

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan Ilmu Pengetahuan dan Teknologi (IPTEK), khususnya pada bidang Teknologi dan Informasi saat ini sudah mengalami kemajuan yang pesat dan memberikan banyak manfaat, sehingga memudahkan hampir semua kegiatan penyebaran informasi, pengelolaan keuangan, dan metode pembayaran dapat dilakukan dengan Teknologi melalui jaringan internet dengan media Website. Kemajuan Teknologi Informasi yang serba digital membawa orang berminat ke dalam dunia bisnis online karena dirasakan lebih mudah dan praktis berkomunikasi dan memperoleh informasi.

WeAreSocial merupakan sebuah perusahaan agensi marketing sosial terpercaya, yang mengeluarkan laporan setiap tahun mengenai data jumlah pengguna website, dan media sosial dari seluruh dunia. Laporan terbaru mengungkapkan bahwa pengguna internet mengalami perkembangan rata-rata lebih dari satu juta pengguna baru setiap hari. Jumlah orang yang menggunakan internet telah meningkat selama setahun terakhir. Ada 4,39 miliar pengguna internet pada tahun 2019, meningkat 366 juta(9 persen) dibandingkan Januari 2018. Rata-rata pengguna internet dunia menghabiskan 6 jam dan 42 menit online setiap hari[1]. Disisi lain, dengan kemajuan internet ini juga memiliki dampak negatif yang mengkhawatirkan pada berkembangnya tindak kejahatan online atau dapat disebut juga “*CYBERCRIME*”. Disertai juga dengan maraknya website phishing.

Phising adalah sebuah tindakan kriminal untuk mencuri informasi pribadi orang lain menggunakan entitas *electronic*, salah satunya adalah website[5]. Informasi ini dicuri dari website yang telah diakses yang mengandung phising atau dengan kata lain masuk ke dalam kategori website phising. Tujuan dari web phising adalah membuat pengguna percaya bahwa mereka berinteraksi dengan situs resmi. Umumnya informasi yang dicari *phisher*(pelaku phising) adalah berupa *username*, *password*, baik itu akun media sosial atau akun nomor kartu kredit dengan cara diarahkan ke sebuah situs website palsu. Maka dari itu perlu adanya deteksi web phising yang berguna untuk melindungi user dari tindak pencurian informasi pengguna..

Menurut buku dengan judul *No-tech hacking* oleh Johnny Long mengutarakan bahwa senjata paling ampuh dalam dunia hacker adalah *social engineering*[2]. Serangan Web Phising memuncak pada tahun 2005 dan phising merupakan cara untuk memikat agar korban dengan mudah jatuh dalam perangkap penipuan, dengan mencari kelemahan di dalam website ,dan kelemahan e-mail, pada dasarnya phising menggunakan hampir semua teknik hacking yang digunakan untuk membuat umpan[3]. Hacking merupakan tindak kejahatan komputer untuk mengakses, mencuri, merusak data secara tidak sah[6].

Support Vector Machine (SVM) dikembangkan oleh Bose, Guyon, dan Vapnik, pertama kali diperkenalkan pada tahun 1992 di *Annual Workshop On Computational Learning Theory*. Support Vector Machine merupakan salah satu metode dalam *supervised learning* yang biasanya digunakan untuk klasifikasi seperti *Support Vector Classification* dan *regresi Support Vector Regression*.

SVM juga dapat mengatasi masalah klasifikasi dan regresi linear maupun non linear[8].

Dalam Penelitian ini penulis mencoba untuk menerapkan Algoritma Support Vector Machine (SVM) untuk klasifikasi Web Phising untuk mengklasifikasikan dan memaksimalkan Data Set yang akan diolah, Sehingga dapat menghasilkan akurasi yang maksimal untuk mendeteksi web phising.

Berdasarkan latar belakang diatas maka peneliti melakukan penelitian dengan judul "Penerapan Algoritma Support Vector Machine (SVM) untuk klasifikasi *Web Phising*".

1.2 Rumusan Masalah

Berdasarkan latar belakang yang sudah terurai maka peneliti merumuskan masalah yaitu "Apakah Algoritma Support Vector Machine dapat diterapkan untuk mengklasifikasikan dan mendeteksi web phising ?"

1.3 Batasan Masalah

Dalam pelaksanaan penelitian ini, berbagai permasalahan yang muncul dalam konteks objek yang lebih luas akan dibatasi sesuai dengan kebutuhan dan kemampuan. Dalam hal ini batasan masalah dalam penelitian ini antara lain:

1. Dalam penelitian ini hanya menggunakan 1 metode saja yaitu Support Vector Machine.

2. Dalam penelitian ini hanya menerapkan Algoritma Support Vector Machine untuk mengklasifikasikan web phishing. Dengan batas sampai hasil akurasi dan hasil penerapan kedalam sistem.

