Journal of Electrical Engineering and Computer (JEECOM)
Vol. 7, No. 1 (2025), DOI: 10.33650/jeecom.v4i2
p-ISSN: 2715-0410; e-ISSN: 2715-6427

Cloud Server Security System Design on Linux Almalinux 8.6 Operating System Based on WHM with DNS Management Using Cloudflare IP Masking

Muhamad Reza Chaedar Fatach[1], Alva Hendi Muhammad[2], Dhani Ariatmanto[3]
[1,2,3] Universitas Amikom Yogyakarta, Yogyakarta, Indonesia

Article Info

Article history:

Received February 9, 2025
Revised February 11, 2025
Accepted April 10, 2025

Keywords:

Security System
Cloud Server
Design
DNS Management
Cloudflare IP Masking

ABSTRACT

Information threats and security are very likely to occur due to the lack of concern for the security of a system, especially in the hardware infrastructure of computer networks, which is still very lacking. Universitas Muhammadiyah Bangka Belitung currently still uses the Linux Centos Operating System with DNS Management for the security system. so there is still some data that is not optimal for its security system, such as student data, lecturers, employees and important data such as online files. This study aims to design a Cloud Server Security System on the Linux Almalinux 8.6 Operating System Based on WHM with DNS Management Using IP Masking Cloudflare. The type of research used is qualitative research, where researchers collect primary and secondary data. With this design, it is produced that security in the Cloud Server increases. Before using IP Masking Cloudflare, server performance was low, with Low Data Access and Management, Low Scalability, Low Access Security, and Low System Integration, but after using IP Masking Cloudflare Server Performance, Data Access and Management, Scalability, Access Security, and System Integration increased. This is because, in server performance, there is already a cache configuration on the server using a configuration based on the cloud server, Access and Data Management already use or have managed access rights properly, such as improvements to directory access rights on the server, Scalability is quite easy and efficient as seen from the configuration between hardware and software used to run well, Access Security already uses https and already uses Cloudflare and firewall to secure data in the cloud server directory so that it is easy to add other configurations and IP can be manipulated, and System Integration already uses https and already uses a firewall that is quite high in security for system integration in it.

Corresponding Author:
Muhammad Reza Chaedar Fatach,
Universitas Amikom Yogyakarta, Jl. Ring Road Utara, Ngringin, Condongcatur, Kabupaten Sleman, Daerah Istimewa Yogyakarta 55281, Indonesia
Email: muhamad.reza.cf@students.amikom.ac.id

1. INTRODUCTION

The development of information technology in Indonesia is currently growing rapidly, especially in network technology. The development of network technology is currently moving towards Cloud Computing. Cloud computing is a modern computing technology that began to develop in 2005 using computer network services or internet networks. Cloud computing has grown rapidly and dramatically throughout the world. The number of devices connected to the cloud is estimated to range from 23 to 25 billion between 2025 and 2030, while the number of IoT devices is projected to reach 40 billion IoT devices by 2030 (Jhon & Fraser, 2024). Cloud Computing is the provision of computing services, including servers, storage, databases, networks, software, analytics, and others via the internet (Cloud) (Jhon & Fraser, 2024). The existence of cloud computing

presents cloud servers, where cloud servers are virtualization technology with the concept of dividing single hardware into several virtual resources.

The use of information technology such as network technology is a must, especially in educational institutions, especially universities because it is very much needed in the field of academic administration services in universities. In implementing policies to strengthen governance, accountability, and the public image of higher education institutions, the implementation of information systems in higher education management services is very necessary. However, currently many universities have not fully migrated to cloud servers. One of the factors is that hardware is still not available due to the relatively expensive cost and the need for a related server migration process from dedicated to virtual which of course will interfere with the resulting performance. However, there are vulnerabilities in the data directory and database security system in the cloud server. Vulnerabilities in the data directory and database security system can be brute force, dface, malware. One of the causes of threats to information and data security is that data can already be accessed online because the data is stored in Cloud Computing. Along with the rapid development of data storage technology, Cloud Computing is one of several data storage network technologies that are currently developing rapidly so that data stored in cloud computing is important and confidential data that not everyone can access (Dwi & Ujianto, 2020). Therefore, information and data security in cloud systems is very important and an asset that must be maintained.

