Rancang Bangun Sistem *Log Server* Berbasis RSyslog dan MySQL Untuk *Monitoring* Aktivitas Komputer Laboratorium

Adinda Nazalia Hadianti[1], Arrizqi Fauzy Aufar[2], Rosydah Rihadhatu Aisyiyah[3], Rakhmad Fahmi Putra[4]

Program Studi Informatika, Universitas Muhammadiyah Sidoarjo, Sidoarjo
Jl. Mojopahit No.666 B Sidoarjo 61215
[1]adindanazalia18@gmail.com
[2]arrizqifauzyaufar@gmail.com
[3]rosydahaisyiyah@gmail.com
[3]fahmiputrarakhmad@gmail.com

Intisari — **Di era kebutuhan akan internet semakin meningkat di masyarakat dan ilmu pengetahuan. Hal ini tidak hanya berdampak positif pada pertumbuhan pengguna, tetapi juga dapat berdampak negatif yang dapat berujung pada pelanggaran penggunaan internet. Oleh karena itu, diperlukan sistem monitoring agar dapat memantau aktivitas yang dilakukan oleh user terhadap perangkat komputer yang digunakan. Sederhananya, seperti mengirim pesan log kepada sistem yang terpusat. RSyslog server adalah sebuah perangkat lunak gratis yang digunakan pada sistem komputer untuk meneruskan pesan log dengan melalui jaringan IP. Pesan log yang telah terekam di RSyslog server kemudian disimpan ke dalam database dengan menggunakan MySQL. Dalam hal ini, MySQL sebagai media penyimpanan yang telah memiliki format penyimpanan pesan log yang direkam oleh RSyslog sehingga memudahkan administrator untuk memantau dan mengelola pesan log yang telah disimpan. Sehingga pengimplementasian artikel ilmiah ini menggunakan metode Network Development life cycle (NDLC) untuk mendapatkan gambaran dari alur perancangan Rsyslog server agar dapat digunakan oleh administrator sistem. Dengan dirancangnya sistem administrator agar dapat memantau pesan log dari komputer lain, dapat memudahkan perawatan komputer dalam satu jaringan dan dapat meminimalisir tindak kejahatan yang dilakukan oleh pengguna komputer.**
Kata kunci — **Log Server, Rsyslog, MySql, Monitoring, Cyber Security.**

Abstract — **In this era, the need for internet is increasing in society and science. This not only has a positive impact on user growth, but can also have a negative impact which can lead to internet usage violations. Therefore, a monitoring system is needed in order to monitor the activities carried out by the user on the computer equipment used. Simply put, it's like sending log messages to a centralized system. RSyslog server is a free software used on computer systems to forward log messages over IP networks. Log messages that have been recorded on the RSyslog server are then stored in a database using MySQL. In this case, MySQL as a storage medium has a log message storage format recorded by RSyslog, making it easier for administrators to monitor and manage the stored log messages. So that the implementation of this scientific article uses the Network Development life cycle (NDLC) method to get an overview of the Rsyslog server design flow so that it can be used by system administrators. By designing a system administrator to be able to monitor log messages from other computers, it can facilitate computer maintenance in one network and can minimize crimes committed by computer users.**
Keywords — **Server Log, Rsyslog, MySql, Monitoring, Cyber Security.**

I. PENDAHULUAN

Di era teknologi informasi dan ilmu pengetahuan yang semakin berkembang, kebutuhan akan internet semakin meningkat di masyarakat. Hal ini tidak hanya berdampak positif pada pengguna, tetapi juga dapat berdampak negatif yang berujung pada pelanggaran penggunaan internet. Oleh karena itu, diperlukan sistem monitoring agar dapat memantau aktivitas yang dilakukan oleh user terhadap perangkat komputer yang digunakan. Sederhananya, seperti mengirim pesan log kepada sistem yang terpusat [1]. Salah satu sistem monitoring yang telah dipercaya adalah Rsyslog Server.

