1. PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi digital yang semakin meningkat telah memberikan dampak besar terhadap berbagai aspek kehidupan manusia dan menyebabkan perubahan dalam cara masyarakat dan organisasi berkomunikasi, berbisnis, dan mengakses informasi. Penggunaan platform digital seperti website banyak dimanfaatkan sebagai platform e-*commerce*, personal web maupun sistem informasi untuk perusahaan. Dalam lingkungan perusahaan, website biasanya menyimpan data-data penting pengguna seperti, nomor KTP, alamat, nomor handphone, dan data penting lainnya. Data-data tersebut merupakan informasi sensitif dan dapat berbahaya jika tidak disimpan dengan baik. Maka dari itu menjaga keamanan merupakan faktor yang penting untuk mencegah serangan siber seperti *hacker* dan *malware* yang dapat menyebabkan kebocoran data dan merusak reputasi bisnis.

Universitas Kristen Petra sebagai institusi perguruan tinggi mempunyai infrastruktur jaringan yang kompleks dan memiliki banyak web server yang digunakan oleh banyak mahasiswa, staf, dan dosen. Maka dari itu menjaga keamanan data dari serangan siber sangatlah penting. Universitas Kristen Petra telah mengimplementasikan firewall yang digunakan untuk melindungi sistem dan jaringan dari serangan siber. *Firewall* kemudian menghasilkan sebuah log dimana terdapat berbagai informasi terkait aktivitas jaringan seperti informasi ip tujuan, ip sumber, *port* dan protokol, aksi *firewall* seperti *allowed* atau *blocked*, jenis serangan, tingkat ancaman, dll secara *real-time*. Meskipun *firewall* menyediakan informasi secara *real-time,* kebutuhan menganalisa keamanan untuk mencari informasi serangan yang terjadi sebelumnya masih sulit dilakukan. Hal ini dikarenakan volume data yang sangat banyak sehingga tim keamanan kesulitan untuk melakukan analisa dan merespons ancaman dengan cepat. Seperti yang terjadi di Pusat Pengembangan Sistem Informasi Universitas Kristen Petra dimana server terkena serangan DDoS dan *Malware* atau *trojan* tetapi tidak dapat direspons secara langsung yang menyebabkan server lemot hingga terputus. Maka dari itu diperlukan notifikasi untuk memberikan peringatan kepada masing-masing korban mengenai serangan yang terjadi pada servernya agar dapat direspon dengan cepat.

Selain itu, Setiap minggunya, *firewall* memberikan laporan keamanan yang merupakan hasil analisa jaringan yang memberikan informasi tentang server yang paling banyak diserang, server yang rentan, dan masih banyak lagi. Data ini dapat dimanfaatkan untuk menghasilkan pemahaman yang lebih dalam tentang serangan dan kerentanan dengan mengIntegrasi data laporan dengan data *real-time*. Dengan melakukan kombinasi data dapat menambah pengetahuan untuk melakukan deteksi yang lebih akurat. Data historis merupakan data format file PDF dimana bermanfaat untuk

menganalisis serangan yang berulang sehingga dapat membantu tim keamanan untuk mengenali ancaman yang sudah terjadi. Sedangkan data *real-time* adalah data yang didapat dari sistem *monitoring* dimana digunakan untuk memberikan informasi tentang ancaman yang sedang terjadi. Dengan memanfaatkan dua data ini, sistem keamanan dapat meningkatkan deteksi dini dan merespons ancaman dengan lebih cepat dan tepat dari informasi yang telah diperoleh.

Dengan teknologi AI yang semakin berkembang, program LLM atau Bahasa Besar semakin banyak digunakan dalam berbagai aplikasi. Teknologi LLM mampu mengenali dan menghasilkan teks, serta memproses bahasa dan dapat berinteraksi dan berkomunikasi dengan pengguna (Sari, 2024). LLM dapat digunakan sebagai AI Generatif untuk menghasilkan *output* berdasarkan perintah *input* dalam bahasa manusia. Dalam ruang lingkup *cybersecurity*, LLM dapat digunakan untuk mendapatkan informasi tentang praktik keamanan siber yang baik secara umum dan memberikan kemudahan serta efektifitas pada tim keamanan dalam operasi keamanan siber (Rahmani, 2024). Contoh Teknologi model bahasa besar (LLM) adalah ChatGPT dan Llama . ChatGPT adalah chatbot yang yang dapat meregenerasi *text* yang dapat meniru bahasa manusia, memahami konteks serta mempunyai ingatan dari *user input*. Akan tetapi ChatGPT dapat menghasilkan respons yang bias atau tidak masuk akal karena mempunyai keterbatasan dalam dataset (Hou & Lian, 2024). Sedangkan Llama adalah LLM open source dimana dibuat khususnya untuk di *custom* sesuai dengan kebutuhan (Hillier, 2023). Akan tetapi tanpa adanya dataset tambahan, Llama juga tidak dapat menghasilkan *output* yang benar. Maka dari itu, untuk mengatasi permasalahan ini RAG digunakan dengan LLM untuk menambah pengetahuan dari berbagai dokumen seperti pdf, teks, html, dll (Bogale et al., 2024).

