Neptunus: Jurnal Ilmu Komputer dan Teknologi Informasi
Volume. 4 Nomor. 1 Februari 2026
e-ISSN : 3031-898X; p-ISSN : 3031-8998, Hal. 62-75
DOI: https://doi.org/10.61132/neptunus.v4i1.1439
Tersedia: https://journal.arteii.or.id/index.php/Neptunus

Implementasi Website Deteksi Phishing Link Menggunakan SSL Validation dan Url Scoring

Rusma Riansyah[1*], Dimas Aqila Aptanta[2], Hafiz Aryanda[3], Muhammad Farhan[4], Ibnu Rusydi[5]
[1,2,3,4,5] Jurusan Ilmu Komputer, Universitas Islam Negeri Sumatera Utara, Indonesia
Email: riansyahrusma@gmail.com[1], dimasaqila71@gmail.com[2], hafizaryandaaa@gmail.com[3], muhammadfarhan3737iyan@gmail.com[4], ibnurusydi@dharmawangsa.ac.id[5],

**Korespondensi Penulis: riansyahrusma@gmail.com*

Abstract. *The rapid expansion of internet usage has led to a significant increase in cybersecurity threats, particularly phishing attacks delivered through malicious links. Phishing links are designed to imitate legitimate websites in order to deceive users and steal sensitive information. This study presents the implementation of a phishing link detection website based on SSL validation and URL scoring mechanisms. The proposed system integrates heuristic-based URL analysis with real-time SSL certificate validation obtained through the SSL handshake process. Digital certificates are verified using RSA-based digital signature verification issued by trusted Certificate Authorities (CAs). In addition, the SHA-256 hash algorithm is employed to generate certificate fingerprints and URL hashes to ensure data integrity and uniqueness. The system also evaluates HTTPS usage, domain and certificate consistency, certificate validity period, and RSA public key strength. All validation results are processed using a URL scoring system to generate a security score ranging from 0 to 100, which classifies links into safe, suspicious, or dangerous categories. Experimental results demonstrate that the proposed website is capable of effectively identifying phishing indicators and providing transparent cryptographic evidence in real time. This approach can assist users in making informed decisions and improving protection against phishing threats in web environments.*

Keywords: *Phishing Link, SSL Validation, RSA Cryptography, SHA-256, URL Scoring.*

Abstrak. *Pesatnya pertumbuhan penggunaan internet telah meningkatkan ancaman keamanan siber, khususnya serangan phishing yang disebarkan melalui tautan berbahaya. Phishing link dirancang untuk menyerupai situs resmi dengan tujuan menipu pengguna dan mencuri informasi sensitif. Penelitian ini menyajikan implementasi sebuah website deteksi phishing link yang mengintegrasikan validasi SSL dan mekanisme URL scoring. Sistem yang diusulkan mengombinasikan analisis heuristik URL dengan validasi sertifikat SSL secara real-time melalui proses SSL handshake. Sertifikat digital diverifikasi menggunakan mekanisme tanda tangan digital berbasis algoritma RSA yang diterbitkan oleh Certificate Authority (CA) terpercaya. Selain itu, algoritma hash SHA-256 digunakan untuk menghasilkan fingerprint sertifikat dan hash URL guna menjamin integritas serta keunikan data. Sistem juga melakukan evaluasi terhadap penggunaan protokol HTTPS, kesesuaian domain dengan sertifikat, masa berlaku sertifikat, serta kekuatan kunci publik RSA. Seluruh hasil validasi diproses menggunakan sistem URL scoring untuk menghasilkan skor keamanan dalam rentang 0 hingga 100 yang digunakan untuk mengklasifikasikan tautan ke dalam kategori aman, mencurigakan, atau berbahaya. Hasil pengujian menunjukkan bahwa website yang dikembangkan mampu mengidentifikasi indikasi phishing secara efektif serta menyajikan bukti kriptografi yang transparan secara real-time. Pendekatan ini diharapkan dapat meningkatkan kesadaran pengguna serta memberikan perlindungan awal terhadap ancaman phishing di lingkungan web.*

Kata kunci: Phishing Link, Validasi SSL, Kriptografi RSA, SHA-256, URL Scoring.

1. LATAR BELAKANG

Serangan phishing merupakan salah satu ancaman keamanan siber yang semakin sering terjadi seiring meningkatnya penggunaan layanan digital di berbagai sektor, termasuk finansial, pemerintahan, dan pendidikan (Mahmud & Wirawan, 2024). Phishing umumnya memanfaatkan tautan atau URL yang tampak sah untuk mengecoh pengguna agar memberikan data sensitif seperti kredensial akun atau informasi pribadi (Perdana, 2025). Teknik manipulasi

Naskah Masuk: November 22, 2025; Revisi: Desember 25, 2025; Diterima: Januari 10, 2026; Tersedia: Januari 30, 2026; Terbit: Februari 03, 2026;

URL dan penggunaan domain yang menyerupai situs resmi telah memberikan tantangan signifikan dalam mendeteksi tautan berbahaya secara otomatis (Hartanto et al., 2025). Berbagai pendekatan telah dikembangkan untuk mengidentifikasi phishing link, termasuk ekstraksi fitur URL dan penggunaan algoritma klasifikasi machine learning untuk membedakan tautan berbahaya dan aman (Syahli et al., 2025), (Irawan et al., 2021) dan (Lukito & Handaya, 2025). Pendekatan tersebut terbukti efektif, tetapi sering kali tidak mempertimbangkan validasi sertifikat digital berbasis kriptografi secara menyeluruh.