Rsyslog Server merupakan sebuah perangkat lunak tidak berbayar yang digunakan pada sistem komputer untuk meneruskan pesan log dengan melalui jaringan IP[1]. Rsyslog dapat dikategorikan sebagai sistem pemrosesan log yang aman dan powerful. Rsyslog server menerima log dari beberapa server fisik atau virtual melalui

sistem jaringan dan memonitor status berbagai layanan. Administrator Rsyslog server dapat memantau server lain, perangkat jaringan, dan log aplikasi jarak jauh dari satu lokasi yang dikelola secara terpusat. RSyslog menerapkan protokol Syslog sebagai dasarnya. RSyslog server memperluas protokol Syslog dengan fitur dukungan operasi yang lebih stabil dengan dukungan protokol RELP.

Penggunaan perangkat lunak seperti Rsyslog Server juga memperkuat keamanan perangkat komputer. Saat ini keamanan perangkat komputer menjadi topik yang hangat. Kerentanan perusahaan atau instansi terhadap serangan dari luar menjadikan kelemahan perusahaan dalam bidang keamanan informasi yang mengakibatkan kebocoran data. Akibat dari kurangnya pengetahuan sebuah perusahaan atau instansi menjadikan serangan yang berdampak besar bagi sebuah perusahaan[2]. Banyak perusahaan yang mengalami kebangkrutan diakibatkan hilangnya kepercayaan konsumen karena kebocoran data informasi. Dengan demikian penggunaan Rsyslog membantu menanggulanginya dengan merekam pesan log pada setiap aktivitas sistem yang berjalan dan memperkuat perangkat jaringan perusahaan atau instansi tersebut[3].

Banyaknya perangkat komputer dan jaringan yang dicatat lognya secara langsung dalam waktu yang bersamaan dengan aktivitas pengguna komputer, membuat kinerja komputer server semakin terbebani. Log tersebut juga harus ditampilkan kembali agar administrator dapat memantau pesan log yang muncul. Oleh sebab itu, perancangan RSyslog server harus menggunakan teknik penyimpanan dan topologi jaringan yang baik sehingga ketika terjadi kegagalan pada salah satu perangkat tidak akan mengganggu pengiriman pesan log dari komputer lain[2]. Sehingga dalam hal ini penyimpanan pesan log secara langsung pada RSyslog server dan menampilkan kembali pesan log pada sistem administrator dapat dilakukan secara cepat dan terstruktur[3]. Untuk menyimpan pesan Log yang diterima oleh RSyslog server maka diperlukan tempat penyimpanan berupa database untuk dapat menampilkan kembali log yang telah diterima kepada sistem administrator.

Dalam penelitian ini penulis menggunakan database MySql untuk memudahkan penyimpanan data log yang nantinya akan ditampilkan pada administrator. MySQL merupakan salah satu Relational Database Management System (RDBMS) yang saat ini sedang banyak digandrungi oleh para pengembang aplikasi database, baik untuk aplikasi desktop maupun aplikasi web untuk menyimpan, mengatur, dan mengelola data pada aplikasi tersebut. Pesan log yang diterima RSyslog server disimpan dalam MySQL database [4].

Dalam mengimplementasikan RSyslog server diperlukan juga bahasa pemprograman dalam menjalankannya. Bahasa pemprograman yang sesuai untuk digunakan dalam penelitian ini adalah bahasa pemprograman PHP: Hypertext Preprocessor. PHP adalah bahasa sederhana namun powerful yang dirancang untuk membuat konten HTML[5]. Fungsi PHP dalam hal ini digunakan untuk menampilkan pesan log yang diterima oleh database RSyslog server agar lebih mudah untuk pengguna melihat tampilannya.

Dalam penelitian ini, peneliti menggunakan RSyslog, yaitu sistem yang membantu melakukan monitoring aktivitas pada komputer dengan meneruskan log aktivitas komputer dari laboratorium komputer Universitas Muhammadiyah Sidoarjo. Pada penelitian ini menggunakan MySql sebagai database dan bahasa pemprograman PHP untuk mengoprasikannya. Meskipun sistem ini cukup efektif, sistem ini juga memiliki beberapa fitur yang perlu pembelajaran lebih lanjut untuk dapat mengaplikasikannya. Sistem ini nantinya digunakan untuk melakukan monitoring kepada seluruh komputer yang terdapat pada labolatorium komputer. RSyslog ini memfokuskan pada jaringan dari sebagai akses utama untuk memonitor aktivitas komputer.

