

Pendeteksi Phishing Menggunakan Metode Rule Based Attribute Checking

Raja Ryan Pradana¹, Parman Sukarno², Erwid Musthofa Jaded³

^{1,2,3}Fakultas Informatika, Universitas Telkom, Bandung

¹rajaryanpradana@students.telkomuniversity.ac.id, ²parmansukarno@telkomuniversity.ac.id,

³jaded@telkomuniversity.ac.id

Abstrak

Internet merupakan bagian penting dari kehidupan saat ini. Namun, seiring dengan berjalannya waktu, internet juga menjadi sarana penyerangan oleh oknum-oknum tidak bertanggung jawab dan salah satu tindak kejahatan ini adalah *phishing*. Dengan *phishing* orang akan dapat mencuri informasi pribadi dari korban. Untuk penanganannya, ada beberapa cara yang bisa dilakukan seperti mendeteksi URL yang akan dimasuki apakah merupakan URL *phishing* atau tidak.

Dari beberapa penelitian terkait pendeteksi *phishing* seperti metode PRISM: An algorithm for inducing modular rules dan Phishing Websites Detection Using Data Mining Classification Model, akurasi yang dihasilkan masih rendah yaitu 84% dan 87% untuk metode tersebut. Oleh karena itu tujuan dari metode penelitian yang diajukan ini adalah untuk meningkatkan akurasi pendeteksian *phishing* tersebut. Metode yang diajukan dalam penelitian ini menggunakan metode Rule Based Attribute Checking dimana sistem akan mengambil sembilan atribut yang paling berpengaruh dalam pendeteksian *phishing* dan setiap atribut diberikan bobot sesuai tingkatannya. Sistem kemudian menjumlahkan total dari bobot yang didapat untuk menentukan status URL yang diperiksa apakah URL tersebut *trustworthy*, *fairly legitimate*, *unsolved*, *suspicious*, atau *phishy*. Dengan menggunakan 200 dataset yang diambil secara acak(100 *phishing* dan 100 *legitimate*) untuk pengujian, metode ini berhasil mencapai akurasi pendeteksian sebesar 85.5%.

Kata kunci : *Phishing*, pendeteksi, atribut, *rule based*

Abstract

Internet is an important part of life today. However, over time, the internet is also a means to attack by unscrupulous individuals and one of these crimes is *phishing*. With *phishing* people will be able to steal personal information from victims. To handle this, there are several ways that can be done and one of them is detecting the URL whether it is a *phishing* URL or not before entering the URL.

There have been several studies related to *phishing* detection such as PRISM: An algorithm for inducing modular rules dan Phishing Websites Detection Using Data Mining Classification Model. But, the accuracy of these methods can only reach 84% and 87%. Therefore with this new proposed method we aim for higher accuracy in detecting *phishing*. This proposed method use Rule Based Attribute Checking where the system will check nine attributes that have the most impact in detecting *phishing* and the system will give certain amount of score for each attribute. After accumulating the total score that the URL gets, the system will determine it's status ranging from *trustworthy*, *fairly legitimate*, *unsolved*, *suspicious*, or *phishy*. Using 200 random datasets(100 *phishing* and 100 *legitimate*) for testing purpose, we managed to achieve a total accuracy of 85.5% with this method

Keywords: *Phishing*, detector, attribute, rule based

1. Pendahuluan

Latar Belakang

Internet pada masa ini merupakan hal yang tidak bisa lepas dari kehidupan sehari-hari. Hal ini pun membuat orang saat ini bergantung pada internet dan sudah sangat banyak kegiatan yang mewajibkan terhubung internet sehingga jika internet di dunia ini berhenti untuk satu tahun maka akan merusak alur kegiatan penting seperti perbankan, penerbangan, dan juga akan menyebabkan kerugian yang sangat besar. Menurut situs *brooking*, matinya internet dapat menyebabkan kerugian negara sebesar 2.4 miliar USD [6].

Sayangnya, pengguna internet tidak paham bahwa banyak pencuri data di internet. Ini yang menjadi pemicu orang-orang sering memasukkan data dan informasi pribadi penting yang harusnya tidak boleh diketahui oleh siapapun. Melihat peluang ini banyak bermunculan orang-orang yang mencoba untuk bisa mencuri data penting