KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
REPUBLIK INDONESIA
UNIVERSITAS SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
PROGRAM STUDI S1 ILMU KOMPUTER

Jalan Universitas No. 9 Kampus USU, Kec. Medan Baru, Medan 20155
Tel/Fax: 061 8228048, e-mail: ilkom@usu.ac.id, laman: http://ilkom.usu.ac.id

FORM PENGAJUAN JUDUL

Nama : Muhammad Habib Laits Yafa

NIM : 201401008

Judul diajukan oleh* : ☐ Dosen
☑ Mahasiswa

Bidang Ilmu (tulis dua bidang) : Artificial Intelligence, Sistem Pakar

Uji Kelayakan Judul** : ○ Diterima ○ Ditolak

Hasil Uji Kelayakan Judul :

Calon Dosen Pembimbing I:
Dian Rachmawati S.Si., M.Kom.
NIP. 198307232009122004

Calon Dosen Pembimbing II:
Dr. Amalia S.T., M.T.
NIP. 197812212014042001

Medan, Maret 2025
Ka. Laboratorium Penelitian

(Dr. Pauzi Ibrahim Nainggolan S.Komp.,M.Sc.)
NIP. 198809142020011001

** Centang salah satu atau keduanya*
*** Pilih salah satu*

KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
REPUBLIK INDONESIA
UNIVERSITAS SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
PROGRAM STUDI S1 ILMU KOMPUTER

Jalan Universitas No. 9 Kampus USU, Kec. Medan Baru, Medan 20155
Tel/Fax: 061 8228048, e-mail: ilkom@usu.ac.id, laman: http://ilkom.usu.ac.id

RINGKASAN JUDUL YANG DIAJUKAN

Judul / Topik Skripsi	Sistem Pakar Deteksi Serangan *Phishing* pada Website Menggunakan *Rule-Based System*
Latar Belakang dan Penelitian Terdahulu	Dalam era digital kemajuan teknologi informasi, internet menjadi sarana utama bagi individu maupun organisasi untuk melakukan aktivitas sehari-hari. Sayangnya pengguna internet tidak paham maraknya pencurian data di internet, ini yang menjadi pemicu orang-orang untuk memasukkan data dan informasi pribadi mereka yang harusnya tidak boleh diketahui oleh siapapun. Melihat peluang ini berbagai macam kejahatan dunia maya juga semakin berkembang, salah satunya adalah serangan *phishing*. *Phishing* merupakan salah satu bentuk dari teknik penipuan yang digunakan oleh penyerang atau *cyber* yang terus berkembang, di mana penyerang mencoba untuk memperoleh informasi sensitif seperti *username*, *password*, data keuangan, atau informasi pribadi lainnya dengan menyamar sebagai entitas tepercaya melalui berbagai platform digital, terutama situs web. serangan phishing menjadi ancaman yang signifikan terhadap keamanan data pribadi dan bisnis. Keberhasilan serangan ini sering kali disebabkan oleh kurangnya kesadaran pengguna serta teknik yang semakin canggih yang digunakan oleh penyerang. Salah satu cara untuk mendeteksi serangan phising ini dengan menggunakan sistem pakar yang dapat menjadi solusi teknologi yang meniru proses berpikir seorang pakar dalam mengidentifikasi potensi bahaya melalui analisis aturan *rule-based system.* Sistem ini menyimpan aturan dan pengetahuan dalam menganalisis situs yang berpotensi menjadi situs *phising* sehingga dapat mengurangi dampak kerugian yang ditimbulkan oleh serangan *phising.* *Rule Based system* menawarkan keunggulan dalam hal transparansi dan kemudahan interpretasi memungkinkan pengguna untuk memahami bagaimana keputusan yang dapat diambil berdasarkan aturan yang jelas dan logis. Rule Based ini juga merupakan sistem berbasis aturan dari suatu perangkat lunak yang dapat menyajikan keahlian pakar dalam bentuk aturan-aturan tertentu yang didalamnya menerapkan batasan, atau kondisi pada desain yang di formulasikan dan diusulkan dengan hasil seperti, lulus, gagal ,atau sebuah peringatan yang tidak diketahui pada *website.* Das (2013) menyoroti kemampuan sistem pakar berbasis rule-based dalam mengatasi kejahatan di situs *website* seperti *phising*, yang memerlukan respon cepat dan akurat. Dengan demikian, penelitian ini bertujuan untuk mengembangkan sistem pakar deteksi serangan *phishing* pada situs web dengan menggunakan pendekatan *rule-based system*, di mana aturan-aturan tertentu akan diterapkan untuk memeriksa keberadaan elemen-elemen yang mencurigakan dalam situs web. Pendekatan ini diharapkan dapat mempercepat proses deteksi dan meningkatkan tingkat akurasi dalam mengenali situs *phishing*.