Universitas Muhammadiyah Bangka Belitung is one of the higher education institutions that uses information technology in running the learning process and institutional management. However, in the process of utilizing information technology, during use and implementation in the field, various threats can occur. One of the possible threats is information security. Threats in information security are any events that can cause damage to the system and cause loss of confidentiality, availability, or integrity by modifying important information or deleting files (Matondanga, Isnainiyah, & Muliawati, 2018). This is very likely to occur due to the lack of concern for the security of a system, especially in the computer network hardware infrastructure which is still very lacking. Currently still using the Linux Centos Operating System with DNS Management for the security system. System security is important for maintaining data and information on the server. The reality in the field, there are still some data that are not optimal for their security systems such as student data, lecturers, employees and important data such as online files that have not been encrypted and there is still data that can be accessed by many people or the public without permission from the related role, namely the admin user in a system, still not optimal for the settings in the cloud computing such as settings in setting DNS to the directory in the cloud server. This is important to limit because not everyone can open it, therefore, from the description above, the researcher will create a security system for the data on the cloud server of the Muhammadiyah University of Bangka Belitung which uses an IP Masking-Based Proxy Server. A proxy server is used because with a proxy server the company management will be able to limit internet bandwidth usage, regulate internet usage and reduce attacks by viruses, worms, spyware and DDOS (Distributed Denial of Service) (Rachman & Aminullah, 2013; Aryachandra, et al, 2024).

To overcome this, there are various ways that can be done, one of which is by adding an IP mask. This is done so that the system is even better in terms of security where the previous public IP is visible to the public and adding an IP mask will change the public IP to be invisible to the public and the measuring tool that will be used is ping testing via a terminal using the Mac OS Operating System. Using an IP Mask on the security system can provide a fast and elegant solution to the problem of providing unlimited networks for mobile hosts (Perkins & Bhagwat, 1994; Liu & Albitz, 2006). While Coudflard to achieve partial Cloudflare proxy bypass (De Souza Oliveira, et al, 2022) and Cloudflare hosting for access speed are successful ((Jayanti, Umar, and Riadi, 2020). IP Masking Cloudflare can 1) hide the original server IP where Cloudflare acts as an intermediary (reverse proxy) between visitors and the original server, All incoming traffic will pass through Cloudflare, so the original server IP is not visible to the public, and protect against direct attacks on the server IP, such as DDoS or security exploits; 2) avoid IP blocking by third parties where if a service or firewall blocks the original server IP, using Cloudflare IP can avoid the blocking and Cloudflare IP is more difficult to block because it is used by many other sites; 3) overcome access problems when HTTPS Redirect where if there is a plugin or extension conflict when forcing an HTTPS redirect, Cloudflare can handle the redirect with the Page Rules rule or the "Always Use HTTPS" setting and reduce the potential for conflicts originating from plugins or web servers that incorrectly set the redirect; and 4) ensure security and performance where Cloudflare offers features such as firewalls, rate limiting, and caching to reduce server load and with caching enabled, requests to the original server are reduced, reducing the risk of downtime due to traffic spikes. Therefore, it is important to design a Cloud Server Security System on the Linux Almalinux 8.6 Operating System Based on WHM with DNS Management Using Cloudflare IP Masking.

2. METHOD (10 PT)

1) Types, Nature and Research Approaches

A) Types of research

The type of research used in this study is qualitative research where researchers can identify subjects, study appropriate situations and environments.

B) Nature of Research

The nature of this research is descriptive, namely describing the phenomenon of the Cloud Server data security system at the Muhammadiyah University of Bangka Belitung on the Linux Almalinux 8.6 Operating System Based on WHM with DNS Management Using Cloudflare IP Masking.

