JURITEK: Jurnal Ilmiah Teknik Mesin, Elektro dan Komputer

E-ISSN: 2809-0799
P-ISSN: 2809-0802

Penerapan Graylog sebagai Sistem Monitoring Aktivitas Jaringan Menggunakan Syslog Pada Lingkungan Enterprise

Afdhal Dinil Haq[1], Edi Surya Negara[2]

[1] Afiliasi 1; email : Universitas Bina Darma, afdhaldinilhaq121105@gmail.com
[2] Afiliasi 2; email : Universitas Bina Darma, e.s.negara@binadarma.ac.id
*** Penulis Korespondensi:** Afdhal Dinil Haq

Abstract: Network activity monitoring is an important process in maintaining service availability and supporting information technology infrastructure security in enterprise environments. Network devices generate log data that can be utilized to monitor system activities, detect network disruptions, and support analysis processes. However, managing logs distributed across multiple devices often makes monitoring activities less effective and more difficult for network administrators. This study aims to implement Graylog as a network activity monitoring system using Syslog to provide centralized log management. The research method consisted of system requirement identification, architecture design, Graylog implementation on Ubuntu Server 22.04.5 LTS, Syslog UDP configuration on a Cisco SG300-28PP switch, and testing of log collection and visualization processes. The system was developed using Graylog 6.1.16 as the log management platform, OpenSearch 2.19.5 as the indexing and search engine, and MongoDB 7.0.34 as the configuration database. The results show that Graylog successfully receives, stores, manages, and displays log data generated by network devices in a centralized manner. In addition, the search and dashboard features provide structured visualization of network activities, enabling administrators to perform monitoring and analysis more efficiently. Based on the testing results, all major functions of the monitoring system operated as expected. Therefore, the implementation of Graylog and Syslog can be considered an effective solution for centralized network activity monitoring in enterprise environments.

Keywords: Graylog; Syslog; Network Monitoring; Log Management; Network Security; Enterprise Networke

Abstrak: Monitoring aktivitas jaringan merupakan kegiatan penting dalam menjaga ketersediaan layanan dan mendukung keamanan infrastruktur teknologi informasi pada lingkungan enterprise. Perangkat jaringan menghasilkan data log yang dapat digunakan untuk memantau aktivitas sistem, mendeteksi gangguan, dan membantu proses analisis jaringan, namun pengelolaan log yang tersebar pada setiap perangkat sering menyulitkan administrator dalam melakukan pemantauan secara efektif. Penelitian ini bertujuan menerapkan Graylog sebagai sistem monitoring aktivitas jaringan menggunakan Syslog untuk menyediakan pengelolaan log yang terpusat. Metode penelitian yang digunakan meliputi identifikasi kebutuhan sistem, perancangan arsitektur, implementasi Graylog pada Ubuntu Server 22.04.5 LTS, konfigurasi Syslog UDP pada perangkat Cisco SG300-28PP, serta pengujian penerimaan dan visualisasi data log. Sistem dibangun menggunakan Graylog 6.1.16 sebagai platform manajemen log, OpenSearch 2.19.5 sebagai mesin indeks dan pencarian data, serta MongoDB 7.0.34 sebagai basis data konfigurasi. Hasil penelitian menunjukkan bahwa Graylog berhasil menerima, menyimpan, mengelola, dan menampilkan data log yang dikirimkan oleh perangkat jaringan secara terpusat. Selain itu, fitur pencarian dan dashboard monitoring mampu menyajikan informasi aktivitas jaringan secara lebih terstruktur sehingga memudahkan proses pemantauan dan analisis. Berdasarkan hasil pengujian yang dilakukan, seluruh fungsi utama sistem monitoring dapat berjalan sesuai dengan kebutuhan yang telah ditentukan sehingga implementasi Graylog dan Syslog dapat digunakan sebagai solusi monitoring aktivitas jaringan pada lingkungan enterprise.

Kata kunci: Graylog; Syslog; Monitoring Jaringan; Manajemen Log; Keamanan Jaringan; Enterprise Network

Diterima: June 25, 2026
Direvisi: June 30, 2026
Diterima: July 17, 2026
Diterbitkan: July 17, 2026
Versi sekarang: July 30, 2026

1. Pendahuluan

Perkembangan teknologi informasi yang semakin pesat menyebabkan ketergantungan organisasi dan perusahaan terhadap infrastruktur jaringan komputer terus meningkat. Berbagai layanan seperti komunikasi data, akses aplikasi, pertukaran informasi, penyimpanan data, serta layanan berbasis internet memerlukan jaringan yang stabil dan tersedia secara berkelanjutan agar aktivitas operasional dapat berjalan dengan baik. Oleh karena itu, pengelolaan dan pemantauan jaringan menjadi salah satu aspek penting dalam menjaga kualitas layanan teknologi informasi pada lingkungan enterprise [1].

Monitoring jaringan merupakan proses pengamatan terhadap kondisi perangkat, layanan, dan aktivitas yang terjadi pada infrastruktur jaringan secara berkelanjutan. Melalui monitoring jaringan, administrator dapat memperoleh informasi mengenai kinerja perangkat, penggunaan sumber daya, status layanan, serta berbagai kejadian yang terjadi selama sistem beroperasi. Informasi tersebut dapat digunakan untuk mendeteksi gangguan lebih awal, mengurangi waktu penanganan masalah, serta mendukung proses pengambilan keputusan dalam pengelolaan infrastruktur teknologi informasi [2].

Selain berperan dalam menjaga ketersediaan layanan, monitoring jaringan juga memiliki peran penting dalam mendukung keamanan jaringan. Setiap perangkat jaringan menghasilkan data log yang berisi catatan aktivitas dan peristiwa yang terjadi selama perangkat beroperasi. Informasi yang tersimpan dalam log dapat berupa aktivitas pengguna, perubahan konfigurasi, status layanan, hingga pesan kesalahan yang muncul pada sistem. Data log tersebut dapat dimanfaatkan sebagai sumber informasi untuk mendukung proses monitoring, analisis gangguan, dan investigasi insiden keamanan [3].

Seiring dengan bertambahnya jumlah perangkat yang terhubung ke jaringan, volume data log yang dihasilkan juga meningkat secara signifikan. Pengelolaan log yang dilakukan secara terpisah pada setiap perangkat dapat menyulitkan administrator dalam melakukan pencarian informasi dan analisis ketika terjadi gangguan pada jaringan. Kondisi tersebut mendorong kebutuhan akan sistem manajemen log terpusat yang mampu mengumpulkan, menyimpan, mengelola, dan menampilkan data log dari berbagai sumber dalam satu platform monitoring [4].