Validasi Secure Sockets Layer (SSL) dan Transport Layer Security (TLS) merupakan salah satu mekanisme utama untuk menjamin integritas dan kerahasiaan komunikasi antar web server dan klien (Raihan et al., 2024). Sertifikat digital yang dikeluarkan oleh Certificate Authority (CA) dipercaya jika tanda tangan digitalnya diverifikasi menggunakan algoritma kriptografi asimetris seperti RSA (Fatiha et al., 2024). Selain itu, algoritma hash seperti SHA-256 banyak digunakan untuk menghasilkan fingerprint sertifikat dan memastikan integritas data (Suwarno & Hardjianto, 2024). Namun, masih sedikit sistem deteksi phishing link yang menggabungkan validasi SSL/TLS secara real-time dengan analisis URL scoring, sehingga informasi kriptografi yang lebih teknis belum disajikan secara transparan kepada pengguna.

Masalah lain yang sering muncul adalah sistem deteksi hanya memberikan klasifikasi binary tanpa menjelaskan alasan teknis di balik keputusan tersebut (Fauzan et al., 2025), (Muliono et al., 2023) dan (Aryanti & Nabila, 2025) . Kurangnya bukti kriptografi yang jelas membuat tingkat kepercayaan pengguna terhadap hasil analisis menjadi rendah. Untuk itu, pendekatan yang menggabungkan analisis heuristik URL dengan validasi sertifikat digital berbasis kriptografi menjadi sangat penting untuk meningkatkan akurasi dan keandalan sistem deteksi.

Penelitian ini mengusulkan implementasi sebuah website deteksi phishing link yang mengintegrasikan validasi SSL/TLS secara langsung melalui handshake, verifikasi tanda tangan digital RSA, hashing menggunakan SHA-256, serta penilaian risiko dengan skoring URL terstruktur. Hasil analisis ditampilkan dalam bentuk skor keamanan dan bukti kriptografi yang mudah dipahami oleh pengguna. Dengan pendekatan ini, diharapkan sistem dapat membantu meningkatkan kesadaran dan perlindungan pengguna terhadap ancaman phishing di lingkungan internet.

2. KAJIAN TEORITIS

Penelitian mengenai deteksi phishing link telah banyak dilakukan dengan berbagai pendekatan, terutama melalui analisis fitur URL dan pemanfaatan algoritma machine learning. (Mahmud & Wirawan, 2024) menunjukkan bahwa klasifikasi berbasis fitur URL mampu mengidentifikasi pola phishing secara efektif, namun pendekatan tersebut masih bergantung pada karakteristik statis URL. Pendekatan serupa juga dikembangkan oleh (Perdana, 2025) dan (Syahli et al., 2025) yang mengintegrasikan ekstraksi fitur URL dengan model klasifikasi untuk mendeteksi phishing berbasis web. Meskipun hasil yang diperoleh cukup baik, sebagian besar penelitian tersebut belum memasukkan aspek validasi sertifikat SSL secara mendalam sebagai bagian dari proses deteksi.

Penelitian lain menekankan penggunaan algoritma pembelajaran mesin seperti Support Vector Machine, Random Forest, dan Decision Tree untuk meningkatkan akurasi deteksi phishing (Lukito & Handaya, 2025). Pendekatan ini mampu mengenali pola kompleks dalam struktur URL, namun memiliki keterbatasan dalam menjelaskan alasan teknis di balik hasil klasifikasi. Kurangnya transparansi ini menjadi tantangan karena pengguna tidak memperoleh bukti teknis atau kriptografi yang mendasari keputusan sistem (Hartanto et al., 2025). Oleh karena itu, diperlukan pendekatan yang tidak hanya berfokus pada klasifikasi, tetapi juga menyajikan bukti keamanan yang dapat diverifikasi.

Secure Sockets Layer (SSL) dan Transport Layer Security (TLS) merupakan protokol keamanan yang digunakan untuk menjamin kerahasiaan dan integritas komunikasi data pada jaringan internet (Fauzan et al., 2025). SSL/TLS bekerja dengan memanfaatkan sertifikat digital yang diterbitkan oleh Certificate Authority (CA) untuk memverifikasi identitas server. Sertifikat digital tersebut mengandung informasi penting seperti nama domain, masa berlaku, algoritma kriptografi, dan tanda tangan digital yang memastikan keaslian sertifikat. Validasi SSL menjadi indikator utama dalam menilai keamanan sebuah website, khususnya dalam mendeteksi situs palsu yang digunakan dalam serangan phishing.

