**RANCANG BANGUN APLIKASI PENDETEKSI DAN PENDATAAN LINK PHISHING BERBASIS WEBSITE DENGAN TEKNOLOGI ARTIFICIAL INTELLIGENCE (AI)**

**SKRIPSI**

**OLEH:**

**Febrina Diponegoro**

**201910225023**



**PROGRAM STUDI INFORMATIKA**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS BHAYANGKARA JAKARTA RAYA**

**TAHUN 2023**

**LEMBAR PENGESAHAN PEMBIMBING**

# BAB I PENDAHULUAN

## Latar Belakang

*Criminal* merupakan suatu tindakan kejahatan yang dapat melanggar nilai, norma, hukum serta perilaku yang dapat meresahkan dan merugikan banyak pihak. *Criminal* atau kriminalitas dapat dilakukan secara individu, kelompok maupun komunitas. Terdapat banyak faktor motif *criminal* terjadi, dengan beragam jenis sosial. Salah satu jenis kejahatan atau *criminal* ialah *Cyber crime* atau kejahatan di dunia maya.

*Cyber crime* atau serangan siber merupakan salah satu bentuk kejahatan yang ada di kalangan masyarakat. Bentuk kejahatan ini terlihat seprti tak kasat mata, namun akibatnya dapat merugikan banyak pihak. Mengutip *TechTarget*, *cyber crime* diartikan sebagai aktivitas kriminalisme yang melibatkan komputer, jaringan dan perangkat yang terhubung dengan jaringan. Pelaku kejahatan siber menargetkan data pribadi atau perusahaan untuk dicuri dan atau dijual kembali. *Cyber crime* atau kejahatan dunia maya sendiri merupakan salah satu dampak negative dari penggunaan internet. Menurut *Organization of European Community Development (OECD) cyber crime* adalah semua bentuk akses ilegal terhadap suatu transmisi data. Itu artinya, semua bentuk kegiatan yang tidak sah dalam suatu sistem komputer termasuk dalam tindak kejahatan. Secara umum, pengertian *cyber crime* ini biasa diartikan sebagai tindak kejahatan di ranah dunia maya yang memanfaatkan teknologi komputer dan jaringan internet sebagai sasaran. Tindakan *cyber crime* ini muncul seiring dengan kian majunya teknologi digital, komunikasi dan informasi yang semakin canggih. Salah satu kejahatan didunia maya yang sangat sering terjadi di khalangan masyarakat indoneisa ialah *phishing*.

*Phishing* berasal dari kata *fishing* yang berarti memancing, mempunyai makna sebagai memancing data-data pribadi seperti nama pengguna dan kata sandi target. *Phishing* biasa berbentuk link url yang dikirimkan melalui media chat yang bert ujuan untuk mengelabui target dengan cara memancing dan mengarahkan orang-orang atau target ke suatu halaman website.

*Uniform Resource Locator* merupakan panjangan dari URL yang merupakan serangkaian karakter berupa huruf, angka, dan symbol yang menuju kealamat di world wide web (WWW) untuk mengidetifikasi lokasi sebuah file dalam sebuah internet. Ketika URL dibuka maka akan menampilkan isi dari apa yang berada didalam website tersbut, isi website tersebut sangat beragam sesuai dengan developernya. Namun, isi dari website tersebut juga bias berupa laman login palsu.

*Phishing* meparukan kejahatan dunia maya dimana target dihubungi melalui email, sms, atau pesan teks lainnya oleh seseorang yang menyamar menjadi lembaga atau perusahaan yang sah untuk memikat target atau individu agar memberikan data sensitif seperti informasi yang dapat diidentifikasi secara pribadi. *Phishing* biasanya berbentuk *link* *url* yang dibuat semirip mungkin dengan aslinya sehingga orang yang menjadi target akan tetap mempercayai link tersebut dan membuka lalu memasukan data pribadi mereka seperti nama pengguna dan kata sandi atau data lainnya yang bersifat rahasia

Saat ini, kasus *phishing* di Indonesia semakin meningkat mulai dari individu maupun pegawai perusahaan dengan kerugian yang tidak sedikit jumlahnya. Untuk itu aplikasi ini diciptakan agar masyarakat dapat dengan mudah memastikan apakah link yang didapat merupakan link url *phishing* atau bukan.

