the analysis are expected to become recommendations for the cybersecurity investigation and management process related to threats to cloud services with private schemes cloud computing.

Keywords: *Threat, MITC, Cloud Forensics, Cybersecurity and ISO 27032.*

I. INTRODUCTION

Cloud-based services are service system mechanisms used by companies in conducting computerized and integrated transactions in a computer network. The origins of ideas related to Cloud Computing can be traced back to around 1950s. This generation is characterized by the mainframe Time-Sharing concept and is valid until today's industrial 4.0 era. Cloud Service Providers (CSPs) generally configure so that they can be accessed on the public internet for their services. Services offered by Cloud Service Providers platform as a service (PaaS), infrastructure as a service (IaaS) and software as a service (SaaS) [1] [2] [3] [4].There are four deployment models in cloud computing which can be summarized as: Private cloud (In-house), where the cloud infrastructure is provided for exclusive use by a single organization consisting of many consumers. Community cloud, where the cloud infrastructure is provided for exclusive use by certain consumer communities of the organizations that have collaborated. Public cloud, where the cloud infrastructure is provided for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. Hybrid cloud, where the cloud infrastructure is a composition of two or more different cloud infrastructures (private, community, public) that remain unique entities, but are bound together by standard or proprietary technologies that enable data and application portability [1], [5].Cloud Computing is the most popular internet-based computing model. The National Institute of Standards and Technology NIST defines Cloud Computing as a model that provides a centrally configurable pool of computing resources that can be released without requiring customer interaction, with minimal management and maintenance efforts. In addition, it allows convenient and on-demand network access [3].

Companies that prioritize the security side of their data want a system that is safe from a series of cyber crimes. Private cloud computing scheme is a solution that can be implemented as an alternative. The implemented private cloud is an effort to maintain information security, including company and consumer/user data. Private cloud computing scheme as an effort to anticipate various kinds of threats that may occur. Threats posed and directed against organizations are a significant problem across industry and government organizations. Threats on cloud systems are attacks that are carried out intentionally or unintentionally. Threats are broadly identified in two categories: Exider Threats, namely attacks by outsiders who have specific aims and objectives on the system. Insider threat is an attack by someone inside the

system that has a specific purpose [6]–[9].The case of the Man In The Cloud attack is interesting to discuss, where the case is a threat in the exider threat category but is assumed to be an insider threat. Identity engineering by hackers themselves to be recognized as insiders in the system is something that needs more in-depth investigation. The investigation carried out is aimed at validating that the threat of the Man In The Cloud case can be analyzed. The validation results will be useful for determining the category of threats that occur. The method used for the investigation and validation process is the ADAM (The Advance Data Acquisition Model) method. The ADAM method was chosen because it is a method developed from several previous methods based on previous studies. The ADAM method is recommended to be used in carrying out a series of investigative processes against digital evidence to the reporting stage of the results of the investigation because the stages are more detailed than other methods [1], [10].Ignorance of the threat of cyber crime is a problem that often occurs.

This is motivated by ignorance of cybersecurity mechanisms. The development of socio-technical management processes to optimize technical and non-technical security measures aimed at providing optimal enterprise security protection has not yet been achieved. The reason is that over the past decade, extensive research has shown that humans remain the weakest factor in enterprise security. As a result, most cyberattacks are the result of human behavior or error [11] [12].An insider threat is a malicious threat from people within an organization that typically involves intentional fraud, theft of confidential or commercially valuable information, or the sabotage of computer systems. While the exider threat is the same action but carried out by people from outside the organization. Technical threats in the form of attacks that occur on cloud services are very diverse with various attack methods. One method of attack is Man In The Cloud. In 2015, a new attack method emerged in cloud services, namely Man in the Cloud. (MITC). This MITC attack is different from the Man in the Browser (MITB) and Man in the Midlle (MITM) attacks that have happened a lot [10], [13]–[16].Digital Forensics can be defined as a discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications and storage devices in a manner that is admissible as evidence in court [17]. The digital forensics process can be divided into four distinct phases: Collection of artifacts (both digital evidence and supporting materials) that are considered to have potential value to be collected. Preservation of original artifacts in a reliable, complete, accurate and verifiable manner. Artifact screening analysis to remove or enter items that are considered valuable. A presentation in which evidence is presented to support the investigation.