Salah satu protokol yang umum digunakan dalam pengiriman data log adalah Syslog. Syslog merupakan standar protokol yang memungkinkan berbagai perangkat jaringan mengirimkan pesan log ke server log terpusat secara otomatis. Dengan menggunakan Syslog, proses pengumpulan data log dapat dilakukan secara lebih efisien karena administrator tidak perlu melakukan pemeriksaan log secara langsung pada masing-masing perangkat. Selain itu, Syslog mendukung integrasi dengan berbagai platform monitoring dan manajemen log yang banyak digunakan pada lingkungan enterprise [5].

Graylog merupakan salah satu platform manajemen log terpusat yang menyediakan berbagai fitur untuk menerima, mengelola, mencari, dan memvisualisasikan data log. Graylog memungkinkan administrator memperoleh informasi mengenai aktivitas jaringan melalui antarmuka yang terstruktur dan mudah dipahami. Fitur pencarian log, analisis data, serta dashboard monitoring yang tersedia pada Graylog dapat membantu proses pemantauan dan identifikasi permasalahan jaringan secara lebih efektif [6].

Beberapa penelitian sebelumnya telah membahas implementasi sistem monitoring jaringan dan pengelolaan log menggunakan berbagai platform. Marwan dan Putra [7] mengimplementasikan sistem monitoring jaringan menggunakan LibreNMS dan Syslog Server untuk mendukung proses pemantauan perangkat jaringan secara terpusat. Penelitian lain yang dilakukan oleh Sukma dkk. [8] menunjukkan bahwa visualisasi data log dapat membantu administrator dalam melakukan analisis aktivitas jaringan secara lebih cepat dan informatif. Selain itu, Hadžiosmanović dkk. [9] menjelaskan bahwa data log dapat dimanfaatkan sebagai sumber informasi yang efektif untuk mendukung proses monitoring dan identifikasi aktivitas yang terjadi pada sistem.

Meskipun berbagai penelitian telah membahas monitoring jaringan dan pengelolaan log, sebagian besar penelitian masih berfokus pada monitoring perangkat atau visualisasi data log secara terpisah. Implementasi Graylog sebagai platform manajemen log terpusat yang memanfaatkan Syslog untuk monitoring aktivitas jaringan pada lingkungan enterprise masih relatif terbatas. Oleh karena itu, diperlukan implementasi sistem monitoring yang mampu mengintegrasikan proses pengumpulan, penyimpanan, pencarian, dan visualisasi data log dalam satu platform yang terpusat.

Penelitian ini bertujuan untuk menerapkan Graylog sebagai sistem monitoring aktivitas jaringan menggunakan Syslog pada lingkungan enterprise. Implementasi dilakukan dengan

membangun server monitoring berbasis Ubuntu Server yang menjalankan Graylog, OpenSearch, dan MongoDB, serta mengintegrasikan perangkat jaringan Cisco SG300-28PP sebagai sumber data log. Hasil penelitian diharapkan dapat memberikan solusi monitoring aktivitas jaringan yang terpusat, mudah diimplementasikan, dan mampu membantu administrator dalam melakukan pemantauan serta analisis aktivitas jaringan secara lebih efektif.

2. Tinjauan Literatur

Implementasi sistem monitoring aktivitas jaringan pada penelitian ini didukung oleh beberapa konsep dan teknologi yang saling berkaitan. Tinjauan literatur dilakukan untuk memahami prinsip monitoring jaringan, keamanan jaringan, pengelolaan log, serta teknologi yang digunakan dalam implementasi sistem, yaitu Syslog, Graylog, OpenSearch, MongoDB, dan Ubuntu Server. Selain itu, beberapa penelitian terdahulu juga digunakan sebagai referensi untuk mengetahui perkembangan implementasi sistem monitoring log pada lingkungan jaringan enterprise.

2.1. Monitoring Jaringan

Monitoring jaringan merupakan proses pengamatan dan pengumpulan informasi dari perangkat serta layanan jaringan untuk mengetahui kondisi operasional jaringan secara berkelanjutan. Monitoring dilakukan untuk memperoleh informasi mengenai ketersediaan layanan, performa perangkat, penggunaan sumber daya, serta aktivitas yang terjadi pada infrastruktur jaringan. Informasi tersebut dapat digunakan untuk mendeteksi gangguan lebih awal, membantu proses pemeliharaan, dan mendukung pengambilan keputusan dalam pengelolaan jaringan [10].

Pada lingkungan enterprise, monitoring jaringan menjadi semakin penting karena jumlah perangkat yang terhubung ke jaringan terus bertambah dan menghasilkan data dalam jumlah besar. Tanpa adanya mekanisme monitoring yang baik, administrator akan mengalami kesulitan dalam mengidentifikasi gangguan maupun mengetahui kondisi jaringan secara menyeluruh. Oleh karena itu, sistem monitoring yang mampu mengumpulkan dan menampilkan informasi secara terpusat menjadi salah satu kebutuhan utama dalam pengelolaan infrastruktur teknologi informasi modern [11].

Selain digunakan untuk menjaga ketersediaan layanan, monitoring jaringan juga mendukung aspek keamanan dengan menyediakan informasi mengenai aktivitas yang terjadi pada perangkat jaringan. Data yang diperoleh melalui proses monitoring dapat digunakan untuk mendeteksi anomali, mengidentifikasi potensi gangguan, serta membantu proses investigasi ketika terjadi insiden keamanan [12].

2.2 Keamanan Jaringan

Keamanan jaringan merupakan serangkaian mekanisme yang diterapkan untuk melindungi perangkat, layanan, dan data dari berbagai ancaman yang dapat mengganggu operasional sistem. Tujuan utama keamanan jaringan adalah menjaga kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) informasi yang dipertukarkan melalui jaringan komputer [13].

Ancaman terhadap jaringan dapat berasal dari berbagai sumber, seperti akses tidak sah, malware, kesalahan konfigurasi, maupun penyalahgunaan hak akses oleh pengguna. Untuk mengurangi risiko tersebut, organisasi perlu menerapkan berbagai mekanisme pengamanan, termasuk pengelolaan hak akses, segmentasi jaringan, penggunaan perangkat keamanan, serta monitoring aktivitas jaringan secara berkelanjutan [14].