## Identifikasi Masalah

Berdasarkan latar belakang masalah tersebut, maka permasalahan yang muncul dapat di identifikasikan sebagai berikut :

1. Sering terjadinya kasus *phishing* di masyarakat yang sangat dapat merugikan
2. Kurangnya kewaspadaan terhadap *link-link phishing*

## Rumusan Masalah

Berdasarkan masalah yang dihadapi, penulis merumuskan beberapamasalah yang ada dalam penelitian ini sebagai berikut :

1. Bagaimana cara meminimalkan angka terjadinya kasus pencurian data pada masyarakat?
2. Bagaimana membuat masyarakat dari berbagai khalangan dapat dengan mudah mengidentifikasi sebuah link url yang mencurigakan?

## Batasan Masalah

Berdasarkan identifikasi masalah, penulis membuat batasan masalah dalam penelitian ini, yaitu :

1. Sistem hanya dapat menganalisa berupa link
2. Sistem menggunakan algoritma *Decision TreeI*

## Tujuan dan Manfaat Penelitian

Dalam penelitian ini penulis memiliki tujuan dan manfaat berupa

### 1.5.1 Tujuan Penelitian

Adapun tujuan yang ingin di capai dari penelitian ini adalah sebagai berikut:

1. Membangun sebuah program untuk mendeteksi link aman atau *phishing*
2. Menyediakan layanan sistem pendeteksi link *phishing* agar terhindar serta mengurang angka kasus kerugian akibat link *phishing*

### 1.5.2 Manfaat Penelitian

Dalam penelitian ini diharapkan dapat memberikan manfaat berupa :

#### 1.5.2.1 Manfaat Teoritis

Jika dilihat manfaatnya secara teoritis, penelitian ini diharapkan dapat meminimalisirkan terjadinya kejahatan siber serta terjadinya kerugian baik secara perorangan maupun perusahaan

#### 1.5.2.2 Manfaat Praktis

##### 1.5.2.2.1 Bagi Perusahaan

Manfaat bagi Perusahaan adalah untuk membuat para pegawai perusahaan tersebut mendapatkan akses lebih mudah dalam mengidentifikasi link yang dicurigai agar data perusahaan tidak berhasil dicuri oleh pelaku dan dijual yang dapat menyebabkan kerugian bagi perusahaan tersebut.

##### 1.5.2.2.2 Bagi Masyarakat

Manfaat bagi masyarakat adalah untuk menghindari terjadinya pencurian data pribadi individu yang menyangkut kepentingan keuangan atau pekerjaan individu tersebut.

## Sistematika Penulisan

Penyusunan skripsi ini, pada umumnya mencakup 5 (lima) bagian yang terdiri atas beberapa bab dan sub bab, yaitu :

### BAB I PENDAHULUAN

Pada bab ini penulis menyajikan tentang latar belakang maksud dari tujuan indentifikasi masalah, batasan masalah, metode penelitian, dan sistematika penulisan.

### BAB II LANDASAN TEORI

Pada bab ini memuat tinjauan pustaka tentang penelitian sebelumnya berkaitan dengan topik skripsi yang dipilih dengan teori-teori yang mendukung.

### BAB III METODOLOGI PENELITIAN

Dalam bab ini setidaknya membahas mengenai objek penelitian dan kerangka dari penulisan skripsi ini.

### BAB IV PERANCANGAN DAN PEMBANGUNAN SISTEM

Dalam bab ini menjelaskan tentang proses perancangan sistem perangkat keras serta perangkat lunak yang dibutuhkan dalam membangun sistem. Pada bab ini juga melakukan pengujian terhadap sistem yang dibuat untuk mengetahui apakah sudah benar-benar berjalan seperti yang diharapkan.

### BAB V PENUTUP

Pada bab ini di menyajikan kesimpulan penelitian serta saran yang berhubungan dengan penyusunan laporan tugas akhir.