C) Research Approach

This research approach is a qualitative approach where researchers collect data by being directly involved in research activities and data collection. The purpose of qualitative research is to describe the conditions in the natural environment in detail and in depth and to understand the actual conditions according to the conditions in the field.

2) Method of collecting data

In general, the data collection carried out in this study is as follows:

A) Data Types

The types of data used in this study are as follows:

Primary Data

This data was obtained directly. In this case, primary data was obtained through direct consultation with system development at Muhammadiyah University of Bangka Belitung.

Secondary Data

This data is obtained from the results of observations and data collection related to the research. Cloud Server data security system on the Linux Almalinux 8.6 Operating System Based on WHM with DNS Management Using IP Masking Cloudflare from several sources such as articles, journals, books, and other data sources.

B) Data Collection Sources

The data collection sources in this study come from several methods, namely:

Observation

In this observation method, direct observation was carried out on the network development system at Muhammadiyah University of Bangka Belitung which is tasked with managing and storing system data at the institution.

Interview

Conduct direct meetings with information sources by asking questions about the data security system process.

Literature Study

Literature study in general is a way to solve problems by tracing previous sources related to research. Sources can be obtained through literature studies in the form of books, articles, and writings that are directly or indirectly related to "Cloud Server Security System Design on Linux Almalinux 8.6 Operating System Based on WHM with DNS Management Using IP Masking Cloudflare".

3) Data Analysis Methods

A) Data Analysis Methods Using Traffic Patterns

The data analysis method in this study uses traffic patterns. Traffic patterns are Traffic pattern analysis helps understand the general behavior of users and applications. This involves looking at daily, weekly, or monthly traffic trends, as well as identifying spikes or sudden changes that could indicate unusual activity, then determining the success of the configuration by looking at incoming traffic from existing data. The data comes from traffic logs on the cloud server, then the data is processed using software from cloudflare, namely firewall proxy.

B) Testing method Using PING

Packet Internet Gopher or abbreviated as PING is a command to check server and client responses in an internet network. The term ping refers to the basic function of this software, which is to send a simple request to a specific IP address or host name and then receive a reply.

4) Research Flow

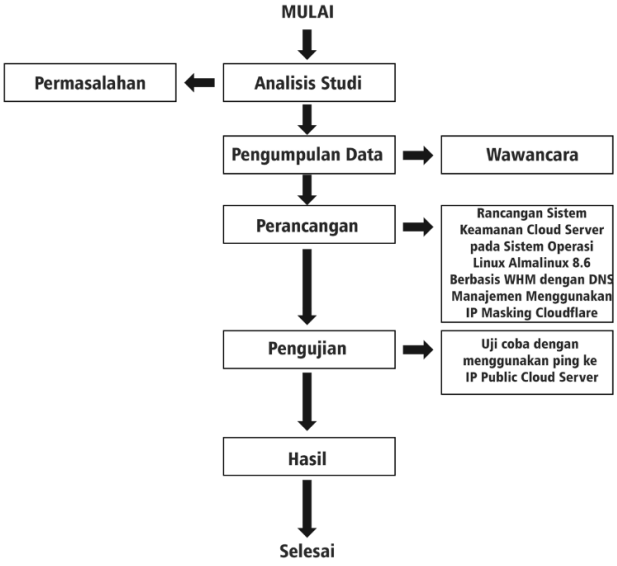

Figure 1. Research Flow

Information :

A) Study Analysis
The study analysis referred to here is formulating existing problems in the field as material to be studied by researchers.

B) Data collection
Researchers will collect data for research through interviews with authorities in the field.

C) Design
Researchers will design a security system according to user needs to solve existing problems.

D) Testing
After completing the design, the researcher will conduct a trial of the security system that has been designed in the field by PING testing using a terminal to the Public Cloud Server IP and see whether the results are appropriate or not.

E) Results
The research results will be used as a reference for future further research.

3. RESULTS AND DISCUSSION

This research focuses on designing a Cloud Server Security System on the Linux Almalinux Operating System with DNS Management Using a Proxy Server Based on IP Masking Cloudflare using the Traffic Patterns and Packet Internet Gopher (PING) methods.