Data log yang dihasilkan oleh perangkat jaringan merupakan salah satu sumber informasi penting dalam mendukung keamanan jaringan. Melalui data log, administrator dapat mengetahui aktivitas yang terjadi pada perangkat, mendeteksi kejadian yang tidak normal, serta melakukan analisis terhadap insiden keamanan yang terjadi pada sistem [15].

2.3 Log dan Manajemen Log

Log merupakan catatan aktivitas yang dihasilkan oleh sistem operasi, aplikasi, server, maupun perangkat jaringan selama proses operasional berlangsung. Informasi yang tersimpan dalam log umumnya mencakup waktu kejadian, identitas perangkat, aktivitas pengguna, status layanan, serta pesan kesalahan yang muncul pada sistem. Oleh karena itu, log sering digunakan

sebagai sumber informasi utama dalam proses monitoring, troubleshooting, dan investigasi keamanan [16].

Seiring meningkatnya jumlah perangkat dan layanan yang digunakan dalam suatu organisasi, volume data log yang dihasilkan juga mengalami peningkatan yang signifikan. Pengelolaan log secara terpisah pada setiap perangkat dapat menyebabkan proses pencarian informasi menjadi lebih sulit dan memerlukan waktu yang lebih lama. Kondisi tersebut mendorong kebutuhan akan sistem manajemen log yang mampu mengumpulkan, menyimpan, mengelola, dan menganalisis data log secara terpusat [17].

Manajemen log memberikan berbagai manfaat, seperti mempermudah pencarian informasi, meningkatkan efektivitas monitoring, mempercepat proses identifikasi masalah, serta mendukung proses audit dan investigasi keamanan. Selain itu, data log yang tersimpan secara terpusat dapat divisualisasikan dalam bentuk dashboard sehingga informasi yang dihasilkan menjadi lebih mudah dipahami oleh administrator jaringan [18].

2.4 Syslog

Syslog merupakan standar protokol yang digunakan untuk mengirimkan dan mengelola data log yang dihasilkan oleh berbagai perangkat jaringan, sistem operasi, maupun aplikasi. Protokol ini banyak digunakan dalam implementasi sistem monitoring karena mampu menyediakan mekanisme pengiriman log yang terstandarisasi dan kompatibel dengan berbagai jenis perangkat dari vendor yang berbeda [19].

Informasi yang dikirimkan melalui Syslog umumnya mencakup waktu kejadian, identitas perangkat pengirim, tingkat keparahan pesan, serta isi pesan log yang menggambarkan aktivitas atau peristiwa yang terjadi pada sistem. Informasi tersebut dapat digunakan untuk mendukung proses monitoring, analisis gangguan, serta investigasi insiden keamanan [20].

Dalam implementasinya, Syslog dapat menggunakan User Datagram Protocol (UDP) maupun Transmission Control Protocol (TCP) sebagai media transport. Penggunaan UDP lebih umum diterapkan karena memiliki kebutuhan sumber daya yang relatif rendah dan mampu mengirimkan data log secara cepat. Oleh karena itu, Syslog banyak digunakan sebagai mekanisme pengumpulan log pada lingkungan enterprise yang memiliki banyak perangkat jaringan [21].

2.5 Graylog

Graylog merupakan platform manajemen log terpusat yang digunakan untuk menerima, memproses, menyimpan, mencari, dan menganalisis data log dari berbagai sumber. Graylog dirancang untuk membantu administrator dalam mengelola data log yang berasal dari perangkat jaringan, server, aplikasi, maupun sistem keamanan melalui satu antarmuka terpusat [22].

Salah satu keunggulan Graylog adalah kemampuannya dalam melakukan pencarian data log secara cepat dan efisien. Administrator dapat melakukan pencarian berdasarkan waktu kejadian, alamat IP, perangkat pengirim, maupun kata kunci tertentu yang terdapat pada pesan log. Kemampuan ini sangat membantu dalam proses troubleshooting dan investigasi keamanan yang membutuhkan penelusuran informasi secara cepat [23].

Selain fasilitas pencarian, Graylog juga menyediakan dashboard monitoring yang memungkinkan data log divisualisasikan dalam bentuk grafik, statistik, maupun indikator tertentu. Visualisasi tersebut membantu administrator memperoleh gambaran kondisi jaringan secara lebih mudah dibandingkan dengan membaca log mentah secara langsung. Dengan kemampuan tersebut, Graylog menjadi salah satu solusi yang banyak digunakan dalam implementasi sistem monitoring dan manajemen log modern [24].

2.6 OpenSearch

OpenSearch merupakan mesin pencarian dan analisis data berbasis open source yang digunakan untuk menyimpan, mengindeks, dan melakukan pencarian data dalam jumlah besar secara efisien. Dalam sistem manajemen log, OpenSearch berperan dalam mengelola data log sehingga proses pencarian dan analisis dapat dilakukan dengan cepat meskipun jumlah data yang tersimpan terus meningkat [25].

Pada implementasi Graylog, OpenSearch berfungsi sebagai komponen penyimpanan dan pengindeksan data log. Setiap log yang diterima oleh Graylog akan diproses dan disimpan ke dalam OpenSearch sehingga dapat diakses kembali melalui fasilitas pencarian maupun visualisasi data. Dengan adanya mekanisme indexing tersebut, proses pencarian log dapat dilakukan secara lebih cepat dibandingkan penyimpanan data tanpa indeks [26].

2.7 MongoDB

MongoDB merupakan sistem manajemen basis data NoSQL yang menyimpan data dalam bentuk dokumen. Pada arsitektur Graylog, MongoDB tidak digunakan sebagai media penyimpanan utama data log, melainkan sebagai basis data yang menyimpan konfigurasi sistem dan metadata yang diperlukan oleh Graylog [27].

Informasi yang disimpan pada MongoDB meliputi konfigurasi input, pengaturan pengguna, hak akses, dashboard, stream, serta berbagai konfigurasi internal lainnya. Keberadaan MongoDB sangat penting karena mendukung pengelolaan konfigurasi yang memungkinkan Graylog beroperasi secara konsisten dan terstruktur [28].

2.8 Ubuntu Server

Ubuntu Server merupakan sistem operasi berbasis Linux yang banyak digunakan sebagai platform untuk menjalankan berbagai layanan server. Sistem operasi ini dikenal memiliki stabilitas yang baik, dukungan komunitas yang luas, serta kompatibilitas dengan berbagai aplikasi open source yang digunakan pada lingkungan enterprise [29].