# BAB II LANDASAN TEORI

## 2.1 Penelitian Relevan

Menurut [1] Keamanan informasi sangat penting untuk diamankan karena orang mengandalkan jaringan dan komunikasi. Oleh karena itu, melindungi informasi merupakan tantangan utama dengan jumlah pengguna yang meningkat pesat dalam beberapa tahun terakhir. Tujuan dari artikel ini adalah untuk meninjau Confidentiality, Integrity and Availability (CIA) dalam keamanan informasi. Artikel ini berfokus pada masalah keamanan informasi dan persyaratan keamanan informasi. Artikel, jurnal, dan makalah konferensi yang ditinjau oleh para peneliti diterbitkan pada 2016-2021. Masalah keamanan dianalisis dalam metodologi baru-baru ini. Hasil hubungan antara CIA dalam setiap persyaratan keamanan informasi berada pada tingkat sedang. Disarankan diperlukan program kesadaran risiko keamanan siber bagi masyarakat. Oleh karena itu, setiap pengguna dapat memperoleh keuntungan penuh dalam jaringan dan platform digital.

Di kutip [2] Serangan *phishing*, yang telah ada selama beberapa dekade dan terus menjadi masalah besar hingga saat ini, merupakan ancaman berat di dunia maya. Penyerang mengadopsi berbagai metode baru dan kreatif untuk melakukan serangan *phishing*, yang berkembang pesat. Oleh karena itu, ada kebutuhan untuk melakukan tinjauan komprehensif terhadap pendekatan *phishing* di masa lalu dan saat ini. Dalam makalah ini, ulasan tentang pendekatan yang digunakan selama serangan *phishing* disajikan. Makalah ini terdiri dari tinjauan literatur, diikuti dengan pemeriksaan komprehensif tentang karakteristik teknik serangan *phishing* klasik, modern, dan canggih yang ada. Tujuan dari makalah ini adalah untuk membangun kesadaran akan teknik *phishing*, mendidik individu tentang serangan ini, dan mendorong penggunaan teknik pencegahan *phishing*, selain mendorong wacana di kalangan komunitas profesional tentang topik ini.

Dalam penelitian [3] artikel ini adalah untuk menganalisis konsep «kebersihan dunia maya», «keamanan dunia maya», «perlindungan dunia maya», dan mengklarifikasi peran proses tersebut yang ditafsirkan dengan istilah-istilah ini dalam kehidupan manusia modern; untuk mengidentifikasi pencapaian utama dalam sistem hukum Ukraina terkait regulasi ranah sibernetika hukum; untuk menyoroti aturan utama untuk mengamati kebersihan dunia maya. Metodologi penelitian telah dilaksanakan dengan menggunakan metode ilmiah analisis terminologi ketika membandingkan definisi istilah yang relevan. Metode statistik telah digunakan untuk menggeneralisasi indikator kuantitatif yang mencirikan peningkatan minat lembaga pendidikan tinggi dalam pelatihan spesialis keamanan siber. Perbandingan dan generalisasi memungkinkan untuk mengungkapkan secara komprehensif masalah yang diangkat dalam penelitian ini. Kebaruan ilmiah dari penelitian ini adalah sebagai berikut: menekankan pentingnya kerjasama dan kebutuhan organisasi Ukraina dengan mitra asing di bidang perlindungan informasi yang terkandung dalam ruang cyber; mengidentifikasi dan menelusuri kecenderungan peningkatan keamanan siber dalam konteks ilmu pengetahuan, pendidikan, dan ketatanegaraan. Kesimpulan. Studi masalah untuk memastikan perlindungan dunia maya informasi, serta keamanan dunia maya saat menggunakan Internet dan kebersihan dunia maya di Ukraina, menyoroti visi bahwa spesialis Ukraina telah membuat langkah maju yang signifikan dalam masalah ini. Ini dikonfirmasi oleh data statistik internasional. Analisis undang-undang, tindakan hukum normatif, dan dokumen peraturan yang baru diadopsi di tingkat nasional telah mengkonfirmasi tesis bahwa undang-undang Ukraina dalam masalah keamanan dunia maya secara bertahap mengubah orientasi dirinya ke kecenderungan global, dan meminjam pengalaman asing yang *positif*. Namun, masih ada masalah mendesak yang belum terselesaikan, yang dasarnya adalah pengurangan konseptual aparat keamanan siber untuk diperbaiki pada interpretasi tingkat legislatif. Isu-isu intensifikasi kerja sama internasional lebih lanjut dalam berbagai hal.