1.4 Maksud dan Tujuan Penelitian

Dalam pembuatan penelitian ini, adapun maksud dan tujuannya adalah sebagai berikut:

1. Maksud

Merancang aplikasi *website* untuk mendeteksi URL/Website phishing menggunakan algoritma Support Vector Machine berbasis Website.

2. Tujuan

- a. Dapat membantu pengguna sebagai alat untuk mendeteksi URL/Website phishing.
- b. Memenuhi syarat kelulusan dan menyandang gelar sarjana Komputer Strata I Informatika dalam bidang Informatika dan Komputer pada Universitas "AMIKOM" Yogyakarta.
- c. Menerapkan ilmu yang telah didapat selama mengikuti pendidikan di Universitas "AMIKOM" Yogyakarta sebagai praktik nyata mengembangkan Kemampuan teknis maupun teori.
- d. Menerapkan Algoritma Support Vector Machine untuk klasifikasi Web phishing.

1.5 Manfaat Penelitian

Manfaat yang ingin di capai dalam penelitian ini adalah:

1. Bagi Penulis :
 - a. Sebagai penerapan ilmu yang di dapat di dalam perkuliahan.
 - b. Pembuatan karya ilmiah sebagai bukti turut berperan serta dalam pengembangan ilmu pengetahuan khususnya dalam bidang teknologi.
2. Bagi Masyarakat :
 - a. Memberi kemudahan dalam mendeteksi situs atau URL web yang berbahaya (Web Phising).
 - b. Pengguna dapat mengetahui dan mendeteksi situs atau URL website yang berbahaya (Web Phising).
3. Bagi Akademik :
 - a. Sambungan wawasan pengetahuan mengenai perancangan dan penerapan aplikasi website pendeteksi website atau URL phising.
 - b. Referensi maupun pedoman untuk pembelajaran dan pengembangan aplikasi website dengan menggunakan Algoritma Support Vector Machine.

1.6 Metode Penelitian

1.6.1 Metode Pengumpulan Data

Metode pengumpulan data yang akan dilakukan untuk penelitian ini, yaitu:

1. Data Website Phising diambil / didapatkan dari UCI Machine Learning Repository

1.6.2 Metode Pengembangan Sistem

Metode pengembangan sistem yang digunakan dengan tahapan sebagai berikut :

1. Analisis

Proses ini dilakukan dengan menganalisis kebutuhan sistem yang akan dibangun, yaitu kebutuhan fungsional dan kebutuhan non fungsional.

2. Perancangan

Merancang desain proses yang dapat dikerjakan oleh sistem, dan desain antarmuka sistem.

3. Implementasi

Proses perubahan perancangan yang telah dibuat ke dalam bentuk kode program hingga menjadi sebuah aplikasi.

4. Pengujian

Merupakan tahapan akhir dari proses, dilakukan agar dapat mengetahui apakah software yang dibuat telah selesai.

1.7 Sistematika Penulisan

Sistematika penulisan skripsi ini di bagi dalam beberapa bab dengan pokok permasalahan sebagai berikut :

1.7.1 BAB I PENDAHULUAN

Pada bab ini dijelaskan mengenai latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan dalam penjabaran penelitian dan metode penelitian.

1.7.2 BAB II LANDASAN TEORI

Pada bab ini dijelaskan mengenai landasan teori dan kajian pustaka dari berbagai penelitian yang memiliki keterkaitan dengan penelitian ini. Kajian pustaka berguna untuk memperkuat dasar dan alasan dilakukanya penelitian ini. Selain kajian pustaka , pada bab ini juga dijelaskan mengenai teori-teori terkait yang bersumber dari buku, jurnal, ataupun website yang berfungsi sebagai dasar dalam melakukan penelitian agar dapat memahami konsep atau teori penyelesaian permasalahan yang ada.

1.7.3 BAB III ANALISIS DAN PERANCANGAN

Bab ini berisi tentang analisis masalah, analisis sistem, tahapan pengembangan sistem, dan perancangan arsitektur sistem.

1.7.4 BAB IV IMPLEMENTASI DAN PEMBAHASAN

Pada bab ini akan dilakukan uji coba dan analisis terhadap metode *Support Vector Machine*. Uji coba ini dilakukan berdasarkan skenario uji coba yang telah dirancang untuk menerapkan *Support Vector Machine* untuk klasifikasi Web Phising. Selain itu pada bab ini juga dijelaskan mengenai analisis hasil uji coba.

1.7.5 BAB V PENUTUP

Bab ini berisi kesimpulan dari penelitian dan juga saran bagi penelitian mendatang yang berasal dari kekurangan maupun temuan dari penelitian ini.