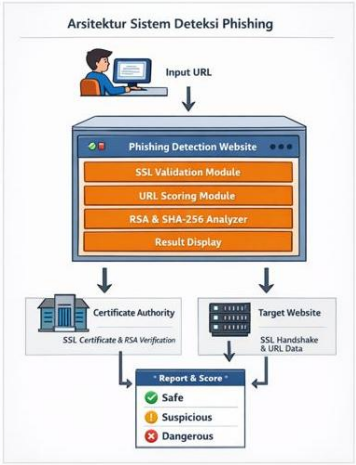
Tanda tangan digital pada sertifikat SSL menggunakan algoritma kriptografi asimetris, salah satunya RSA. RSA bekerja dengan pasangan kunci publik dan kunci privat, di mana CA menandatangani sertifikat menggunakan kunci privatnya, dan klien memverifikasi tanda tangan tersebut menggunakan kunci publik CA (Aryanti & Nabila, 2025). Proses ini memastikan bahwa sertifikat tidak dimodifikasi dan benar-benar diterbitkan oleh CA yang sah. Selain itu, algoritma hash SHA-256 digunakan untuk menghasilkan nilai hash yang unik sebagai fingerprint sertifikat, sehingga integritas data dapat dipastikan (Suwarno & Hardjianto, 2024).

Selain aspek kriptografi, analisis heuristik URL juga berperan penting dalam mendeteksi phishing link. Analisis ini mencakup pemeriksaan panjang URL, penggunaan alamat IP, struktur subdomain, karakter mencurigakan, serta penggunaan Top-Level Domain (TLD) berisiko tinggi (Eriana et al., 2025). Kombinasi antara validasi SSL dan analisis heuristik URL dapat meningkatkan akurasi deteksi karena mampu menilai keamanan baik dari sisi teknis kriptografi maupun struktur URL itu sendiri.

Berdasarkan kajian pustaka tersebut, dapat disimpulkan bahwa masih terdapat celah penelitian dalam pengembangan sistem deteksi phishing link yang mengintegrasikan validasi SSL berbasis kriptografi secara real-time dengan sistem penilaian risiko URL. Oleh karena itu, penelitian ini mengusulkan sebuah website deteksi phishing link yang menggabungkan verifikasi tanda tangan digital RSA, hashing SHA-256, serta URL scoring untuk menghasilkan analisis keamanan yang akurat, transparan, dan mudah dipahami oleh pengguna. Pendekatan ini diharapkan mampu melengkapi penelitian sebelumnya serta memberikan kontribusi dalam pengembangan sistem keamanan web berbasis kriptografi.

3. METODE PENELITIAN

Penelitian ini menggunakan metode perancangan dan implementasi sistem (*system development research*) yang bertujuan untuk membangun sebuah website deteksi phishing link berbasis validasi SSL dan mekanisme URL scoring. Sistem dirancang sebagai aplikasi berbasis web yang menerima input berupa URL dari pengguna dan menghasilkan informasi tingkat keamanan tautan secara real-time. Perancangan sistem mencakup pembentukan modul input URL, modul analisis heuristik, modul validasi SSL/TLS, modul verifikasi kriptografi berbasis RSA dan SHA-256, serta modul penilaian keamanan menggunakan URL scoring.

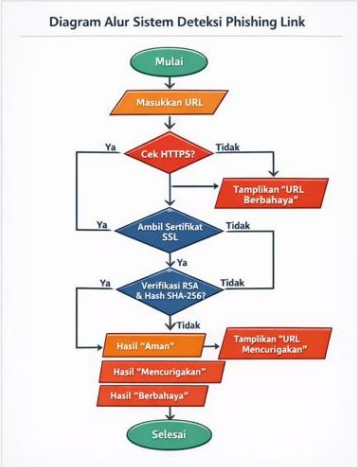


Gambar 1. Arsitektur Sistem Deteksi Phising.

Pengumpulan data dan informasi dilakukan melalui studi literatur dan observasi teknis. Studi literatur digunakan untuk memperoleh pemahaman mengenai karakteristik phishing link, mekanisme kerja SSL/TLS, tanda tangan digital RSA, serta algoritma hash SHA-256 dalam sistem keamanan web. Observasi teknis dilakukan dengan mengamati struktur URL dan sertifikat SSL dari berbagai website sebagai dasar perancangan parameter analisis keamanan.

Pengumpulan data dan informasi dilakukan melalui studi literatur dan observasi teknis. Studi literatur digunakan untuk memperoleh pemahaman mengenai karakteristik phishing link, mekanisme kerja SSL/TLS, tanda tangan digital RSA, serta algoritma hash SHA-256 dalam sistem keamanan web. Observasi teknis dilakukan dengan mengamati struktur URL dan sertifikat SSL dari berbagai website sebagai dasar perancangan parameter analisis keamanan

Proses pengolahan data dimulai dengan menerima URL dari pengguna, kemudian dilakukan proses parsing untuk mengekstraksi informasi domain dan struktur URL. Selanjutnya, sistem melakukan analisis heuristik URL yang meliputi pemeriksaan penggunaan protokol HTTPS, panjang URL, penggunaan alamat IP, struktur subdomain, karakter mencurigakan, serta Top-Level Domain (TLD) berisiko. Setelah itu, sistem melakukan proses validasi sertifikat SSL melalui mekanisme SSL handshake untuk memperoleh sertifikat digital dari server tujuan.



Gambar 2. Diagram Alur Sistem Deteksi Phising Link.

Sertifikat digital yang diperoleh kemudian dianalisis dengan melakukan verifikasi tanda tangan digital menggunakan algoritma RSA, pemeriksaan kesesuaian domain dengan sertifikat, masa berlaku sertifikat, otoritas penerbit sertifikat, serta kekuatan kunci publik RSA. Selain itu, algoritma hash SHA-256 digunakan untuk menghasilkan fingerprint sertifikat dan hash URL sebagai bukti integritas data. Seluruh hasil analisis tersebut diproses menggunakan mekanisme URL scoring untuk menghasilkan skor keamanan yang merepresentasikan tingkat risiko phishing.