Traditionally, two categories of digital forensics exist namely, static digital / "write block" and "live forensics", there are two categories as a result of the evolution of forensics to create and document sophisticated incidents. Static forensics involves the analysis of static data such as hard drives obtained using traditional formal acquisition procedures.Live Forensics involves analyzing system memory and other relevant data while the analyzed system remains running [10], [17]–[19].Cybersecurity framework berisi tahapan kontrol teknis yang didefinisikan dalam standar yang sudah ditetapkan pada skala internasional. Ada beberapa organisasi yang memiliki praktik cybersecurity yang baik dan memanfaatkan kontrol keamanan informasi ISO/IEC 27001 pada sistemnya. Proses penerapan kontrol teknis keamanan siber menjadi lebih mudah jika organisasi mematuhi standar ISO27001. The ISO 27032 standard presents cyber security technical controls to protect against: Social engineering attacks, Hacking, Malicious, software (malware) [2], [5]–[7], [20], [21].

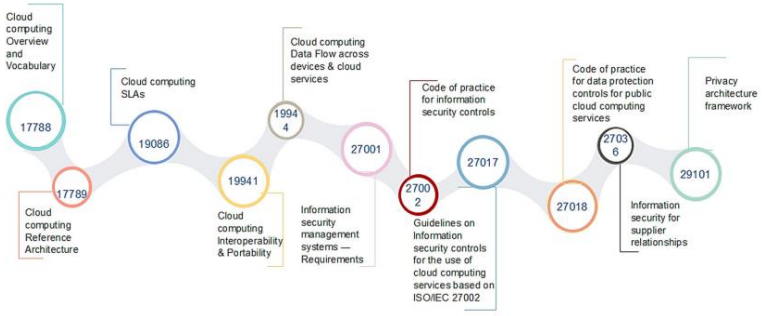

Fig 1. ISO Cloud Computing Standards

Technical controls include secure coding: Secure coding controls must be in place to secure information collected by products in cyberspace. Network monitoring and response: Controls must be in place to ensure network services remain reliable, secure and available. Cyberspace should not compromise the quality of network service. Server-level controls: Controls must be in place to ensure servers are securely accessible from cyberspace and protected from unauthorized access and malicious content. Application-level controls: Implement controls to protect against unauthorized editing of data; recording transactions and handling errors. End-user workstation controls: Controls must be in place to protect end-user infrastructure across the organization against known exploits and attacks [22], [23].Based on the general problems described and studies from similar research as well as theories from previous research, it is interesting to conduct an in-depth study of cloud services related to threats that occur with MITC attack techniques. Explaining MITC regarding whether its handling is the same as other attack techniques. Provide an explanation regarding the types of MITC attacks based on actors from outside parties who fabricate identities if the cloud service is private [5], [10], [16], [24], [25].

II. METHODS

Fig 2. Research Process Flow

There are several research variables used in determining the focus of the research to be carried out. The research variables used include :

1. The dependent variable (dependent variable) is a variable that depends on other variables.
2. The independent variable (independent variable) is a variable that does not depend on other variables.

Table 1. Research Variable Indikator

No.	Independent Variable Indicator	Dependent Variable Indicator
1	Cloud Computing	Private Cloud Computing Scheme
2	Threat	Man in the Cloud attack technique
3	Investigation	Acquisition with ADAM Method
4	Security	Standard Cyber Security Analysis Cyber Security Framework analysis

1. Dependent Variable

a) Cloud Computing

Justification : This variable was determined because it became the focus of the research scope as seen from the research results in terms of identifying threats based on existing attack techniques on a cloud service.

b) Threat

Justification : This variable was set because it is a sign of the success of this research by determining the type of threat based on the type of attack carried out.

c) Investigation

Justification : This variable was set because it is a sign of the success of this research by acquiring digital evidence.

d) Security

Justification : This variable was determined because it is a sign of the success of this research by conducting a threat analysis based on attack techniques carried out from a cybersecurity point of view.

2. Independent Variable

a) Private Cloud Computing Scheme

Justification : This research variable is used to determine the cloud service scheme as the focus of the research to be carried out.

b) Man in the Cloud attack technique
Justification : The variables used to determine the attack technique that is the focus of the threat category analysis.

c) Acquisition with ADAM Method
Justification : The variables used to determine the method of digital evidence acquisition in the investigative process.

d) Standard Cyber Security Analysis
Justification : Analysis based on ISO 27032 cybersecurity guidelines is used as an evaluation of threats based on Man in the Cloud attack technique.

e) Cyber Security Framework Analysis
Justification : Analysis based on the NIST cybersecurity framework's step is used as an evaluation of threats based on the Man in the Cloud attack technique.