II. METODOLOGI PENELITIAN

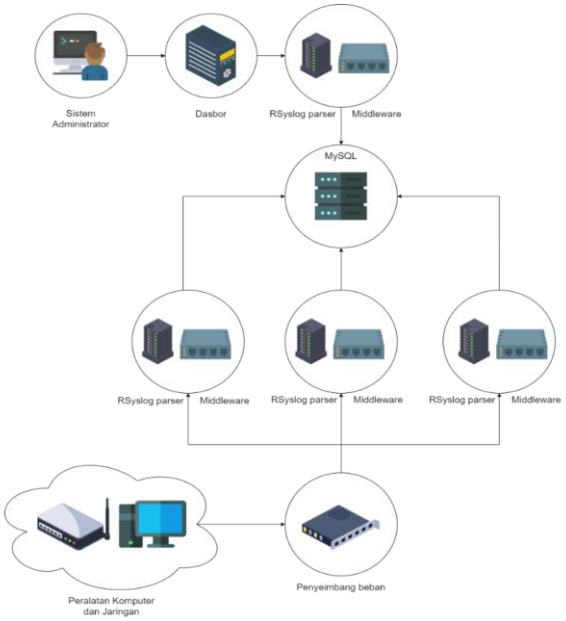
Metode yang digunakan dalam penelitian ini adalah Network Development Life Cycle (NDLC). Tahapan dalam metode ini meliputi analisis, perancangan, simulasi, dan implementasi. Berikut penjelasan tahap yang akan dilakukan:

A. Tahap Anlisis

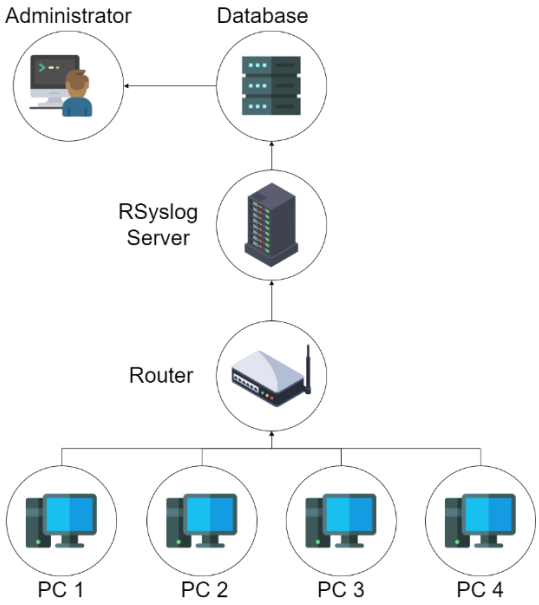
Setelah melakukan analisis lapangan terhadap Laboratorium Informatika menghasilkan topologi jaringan RSyslog server seperti pada Gambar 1. Pesan log antar komputer didistribusikan melalui jaringan dengan menggunakan sistem operasi linux dan windows lalu diteruskan ke Rsyslog server menggunakan router kemudian disimpan dalam database agar dapat ditampilkan ke administrator sistem.

B. Tahap Perancangan

Dalam tahap perancangan sistem, RSyslog server guna administrator sistem dapat memantau server yang sedang berjalan. Sehingga dibutuhkan beberapa alat jaringan agar dapat saling terhubung. Pada Gambar 2, terjadi interaksi sistem pemantauan antara administrator sistem dan komputer di laboratorium informatika. Semua data pesan Log yang terekam dalam RSyslog akan disimpan dalam database MySQL.

