INTISARI

Phishing merupakan ancaman siber signifikan yang dapat mengakibatkan kerugian finansial dan kebocoran data, sehingga diperlukan sistem deteksi yang efektif. Penelitian ini bertujuan untuk meningkatkan efektivitas aplikasi pendeteksi phishing berbasis web dengan membandingkan dua algoritma machine learning: logistic regression dan decision tree, dalam mengklasifikasikan fitur-fitur phishing web, termasuk fitur berbasis Address Bar, Abnormal, HTML dan JavaScript, serta fitur berbasis Domain. Dengan membandingkan kedua algoritma ini, penelitian ini berupaya mengidentifikasi algoritma yang paling efektif dalam mendeteksi serangan phishing secara cepat dan akurat. Diharapkan hasil penelitian ini dapat mengurangi risiko pencurian identitas, kebocoran data perusahaan, dan kerugian finansial akibat serangan phishing, serta meningkatkan kemampuan sistem deteksi phishing untuk beradaptasi dengan ancaman yang terus berkembang. Metode penelitian melibatkan penerapan kedua algoritma pada dataset phishing yang mencakup 29 fitur dan perbandingan performa keduanya menggunakan metrik akurasi. Hasil pengujian menunjukkan bahwa algoritma Decision Tree memiliki akurasi deteksi phishing yang lebih tinggi, yaitu 95.07%, dibandingkan dengan Logistic Regression yang mencapai akurasi 91.76%. Hal ini menunjukkan bahwa Decision Tree lebih akurat dan efektif dalam mengidentifikasi situs phishing berdasarkan fitur-fitur dalam dataset. Selain itu, dalam pengembangan website pendeteksi phishing digunakan metode Rapid Application Development (RAD) untuk memastikan proses pengembangan sistem deteksi yang cepat dan efisien, sehingga aplikasi dapat dengan cepat beradaptasi terhadap ancaman phishing yang terus berkembang.

Kata kunci: Sistem Deteksi, Phishing, Website, Logistic Regression, Decision Tree. Rapid Application Development (RAD)

ABSTRACT

Phishing is a significant cyber threat that can lead to financial losses and data breaches, necessitating an effective detection system. This study aims to enhance the effectiveness of web-based phishing detection applications by comparing two machine learning algorithms: logistic regression and decision tree, in classifying phishing web features, including Address Bar-based, Abnormal, HTML and JavaScript, and Domain-based features. By comparing these algorithms, this research seeks to identify the most effective algorithm for detecting phishing attacks quickly and accurately. The study expects to reduce the risks of identity theft, corporate data breaches, and financial losses due to phishing attacks, while also improving the phishing detection system's ability to adapt to evolving threats. The research method involves applying both algorithms to a phishing dataset comprising 29 features and comparing their performance using accuracy metrics. The results show that the Decision Tree algorithm has a higher phishing detection accuracy, at 95.07%, compared to Logistic Regression, which achieves an accuracy of 91.76%. This indicates that Decision Tree is more accurate and effective in identifying phishing sites based on the features in the dataset. Additionally, the development of the phishing detection website employs the Rapid Application Development (RAD) method to ensure a fast and efficient detection system development process, allowing the application to quickly adapt to the continuously evolving phishing threats.

Keywords: Detection System, Phishing, Website, Logistic Regression, Decision Tree, Rapid Application Development (RAD)