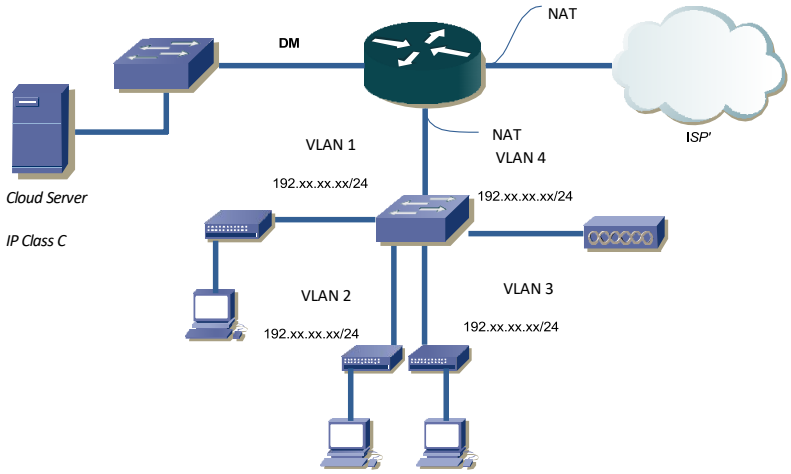

Fig 3. Private Cloud Service Network Topology

After compiling a mind map and explaining the correlation of forensics and security disciplines on cloud services, the next step is to determine the procedure scheme for conducting research. This procedure is a series of steps that will be carried out and becomes a research framework in the form of a proposed methodology. The proposed methodology is one of the contributions in this research.The case scenarios and simulations in this study were adapted to private cloud computing services that were adopted from cases that occurred in the Tasikmalaya City Discominfo environment, to maintain confidentiality, the names and places were disguised as "XYZ Organization". The names and services of the private cloud service infrastructure system built in the lab are adapted to the conditions in the field. Acquisition using the ADAM method and evaluation with analysis based on the cybersecurity framework. The results of the two processes will then be analyzed and validated for the type of threat in the stages of the cybersecurity investigation and analysis process.In this case scenario, the "XYZ Organization" service has private cloud computing services for its business needs, then one of the members with the initials "p" accesses the organization's cloud services from outside the "xyz organizatiol" network. Unaware of the access that was made from the cafe via the public ip hotspot, there was a hacker who was carrying out a MITM attack. All hotspot clients in the cafe are trapped in sniffing & spoofing. Sure enough, after "P" left the cafe, the hacker with the initials "Mr.X" took advantage of the previously obtained data to access private cloud computing services at the "xyz organization".This “Mr.X” accesses the private cloud service with the permissions as “P”. That's because private cloud services in the "XYZ Organization" are very easy to manipulate for permissions. Permission on the network is done only with MAC Address detection, authentication is used only username and password without encryption. It is very easy to do piracy or MITC. After successfully accessing the private cloud service server then "Mr.X" performs DDoS. The server admin thought that "p" was the one who carried out the DDoS attack, but in reality it was not. This threat looks like an insider threat but in context it is clear it is not an insider or a fake insider.

The investigation stage using the ADAM method is carried out an investigation process on case simulations using private cloud computing services. The investigation was carried out starting with the private cloud computing service or from the server side, then from the network side, namely monitoring the data traffic going out/into the private cloud computing service server and getting digital evidence at the sessions layer (layer 5 on 7 OSI layers) by using the Wireshark tool, then investigating the desktop or laptop and smartphones connected to the service.The success in conducting an investigation is knowing the location or position of digital evidence, whether on the private cloud server, desktop PC, laptop or smartphone. In addition, other parameters are ip source, mac-address, username and password, system log data, can open encryption files, other resources that can be used as additional digital evidence, then the digital evidence can be verified and matched between the digital evidence contained in the document. side of private cloud servers, desktop PCs, laptops and smartphones.After conducting an investigation with the acquisition of digital evidence using the ADAM method, the next step is to conduct an analysis based on several cybersecurity frameworks. The purpose of conducting an analysis with several cybersecurity frameworks is to find out the difference in point of view of cases that occur based on the cybersecurity framework. Threats that occur will also be studied from the point of view of the CIA concept. The results of the analysis will later be used as reference material for evaluating threats with MITC attack techniques on private cloud computing services.Based on the introduction, literature review and proposed research methodology that has been described, the author intends to conduct investigations and analysis as research contributions that aim to detect and validate threat categories with Man in the Cloud attack techniques on private cloud computing services. The investigation process aims to detect the status of the actor (actor) based on digital traces that have been successfully acquired using the ADAM Method. The evaluation is based on a study of the cybersecurity standard and cybersecurity framework (ISO 27032, NIST CSF) regarding threats based on actors using Man in the Cloud attack techniques on private cloud computing services.