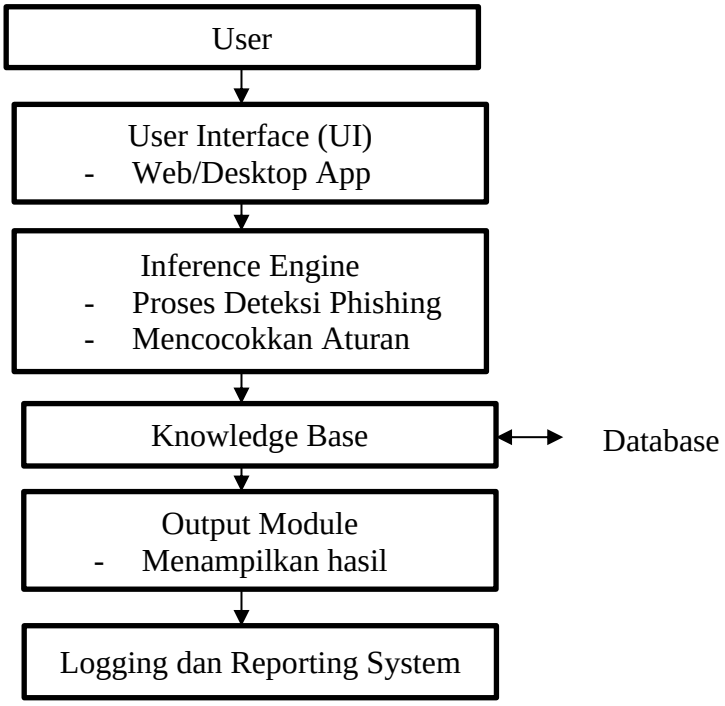
Beberapa penelitian sebelumnya telah mengkaji penggunaan berbagai teknik untuk mendeteksi serangan *phishing.* Salah satunya adalah penelitian oleh Aksoy et al. (2018) yang mengusulkan pendekatan berbasis analisis URL untuk mendeteksi situs *phishing*. Dalam penelitiannya, digunakan model machine learning untuk mengklasifikasikan URL berdasarkan fitur yang diekstrak. Meskipun pendekatan ini memiliki tingkat akurasi yang tinggi, namun memerlukan dataset yang besar dan pelatihan yang intensif.

Di sisi lain, penelitian oleh Alsharnouby et al. (2016) mengembangkan teknik untuk mendeteksi *phishing* menggunakan fitur dari tampilan halaman web (seperti desain visual dan elemen interaktif). Walaupun hasilnya cukup menjanjikan, sistem tersebut kurang efektif dalam mendeteksi *phishing* yang dilakukan melalui teknik *social engineering*.

Sistem pakar berbasis aturan telah diuji coba oleh beberapa peneliti lainnya, seperti penelitian oleh Ouyang et al. (2017), yang mengembangkan sistem berbasis aturan untuk mendeteksi serangan *phishing* pada email. Penelitian ini menunjukkan bahwa penggunaan aturan berbasis pengetahuan dapat sangat efektif dalam mendeteksi serangan *phishing* yang lebih tradisional. Namun, penerapan pada *website* memerlukan penyesuaian lebih lanjut, karena situs *phishing* seringkali menyamarkan diri dengan teknik yang lebih canggih dan dinamis.