Pada penelitian ini, Ubuntu Server 22.04.5 LTS digunakan sebagai platform utama untuk menjalankan Graylog, OpenSearch, dan MongoDB. Pemilihan Ubuntu Server didasarkan pada kemudahan instalasi, dukungan dokumentasi yang lengkap, serta kemampuannya dalam menjalankan layanan monitoring secara stabil untuk mendukung proses pengumpulan dan pengelolaan data log jaringan [30].

3. Metode

Penelitian ini menggunakan metode implementasi sistem untuk membangun dan menguji sistem monitoring aktivitas jaringan menggunakan Graylog dan Syslog pada lingkungan enterprise. Metode yang digunakan meliputi identifikasi kebutuhan sistem, perancangan arsitektur monitoring, instalasi dan konfigurasi perangkat lunak pendukung, integrasi perangkat jaringan sebagai sumber data log, serta pengujian terhadap fungsi-fungsi utama sistem monitoring yang telah dibangun.

Seluruh tahapan penelitian dilakukan secara bertahap untuk memastikan setiap komponen dapat terintegrasi dengan baik dan mampu mendukung proses pengumpulan, pengelolaan, pencarian, serta visualisasi data log secara terpusat.

3.1. Tahapan Penelitian

Penelitian ini dilakukan melalui beberapa tahapan yang disusun secara sistematis untuk memastikan implementasi sistem monitoring aktivitas jaringan dapat berjalan sesuai dengan tujuan yang telah ditetapkan. Tahapan penelitian dimulai dari identifikasi kebutuhan sistem, perancangan arsitektur monitoring, instalasi dan konfigurasi perangkat lunak pendukung, integrasi perangkat jaringan sebagai sumber log, hingga pengujian dan analisis hasil implementasi.

Tahap identifikasi kebutuhan dilakukan untuk menentukan perangkat keras, perangkat lunak, serta kebutuhan jaringan yang diperlukan dalam pembangunan sistem monitoring. Pada tahap ini dilakukan analisis terhadap infrastruktur yang digunakan, termasuk spesifikasi server monitoring dan perangkat jaringan yang akan menjadi sumber data log.

Tahap berikutnya adalah perancangan sistem monitoring yang mencakup perancangan arsitektur komunikasi antara perangkat jaringan, Graylog, OpenSearch, dan MongoDB. Perancangan dilakukan untuk memastikan seluruh komponen dapat saling terintegrasi dalam proses pengumpulan, penyimpanan, pencarian, dan visualisasi data log.

Setelah perancangan selesai, dilakukan instalasi dan konfigurasi Graylog, OpenSearch, dan MongoDB pada server Ubuntu Server 22.04 LTS. Selanjutnya dilakukan konfigurasi Syslog pada perangkat Cisco SG300-28PP agar perangkat dapat mengirimkan data log menuju server Graylog menggunakan protokol Syslog UDP.

Tahap pengujian dilakukan untuk memastikan log dari perangkat jaringan dapat diterima, disimpan, dicari, dan ditampilkan pada dashboard monitoring Graylog. Hasil pengujian kemudian dianalisis untuk mengevaluasi keberhasilan implementasi sistem monitoring aktivitas jaringan yang dibangun.

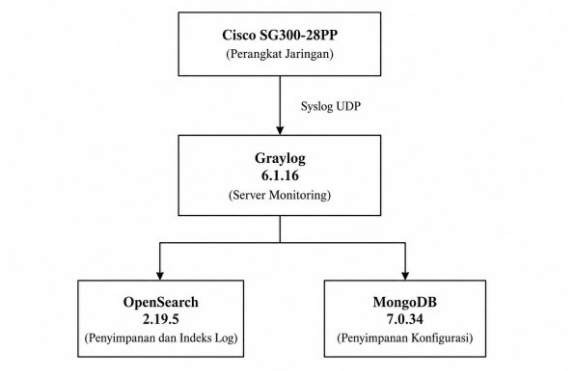
3.2. Arsitektur Sistem

Sistem monitoring aktivitas jaringan yang diimplementasikan pada penelitian ini menggunakan arsitektur log terpusat (centralized log management) dengan memanfaatkan Graylog sebagai platform utama pengelolaan log. Arsitektur sistem dirancang untuk mengumpulkan, menyimpan, mengelola, dan menampilkan data log yang berasal dari perangkat jaringan secara terpusat sehingga proses monitoring dapat dilakukan dengan lebih efektif.

Perangkat jaringan yang digunakan pada penelitian ini adalah Cisco SG300-28PP yang berfungsi sebagai sumber data log. Perangkat tersebut dikonfigurasi untuk mengirimkan pesan log menggunakan protokol Syslog UDP menuju server monitoring. Data log yang dikirim kemudian diterima dan diproses oleh Graylog sebagai platform manajemen log.

Dalam implementasinya, Graylog terintegrasi dengan OpenSearch dan MongoDB sebagai komponen pendukung utama. OpenSearch digunakan sebagai mesin indeks dan pencarian data log sehingga proses penyimpanan dan pencarian informasi dapat dilakukan secara cepat dan efisien. Sementara itu, MongoDB berfungsi sebagai basis data yang menyimpan konfigurasi sistem, metadata, informasi pengguna, serta pengaturan internal yang dibutuhkan oleh Graylog.

Melalui integrasi ketiga komponen tersebut, seluruh aktivitas yang tercatat pada perangkat jaringan dapat dikumpulkan dan disajikan dalam satu antarmuka monitoring yang terpusat. Arsitektur sistem monitoring yang digunakan pada penelitian ini ditunjukkan pada Gambar 1.



Gambar 1. Arsitektur Sistem Monitoring Aktivitas Jaringan Menggunakan Graylog dan Syslog

3.3. Perangkat dan Perangkat Lunak

Implementasi sistem monitoring aktivitas jaringan pada penelitian ini menggunakan kombinasi perangkat keras dan perangkat lunak yang saling terintegrasi. Perangkat keras yang digunakan terdiri atas satu unit switch Cisco SG300-28PP sebagai sumber data log dan satu server monitoring yang menjalankan layanan Graylog, OpenSearch, dan MongoDB.