Analisis data dilakukan dengan menginterpretasikan skor keamanan dan indikator yang dihasilkan oleh sistem untuk mengklasifikasikan URL ke dalam kategori aman, mencurigakan, atau berbahaya. Hasil analisis ditampilkan dalam bentuk skor keamanan, status risiko, serta visualisasi bukti kriptografi yang mudah dipahami oleh pengguna.

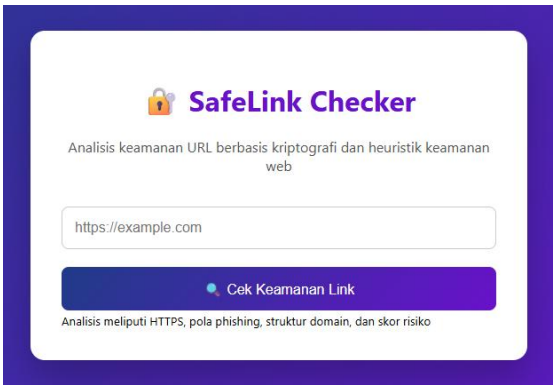
4. HASIL DAN PEMBAHASAN

Hasil Implementasi Sistem Deteksi Phishing Link

Hasil dari penelitian ini berupa sebuah website deteksi phishing link yang mampu menganalisis keamanan suatu URL secara real-time menggunakan kombinasi analisis heuristik URL dan validasi SSL berbasis kriptografi. Sistem yang dikembangkan dapat menerima input URL dari pengguna, kemudian melakukan serangkaian proses pemeriksaan untuk menentukan tingkat keamanan tautan tersebut. Hasil analisis ditampilkan dalam bentuk skor keamanan, status risiko, serta informasi teknis kriptografi yang mendukung hasil penilaian.

Website berhasil diimplementasikan menggunakan bahasa pemrograman PHP dengan memanfaatkan pustaka OpenSSL untuk melakukan proses SSL handshake, verifikasi tanda tangan digital RSA, serta perhitungan hash SHA-256. Sistem dapat menampilkan informasi sertifikat SSL seperti Common Name (CN), Certificate Authority (CA), masa berlaku sertifikat, algoritma kriptografi yang digunakan, dan fingerprint SHA-256. Hal ini sejalan dengan penelitian sebelumnya yang menyatakan bahwa validasi sertifikat SSL merupakan indikator penting dalam mendeteksi keaslian website (Mahmud & Wirawan, 2024).

Website deteksi phishing link yang dikembangkan memiliki halaman utama yang berfungsi sebagai antarmuka input URL. Halaman ini dirancang dengan tampilan sederhana dan informatif agar pengguna dapat dengan mudah memasukkan tautan yang ingin dianalisis. Elemen utama pada halaman depan meliputi kolom input URL, tombol analisis, serta informasi singkat mengenai fungsi sistem.



Gambar 3. Tampilan Halaman Utama Website Deteksi Phishing Link.

Tampilan halaman utama tersebut dirancang responsif sehingga dapat diakses dengan baik melalui berbagai perangkat. Desain antarmuka yang sederhana bertujuan untuk meningkatkan kenyamanan pengguna dan mempercepat proses analisis tautan.

Analisis Heuristik URL

Analisis heuristik URL dilakukan sebagai tahap awal untuk mengidentifikasi indikasi phishing berdasarkan karakteristik struktur URL. Parameter yang dianalisis meliputi penggunaan protokol HTTPS, panjang URL, penggunaan alamat IP, jumlah subdomain, karakter mencurigakan, serta Top-Level Domain (TLD) berisiko. Setiap parameter diberikan bobot tertentu yang berpengaruh terhadap skor keamanan akhir.

Hasil pengujian menunjukkan bahwa URL yang tidak menggunakan HTTPS, memiliki panjang URL berlebihan, atau menggunakan alamat IP secara langsung cenderung memperoleh skor keamanan yang rendah. Temuan ini sejalan dengan penelitian (Syahli et al., 2025) yang menyatakan bahwa pola struktur URL dapat digunakan sebagai indikator awal dalam mendeteksi phishing link. Dengan demikian, analisis heuristik URL pada sistem ini mampu menyaring URL berisiko sebelum dilakukan pemeriksaan kriptografi lebih lanjut.

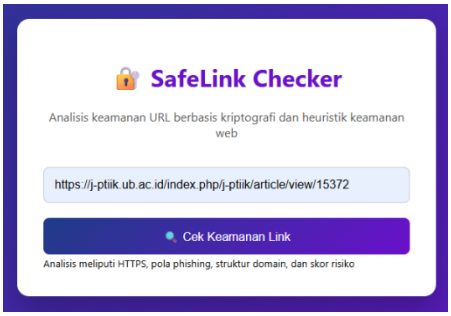
Validasi SSL dan Verifikasi Kriptografi

Tahap selanjutnya adalah validasi sertifikat SSL yang dilakukan melalui proses SSL handshake untuk memperoleh sertifikat digital dari server tujuan. Sertifikat yang diperoleh kemudian dianalisis untuk memastikan keaslian dan keamanannya. Proses validasi meliputi pemeriksaan kesesuaian domain dengan sertifikat, masa berlaku sertifikat, serta otoritas penerbit sertifikat (Certificate Authority).

