Implementation of A Cyberpanel-Based Partial Cloud Server As A Prevention Of Security Information Management System (SIMS) Encryption

Cholid Mawardi[1], Deni Kuswoyo[2], Naufal Falah[3]

{cholid@polimedia.ac.id[1], deni.kuswoyo@polimedia.ac.id[2], panggilajanopal2@gmail.com[3]}
Politenik Negeri Media Kreatif, Indonesia[123]

Abstract. The encryption process in each information system security element is very important, some activities that connect an information system must have a good level of encryption to prevent a system from being hacked. The side of the system that uses a server must also have a good level of security, both in terms of the level of ability to ward off certain malware or phishing in the encryption system. The Security Information Management System (SIMS) secures several data security settings, including in a server. It is hoped that this research can have one main objective, which is an alternative method of dividing server conditions into multiple server accounts that makes data security conditions more secure. The partial cloud server method can also balance the server system overload conditions to be easy to control. Several separately created IP (Internet Protocol) addresses cause the hacker test group to switch to the IP address

Keywords: *encryption, server, proxy, partial, cloud.*

1 INTRODUCTION

The development of information and communication technology is experiencing developments which is quite rapid [1]. The security system of an information system and website is the main gateway in terms of information services. An inevitability when a system becomes operational in an institution. The security system must also be in line with operational implementation. Understanding the importance of an information system security, judging from the aspect of the event parameters that are often seen when a lot of hackers manage to take over the account of a system in a very short time. Like the incident below that happened to the Creative Media State Polytechnic by controlling one block server and only having a sub domain under the main website, hackers were able to control several accounts and then change the index file in just a matter of seconds. This is where the importance of the system data security structure, if it only relies on the block side of one server, then hackers will be able to master several other system accounts with the same server block [1].

Encryption of data security in an information system can already be illustrated by changing the main keyword into a different language structure with customized recipient code. For example, when the word we create in encryption, it will turn the process into a certain code that is very difficult for hackers to master. In grouping server IPs, several security has been observed to ward off some possible malware or hackers directly. However, by placing a system in 1 server block, it is very vulnerable to hacking. Therefore, researchers have a main plan to divide several systems into several server blocks or better known as partial cloud servers [2].

JICOMS 2022, November 16, Jakarta, Indonesia

DOI 10.4108/eai.16-11-2022.2326064

A cloud server is a shared, centralized server resource that multiple users can access on demand and that is located on a network, typically the Internet. Processing power, storage, and applications are all things that cloud servers can do just like regular physical servers. A cloud computing environment allows for the placement of cloud servers virtually anywhere in the world to deliver services remotely. Traditional dedicated server hardware, in contrast, is often placed locally for the sole purpose of one company. The information system requires' prima donna is currently cloud servers.

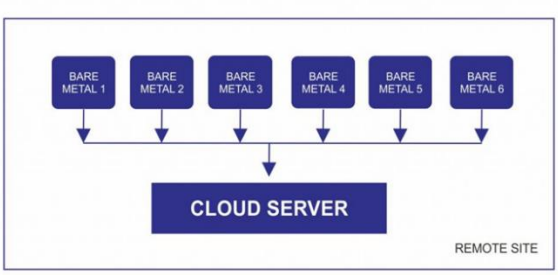

Fig 1. Cloud Server Architecture

Cloud servers are possible through virtualization. Management software called a hypervisor is installed on a physical server to connect and virtualize it: extract their combined resources and group them together to create a virtual server. These virtual resources can then be automated and provisioned in the cloud for shared use within a single organization or across multiple organize.

The cloud is the top layer of a typical fog computing environment. This tier consists of a centralized data center with capacity to store all data from fog nodes/servers. It usually has the capacity to store large amounts of data. It will cause huge network congestion, and the quality of service delay will also increase [2]. Cloud computing, through the proposed model, has the potential to bring many benefits to the general public, especially businesses and small businesses, but also in general use.[3]

1 Method

When data is outsourced to the cloud, its security is compromised. Encryption is an effective technique for protecting data security. [4] In this research method, it is divided into 2 flowcharts to support efforts to prevent system hacking with the partial cloud server method, namely:

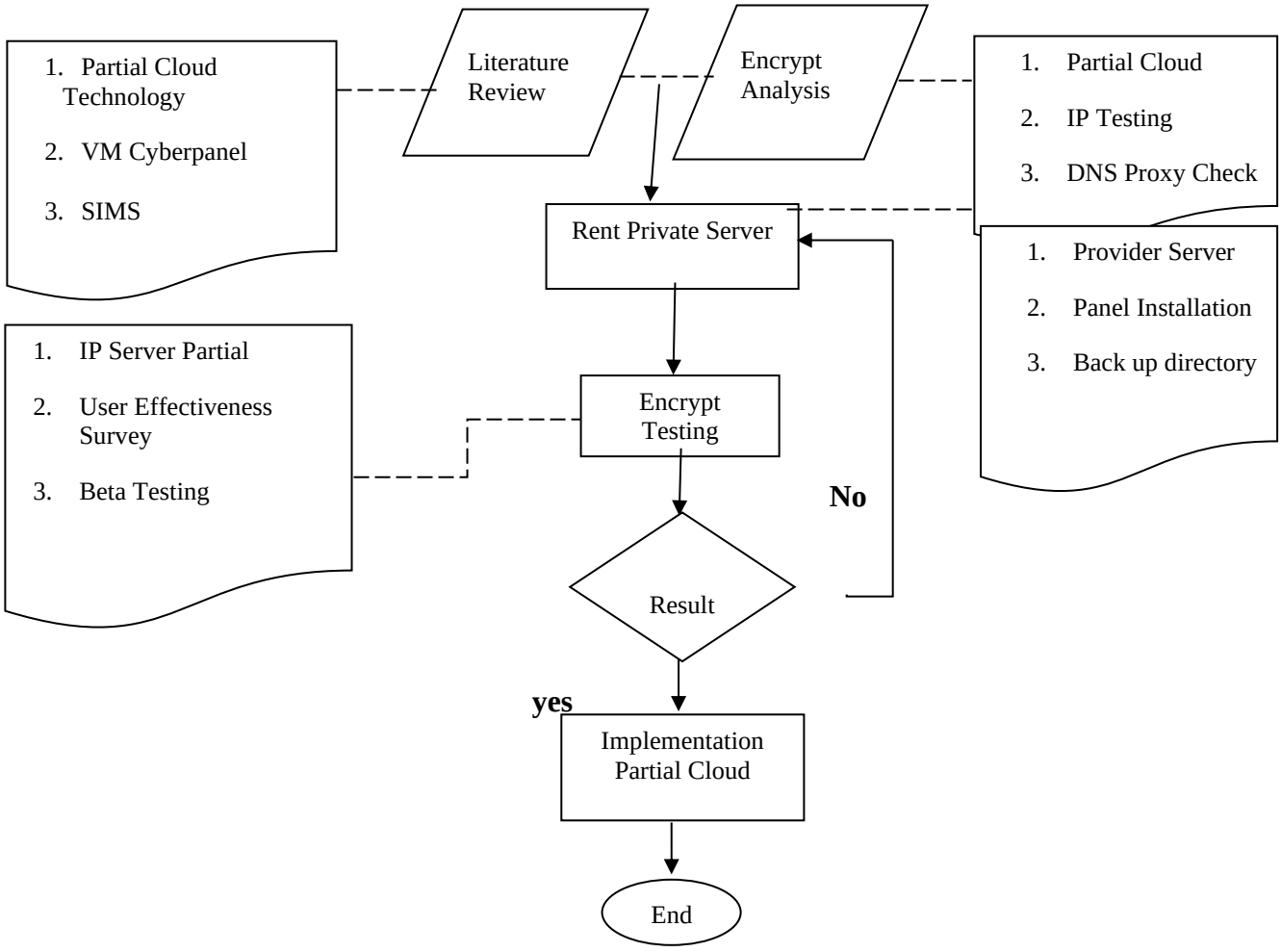

Fig 2. Research Method

1. The Research Team will carry out several stages including conducting analysis, literature studies of several possible case examples that have occurred against cyber security attacks.

2. To solve the problem, various methods are needed. The Research Team used the partial cloud method to break down several server blocks into many parts.

3. Perform encryption testing of the new server IP. Here the research team conducted 4 Public IP tests. 36.91.xx.234 onwards.