Adapun perangkat lunak yang digunakan meliputi Ubuntu Server 22.04.5 LTS sebagai sistem operasi server, Graylog 6.1.16 sebagai platform manajemen log, OpenSearch 2.19.5 sebagai mesin indeks dan pencarian data log, serta MongoDB 7.0.34 sebagai basis data konfigurasi Graylog. Seluruh perangkat lunak tersebut diinstal dan dikonfigurasi pada server monitoring sehingga dapat mendukung proses pengumpulan dan pengelolaan data log secara terpusat.

Spesifikasi perangkat dan perangkat lunak yang digunakan pada penelitian ini ditunjukkan pada Tabel 1.

Pada bagian ini, penulis perlu menjelaskan perangkat keras dan perangkat lunak yang digunakan, sumber dataset, analisis data awal, hasil, dan analisis/pembahasan hasil. Sangat disarankan untuk menyajikan hasil dengan gambar, grafik, dan tabel. Rumus atau alat ukur evaluasi juga perlu disertakan di sini. Harus ada pembahasan/analisis, dan Anda tidak bisa hanya menulis ulang hasil dalam bentuk kalimat, tetapi Anda perlu memberikan penjelasan tentang hubungannya dengan hipotesis awal. Selain itu, bagian ini perlu membahas dan menguraikan temuan-temuan penting.

Tabel 1. Perangkat Keras dan Perangkat Lunak yang Digunakan pada Penelitian

Komponen	Spesifikasi

Perangkat Jaringan	Cisco SG300-28PP Managed Switch
Sistem Operasi	Ubuntu Server 22.04.5 LTS
Log Management	Graylog 6.1.16
Search Engine	OpenSearch 2.19.5
Database	MongoDB 7.0.34
Protokol Log	Syslog UDP

Berdasarkan Tabel 1, sistem monitoring dibangun menggunakan kombinasi perangkat keras dan perangkat lunak yang mendukung proses pengumpulan, penyimpanan, pengindeksan, dan visualisasi data log secara terpusat. Integrasi antara Graylog, OpenSearch, dan MongoDB memungkinkan sistem monitoring beroperasi secara optimal dalam mendukung pemantauan aktivitas jaringan pada lingkungan enterprise.

3.4. Implementasi Sistem

Implementasi sistem monitoring dilakukan dengan menginstal dan mengonfigurasi Graylog, OpenSearch, dan MongoDB pada server yang menggunakan sistem operasi Ubuntu Server 22.04.5 LTS. Graylog berfungsi sebagai platform utama untuk menerima, mengelola, dan menampilkan data log, sedangkan OpenSearch digunakan sebagai mesin indeks dan pencarian data log. MongoDB digunakan untuk menyimpan konfigurasi sistem dan metadata yang dibutuhkan oleh Graylog.

Setelah seluruh layanan berhasil dijalankan, dilakukan konfigurasi input Syslog UDP pada Graylog untuk menerima data log dari perangkat jaringan. Selanjutnya, perangkat Cisco SG300-28PP dikonfigurasi agar mengirimkan log secara otomatis menuju server monitoring menggunakan protokol Syslog UDP.

Data log yang diterima oleh Graylog kemudian diproses dan disimpan ke dalam OpenSearch sehingga dapat dicari dan dianalisis melalui antarmuka Graylog. Implementasi ini memungkinkan seluruh aktivitas yang tercatat pada perangkat jaringan dikumpulkan secara terpusat sehingga memudahkan proses monitoring dan analisis aktivitas jaringan.

3.5. Pengujian Sistem

Pengujian sistem dilakukan untuk memastikan bahwa seluruh komponen yang terlibat dalam sistem monitoring dapat berfungsi sesuai dengan tujuan penelitian. Pengujian difokuskan pada kemampuan sistem dalam menerima data log dari perangkat jaringan, menampilkan log pada antarmuka Graylog, melakukan pencarian data log, menampilkan dashboard monitoring, serta memastikan layanan pendukung dapat berjalan dengan baik.

Metode pengujian yang digunakan adalah pengujian fungsional (functional testing), yaitu dengan memverifikasi setiap fungsi utama sistem berdasarkan skenario yang telah ditentukan. Hasil pengujian kemudian dianalisis untuk mengetahui tingkat keberhasilan implementasi sistem monitoring aktivitas jaringan menggunakan Graylog dan Syslog pada lingkungan enterprise.

4. Hasil dan Pembahasan

Bagian ini menyajikan hasil implementasi sistem monitoring aktivitas jaringan menggunakan Graylog dan Syslog pada lingkungan enterprise. Sistem yang dibangun bertujuan untuk mengumpulkan, mengelola, dan memvisualisasikan data log yang berasal dari perangkat jaringan secara terpusat. Hasil implementasi dievaluasi berdasarkan kemampuan sistem dalam menerima log, melakukan pencarian data log, menampilkan informasi monitoring, serta mendukung proses pengawasan aktivitas jaringan secara lebih efektif.

4.1. Implementasi Sistem Monitoring

Implementasi sistem monitoring diawali dengan instalasi dan konfigurasi Graylog, OpenSearch, dan MongoDB pada server monitoring berbasis Ubuntu Server 22.04.5 LTS. Setelah seluruh layanan berjalan dengan baik, dilakukan pembuatan input Syslog UDP pada Graylog sebagai mekanisme penerimaan data log dari perangkat jaringan.

Perangkat Cisco SG300-28PP kemudian dikonfigurasi untuk mengirimkan data log menuju server monitoring menggunakan protokol Syslog UDP. Konfigurasi tersebut

memungkinkan Graylog menerima seluruh aktivitas yang direkam oleh perangkat jaringan secara otomatis dan terpusat.

Gambar 2 menunjukkan bahwa input Syslog UDP berhasil dibuat dan berada dalam kondisi aktif sehingga sistem siap menerima data log yang dikirimkan oleh perangkat jaringan.