Selain itu, sistem melakukan verifikasi tanda tangan digital berbasis algoritma RSA untuk memastikan bahwa sertifikat benar-benar ditandatangani oleh CA yang sah. RSA merupakan algoritma kriptografi asimetris yang umum digunakan dalam tanda tangan digital dan aplikasi keamanan web, terutama dalam SSL/TLS, karena kemampuan kriptografisnya untuk memverifikasi keaslian pesan dengan pasangan kunci publik dan privat (Mahfud & Utomo, 2022). Algoritma hash SHA-256 digunakan untuk menghasilkan fingerprint sertifikat sebagai bukti integritas data, karena fungsi hash kriptografis ini menghasilkan nilai unik yang sangat sensitif terhadap perubahan input (Perdana et al., 2023)

Uji Coba Sistem Menggunakan Contoh URL

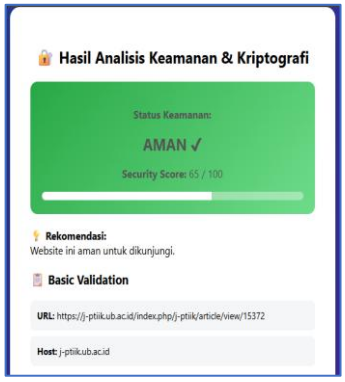
Untuk menguji kinerja sistem, dilakukan uji coba menggunakan satu contoh URL yang dimasukkan melalui halaman utama website. URL uji dimasukkan oleh pengguna pada kolom input, kemudian sistem memproses URL tersebut secara otomatis sesuai dengan alur yang telah dirancang.



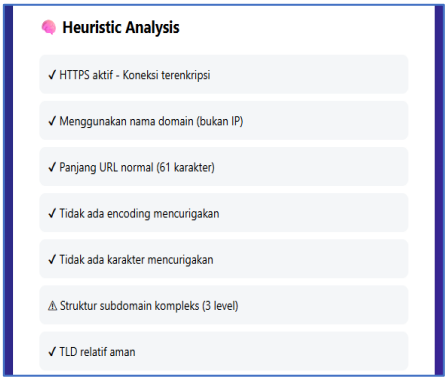
Gambar 4 Tampilan Uji Coba Pada Contoh URL.

Pada tahap awal, sistem melakukan parsing URL untuk mengekstraksi informasi domain dan struktur URL. Selanjutnya, sistem menjalankan analisis heuristik untuk mengidentifikasi indikasi phishing berdasarkan karakteristik URL. Setelah itu, sistem melanjutkan ke tahap validasi SSL dan verifikasi kriptografi untuk memastikan keaslian sertifikat digital dari website tujuan.

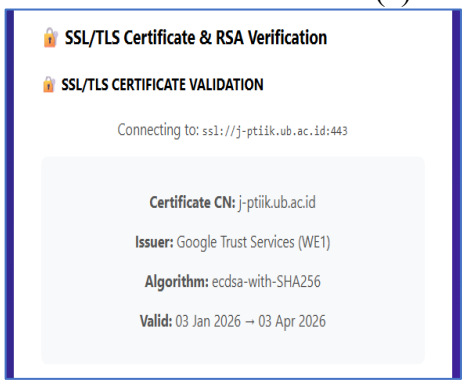
Hasil dari proses uji coba ditampilkan pada halaman hasil analisis yang menyajikan skor keamanan, status risiko, serta detail hasil validasi SSL dan kriptografi. Informasi yang ditampilkan mencakup status HTTPS, hasil verifikasi tanda tangan digital RSA, fingerprint SHA-256, serta klasifikasi risiko keamanan URL.



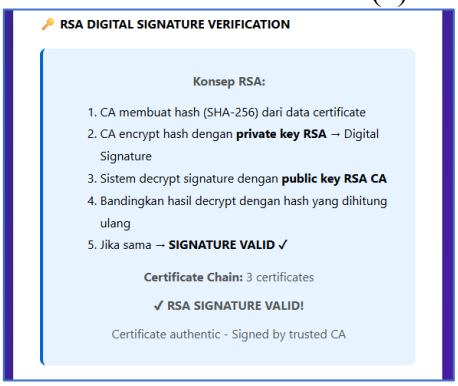
Gambar 5 Tampilan Halaman Hasil Analisis Keamanan URL (1).



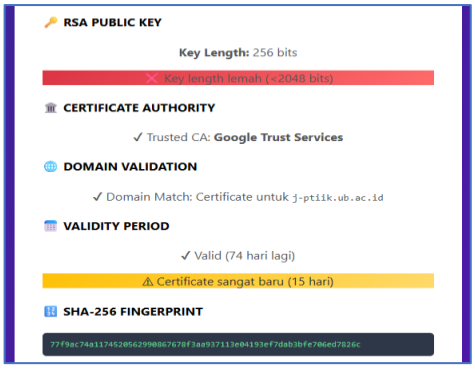
Gambar 6 Tampilan Halaman Hasil Analisis Keamanan URL (2).



Gambar 7 Tampilan Halaman Hasil Analisis Keamanan URL (3).



Gambar 8 Tampilan Halaman Hasil Analisis Keamanan URL (4).



Gambar 9 Tampilan Halaman Hasil Analisis Keamanan URL (5).