Pada kutipan [4] Keamanan informasi menggambarkan usaha untuk melindungi komputer dan non peralatan komputer, fasilitas, data, dan informasi dari penyalahgunaan oleh orang yang tidak bertanggung jawab. Keamanan informasi dimaksudkan untuk mencapai kerahasiaan, ketersediaan, dan integritas di dalam sumber daya informasi dalam suatu perusahaan. Keamanan Sistem informasi terdiri atas perlindungan harian, yang disebut keamanan informasi (information security) dan persiapan-persiapan operasional. Tujuan penulisan artikel ini guna membangun hipotesis pengaruh antar variabel untuk digunakan pada riset selanjutnya. Hasil artikel literature review ini adalah: 1) Keamanan Informasi berpengaruh terhadap Keamanan Sistem Informasi; 2) Teknologi Informasi berpengaruh terhadap Keamanan Sistem Informasi; dan 3) Network berpengaruh terhadap Keamanan Sistem Informasi.

Penelitian [5] Dengan perkembangan Internet, keamanan jaringan telah menarik perhatian banyak orang. Dapat dikatakan bahwa lingkungan jaringan yang aman adalah dasar dari perkembangan Internet yang cepat dan sehat. Phishing adalah kelas penting penjahat dunia maya yang merupakan tindakan jahat yang menipu pengguna agar mengklik tautan phishing, mencuri informasi pengguna, dan pada akhirnya menggunakan data pengguna untuk memalsukan login dengan akun terkait untuk mencuri dana. Keamanan jaringan adalah masalah serangan dan pertahanan yang berulang. Metode phishing dan teknologi deteksi phishing terus diperbarui. Metode tradisional untuk mengidentifikasi tautan phishing bergantung pada daftar hitam dan daftar putih, tetapi ini tidak dapat mengidentifikasi tautan phishing baru. Oleh karena itu, kami perlu memecahkan cara memprediksi apakah tautan yang baru muncul adalah situs web phishing dan meningkatkan akurasi prediksi. Dengan kematangan teknologi pembelajaran mesin, prediksi telah menjadi kemampuan yang vital. Makalah ini menawarkan survei canggih tentang metode deteksi situs web phishing. Ini dimulai dengan siklus hidup phishing, memperkenalkan metode anti-phishing umum, terutama berfokus pada metode mengidentifikasi tautan phishing, dan memiliki pemahaman mendalam tentang solusi berbasis pembelajaran mesin, termasuk pengumpulan data, ekstraksi fitur, pemodelan, dan kinerja evaluasi. Makalah ini memberikan perbandingan terperinci dari berbagai solusi untuk deteksi situs web phishing.

## 2.2 Keamanan Data

Keamanan data adalah sesuatu yang sangat penting dan perlu dilakukan yang mempunyai tujuan memastikan data tidak dapat diakses dan digunakan oleh pihak ke tiga yang merupakan orang yang tidak berhak menerima informasi.

## 2.3 Keamanan Sistem

Keamanan informasi adalah suatu prosedur untuk mencegah pencurian pada data, dan kerusakan pada sistem informasi perusahaan. Beberapa sistem keamanan yang digunakan untuk melindungi jaringan imformasi melibatkan hardware, software, jaringan komunikasi, dan data dalam computer. Sayangnya, masih banyak perusahaan yang mengabaikan pentingnya keamanan sistem.

Banyak juga yang berinvestasi untuk menjaga keamanan sistem informasi perusahaan dan memakan jumlah biaya yang tidak sedikit. Namun, hal ini dapat mencegah risiko kerugian bisnis pada perusahaan.

Berikut aspek-aspek yang penting dalam keamanan sistem informasi :

1. Privasi atau kerahasiaan informasi bertujuan agar data tidak bisa diakses oleh sembarang orang.
2. Integritas, data akan tetap aman seperti semula dan tidak akan mengalami perubahan secara sengaja ataupun tidak disengaja.
3. Autentikasi untuk mengidentifikasi pengakses data.
4. Tanda tangan sebagai bukti sah suatu informasi..

## 2.4 Konsep Dasar Sistem

## 2.4.1 Pengertian Website

## 2.4.2 Pengertian Phishing

## 2.4.3 Pengertian Ai

## 2.4.4 Pengertian Deteksi

## 2.5 UML(Unified Modeling Language)

## 2.6 Metode Perancangan Aplikasi