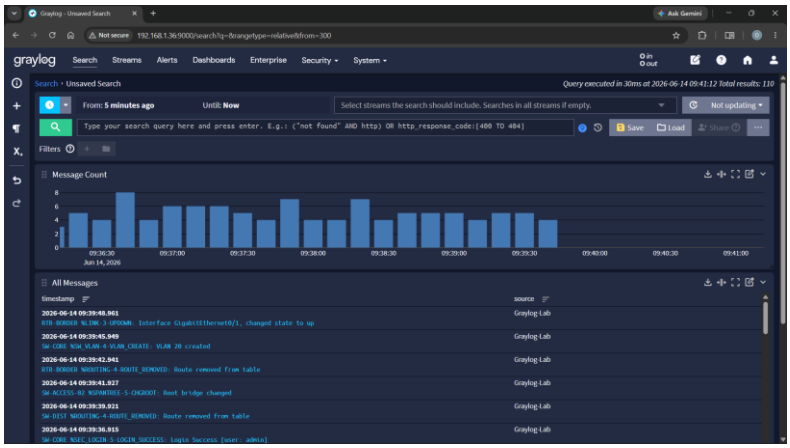
Gambar 2. Konfigurasi dan Status Input Syslog pada Graylog

4.2 Penerimaan Data Log

Setelah konfigurasi Syslog selesai dilakukan, perangkat jaringan mulai mengirimkan data log ke server monitoring. Graylog berhasil menerima dan menampilkan data log yang berasal dari perangkat Cisco SG300-28PP secara real-time. Informasi yang diterima meliputi waktu kejadian, alamat IP sumber, identitas perangkat, serta pesan aktivitas yang dicatat oleh perangkat jaringan.

Data log yang diterima selanjutnya diproses dan disimpan sehingga dapat digunakan untuk kebutuhan monitoring maupun analisis aktivitas jaringan.

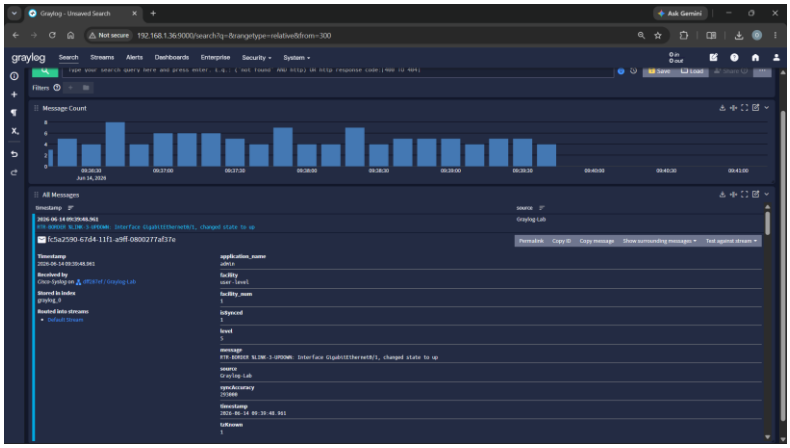
Gambar 3 memperlihatkan data log yang berhasil diterima oleh Graylog dari perangkat jaringan yang telah dikonfigurasi.



Gambar 3. Data Log Perangkat Jaringan yang Berhasil Diterima oleh Graylog

Selain menampilkan daftar log, Graylog juga menyediakan informasi yang lebih rinci mengenai setiap pesan yang diterima. Informasi tersebut mencakup waktu kejadian, sumber log, alamat IP perangkat, serta isi pesan yang dikirimkan oleh perangkat jaringan.

Fasilitas ini membantu administrator dalam melakukan analisis terhadap aktivitas yang terjadi pada jaringan serta mempermudah proses identifikasi ketika ditemukan kondisi yang memerlukan perhatian lebih lanjut. Detail informasi log yang diterima oleh Graylog ditunjukkan pada Gambar 4.



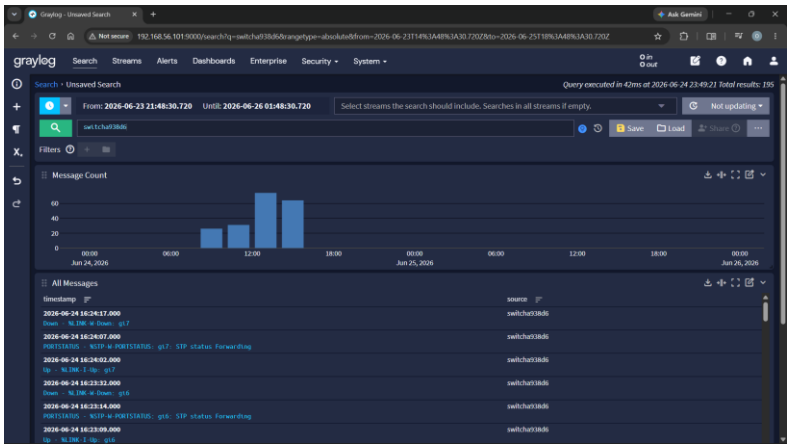
Gambar 4. Detail Informasi Pesan Log pada Graylog

4.3. Pencarian Data Log

Salah satu fitur utama yang disediakan oleh Graylog adalah kemampuan pencarian data log secara cepat dan terpusat. Fitur ini memungkinkan administrator jaringan untuk menemukan informasi tertentu berdasarkan kata kunci, alamat IP, sumber log, maupun rentang waktu tertentu. Kemampuan pencarian tersebut sangat penting dalam proses monitoring dan analisis aktivitas jaringan karena jumlah log yang tersimpan dapat terus bertambah seiring waktu.

Pada implementasi yang dilakukan, data log yang telah diterima dan disimpan oleh sistem dapat dicari melalui antarmuka Graylog menggunakan berbagai parameter pencarian. Hasil pencarian ditampilkan secara langsung sehingga administrator dapat memperoleh informasi yang dibutuhkan tanpa harus melakukan pemeriksaan pada setiap perangkat jaringan secara manual.

Kemampuan pencarian ini membantu mempercepat proses identifikasi aktivitas jaringan, penelusuran kejadian tertentu, serta investigasi terhadap kondisi yang dianggap tidak normal. Hasil pencarian data log pada Graylog ditunjukkan pada Gambar 5.