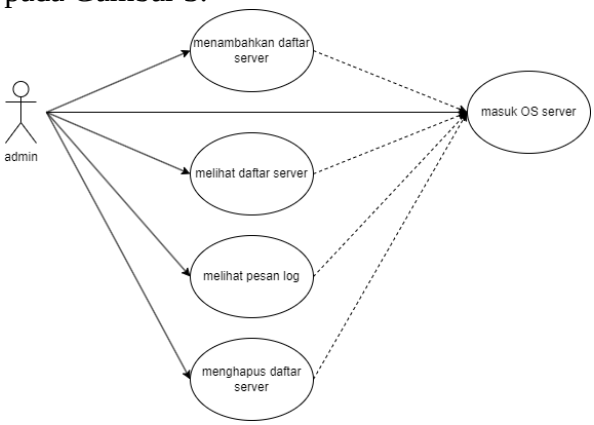


Gbr. 1 Arsitektur Sistem



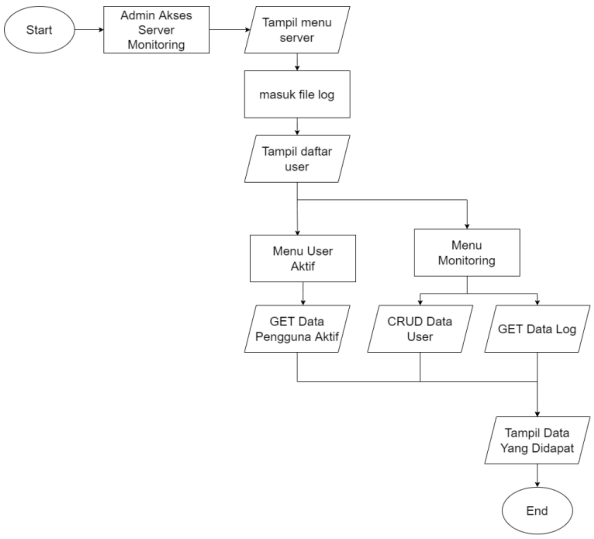
Gbr. 2 Perancangan Sistem Monitoring Log

Untuk dapat mengakses sistem, Administrator harus mengakses file yang ada di RSyslog server seperti yang digambarkan pada Gambar 3.



Gbr. 3 *Use case* Pemantauan Administrator sistem

Seperti yang ada pada Gambar 3, Use Case digunakan untuk menggambarkan bagaimana administrator dapat memantau pesan Log. Sebelum dapat memantau pesan Log, administrator harus mengaksesnya melalui server OS dan masuk sebagai admin. Selanjutnya administrator mengakses file yang tersimpan dalam database MySQL agar dapat melakukan pemantauan pesan Log dari komputer lain melalui jaringan IP. Gambar 4 membantu administrator sistem untuk melogika alur dalam mengakses RSyslog server[1].



Gbr. 4 *Flowchart* administrator monitoring pesan log

C. Tahap Simulasi

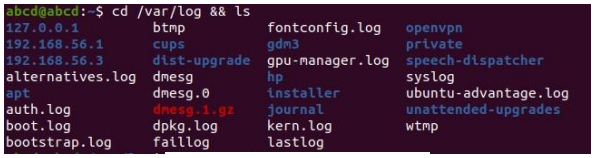
Sebelum menerapkan RSyslog server pada jaringan Laboratorium Informatika, uji coba RSyslog server dijalankan dengan menggunakan Virtualbox agar tidak menganggu pada jaringan utama. Dimana dalam kasus ini menggunakan empat Virtual sistem operasi dan satu sebagai server, dengan menggunakan konfigurasi yang sama. Dimana, menggunakan protokol UDP untuk mengirim pesan log dari perangkat klien menuju perangkat server.

D. Tahap Implementasi

Tahap ini semua konsep dan rancangan pada sistem yang telah dilakukan dengan virtual, diimplementasikan dalam jaringan Laboratorium Informatika. RSyslog bertugas sebagai *software* perekam pesan log yang selanjutnya akan disimpan kedalam *database* MySQL agar administrator dapat memantau pesan log yang diterima. penerima pesan log dan satu komputer sebagai pengirim pesan log. Rsyslog merupakan cara yang efisien untuk memantau kinerja dan aktivitas dari komputer client di ruang lingkup Laboratorium Informatika. Dimana dalam pemantauannya, Administrator harus memilih file log yang memiliki nama unik dari setiap komputer sesuai dengan IP yang dimiliki seperti yang terlihat pada gambar 5[6].