Gambar 10 Tampilan Halaman Hasil Analisis Keamanan URL (6).

Uji coba ini menunjukkan bahwa sistem mampu mengintegrasikan proses input URL, analisis heuristik, validasi SSL, dan penilaian keamanan ke dalam satu alur kerja yang terstruktur. Penyajian hasil dalam bentuk visual memudahkan pengguna dalam memahami tingkat keamanan URL yang diuji.

Untuk mengevaluasi kinerja sistem deteksi phishing link, dilakukan pengujian terhadap beberapa URL dengan karakteristik yang berbeda. Pengujian ini bertujuan untuk mengetahui kemampuan sistem dalam mengklasifikasikan tingkat keamanan URL berdasarkan analisis heuristik dan validasi SSL yang telah diterapkan. URL yang diuji terdiri dari website resmi dengan sertifikat SSL valid serta URL yang memiliki karakteristik mencurigakan yang umum ditemukan pada serangan phishing.

Tabel 1. Hasil Uji Coba Sistem Deteksi Phishing Link

No	URL Uji	HTTPS	SSL Valid	RSA Key (bit)	Skor Keamanan	Kategori Risiko
1	https://share.google/sPQGTqsfmKuD8HukZ	Ya	Valid	256	25	Berbahaya
2	https://www.wa-75jt.blogspot.com	Ya	Failed	–	45	mencurigakan
3	http://login-paypal.verify-user.tk	Tidak	Failed	–	35	Berbahaya
4	https://chatgpt.com/c/69689c8a-2ae0-8320-82bd-50310391d42c	Ya	Valid	256	70	Aman
5	https://account-security.example.com	Ya	Failed	–	50	Mencurigakan

Berdasarkan hasil uji coba yang ditampilkan pada tabel hasil pengujian, sistem deteksi phishing link menunjukkan kemampuan yang baik dalam mengidentifikasi tingkat risiko keamanan dari berbagai URL dengan karakteristik yang berbeda. Setiap URL dianalisis berdasarkan penggunaan protokol HTTPS, validitas sertifikat SSL, kekuatan kriptografi RSA, serta skor keamanan yang dihasilkan dari mekanisme URL scoring.

Pada URL uji pertama, meskipun menggunakan protokol HTTPS dan memiliki sertifikat SSL yang valid, sistem memberikan skor keamanan yang rendah dan mengklasifikasikannya sebagai berbahaya. Hal ini disebabkan oleh penggunaan struktur domain yang tidak lazim serta karakteristik URL yang menyerupai layanan berbagi tautan, yang sering dimanfaatkan dalam skema phishing. Panjang kunci RSA yang rendah juga menjadi indikator tambahan yang menurunkan tingkat kepercayaan terhadap URL tersebut.

URL uji kedua menggunakan protokol HTTPS, namun validasi sertifikat SSL mengalami kegagalan. Domain yang digunakan berasal dari platform blog gratis yang sering disalahgunakan untuk tujuan phishing. Kondisi ini menyebabkan skor keamanan berada pada kategori menengah dan diklasifikasikan sebagai mencurigakan, karena meskipun koneksi terenkripsi tersedia, keabsahan identitas server tidak dapat diverifikasi secara penuh.

Pada URL uji ketiga, sistem mendeteksi bahwa URL tidak menggunakan protokol HTTPS dan sertifikat SSL tidak tersedia. Selain itu, struktur domain yang meniru layanan pembayaran digital resmi merupakan indikator kuat terjadinya phishing. Kombinasi faktor tersebut menghasilkan skor keamanan yang rendah dan klasifikasi risiko berbahaya. Temuan ini menunjukkan bahwa analisis heuristik URL berperan penting dalam mendeteksi phishing bahkan sebelum proses validasi kriptografi dilakukan.

URL uji keempat menunjukkan hasil yang lebih baik dibandingkan URL lainnya. Penggunaan HTTPS, sertifikat SSL valid, serta struktur domain yang sesuai menghasilkan skor keamanan yang tinggi dan diklasifikasikan sebagai aman. Meskipun demikian, sistem tetap melakukan pemeriksaan kriptografi untuk memastikan keaslian sertifikat dan integritas data, sehingga hasil analisis dapat dipercaya oleh pengguna.

Pada URL uji kelima, meskipun menggunakan HTTPS, kegagalan validasi sertifikat SSL menyebabkan penurunan skor keamanan. Domain generik yang tidak terverifikasi juga meningkatkan potensi risiko phishing. Oleh karena itu, sistem mengklasifikasikan URL ini sebagai mencurigakan, karena masih terdapat indikasi risiko meskipun tidak sekuat URL berbahaya lainnya.

Secara keseluruhan, pembahasan tabel hasil uji coba menunjukkan bahwa sistem mampu mengombinasikan analisis heuristik URL dan validasi kriptografi secara efektif. Sistem tidak hanya bergantung pada penggunaan HTTPS, tetapi juga mempertimbangkan keabsahan sertifikat SSL, kekuatan kriptografi, serta pola struktur URL dalam menentukan tingkat risiko phishing. Hasil ini mendukung pendekatan penelitian yang menekankan pentingnya analisis multilayer dalam sistem deteksi phishing link.