Gambar 5. Pencarian Data Log Menggunakan Fitur Search pada Graylog

4.4. Dashboard Monitoring

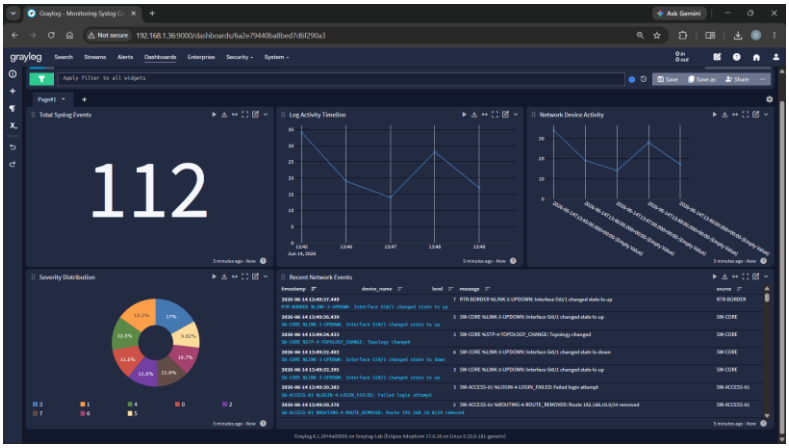
Selain menyediakan fasilitas pengelolaan dan pencarian log, Graylog juga mendukung visualisasi data melalui dashboard monitoring. Dashboard digunakan untuk menyajikan informasi yang berasal dari data log dalam bentuk yang lebih mudah dipahami sehingga administrator dapat memperoleh gambaran kondisi jaringan secara cepat.

Dashboard yang dibangun pada penelitian ini menampilkan informasi monitoring berdasarkan data log yang diterima dari perangkat jaringan. Informasi tersebut dapat berupa jumlah log yang diterima, aktivitas perangkat, distribusi pesan log, maupun indikator lainnya yang mendukung proses pengawasan jaringan.

Melalui dashboard monitoring, administrator tidak perlu melakukan analisis terhadap log mentah secara langsung karena informasi telah disajikan dalam bentuk visual yang lebih

informatif. Hal ini membantu meningkatkan efisiensi proses monitoring serta mempercepat pengambilan keputusan ketika ditemukan aktivitas yang memerlukan perhatian lebih lanjut.

Dashboard monitoring yang berhasil dibangun menggunakan Graylog ditunjukkan pada Gambar 6.



Gambar 6. Dashboard Monitoring Aktivitas Jaringan pada Graylog

4.5. Hasil Pengujian Sistem

Setelah seluruh proses implementasi selesai dilakukan, pengujian sistem dilakukan untuk memastikan bahwa setiap fungsi utama dapat berjalan sesuai dengan tujuan penelitian. Pengujian difokuskan pada kemampuan sistem dalam menerima log dari perangkat jaringan, melakukan pencarian data log, menampilkan dashboard monitoring, menerima data melalui input Syslog, serta memastikan layanan pendukung dapat beroperasi dengan baik.

Hasil pengujian menunjukkan bahwa seluruh fungsi utama sistem berhasil dijalankan tanpa kendala. Ringkasan hasil pengujian sistem ditunjukkan pada Tabel 2.

Tabel 2. Hasil Pengujian Sistem Monitoring Aktivitas Jaringan

No	Skenario Pengujian	Hasil Pengujian	Status
1	Penerimaan log dari perangkat jaringan	Log berhasil diterima oleh Graylog	Berhasil
2	Pencarian data log	Data log dapat dicari dan ditampilkan	Berhasil
3	Dashboard monitoring	Dashboard dapat menampilkan visualisasi log	Berhasil
4	Input Syslog UDP	Input berjalan dan menerima data log	Berhasil
5	Layanan Graylog, OpenSearch, dan MongoDB	Seluruh layanan berjalan normal	Berhasil

Setelah Berdasarkan hasil pengujian yang telah dilakukan, seluruh fungsi utama sistem monitoring berhasil beroperasi sesuai dengan kebutuhan yang telah ditetapkan. Sistem mampu menerima, menyimpan, mengelola, dan menampilkan data log secara terpusat melalui Graylog. Selain itu, fitur pencarian log dan dashboard monitoring dapat digunakan dengan baik untuk mendukung proses pemantauan aktivitas jaringan.

Hasil tersebut menunjukkan bahwa penerapan Graylog sebagai sistem monitoring aktivitas jaringan menggunakan Syslog dapat diimplementasikan dengan baik pada lingkungan enterprise. Sistem yang dibangun mampu membantu administrator dalam melakukan pengawasan aktivitas jaringan secara lebih efektif melalui pengelolaan log yang terpusat dan penyajian informasi yang lebih mudah dipahami.

5. Perbandingan

Beberapa penelitian sebelumnya telah memanfaatkan sistem manajemen log untuk mendukung kegiatan monitoring jaringan dan keamanan informasi. Namun, sebagian besar penelitian berfokus pada implementasi log management pada lingkungan server, analisis

keamanan, maupun integrasi dengan berbagai sumber data log. Penelitian ini berfokus pada implementasi Graylog sebagai sistem monitoring aktivitas jaringan menggunakan Syslog pada lingkungan enterprise dengan memanfaatkan perangkat jaringan Cisco sebagai sumber data log.

Perbandingan penelitian ini dengan penelitian terdahulu disajikan pada Tabel 3.

Tabel 3. Perbandingan Penelitian Terdahulu dan Penelitian yang Diusulkan

Penelitian	Platform	Sumber Log	Fokus Penelitian
Marwan & Putra (2023) [17]	LibreNMS dan Syslog Server	Router, switch, access point, dan server	Implementasi monitoring jaringan dan Syslog Server mampu menyediakan pemantauan perangkat serta riwayat log secara terpusat.
Putra et al. (2024) [18]	LibreNMS	Infrastruktur jaringan organisasi	Sistem monitoring berhasil menampilkan kondisi perangkat jaringan dan mempermudah pemantauan kinerja jaringan.
Efendy & Mizanul (2022) [19]	LibreNMS	Perangkat jaringan perusahaan	Implementasi monitoring membantu administrator dalam mendeteksi gangguan dan melakukan troubleshooting jaringan secara lebih cepat.
Penelitian Ini	Graylog	Cisco SG300-28PP	Monitoring aktivitas jaringan menggunakan Syslog pada lingkungan enterprise

Berdasarkan Tabel 3, penelitian yang dilakukan memiliki kesamaan dengan penelitian terdahulu dalam penggunaan Graylog sebagai platform manajemen log. Perbedaannya terletak pada fokus implementasi yang secara khusus memanfaatkan perangkat jaringan Cisco sebagai sumber data log dan menerapkan Syslog sebagai mekanisme pengiriman data menuju sistem monitoring.

Selain itu, penelitian ini tidak hanya menampilkan proses penerimaan log, tetapi juga menunjukkan implementasi pencarian data log dan visualisasi dashboard monitoring yang mendukung proses pengawasan aktivitas jaringan secara terpusat. Hasil implementasi menunjukkan bahwa Graylog dapat digunakan sebagai solusi monitoring aktivitas jaringan yang efektif pada lingkungan enterprise dengan kebutuhan infrastruktur yang relatif sederhana.