Retrieval-Augmented Generation (RAG) merupakan model bahasa besar / *large language models* (LLM) yang dilengkapi dengan data dari pengetahuan eksternal seperti halaman web perusahaan atau dokumen kebijakan SDM untuk menghasilkan *output* yang akurat dan terkini. Konsep model RAG ini dibangun dengan mengintegrasikan dua komponen NLP: *Information Retrieval* (IR) dan *Natural Language Generation* (NLG) yang mengkombinasikan metode *retrieval* dengan model generatif yang besar untuk menghasilkan respons yang relevan (Khan et al., 2024). Agen RAG dirancang untuk mengambil data dari berbagai sumber, termasuk database terstruktur dan teks tidak terstruktur seperti berita dan postingan media sosial (Afolabi, 2024). RAG dapat membantu model untuk memberikan *output* yang relevan, informatif dan akurat (Bogale et al., 2024). Laporan PDF dari firewall sangfor dapat digunakan dengan menggunakan RAG untuk mendapatkan hasil output yang sesuai.

Ada beberapa metode generative lainya seperti GPT, BERT, atau T5 yang dilatih dari dataset yang besar tetapi mempunyai pengetahuan yang tetap dan mereka hanya dapat menghasilkan

jawaban berdasarkan yang mereka tahu (Khan et al., 2024). Hal ini menjadi kekurangan dari metode-metode tersebut karena, informasi dapat berubah dengan cepat dan memberikan respons yang benar dan akurat sangat dibutuhkan. Seperti pada penelitian yang dilakukan oleh Bhusal et al di tahun 2024 dimana penelitian ini mempunyai fokus masalah pada keterbatasan model *Large Language Models* (LLMs) dalam topik keamanan siber untuk memberikan informasi yang akurat. Penelitian ini menunjukan bahwa LLM masih memiliki keterbatasan wawasan karena masih bergantung pada dataset tertentu. Penelitian lain yang dilakukan oleh Lempinen et al. mengembangkan chatbot yang diintegrasi dengan Wazuh dan menggunakan model GPT 3.5 dimana digunakan untuk membantu pengguna dalam menganalisa log data. Chatbot yang dikembangkan dapat digunakan untuk memblok IP address, merestart Wazuh Agent. Akan tetapi, pada penelitian ini dijelaskan bahwa *fine-tuning* GPT-3.5 tidak memungkinkan, sehingga hasil yang dikeluarkan dari model ini tidak dapat spesifik.

Ahsan melakukan penelitian dengan mengembangkan sistem chatbot menggunakan model LLM *open-source* dan RAG yaitu Falcon-7B dan Llama-2-7b yang di *tuning* dengan data spesifik seperti data OWASP dan NDV. Chatbot ini berhasil digunakan sebagai alat untuk edukasi dalam keamanan siber, tetapi metode yang digunakan masih mempunyai keterbatasan pengetahuan karena kapasitasnya yang rendah. Pada skripsi ini akan dilakukan pengembangan dashboard sistem alert yang dapat memberikan peringatan otomatis kepada admin server yang terkena serangan dan chatbot untuk memudahkan melakukan analisa keamanan dengan memanfaatkan data firewall dimana akan digunakan oleh admin server Universitas Kristen Petra. Model LLM Llama 3.2 dan model Generative RAG digunakan Untuk mendukung pengembangan sistem chatbot dalam menghasilkan *output* yang lebih spesifik menggunakan data PDF yang diperoleh dari *firewall*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang ada, dapat dirumuskan beberapa permasalahan berikut :

1. Bagaimana teknologi *Large Language Models* (LLM) dengan pendekatan *Retrieval-Augmented Generation* (RAG) dapat menghasilkan *output* yang sesuai dari laporan keamanan PDF?
2. Bagaimana sistem *alert* dapat meningkatkan efisiensi dalam merespons ancaman?

1.3 Tujuan

Mengembangkan dashboard sistem *alert* yang dapat memberikan notifikasi kepada server admin Universitas Kristen Petra tentang ancaman yang terjadi serta sistem *chatbot* yang menggunakan model LLM llama dan RAG untuk analisa hasil laporan *firewall* dalam PDF. Sistem ini

bertujuan untuk memberikan kemudahan bagi administrator jaringan dan admin server Universitas Kristen Petra dalam mendeteksi dan merespons ancaman siber.