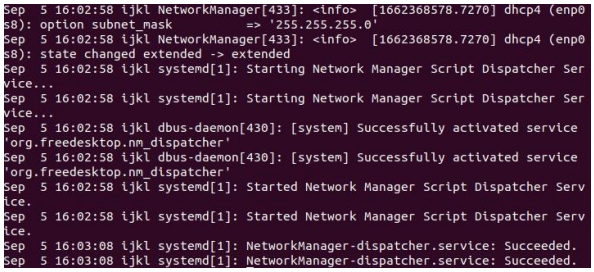
III. HASIL DAN PEMBAHASAN

Implementasi dari RSyslog pada tahap perancangan dilakukan antara dua komputer yang saling terhubung.



Gbr. 5 Daftar File Log

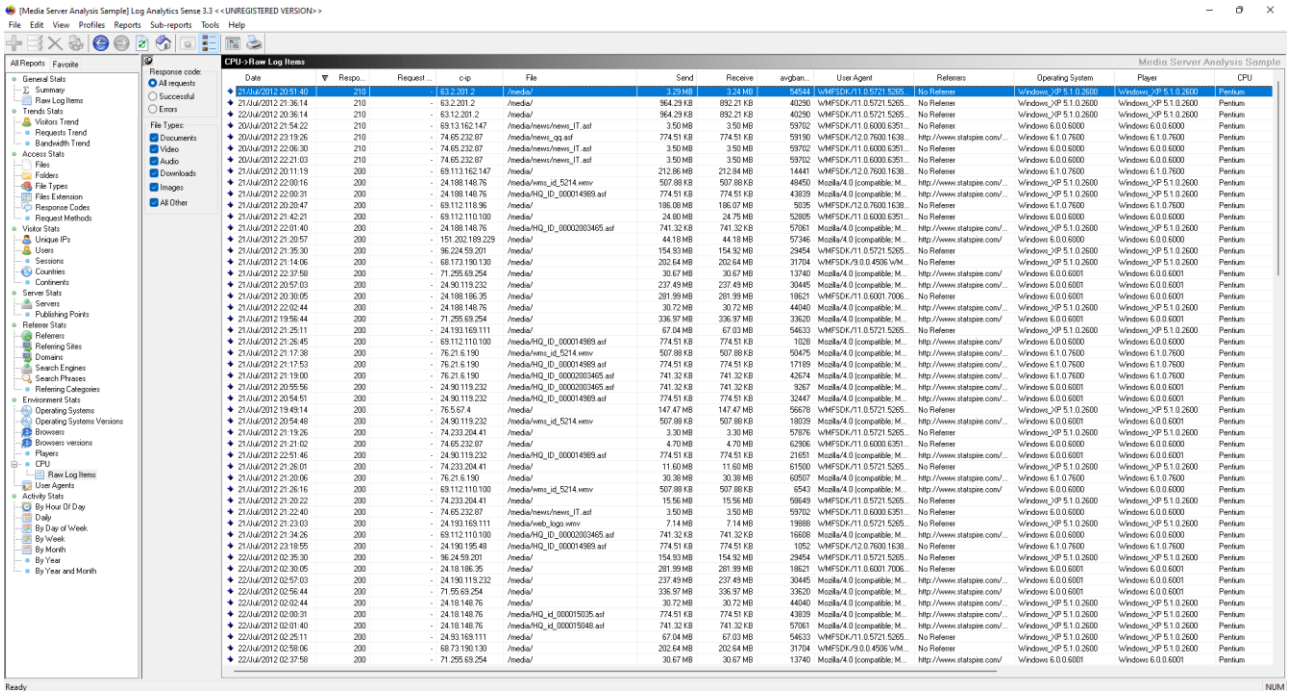
Ketika Administrator ingin melihat pesan log, maka harus diikuti dengan perintah tertenru dan dilanjutkan dengan nama file log yang dituju. Selanjutnya akan muncul daftar pesan log dari komputer yang dituju seperti pada gambar 6.