3.1. Dedicated Server Before Design

Researchers analyzed the dedicated server before designing as shown in Figure 2.

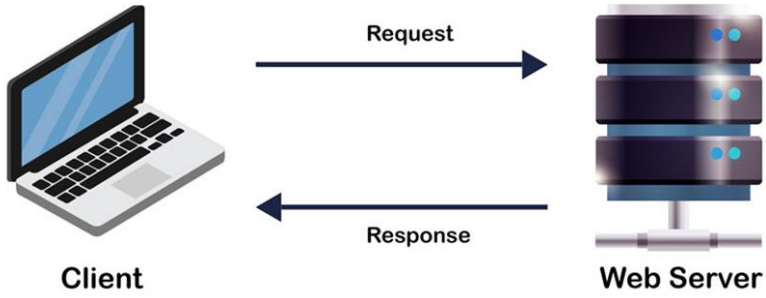

Figure 2. Dedicated Server Before Design

In Figure 2, it can be seen that before the design, the Client/user accessed the website to the server directly without an intermediary, on the server using Windows 10 Home OS and using XAMPP for the web server, online server access using a domain that was directed to the server's Public IP.

3.1.1. Website Access Flow

1. **Client/User**
   1) **Devices**: Using a PC, laptop, tablet, or smartphone.
   2) **Browser**: Applications like Chrome, Firefox, or Edge.
   3) **Access Process**:
      (1) The client enters the domain name (example: www.mydomain.com) in the browser.
      (2) The browser performs DNS resolution to translate the domain to the server's Public IP.
      (3) The request is forwarded to the server via the internet network.
2. **DNS (Domain Name System)**
   1) The domain used has been configured to point to the server's Public IP.
   2) Resolution process:
      (1) The client requests domain information from the DNS server.
      (2) DNS server provides the Public IP associated with that domain.
      (3) Browsers use Public IP to send requests to servers.
3. **Network Connection**
   1) The server uses a public IP that can be accessed directly via the internet.
   2) **Router**The server is set to do port forwarding (for example, port 80 for HTTP and port 443 for HTTPS) to the server's local IP (LAN).

---

4. **Server**
   1) **Operating System (OS)**:
      (1) The server uses Windows 10 Home to run the web server application.
   2) **Web Server**:
      (1) The server runs XAMPP as a platform for:
         - **Apache**: Handle HTTP/HTTPS requests from clients.
         - **MySQL**: Provides database.
         - **PHP**: Process server-side scripts.
      (2) The website is placed in the htdocs folder (example: C:\xampp\htdocs\mywebsite).
5. **Server Process**
   1) **Apache Web Server**:
      (1) Apache accepts HTTP requests from browsers through domains directed to the Public IP.
      (2) Apache looks for the requested file in the htdocs directory.
      (3) If the file is PHP, Apache processes it using the PHP module.
   2) **Database**:
      (1) A query is sent to MySQL to retrieve the requested data.
      (2) The database responds with the appropriate data.
   3) **Response**:
      (1) Apache sends the data file to the client browser.
   4) **Client Displays Website**
      (1) The browser receives a response from the server.
      (2) The response in the form of a dynamic file is displayed to the user.

3.1.2. Flowchart used

1. **Client/User**:
   - The browser accesses www.mydomain.com.
2. **DNS**:
   - Domain resolution to server Public IP.
3. **Network**:
   - The server router performs port forwarding to the local server (LAN IP).
4. **Server**:
   - Apache processes requests and, if necessary, retrieves data from the database.
5. **Client**:
   - The browser receives and displays the response results.