1.4 Ruang Lingkup

Keseluruhan pengerjaan akan dibatasi pada :

1. Sistem *chatbot* hanya menjawab pertanyaan-pertanyaan mengenai hasil analisis server Universitas Kristen Petra
2. Sistem *chatbot* dikembangkan untuk menjawab pertanyaan dari user bukan untuk merekomendasi
3. Menggunakan *Swarm* sebagai *framework multi-agen*
4. Base model LMM yang digunakan adalah Ollama LLama 3.2
5. Menggunakan metode *Retrieval Augmentation Generation (RAG)* untuk analisa data eksternal
6. Data yang digunakan:
    a. Data Historis : data laporan mingguan sangfor
    b. Data Real-time : data log *firewall* yang disimpan pada PostgreSQL
7. Tampilan *chatbot* menggunakan *framework streamlit*
8. *Input* sistem *chatbot* berupa pertanyaan seputar informasi kerentanan dan ancaman siber
9. *Output* sistem *chatbot* berupa kalimat bahasa indonesia seputar analisa dari data pdf sangfor serta dapat berupa statistik
10. Pengujian terhadap hasil respons sistem *chatbot* dilakukan dengan evaluasi akurasi, presisi dan *latency*
11. Sistem *alert* mengirimkan *alert* ke admin melalui whatsapp
12. User hanya dapat melihat analisa server yang sesuai

1.5 Metodologi Penelitian

1. Studi Literatur
    a. Studi tentang *Large Language Model* (LLM) Llama 3.2
    b. Studi tentang *Retrieval-Augmented Generation* (RAG)
    c. Studi tentang *multi agent swarm*
    d. Sistem *alert security* UKP
    e. Studi tentang *chatbot*
2. Perencanaan Model
    a. Server untuk menjalankan model

b. Database untuk penyimpanan data historis
c. Sistem *monitoring real-time*
d. Menentukan alur *chatbot*
e. Menentukan alur sistem *alert*

3. Pengumpulan Data
    a. Pengumpulan data historis atau laporan keamanan mingguan dalam file PDF
    b. Pengumpulan data log *real-time* di database PostgreSQL
4. Pengembangan Sistem
    a. Pembuatan dashboard login untuk user dan admin
    b. Pembuatan dashboard Sistem *Alert* dan *profiling* server
    c. Pembuatan sistem notifikasi melalui email
    d. Mengembangkan sistem *Chatbot* dengan data historis dan *real-time*
    e. Pembuatan dashboard *chatbot*
5. Pengujian dan Analisis
    a. Proses pengujian hasil respons dengan metriks akurasi, presisi dan *latency*
6. Pengambilan Kesimpulan
    a. Pengambilan kesimpulan dari hasil pengerjaan yang dilakukan
7. Pembuatan Laporan
    a. Pembuatan laporan dari hasil yang diperoleh

1.6 Manfaat

Manfaat dari penelitian ini yaitu, menghasilkan sistem *alert* yang memberikan peringatan otomatis kepada admin serta memberikan informasi hasil analisa dari kombinasi data *real-time* dan data history pada jaringan UK Petra. Sistem alert juga memanfaatkan kombinasi data untuk sistem chatbot yang dapat digunakan untuk membantu personel keamanan UK Petra dalam melakukan analisa lebih dalam secara efisien. Dengan adanya sistem alert yang dilengkapi dengan *chatbot* dapat meningkatkan keamanan jaringan UK Petra.

1.7 Sistematika Penelitian

Penulisan laporan skripsi ini menggunakan sistematika penulisan sebagai berikut:

BAB I : PENDAHULUAN

Bab ini membahas tentang latar belakang, rumusan masalah, tujuan dari pembuatan skripsi, ruang lingkup, metodologi penelitian, dan sistematika penulisan.

BAB II : LANDASAN TEORI

Bab ini membahas tentang teori-teori dan metode yang digunakan dalam pembuatan skripsi.

BAB III : DESAIN DAN ANALISIS SISTEM

Bab ini membahas mengenai analisis masalah, analisis kebutuhan serta desain sistem yang akan dibuat.

BAB IV : IMPLEMENTASI

Bab ini akan membahas tentang implementasi sistem dari desain sistem.

BAB V : PENGUJIAN

Bab ini akan membahas pengujian sistem

BAB VI : KESIMPULAN

Bab ini membahas tentang kesimpulan sesuai dengan hasil pengujian.