6. Kesimpulan

Penelitian ini berhasil mengimplementasikan Graylog sebagai sistem monitoring aktivitas jaringan menggunakan Syslog pada lingkungan enterprise. Sistem yang dibangun mampu menerima, menyimpan, mengelola, dan menampilkan data log yang berasal dari perangkat jaringan Cisco SG300-28PP secara terpusat. Integrasi antara Graylog, OpenSearch, dan

MongoDB memungkinkan proses pengelolaan log dilakukan dengan lebih efektif serta mendukung pencarian data log secara cepat dan efisien.

Hasil pengujian menunjukkan bahwa seluruh fungsi utama sistem dapat berjalan dengan baik, meliputi penerimaan log melalui Syslog UDP, penyimpanan dan pengindeksan data log, pencarian informasi log, serta visualisasi data melalui dashboard monitoring. Implementasi yang dilakukan mampu membantu administrator jaringan dalam melakukan pemantauan aktivitas perangkat secara lebih terstruktur dibandingkan dengan pemeriksaan log secara langsung pada masing-masing perangkat.

Penerapan Graylog sebagai platform manajemen log terpusat memberikan kemudahan dalam proses monitoring aktivitas jaringan karena seluruh informasi dapat diakses melalui satu antarmuka monitoring. Dengan demikian, sistem yang dibangun dapat menjadi salah satu solusi yang efektif untuk mendukung pengelolaan dan pengawasan aktivitas jaringan pada lingkungan enterprise.

Penelitian ini masih memiliki keterbatasan karena hanya menggunakan satu perangkat jaringan sebagai sumber data log. Oleh karena itu, penelitian selanjutnya dapat dilakukan dengan menambahkan lebih banyak perangkat jaringan, server, firewall, maupun perangkat keamanan lainnya sehingga cakupan monitoring menjadi lebih luas. Selain itu, pengembangan fitur alerting dan integrasi dengan sistem Security Information and Event Management (SIEM) dapat dilakukan untuk meningkatkan kemampuan deteksi dan respons terhadap potensi ancaman keamanan jaringan.

Kontribusi Penulis: Konseptualisasi, metodologi, implementasi sistem, pengumpulan data, analisis data, serta penulisan naskah dilakukan oleh penulis utama. Proses supervisi, validasi, dan peninjauan naskah dilakukan oleh dosen pembimbing.

Pendanaan: Penelitian ini tidak menerima pendanaan eksternal.

Pernyataan Ketersediaan Data: Data yang digunakan dalam penelitian ini berupa data log yang dihasilkan selama proses implementasi sistem monitoring aktivitas jaringan. Data tersedia dari penulis korespondensi berdasarkan permintaan yang wajar dengan tetap memperhatikan kebijakan keamanan informasi organisasi.

Ucapan Terima Kasih: Penulis mengucapkan terima kasih kepada PT Pupuk Sriwidjaja Palembang atas kesempatan yang diberikan untuk melaksanakan kegiatan magang dan penelitian. Penulis juga mengucapkan terima kasih kepada Program Studi Teknik Informatika Universitas Bina Darma serta seluruh pihak yang telah memberikan dukungan selama pelaksanaan penelitian dan penyusunan artikel ini.

Konflik Kepentingan: Penulis menyatakan tidak ada konflik kepentingan terkait penelitian dan publikasi artikel ini.

Referensi

[1] He, S., He, P., Chen, Z., Yang, T., Su, Y., & Lyu, M. R., "A Survey on Automated Log Analysis for Reliability Engineering", ACM Computing Surveys, vol. 54, no. 6, pp. 1–37, 2021. DOI: 10.1145/3460345
[2] Cândido, J. B., Aniche, M., & van Deursen, A., "Log-Based Software Monitoring: A Systematic Mapping Study", Information and Software Technology, vol. 136, 2021. DOI: 10.1016/j.infsof.2021.106602
[3] Makanju, A., Zincir-Heywood, A. N., & Milios, E. E., "Clustering Event Logs Using Iterative Partitioning", KDD Workshop on Mining Complex Data, 2009.
[4] Gerhards, R., "The Syslog Protocol", RFC 5424, Internet Engineering Task Force (IETF), Mar. 2009.
[5] Lonvick, C., "The BSD Syslog Protocol," RFC 3164, IETF, Aug. 2001.
[6] Liang, C., Benson, T., Kanuparthy, P., & He, Y., "Log-Prophet: Using Syslogs for Data Center Management," IEEE/IFIP NOMS, 2016. DOI: 10.1109/NOMS.2016.7502861
[7] Clemm, A., "Network Management Fundamentals," IEEE Communications Magazine.
[8] Boutaba, R., Salahuddin, M. A., Limam, N., Ayoubi, S., Shahriar, N., Estrada-Solano, F., & Caicedo, O. M., "A Comprehensive Survey on Machine Learning for Networking," IEEE Communications Surveys & Tutorials, 2018. DOI: 10.1109/COMST.2018.2849799
[9] Kent, K., & Souppaya, M., "Guide to Computer Security Log Management," NIST Special Publication 800-92.
[10] Scarfone, K., & Mell, P., "Guide to Intrusion Detection and Prevention Systems," NIST SP 800-94.
[11] Gormley, C., & Tong, Z., "Elasticsearch: The Definitive Guide," O'Reilly Media.
[12] OpenSearch Project Team, "OpenSearch Documentation and Architecture,"
[13] Marwan & Putra, "Perancangan Network Monitoring System (NMS) dan Syslog Server Menggunakan LibreNMS pada PT. Maxindo Mitra Solusi," Journal of Applied Multimedia and Networking, 2023. DOI: 10.30871/jamn.v7i2.6684

[14] Putra, Rosid, Setiawan, & Eviyanti, "Implementasi Sistem Monitoring Jaringan Menggunakan LibreNMS pada Kecamatan Tarik," Indonesian Journal of Applied Technology, 2024. DOI: 10.47134/ijat.v1i1.2119
[15] Efendy & Mizanul, "Implementasi Sistem Monitoring dan Backup Konfigurasi Perangkat Jaringan Menggunakan LibreNMS," Smart Comp, 2022. DOI: 10.30591/smartcomp.v11i4.4253