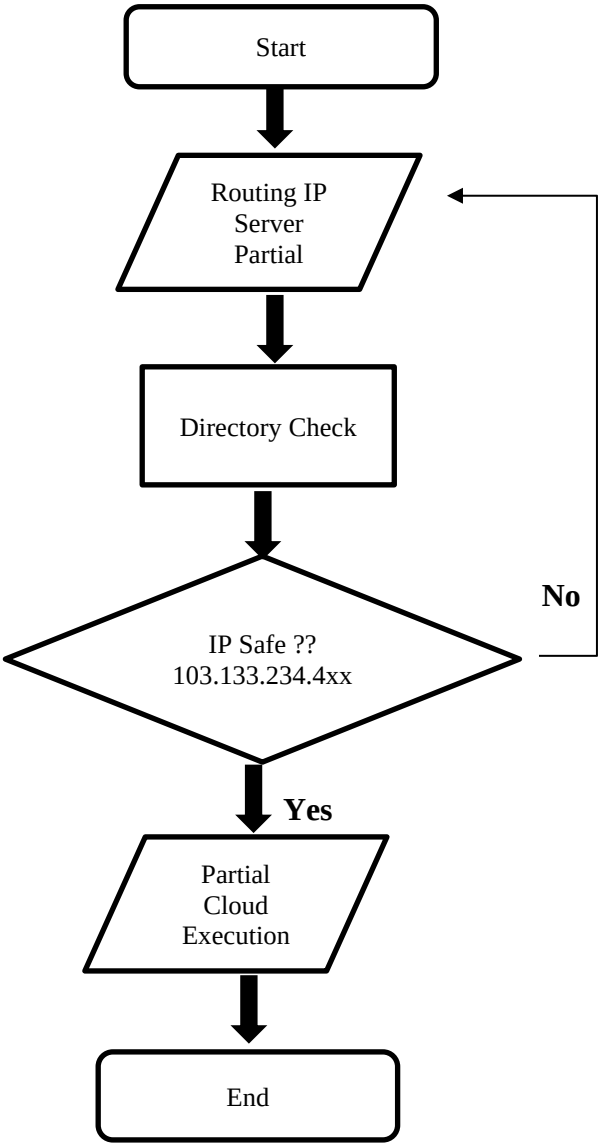

Fig 3. Research Method

In this part of the Flowchart Partial Cloud Server IP Testing, the method carried out is to create as many IPs based on needs and use each cyberpanel panel. The process of routing an IP when it has entered the cyberpanel, is to divide the system directory and test whether the IP is safe? Or it has been contaminated with malware, if there is 1 IP that has been contaminated then

immediately backup the directory data and immediately import the backup data and select the ip that has been created before.

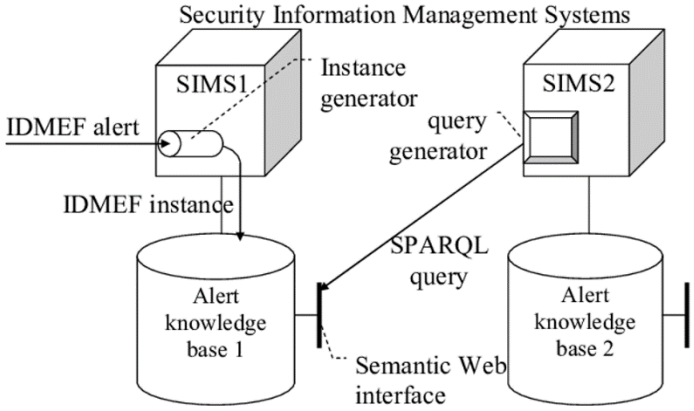

Fig 4. Semantic collaborative SIMS architecture

The armature we propose to partake information among SIMS is grounded on semantic web technologies, as shown in Fig. 1. This figure represents two SIMS but it can be generalized to several of them. Each SIMS will contain an alert knowledge base that contains cases of the IDMEF ontology, described in coming section. Each knowledge base can be queried by other SIMS using a semantic web interface that accepts queries about the ontology.

Additionally, SPARQL provides a way to express queries across multiple distributed data sources through SPARQL query federation [5]. A number of possible queries are generated, ranked, and then presented to the user. These queries are presented using natural language sentences. [6] Some security work has considered applying Semantic Web technologies to malware, spam, or intrusion detection, but few have addressed computationally intensive problems such as fraud detection, for example. Even fewer have been dealt with. An overview of semantic web technologies. [7] Cloud Service users can see the fees charged by their service provider in connection with the services they consume, focusing on metering issues or order confirmations. It describes different types of security attacks and proposes solutions for each type of attack. [8] may be useful for operators wanting to evaluate performance and calculate energy consumption of server clusters [9].

2 Result and Discussion

Results show that Snort and Alert notifications work well and efficiently on security servers and can be processed quickly [10]. desired quality of service[11]. We propose an approach that guides the designer to maximize the benefits of adding "patchability" to the various IPs in the system given the resource overhead[12]. The results obtained in solving server blocks with Partial Cloud using the SIMS (Security Information Management System) Method. When compared to previous studies where only a very few implemented the SIMS scheme, the expected results in this paper can reach the level of network and server security in our institution.