Hasil URL Scoring dan Klasifikasi Risiko

Berdasarkan hasil analisis heuristik dan validasi SSL, sistem menghitung skor keamanan URL menggunakan mekanisme URL scoring. Skor keamanan berada pada rentang 0 hingga 100 dan digunakan untuk mengklasifikasikan URL ke dalam kategori sangat aman, aman, mencurigakan, atau berbahaya. Pendekatan ini memberikan gambaran tingkat risiko yang lebih fleksibel dibandingkan klasifikasi biner.

Hasil pengujian menunjukkan bahwa URL dengan sertifikat SSL valid, domain yang sesuai, serta struktur URL yang wajar memperoleh skor keamanan yang tinggi. Sebaliknya, URL dengan sertifikat tidak valid atau karakteristik URL mencurigakan memperoleh skor yang rendah. Pendekatan ini sejalan dengan penelitian (Perdana, 2025) yang menyatakan bahwa sistem berbasis skor mampu merepresentasikan tingkat risiko keamanan secara lebih akurat.

Pembahasan Hasil Penelitian

Berdasarkan hasil implementasi dan pengujian sistem, website deteksi phishing link yang dikembangkan mampu mengidentifikasi indikasi phishing secara efektif dengan mengombinasikan analisis heuristik URL dan validasi kriptografi. Pendekatan ini memberikan keunggulan dibandingkan metode deteksi phishing yang hanya mengandalkan struktur URL tanpa melakukan pemeriksaan sertifikat digital.

Integrasi mekanisme URL scoring memungkinkan sistem menyajikan hasil analisis dalam bentuk yang mudah dipahami oleh pengguna. Selain itu, penyajian bukti kriptografi seperti fingerprint SHA-256 dan verifikasi tanda tangan digital RSA meningkatkan tingkat kepercayaan pengguna terhadap hasil analisis sistem. Hasil penelitian ini sejalan dengan temuan (Uriawan et al., 2024) yang menyatakan bahwa sistem deteksi phishing berbasis kombinasi heuristik dan kriptografi memiliki tingkat keandalan yang lebih tinggi.

Berdasarkan hasil implementasi dan pengujian, sistem deteksi phishing link yang dikembangkan mampu mendeteksi indikasi phishing secara efektif dengan mengombinasikan analisis heuristik URL dan validasi kriptografi. Integrasi validasi SSL dan verifikasi tanda tangan digital RSA memberikan keunggulan dibandingkan sistem yang hanya mengandalkan struktur URL.

Selain itu, penyajian bukti kriptografi seperti fingerprint SHA-256 dan detail sertifikat SSL meningkatkan transparansi hasil analisis dan kepercayaan pengguna. Hasil penelitian ini mendukung temuan (Uriawan et al., 2024) yang menyatakan bahwa kombinasi analisis URL dan validasi sertifikat digital dapat meningkatkan akurasi deteksi phishing link. Dengan demikian, sistem yang dikembangkan tidak hanya berfungsi sebagai alat deteksi, tetapi juga sebagai media edukasi keamanan siber bagi pengguna.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil perancangan, implementasi, dan pengujian sistem deteksi phishing link yang telah dilakukan, dapat disimpulkan bahwa website yang dikembangkan mampu mendeteksi potensi phishing secara efektif dengan mengombinasikan analisis heuristik URL dan validasi sertifikat SSL berbasis kriptografi. Sistem memungkinkan pengguna untuk melakukan analisis keamanan URL secara langsung melalui antarmuka web yang sederhana dan mudah digunakan. Hasil pengujian menunjukkan bahwa sistem tidak hanya bergantung pada penggunaan protokol HTTPS, tetapi juga melakukan pemeriksaan keabsahan sertifikat SSL, verifikasi tanda tangan digital berbasis RSA, serta pembentukan fingerprint menggunakan algoritma hash SHA-256. Pendekatan ini mampu memberikan penilaian keamanan URL yang lebih akurat dan informatif dibandingkan metode deteksi berbasis satu parameter.

Penerapan mekanisme URL scoring terbukti efektif dalam mengklasifikasikan tingkat risiko URL ke dalam kategori aman, mencurigakan, dan berbahaya. Sistem juga mampu mengidentifikasi URL yang menggunakan HTTPS namun memiliki karakteristik domain atau sertifikat yang mencurigakan, sehingga dapat memberikan peringatan dini kepada pengguna. Dengan demikian, sistem yang dikembangkan tidak hanya berfungsi sebagai alat deteksi phishing, tetapi juga sebagai media edukasi keamanan siber bagi pengguna dalam mengenali risiko tautan berbahaya.

Untuk pengembangan penelitian selanjutnya, sistem deteksi phishing link ini dapat ditingkatkan dengan menambahkan metode berbasis pembelajaran mesin (machine learning) guna meningkatkan akurasi klasifikasi URL berdasarkan pola serangan phishing yang lebih kompleks. Selain itu, integrasi dengan basis data phishing global seperti blacklist URL dapat membantu mempercepat proses deteksi.

Pengembangan selanjutnya juga disarankan untuk menambahkan analisis konten halaman web dan pemeriksaan reputasi domain secara historis agar sistem mampu mendeteksi phishing yang menggunakan teknik penyamaran tingkat lanjut. Dari sisi antarmuka, visualisasi hasil analisis dapat diperluas dalam bentuk grafik interaktif untuk meningkatkan pemahaman pengguna terhadap hasil evaluasi keamanan. Dengan pengembangan tersebut, sistem diharapkan dapat menjadi solusi deteksi phishing yang lebih komprehensif dan adaptif terhadap perkembangan ancaman keamanan siber.

