ANALISIS PERBANDINGAN ALGORITMA MACHINE LEARNING UNTUK DETEKSI URL PHISHING DENGAN PENGEMBANGAN APLIKASI BERBASIS WEB PADA PT BANK CENTRAL ASIA, TBK

Skripsi

Michael Owen Kohar

00000056755

PROGRAM STUDI SISTEM INFROMASI

FAKULTAS TEKNIK DAN INFORMATIKA

UNIVERSITAS MULTIMEDIA NUSANTARA

TANGERANG

2024

ANALISIS PERBANDINGAN ALGORITMA MACHINE LEARNING UNTUK DETEKSI URL PHISHING DENGAN PENGEMBANGAN APLIKASI BERBASIS WEB PADA PT BANK CENTRAL ASIA, TBK

Skripsi

Diajukan sebagai Salah Satu Syarat untuk Memperoleh

Gelar Sarjana Komputer (S.Kom)

Michael Owen Kohar

00000056755

PROGRAM STUDI SISTEM INFROMASI

FAKULTAS TEKNIK DAN INFORMATIKA

UNIVERSITAS MULTIMEDIA NUSANTARA

TANGERANG

2024

HALAMAN PERNYATAAN TIDAK PLAGIAT

Dengan ini saya,

Nama	: Michael Owen Kohar
NIM	: 00000056755
Program studi	: Sistem Informasi

Menyatakan dengan sesungguhnya bahwa Skripsi saya yang berjudul:

Analisis Perbandingan Algoritma Machine Learning Untuk Deteksi Url Phishing Dengan Pengembangan Aplikasi Berbasis Web Pada PT Bank Central Asia, Tbk

merupakan hasil karya saya sendiri, bukan merupakan hasil plagiat, dan tidak pula dituliskan oleh orang lain; Semua sumber, baik yang dikutip maupun dirujuk, telah saya cantumkan dan nyatakan dengan benar pada bagian Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan/penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan karya ilmiah, saya bersedia menerima konsekuensi untuk dinyatakan TIDAK LULUS. Saya juga bersedia menanggung segala konsekuensi hukum yang berkaitan dengan tindak plagiarisme ini sebagai kesalahan saya pribadi dan bukan tanggung jawab Universitas Multimedia Nusantara.

Tangerang, 29 November 2024

(Michael Owen Kohar)

HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH MAHASISWA

Yang bertanda tangan dibawah ini:

Nama	: Michael Owen Kohar
NIM	: 00000056755
Program Studi	: Sistem Informasi
Jenjang	: S1
Judul Karya Ilmiah	: Analisis Perbandingan Algoritma Machine Learning Untuk Deteksi Url Phishing Dengan Pengembangan Aplikasi Berbasis Web Pada PT Bank Central Asia, Tbk

Menyatakan dengan sesungguhnya bahwa saya bersedia:

- Memberikan izin sepenuhnya kepada Universitas Multimedia Nusantara untuk mempublikasikan hasil karya ilmiah saya di repositori Knowledge Center, sehingga dapat diakses oleh Civitas Akademika/Publik. Saya menyatakan bahwa karya ilmiah yang saya buat tidak mengandung data yang bersifat konfidensial dan saya juga tidak akan mencabut kembali izin yang telah saya berikan dengan alasan apapun.

Saya tidak bersedia, dikarenakan:

- Dalam proses pengajuan untuk diterbitkan ke jurnal/konferensi nasional/internasional (dibuktikan dengan *letter of acceptance*)**.

Tangerang, 29 November 2024

(Michael Owen Kohar)

** Jika tidak bisa membuktikan LoA jurnal/HKI selama 6 bulan kedepan, saya bersedia mengizinkan penuh karya ilmiah saya untuk diunggah ke KC UMN dan menjadi hak institusi UMN.

KATA PENGANTAR

Puji Syukur atas selesainya penulisan Skripsi ini dengan judul: Analisis Perbandingan Algoritma Machine Learning Untuk Deteksi Url Phishing Dengan Pengembangan Aplikasi Berbasis Web Pada PT Bank Central Asia, Tbk dilakukan untuk memenuhi satu syarat kelulusan Program Strata 1 Jurusan Sistem Informasi Pada Fakultas Teknik & Infomatika Universitas Multimedia Nusantara. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan tugas akhir ini, sangatlah sulit bagi saya untuk menyelesaikan tugas akhir ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

1. Bapak Dr. Ir. Andrey Andoko, M.Sc., selaku Rektor Universitas Multimedia Nusantara.
2. Bapak Dr. Eng. Niki Prastomo, S.T., M.Sc., selaku Dekan Fakultas Teknik & Informatika Universitas Multimedia Nusantara.
3. Ibu Ririn Ikana Desanti, S.Kom., M.Kom., selaku Ketua Program Studi Sistem Informasi Universitas Multimedia Nusantara.
4. Bapak Jansen Wiratama, S.Kom., M.Kom., sebagai Pembimbing yang telah banyak meluangkan waktu untuk memberikan bimbingan, arahan dan motivasi atas terselesainya tesis ini.
5. PT Bank Central Asia , TBK, sebagai Perusahaan yang telah mengizinkan saya untuk mengangkat topik penelitian ini..
6. Keluarga yang telah memberikan bantuan dukungan material dan moral, sehingga penulis dapat menyelesaikan laporan MBKM ini.