Table 1. Blocks IP with CBPanel

No.	CBPanel	IP Blocks	Assets
1	CBPanel 1	103.176.78.xx	OJS
2	CBPanel 2	103.181.143.xxx	Registration
3	CBPanel 3	103.226.138.xx	Small Web
4	CBPanel 4	103.226.139.xx	Small Web 2

After partial clouding of several servers, the main result is cpu capacity which only has a density of 1.42%

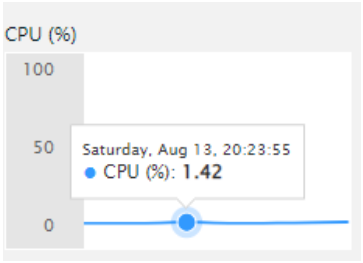

Fig 5. CPU Capacity Usage

Partial Cloud managed to reduce memory capacity up to 3672.78 MB, this result can be ascertained that the use of Partial Cloud Cyberpanel proved to be successful when compared to using 1 server block.

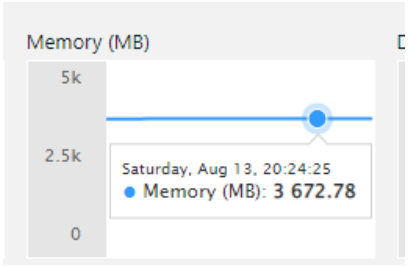

Fig 6. Memory Capacity Usage

3 Conclusion

This research also has a good impact on institutions, especially polymedia, after the cybercrime attack a few months ago, we strongly recommend managing with the partial cloud server method. In addition to being safer if it is divided into several server IP blocks, it is also very helpful when we are going to take backup data. Coupled with the SIMS method, semantic web also helps in the method when we split multiple servers in a partial cloud. With a fairly expensive price because of renting to a vendor, but it doesn't matter if the security of company data can be maintained properly.

5 Acknowledgements

This work was fully supported by The Center of Research and Community Service of Politeknik Negeri Media Kreatif (P3M Polimedia)

References

[1] Mawardi, C. (2017). *Analisa Regulasi Network Sharing Berbasis Multi Operator Core Network (MOCN)* (Doctoral dissertation, Universitas Mercu Buana).

[2] Kunal, S., Saha, A., & Amin, R, An overview of cloud-fog computing: Architectures, applications with security challenges. *Security and Privacy*, vol 2, no. 4 , e72, (2019).

[3] Stergiou, C., Psannis, K. E., Gupta, B. B., & Ishibashi, Y, Security, privacy & efficiency of sustainable cloud computing for big data & IoT. *Sustainable Computing: Informatics and Systems*, vol. 19, pp 174-184, (2018).

[4] Yang, P., Xiong, N., & Ren, J. Data security and privacy protection for cloud storage: A survey. *IEEE Access*, *8*, 131723-131740. (2020)

[5] Kurniawan, K., Ekelhart, A., Kiesling, E., Winkler, D., Quirchmayr, G., & Tjoa, A. M. VloGraph: A Virtual Knowledge Graph Framework for Distributed Security Log Analysis. *Machine Learning and Knowledge Extraction*, vol. 4, no 2, (2022)

[6] Pradel, C., Haemmerlé, O., & Hernandez, N. A semantic web interface using patterns: the SWIP system. In *Graph Structures for Knowledge Representation and Reasoning* (pp. 172-187). Springer, Berlin, Heidelberg (2012).

[7] Kirrane, S., Villata, S., & d'Aquin, M. (2018). Privacy, security and policies: A review of problems and solutions with semantic web technologies. *Semantic Web*, *9*(2), 153-161.

[8] Singh, A., & Chatterjee, K. Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications, vol. 79,* pp. 88-115. (2017).

[9] Binh, L. V. T. Some practical aspects in modeling server clusters with blocks of reserve servers. *Journal of Science and Technology on Information and Communications*, vol. *1, no.* 1-2, pp 65-73. (2018).

[10] Helmiawan, M. A., Julian, E., Cahyan, Y., & Saeppani, A. Experimental Evaluation of Security Monitoring and Notification on Network Intrusion Detection System for Server Security. In *2021 9th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-6). (2021, September). IEEE.

[11] Stallings, W. RSVP: Building Blocks of the Next-Generation Internet. *Local Area Network Handbook*, 269. (2020).

[12] Liu, W. K., Tan, B., Fung, J. M., Karri, R., & Chakrabarty, K. Hardware-Supported Patching of Security Bugs in Hardware IP Blocks. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*. DOI: 10.1109/TCAD.2022.3168513