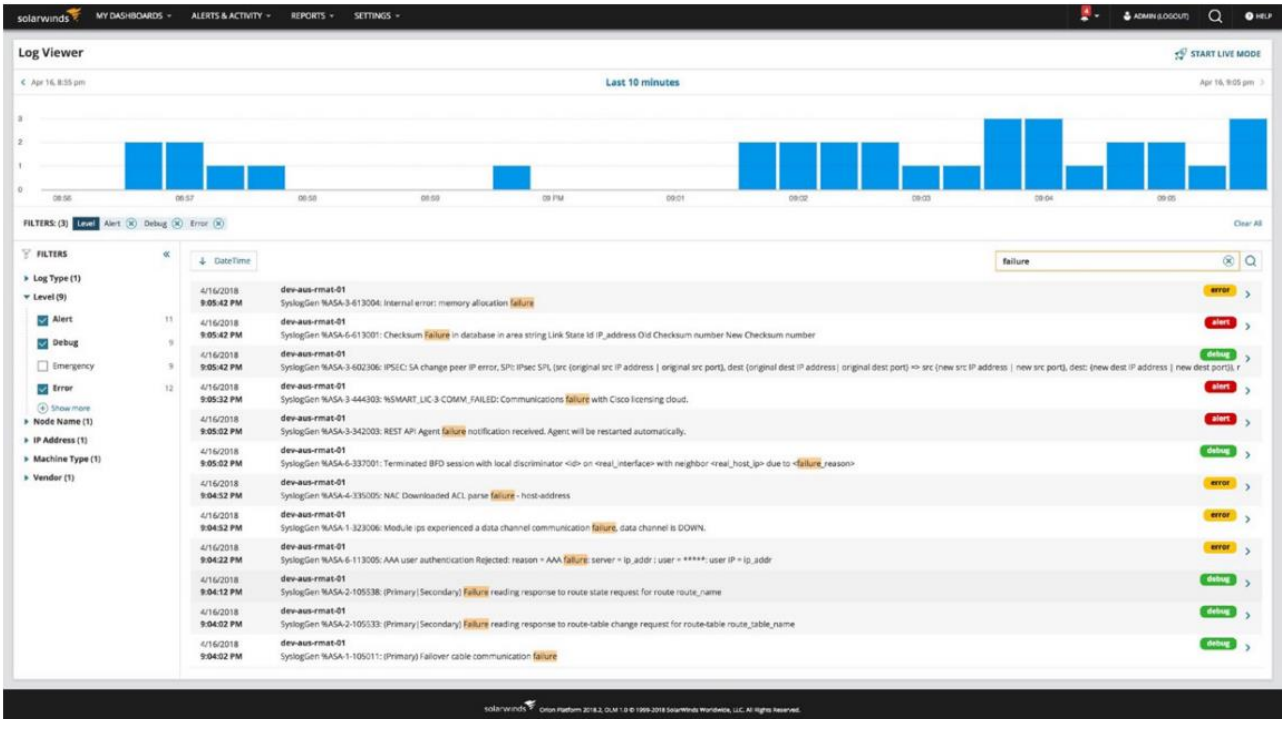
Gbr. 6 Isi Pesan Log

Sebenarnya RSyslog sendiri memiliki aplikasi analyzer tersendiri yang sudah memiliki antarmuka berbasis web. LogAnalyzer merupakan aplikasi gratis berbasis web untuk menganalisis file Log. LogAnalyzer memiliki fitur tersendiri yang tidak tersedia di alat analisis file Log lainnya[7]. LogAnalyzer sangatlah mudah di sisi input (format file log tidak memiliki batasan) dengan tetap mempertahankan format yang tersedia, seperti yang terlihat pada gambar 7. LogAnalyzer memiliki beberapa fitur yang mendukung untuk mengelola dan memantau kinerja serta aktivitas dari komputer yang terhubung. Salah satu fitur yang ada yakni kita bisa melihat kinerja dari CPU komputer sehingga ketika terjadi eror maka akan langsung diketahui. Aplikasi ini juga dapat menyimpan pesan log dengan jangka waktu kurang lebih setahun.