III. RESULT AND ANALYSIS

The investigation process to the cyber security analysis stage is carried out by referring to the simulation and case scenario of MITC. The investigation process is carried out to obtain digital evidence. Investigation using ADAM (Initial Planning, On-site Planning, Digital Data Acquisition). Acquisition Digital Data : The stages achieved for the investigation and the results obtained are described in Table 2. The results of the investigation of the MITC attack scenarios and simulations as a threat to cloud systems on "XYZ Organization" were then analyzed based on the NIST Cybersecurity Framework's steps and ISO 27032 Cybersecurity Guidelines. Thus it can be known where the error that poses the potential threat that occurs.

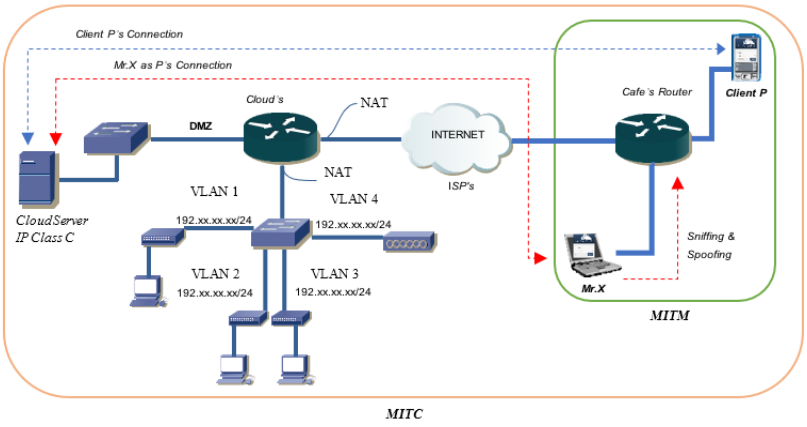

Fig 4. MITC Case Scenarios and Simulations

Table 2. Stages and Results

Stages	Result
Footprintting	IP, MAC Address, OS, Device Name, Location
Tracking	Collected Attacker Identity
Validating	Generate Report from Collected Data Aqcuisition

Table 3. XYZ Organization's Cloud Security Analysis

NIST Cybersecurity Framework's		ISO 27032 Cybersecurity Guidelines	
Priority Scope	Yes	Cyber Security Governance	Yes
Orient	Yes	Risk Assesment and Threatment	No
Create a Current Profile	No	Informatin Asset Management	No
Conduct a risk assesment	No	Implement secure coding	Yes
Create a target profile	No	Network Monitoring Respon	No
Determine, Analyse and priority gaps	No	Server Level Control	No
		Application Level Control	No
		Workstation Level Control	No
		Cyber Insident : Information Sharing	No
		Cyber Insident Handling	No

Based on the results of the investigation, it was found that Mr. X as the perpetrator of MITC had manipulated his identity. The identity "P" is used to log into the private cloud computing system "xyz organization". The private cloud computing system belonging to "XYZ Organization" only uses username and password for login authentication. Mr. X fabricated his identity and changed his laptop's MAC address to the MAC address of "P's" smartphone. Based on the CIA concept, of course, the MAC addresses that are allowed to enter for cloud system access must be limited, but it doesn't just end there. Another additional factor is needed to validate that those who access the private cloud computing system are really registered users. MITC cases that were successfully simulated and investigated were threats from outsiders who were detected as insider threats.

IV. CONCLUSION

Threats to cloud systems are very common. Another additional factor is needed to validate that those who access the private cloud computing system are really registered users. This is important because private cloud computing schemes should only be accessible to people within the organization. Information security, both by system administrators and users, needs to be improved. Awareness of information security is an absolute must to maintain data integrity in the system. Further research can be done by observing the level of account awareness of the cloud system and also testing the level of loss aversion from the user's side.

V. ACKNOWLEDGMENTS

The author expresses his gratitude and highest appreciation to those who have helped in this research.

REFERENCES

[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] 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.

[3] 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.

[4] 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.

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

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] R. R, I. Riadi, and Y. Prayudi, "A Maturity Level Framework for Measurement of Information Security Performance," ***International Journal of Computer Applications***, vol. 141, no. 8, pp. 1–6, May 2016, doi: 10.5120/ijca2016907930.

[21] 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.

[22] 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.

[23] 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.

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

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