Semoga karya ilmiah ini dapat membantu penelitian selanjutnya dan menjadi sumber informasi maupun sumber inspirasi bagi para pembaca.

Tangerang, 29 November 2024

Michael Owen Kohar

ANALISIS PERBANDINGAN ALGORITMA MACHINE LEARNING UNTUK DETEKSI URL PHISHING DENGAN PENGEMBANGAN APLIKASI BERBASIS WEB PADA PT BANK CENTRAL ASIA, TBK

Michael Owen Kohar

ABSTRAK

Penelitian ini berfokus pada ancaman keamanan siber berupa serangan phishing yang semakin meningkat, khususnya di sektor perbankan. PT Bank Central Asia, Tbk (BCA) menjadi salah satu target utama serangan ini karena basis pelanggan yang luas dan data keuangan yang sensitif. Serangan phishing melalui URL palsu dapat menyebabkan kerugian finansial signifikan dan merusak kepercayaan nasabah terhadap layanan perbankan digital. Oleh karena itu, diperlukan sistem deteksi URL phishing berbasis machine learning untuk membantu memitigasi risiko tersebut.

Metode CRISP-DM digunakan dalam penelitian ini untuk memandu pengembangan sistem, meliputi pemahaman bisnis, analisis data, persiapan data, pemodelan, evaluasi, dan implementasi. Data yang digunakan berupa kumpulan URL hasil interaksi digital di BCA, yang telah melalui proses seleksi untuk mengidentifikasi URL phishing dan non-phishing. Beberapa algoritma machine learning, seperti Support Vector Machine (SVM), Random Forest, Decision Tree, dan Naïve Bayes, diterapkan dan dibandingkan berdasarkan akurasi dan kemampuan mendeteksi URL phishing.

Hasil penelitian menunjukkan bahwa algoritma SVM memiliki performa terbaik dengan Akurasi pelatihan adalah 99.82%, dan akurasi pengujian adalah 99.88%, diikuti oleh Decision Tree Akurasi pelatihan (Training Accuracy) adalah 99.26%, dan akurasi pengujian (Testing Accuracy) adalah 98.77%, Random Forest Akurasi pelatihan adalah 99.08%, dan akurasi pengujian adalah 98.65%, dan Naïve Bayes Akurasi pelatihan adalah 92.99%, dan akurasi pengujian adalah 92.51%. Sistem ini kemudian diimplementasikan dalam antarmuka berbasis web menggunakan Flask, yang memudahkan pengguna untuk memvalidasi URL mencurigakan secara real-time.

Kata kunci: deteksi URL, keamanan siber, machine learning, phishing, sistem berbasis web

COMPARATIVE ANALYSIS OF MACHINE LEARNING ALGORITHM FOR PHISHING URL DETECTION WITH WEB-BASED APPLICATION DEVELOPMENT AT PT BANK CENTRAL ASIA, TBK

Michael Owen Kohar

ABSTRACT (English)

This study focuses on the growing threat of cyberattacks, particularly phishing, in the banking sector. PT Bank Central Asia, Tbk (BCA) is one of the primary targets of these attacks due to its large customer base and sensitive financial data. Phishing attacks through fake URLs can lead to significant financial losses and damage customer trust in digital banking services. Therefore, a machine learning-based phishing URL detection system is essential to mitigate these risks.

The CRISP-DM methodology was employed in this research to guide the system development process, including business understanding, data analysis, data preparation, modeling, evaluation, and implementation. The dataset used consists of URLs from digital interactions at BCA, which were processed to identify phishing and non-phishing URLs. Several machine learning algorithms, such as Support Vector Machine (SVM), Random Forest, Decision Tree, and Naïve Bayes, were applied and compared based on their accuracy and phishing detection capabilities.

The research results indicate that the SVM algorithm achieved the best performance with a training accuracy of 99.82% and a testing accuracy of 99.88%, followed by Decision Tree with a training accuracy of 99.26% and a testing accuracy of 98.77%, Random Forest with a training accuracy of 99.08% and a testing accuracy of 98.65%, and Naïve Bayes with a training accuracy of 92.99% and a testing accuracy of 92.51%. The system was then implemented in a web-based interface using Flask, allowing users to validate suspicious URLs in real-time.

Keywords**: **cybersecurity, machine learning, phishing, system-based web, URL detection

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR RUMUS

DAFTAR LAMPIRAN