Ada juga *software* lain seperti *Solarwinds* yang memiliki fitur tambahan seperti penggambaran lalu lintas dan performa perangkat dalam bentuk grafik yang dapat dilihat pada gambar 8. *Solarwinds* merupakan aplikasi berbayar dengan masa percobaan gratis selama 30 hari.



Gbr. 7 Menu dari *LogAnalyzer*



Gbr. 8 *Solarwinds*

IV. PENUTUP

Dari hasil implementasi sistem Rsyslog, dapat ditarik kesimpulan bahwa penggunaan sistem Rsyslog ini sangat efisien untuk mengelola dan memantau pesan log yang terjadi. Konfigurasi dan perancangan alat yang digunakan tidak terlalu rumit. Penggunaan sistem Rsyslog terbukti menghemat biaya perawatan sistem yang dilakukan administrator.

Perancangan system Rsyslog diterapkan dalam sistem operasi ubuntu tanpa menggunakan aplikasi pihak ketiga. Sehingga dalam penerapannya hanya administrator yang dapat mengelola dan memantau pesan log. Sistem ini juga memungkinkan administrator untuk memantau status perangkat jaringan yang terhubung ke jaringan. Saat masalah jaringan muncul sistem Rsyslog dapat mengidentifikasinya lebih cepat sehingga dapat mengambil tindakan segera.

UCAPAN TERIMA KASIH

Ucapan terima kasih disampaikan kepada Universitas Muhammadiyah Sidoarjo yang telah memberikan fasilitas dalam menyelesaikan penelitian ini. Terima kasih juga kami ucapkan kepada kedua orang tua saya dan semua orang yang membantu secara langsung maupun tidak langsung dalam penyusunan jurnal.

REFERENSI

[1] R. Nafis Ibrahim, A. Musthafa, O. Virgantara Putra, T. Informatika Universitas Darussalam Gontor, J. Raya Siman, and J. Timur, "Rancang Bangun Sistem Monitoring Aktivitas Pengguna Hotspot UNIDA Gontor Menggunakan Rsyslog dan Mikrotik API," *J. Ilmu-ilmu Inform. dan Manaj. STMIK*, vol. 15, no. 1, 2021.

[2] D. Zhou, "Research on the Security Early Warning Model of Campus Network Based on Log," *IOP Conf. Ser. Earth Environ. Sci.*, vol. 252, no. 4, 2019, doi: 10.1088/1755-1315/252/4/042080.

[3] R. Sasidharan, "Implementation of High Available and Scalable Syslog Server with NoSQL Cassandra Database and Message Queue," *Am. J. Comput. Archit.*, vol. 9, no. 1, pp. 1–7, 2022, doi: 10.5923/j.ajca.20220901.01.

[4] D. D. J. T. Sitinjak, Maman, and J. Suwita, "Analisa Dan Perancangan Sistem Informasi Administrasi Kursus Bahasa Inggris Pada Intensive English Course Di Ciledug Tangerang," *Ipsikom*, vol. 8, no. 1, pp. 1–19, 2020.

[5] A. Solichin, *Pemrograman Web dengan PHP dan MySQL*, no. January 2005. Jakarta: Universitas Budi Luhur, 2014.

[6] W. Sholihah, S. Pripambudi, and A. Mardiyono, "Log Event Management Server Menggunakan Elastic Search Logstash Kibana (ELK Stack)," *JTIM J. Teknol. Inf. dan Multimed.*, vol. 2, no. 1, pp. 12–20, 2020, doi: 10.35746/jtim.v2i1.79.

[7] R. Andriani, E. S. Pramukantoro, and M. Data, "Pengembangan Sistem Visualisasi Access Log untuk Mengetahui Informasi Aktivitas Pengunjung pada Sebuah Website," *J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya*, vol. 2, no. 6, pp. 2104–2112, 2018.