DAFTAR REFERENSI

Aryanti, A., & Nabila, N. (2025). Deteksi Url Phishing Menggunakan Algoritma Support Vector Machine Berbasis Website. *Jurnal Rekayasa Sistem Komputer*, *8*(2). https://doi.org/https://doi.org/10.31598

Eriana, E. S., Zein, A., Wati, F. E., & Buminata, M. S. A. (2025). Sosialisasi Keamanan Digital Untuk Mengatasi Phishing Dan Apk Berbahaya. *Attamkiim: Jurnal Pengabdian Masyarakat*, *2*(1). https://doi.org/https://doi.org/10.62070/attamkiim.v2i1.248

Fatiha, M. R., Setiawan, I., Ikhsan, A. N., & Yunita, I. R. (2024). OPTIMISASI SISTEM DETEKSI PHISHING BERBASIS WEB MENGGUNAKAN ALGORITMA DECISION TREE. *Jurnal Ilmiah IT CIDA: Diseminasi Teknologi Informasi*, *10*(2). https://doi.org/https://doi.org/10.55635/jic.v10i2.212

Fauzan, R., Vitianingsih, A. V., Cahyono, D., Maukar, A. L., & Suprio, Y. A. B. (2025). Penerapan Algoritma Klasifikasi pada Machine Learning untuk Deteksi Phishing. *Indonesian Journal of Machine Learning and Computer Science*, *5*(2). https://doi.org/https://doi.org/10.57152/malcom.v5i2.1968

Hartanto, B. D., Nugraha, T. A., Ramadhan, B. R., Pratama, M. A., & Alamsyah, R. P. (2025). Edukasi Keamanan Digital untuk Meningkatkan Kewaspadaan Masyarakat Terhadap Link Phising. *Jurnal Pengabdian Sosial*, *2*(9). https://doi.org/https://doi.org/10.59837/nndaqp49

Irawan, A., Heryana, N., Hopipah, H., & Rahma, D. (2021). Identifikasi Website Phishing dengan Perbandingan Algoritma Klasifikasi. *Syntax : Jurnal Informatika*, *10*, 57–67. https://doi.org/10.35706/syji.v10i01.5292

Lukito, & Handaya, W. (2025). Deteksi Website Phishing Menggunakan Teknik Machine Learning. *Jurnal Informatika Atma Jogja*, *6*(1), 69–80. https://doi.org/10.24002/jiaj.v6i1.11538

Mahfud, I., & Utomo, P. (2022). Implementasi Sistem Kriptografi RSA Signature dengan SHA-256 pada Mekanisme Autentikasi REST API. *Prosiding Seminar Nasional Teknoka*, *6*(1), 84–92. https://doi.org/10.22236/teknoka.v6i1.431

Mahmud, A. F., & Wirawan, S. (2024). Deteksi Phishing Website menggunakan Machine LearningMetode Klasifikasi. *Sistemasi:Jurnal Sistem Informasi*, *13*(4). https://doi.org/https://doi.org/10.32520/stmsi.v13i4.3456

Muliono, Y., Ma'ruf, M., & Azzahra, Z. (2023). Phishing Site Detection Classification Model Using Machine Learning Approach. *Engineering, MAthematics and Computer Science (EMACS) Journal*, *5*(2), 63–67. https://doi.org/10.21512/emacsjournal.v5i2.9951

Perdana, A., Syahputra, D. R., Manurung, S. F., Hafizh, T., & Hutasuhut, D. I. G. (2023). IMPLEMENTASI ALGORITMA SHA UNTUK ENKRIPSI TEKS BERBASIS MOBILE. *JURNAL INFORMATIKA DAN TEKONOLOGI KOMPUTER*, *3*(2), 115–122. https://doi.org/https://doi.org/10.55606/jitek.v3i2.1736

Perdana, Y. (2025). Comparative Analysis of Random Forest and XGBoost for Detecting Phishing Websites: A Machine Learning Approach. *Jurnal Kridatama Sains Dan Teknologi*, *7*(2). https://doi.org/https://doi.org/10.53863/kst.v7i02.1933

Raihan, A., Fadhli, M., & Lindawati. (2024). IMPLEMENTATION OF DEEP LEARNING FOR DETECTING PHISHING ATTACKS ON WEBSITES WITH COMBINATION OF CNN AND LSTM. *Jurnal Teknik Informatika*, *5*(5). https://doi.org/https://doi.org/10.52436/1.jutif.2024.5.5.2446

Suwarno, D. B., & Hardjianto, M. (2024). Deteksi Website Phishing Dari Analisis Url Menggunakan Algoritma Random Forest. *Bit (Fakultas Teknologi Informasi Universitas Budi Luhur)*, *21*(2).

Syahli, A., Kurniati, R., & Hidayasari, N. (2025). Alat OSINT Berbasis Web untuk Deteksi URL Phishing Menggunakan Integrasi API. *Techno.COM*, *24*(3). https://doi.org/https://doi.org/10.62411/tc.v24i3.13769

Uriawan, W., Ramadita, R., Putra, R., Siregar, R., & Addiva, R. (2024). *Authenticate and Verification Source Files using SHA256 and HMAC Algorithms*. https://doi.org/10.20944/preprints202407.0075.v1