3.2. Clud Server designed

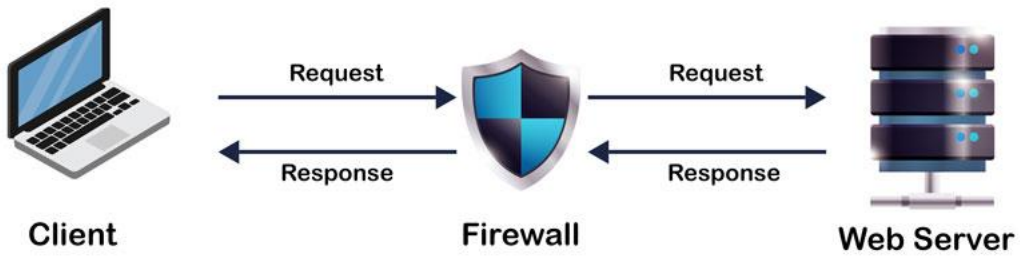

Figure 3. Designed Cloud Server

In figure 3 it can be seen that after the design. On the designed cloud server, the Client/user accesses the website to the server through the firewall first, in the firewall there are script settings in .htaccess to prevent XSS and CSRF, on the server using the Linux OS almalinux 8.6 and using cpanel for its webserver panel, online server access uses a domain that is directed to the Public IP server using DNS from cloudflare.

3.2.1. Website Access Flow

1. **Client/User**
   1) **Devices**: PC, laptop, tablet, or smartphone.
   2) **Browser**: Chrome, Firefox, Edge, or others.
   3) **Access Process**:
      (1) The client enters the domain name (example: www.mydomain.com) in the browser.
      (2) The browser performs DNS resolution to Cloudflare to get the server's Public IP.
      (3) Requests are directed to the server through the firewall first.
2. **DNS (Cloudflare)**
   1) Domain uses Cloudflare DNS to point to the server's Public IP.
   2) Cloudflare can provide additional security features such as:
      (1) **DDoS protection**.
      (2) **Caching to increase access speed**.
      (3) **SSL/TLS for encryption**.
3. **Firewall**
   1) Before reaching the server, the request passes through a firewall which functions to:
      (1) **Filtering malicious requests**.
      (2) **Prevent DDoS attacks or unauthorized access**.
      (3) **Checking HTTP headers and query parameters**.
      (4) **Disguise the existing public IP using a proxy or what can also be called an IP Mask**
   2) The firewall can be Cloudflare WAF (Web Application Firewall) or a firewall on the server such as CSF (ConfigServer Security & Firewall).

4. **Protection in .htaccess**
   1) **Security configuration in .htaccess**used to prevent XSS (Cross-Site Scripting) and CSRF (Cross-Site Request Forgery).
   2) Example script in .htaccess:

```
apache
CopyEdit
# Prevent XSS with Content Security Policy
Header set Content-Security-Policy "default-src 'self';
script-src 'self' 'unsafe-inline'"

# Prevent CSRF by limiting allowed methods
<IfModule mod_rewrite.c>
    RewriteEngine On
    RewriteCond %{REQUEST_METHOD} !^(GET|POST|HEAD)$
    RewriteRule .* - [F,L]
</IfModule>
```

5. **Server**

1) **Operating System (OS)**:
   (1) The server uses AlmaLinux 8.6, which is based on RHEL (Red Hat Enterprise Linux).
   (2) This OS is stable and suitable for cPanel based servers.
2) **Web Server**:
   (1) Using cPanel as a web server management panel.
   (2) cPanel makes it easy to manage domains, website files, databases, and security.
3) **Website Folders**:
   (1) The website files are located at /home/username/public_html/.

6. **Server Process**
   1) **Apache or LiteSpeed Web Server**:
      (1) Apache/LiteSpeed handles requests from clients.
      (2) If a PHP file is called, the server processes it with the PHP module.
   2) **Database**:
      (1) The server uses MySQL to store data.
      (2) Databases can have additional protection such as SQL Injection prevention.
   3) **Response**:
      (1) Apache/LiteSpeed sends the processing results (HTML, CSS, JS) to the client browser.
7. **Client Displays Website**
   1) The browser receives a response from the server.
   2) The website is presented to users with protection from XSS and CSRF.