Berdasarkan penelitian-penelitian terdahulu, meskipun berbagai metode telah dikembangkan, belum ada sistem yang memanfaatkan pendekatan *rule-based* secara efektif dalam mendeteksi *phishing* pada situs web dengan mempertimbangkan berbagai variabel seperti konten, URL, dan elemen-elemen yang mencurigakan dalam halaman web secara *real-time.*

Diagram Arsitektur System



KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
REPUBLIK INDONESIA
UNIVERSITAS SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
PROGRAM STUDI S1 ILMU KOMPUTER

Jalan Universitas No. 9 Kampus USU, Kec. Medan Baru, Medan 20155
Tel/Fax: 061 8228048, e-mail: ilkom@usu.ac.id, laman: http://ilkom.usu.ac.id

Rumusan Masalah	Dari latar belakang yang telah dipaparkan, rumusan masalah yang diajukan dalam penelitian ini adalah: 1. Bagaimana mendesain dan mengembangkan sistem pakar *berbasis rule-based* untuk mendeteksi serangan phishing pada situs web? 2. Bagaimana cara mengidentifikasi aturan-aturan yang relevan dan efektif untuk mendeteksi serangan *phishing* pada situs web? 3. Sejauh mana sistem pakar berbasis aturan ini dapat meningkatkan akurasi dan efisiensi dalam mendeteksi situs *phishing* dibandingkan dengan metode konvensional lainnya?
Metodologi	Metode penelitian yang dilakukan dalam Penelitian ini menggunakan pendekatan *rule-based system* untuk membangun sebuah sistem pakar yang mampu mendeteksi serangan *phishing* pada situs web. Langkah-langkah penelitian yang akan dilakukan meliputi: 1. Analisis Kebutuhan Sistem - Menganalisis karakteristik situs web yang umumnya digunakan dalam serangan *phishing*, termasuk URL, elemen HTML, tampilan visual, dan konten teks. 2. Perancangan Sistem Pakar - Merancang sistem pakar berbasis aturan dengan mengidentifikasi aturan-aturan yang relevan untuk mendeteksi situs *phishing*. Aturan ini dapat berupa pola URL yang mencurigakan, penggunaan elemen-elemen HTML yang tidak biasa, atau penggunaan domain yang tidak sah. 3. Pengumpulan Data - Mengumpulkan dataset yang terdiri dari situs web yang sah dan *phishing*. Data ini akan digunakan untuk menguji keakuratan dan efektivitas sistem dalam mendeteksi *phishing*. 4. Pengembangan Sistem - Membangun sistem pakar dengan menggunakan bahasa pemrograman yang mendukung pengembangan sistem berbasis aturan, seperti Prolog atau Python dengan pustaka yang sesuai. 5. Uji Coba dan Evaluasi - Menguji sistem pakar menggunakan dataset yang telah dikumpulkan dan mengevaluasi kinerjanya berdasarkan tingkat akurasi, presisi, dan *recall*. 6. Analisis dan Dokumentasi - Melakukan analisis terhadap hasil deteksi dan mendokumentasikan beberapa aturan yang digunakan dalam sistem pakar untuk meningkatkan akurasi deteksi.

KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
REPUBLIK INDONESIA
UNIVERSITAS SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
PROGRAM STUDI S1 ILMU KOMPUTER

Jalan Universitas No. 9 Kampus USU, Kec. Medan Baru, Medan 20155
Tel/Fax: 061 8228048, e-mail: ilkom@usu.ac.id, laman: http://ilkom.usu.ac.id

Referensi	Aksoy, S., & Ozturk, M. (2018). *Phishing website detection using machine learning algorithms. Journal of Computational and Theoretical Nanoscience*, 15(3), 1621-1630. Alsharnouby, M., Omer, S., & Shaikh, A. (2016). *Detecting phishing attacks using visual and URL-based features. Proceedings of the International Conference on Information Security and Privacy*, 98-105. Ouyang, X., Lee, W., & Kannan, S. (2017). *Rule-based phishing detection using email content analysis. Proceedings of the 12th International Conference on Internet Security and Privacy*, 121-130. Dhamija, R., Tygar, J. D., & Hearst, M. (2006). *Why phishing works. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 581-590.

Medan, Maret 2025

Mahasiswa yang mengajukan,

(Muhammad Habib Laits Yafa)
NIM. 201401008