3.2.2. Flowchart

1. **Client/User**:
   - The browser accesses www.mydomain.com.
2. **Cloudflare DNS**:
   - Cloudflare translates domains to server Public IPs.
3. **Firewall**:
   - Firewall filters requests based on security rules and disguises the Public IP or is called an IP Mask.
4. **Server (AlmaLinux 8.6 + cPanel)**:
   - The web server processes the request.
   - If necessary, retrieve data from the database.
5. **Client**:
   - The browser receives and displays the website page.

3.2.3. Additional Security That Can Be Implemented

1. **Cloudflare Security Settings**:
   - **WAF (Web Application Firewall)**to block common attacks.
   - **Bot Protection**to prevent suspicious automated access.
   - **Rate Limiting**to limit excessive requests from the same IP.
2. **Server Hardening**:
   - Use CSF (ConfigServer Security & Firewall) to control incoming/outgoing traffic.
   - Disable dangerous PHP functions (disable_functions in php.ini).
3. **SSL/TLS (HTTPS)**:
   - Make sure SSL is active so that communications are encrypted.

3.3. Design Needs

3.3.1. Requirements Before (Dedicated Server)

Before design, the existing hardware (Dedicated Server) was as follows:

1. Processor: 2 Core
2. RAM: 4GB
3. SSD: 80gb

Prior to design, the existing Software (Dedicated Server) was as follows:

1. Operating System: windows 10
2. Application: xampp

3.3.2. After Needs (Cloud Server)

After the design, the existing hardware (Cloud Server) is as follows:

1. Processor: 2 Core
2. RAM: 4GB
3. SSD: 80gb

After the design, the existing hardware (Cloud Server) is as follows:

1. Operating System: Linux Almalinux 8.6
2. Applications: cPanel, Apache/Litespeed

3.4. Discussion

Before using Cloudflare IP Masking, server performance was low, Data Access and Management was Low, Scalability was Low, Access Security was Low, System Integration was Low, but after using Cloudflare IP Masking Server Performance, Data Access and Management, Scalability, Access Security, and System Integration increased.

Table 1. Security Analysis

No	Case	Security Before	Security After
1	Server Performance	Low	High
2	Data Access and Management	Low	High
3	Scalability	Low	High
4	Access Security	Low	High
5	System Integration	Low	High

In Table 1, it shows the security cases before and after the cloud server design. The security analysis of table 1 above is as follows:

a. Server Performance
   Server performance before design is low because there is no cache configuration on the server. This is because previously the server was still using a dedicated server and using xampp without any other configuration. However, for security after the cloud server design it becomes high because there is already a cache configuration on the server. This is because the server already uses a cloud server and has used a configuration based on the cloud server, so that server performance is high.
b. Data Access and Management
   Data Access and Management for previous security was low because data access and management were still widely open, such as access rights to directory data were still not good for users. However, Data Access and Management for security after that was high because it had used or managed access rights properly, such as improvements to directory access rights on the server.
c. Scalability
   Scalability for security was previously low because scalability in a dedicated server is quite difficult and inefficient, for vertical and horizontal scalability it might be possible but there must still be a configuration between the hardware and software used to run properly, for the configuration it is quite troublesome. However, scalability for security after that is high because it is quite easy and efficient, for vertical and horizontal scalability it is easy to do and it is quite easy to configure between the hardware and software used to run properly.
d. Access Security
   Security Access for previous security is low because access to the server still uses http, for https it is quite difficult to configure it on a dedicated server using xampp, there is no firewall to secure data in the server directory and cannot manipulate the IP used or what is called IP Mask because it still uses http access. However, Access Security for security after that is high because access to the server already uses https because it is quite easy to configure it on the cloud server and already uses cloudflare, there is already a firewall to secure data in the cloud server directory, it is easy to add other configurations and IP can be manipulated because it is already https.
e. System Integration
   System Integration for previous security was low because access still used xampp and still used http which had low security for system integration in it. However, System Integration for security after that was high because access already used https and already used a firewall which had high security for system integration in it.

6. CONCLUSION

This study successfully designed a Cloud Server Security System on the Linux Almalinux 8.6 Operating System Based on WHM with DNS Management Using IP Masking Cloudflare. The results of the study concluded that this design can improve security in Cloud Server. With increasing Server Performance, Data Access and Management, Scalability, Access Security, and System Integration. With this design, it resulted in increased security in Cloud Server. Before using IP Masking Cloudflare, server performance was low, Low Data Access and Management, Low Scalability, Low Access Security, Low System Integration, but after using IP Masking Cloudflare Server Performance, Data Access and Management, Scalability, Access Security, and System Integration increased. This is because in server performance there is already a cache configuration on the server using a configuration based on the cloud server, Access and Data Management already use or have managed access rights properly such as improvements to directory access rights on the server, Scalability is quite easy and efficient as seen from the configuration between hardware and software used to run well, Access Security already uses https and already uses cloudflare and firewall to secure data in the cloud server directory so that it is easy to add other configurations and IP can be manipulated, and System Integration already uses https and already uses a firewall that is quite high in security for system integration in it.

ACKNOWLEDGEMENTS

Author thanks ... . In most cases, sponsor and financial support acknowledgments.

REFERENCES

[1] Abdiansyah, MN, 2018, WHM/cPanel Based Hosting Management. Excellent Publishing, Bekasi.

[2] Anklesaria, F., & McCahill, M., 1993, The Internet Gopher. In Intelligent information retrieval: The case of astronomy and related space sciences (pp. 119-125). Dordrecht: Springer Netherlands.

[3] Aryachandra, D., Yanto, IF, Khair, MM, & Pahlevi, MRS (2024). Hiding Webserver IP Address with Cloudflare's Proxy Dns Records. Journal of Social Technology, 4(4), 218-226.

[4] Bijjou, K., 2019, Web Application Firewall Bypassing: An Approach for Penetra. In Depth Security Vol. III: Proceedings of the DeepSec Conferences (Vol. 3, p. 29). BoD–Books on Demand November, 2019

[5] De Souza Oliveira, L., de Sousa, JPC and Ribeiro, JVA, 2022. Bypassing Cloudflare's reverse proxy: a case study Contornando o proxy reverso do Cloudflare: um estudo de caso. Brazilian Journal of Development, 8(4), pp.27250-27259.

[6] Govil, Y., Wang, L. and Rexford, J., 2020. {MIMIQ}: Masking {IPs} with Migration in {QUIC}. In 10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20).

[7] Jayanti, DE, Umar, R. and Riadi, I., 2020. Implementation of Cloudflare Hosting for Access Speed on Trading Websites. SISPHOTHENICS, 10(2), pp.227-238.

[8] John, J., & Fraser, E. A. (2024). DDoS Attacks on Cloud Computing and IoT Devices: Strategies for Mitigation.

[9] Li, Z., Liu, G., Dang, Y., Shang, Z. and Lin, N., 2022. Research on New Virtualization Security Protection Management System Based on Cloud Platform. In Journal of Physics: Conference Series (Vol. 2146, No. 1, p. 012010). IOP Publishing.

[10] Liu, C., & Albitz, P., 2006, DNS and Bind. & Reilly Media, Inc

[11] Matondang, N., Isnainiyah, IN, & Muliawatic, A., 2018, Analysis of information system data security risk management (Case study: XYZ Regional Hospital), RESTI Journal (System Engineering and Information Technology), ISSN: 2580-0760, Vol. 2 Issue 1 April, 2018

[12] Perkins, C.E., & Bhagwat, P. (1994). A mobile networking system based on internet protocol. IEEE personal communications, 1(1), 32-41.

[13] PW, A. Dwi., & Ujianto, EIH, 2020, Security System Analysis of Cloud Computing Using Attack-Centric Method, Progresif: Jurnal Ilmiah Komputer, ISSN: 0216-3284, Vol. 16 Issue 1 February, 2020

[14] Rachman, A., & Aminullah, M., 2013, Design of proxy server and analysis of internet usage using sarg (case study at BMKG Juanda Surabaya), Jurnal Iptek, ISSN: ,2477-507X, Vol. 17 Issue 1 May, 2013