# IMPLEMENTASI JARINGAN LSTM DALAM MENGEMBANGKAN SISTEM DETEKSI URL PHISHING SECARA REAL-TIME

**Jerry Ruslim[1], Viny Christianti Mawardi[2], Manatap Dolok Lauro[3]**

[1]Jurusan Teknik Informatika, Universitas Tarumanagara

*Email: jerry.53200031@stu.untar.ac.id*

[2] Jurusan Teknik Informatika, Universitas Tarumanagara

*Email:*

[3] Jurusan Teknik Informatika, Universitas Tarumanagara

*Email:*

**ABSTRAK**

Phishing adalah bentuk serangan siber dimana pelaku melakukan usaha penipuan terhadap tergetnya agar memberikan informasi sensitif, seperti kata sandi atau informasi kartu kredit, dengan menyamar sebagai entitas yang sah. Serangan ini sering kali dilakukan melalui tautan palsu yang dikirim melalui email, pesan teks, atau situs web yang meniru platform tepercaya. Phishing menjadi ancaman serius bagi individu maupun organisasi, yang dapat menyebabkan kerugian finansial dan pelanggaran privasi. Penelitian ini memperkenalkan aplikasi berbasis web yang dirancang untuk mendeteksi URL phishing menggunakan model Long Short-Term Memory (LSTM), sejenis Recurrent Neural Network (RNN) yang sangat efektif dalam menganalisis data sekuensial, sehingga dipercaya dapat mengenali pola jangka panjang yang sering ditemukan dalam URL phishing. Aplikasi ini dapat menerima input URL dari pengguna dan memprediksi apakah URL tersebut phishing atau sah secara *real-time*. Dataset yang digunakan diperoleh dari Kaggle dan PhishTank, yang berisi tautan situs phishing dan situs sah. Setelah melalui tahap pra-pemrosesan berupa normalisasi, tokenisasi, dan embedding, URL akan dianalisis oleh model LSTM. Aplikasi ini dirancang dengan harapan dapat memberikan informasi yang akurat dan terpercaya tentang keamanan situs web yang dikunjungi pengguna. Dengan adanya informasi yang jelas dan tersedia secara real-time, diharapkan pengguna dapat meningkatkan kewaspadaan terhadap situs web yang mencurigakan. Dengan demikian, akan secara langsung meningkatkan keamanan pengguna.

**Kata Kunci:** Phishing, URL, LSTM, *real-time*

***ABSTRACT***

*Phishing is a form of cyberattack in which perpetrators attempt to deceive their targets into providing sensitive information, such as passwords or credit card information, by impersonating legitimate entities. These attacks are often carried out through fraudulent links sent via email, text messages, or websites that mimic trusted platforms. Phishing poses a serious threat to both individuals and organizations, leading to financial losses and privacy breaches. This study introduces a web-based application designed to detect phishing URLs using the Long Short- Term Memory (LSTM) model, a type of Recurrent Neural Network (RNN) that is highly effective in analyzing sequential data, making it capable of recognizing long-term patterns commonly found in phishing URLs. The application can accept URL input from users and predict whether the URL is phishing or legitimate in real time. The dataset used is sourced from Kaggle and PhishTank, containing links to both phishing and legitimate websites. After going through pre-processing stages, including normalization, tokenization, and embedding, the URLs are analyzed by the LSTM model. This application is designed with the hope of providing accurate and reliable information about the security of the websites visited by users. With clear information available in real time, it is expected that users can enhance their vigilance against suspicious websites. Consequently, this will directly improve user security.*

***Keywords:*** *Phishing, URL, LSTM, real-time*

## 1. PENDAHULUAN

### Latar Belakang

Perkembangan era digital yang pesat telah mempermudah berbagai aktivitas manusia, seperti akses terhadap informasi, transaksi keuangan, dan komunikasi jarak jauh. Namun, kemajuan ini juga diiringi dengan peningkatan ancaman siber yang signifikan. Ancaman ini tidak dapat dipandang sebelah mata karna bisa mengakibatkan kerugian bagi individu, organisasi dan bahkan negara. Serangan siber dapat terjadi dalam berbagai bentuk, seperti pemerasan, peretasan, dan denial of service (DoS), yang semuanya memiliki potensi untuk menimbulkan kerugian yang besar bagi korban.

Salah satu ancaman siber yang paling sering mendapatkan perhatian adalah phishing, di mana pelaku berusaha mendapatkan informasi sensitif dengan menyamar sebagai entitas yang sah. Metode ini terus berkembang dengan pendekatan dan metode yang unik yang dapat menciptakan kerugian finansial serta mengancam privasi data korbannya. Teknik yang sering digunakan dalam phishing termasuk manipulasi tautan, pemalsuan situs web, dan rekayasa sosial. Upaya phishing biasanya ditandai dengan tawaran yang terlalu menarik dan penggunaan bahasa mendesak, sehingga dapat dengan mudah menjerat korban yang tidak waspada.

Untuk melawan ancaman ini, penting untuk meningkatkan keamanan siber. Penelitian ini bertujuan untuk mengembangkan aplikasi web yang dapat mendeteksi upaya phishing menggunakan teknik Long Short-Term Memory (LSTM). LSTM, yang merupakan jenis Recurrent Neural Network (RNN), dipilih karena kemampuannya dalam memproses data sekuensial dan memahami dependensi jangka panjang, sehingga diharapkan dapat secara otomatis mempelajari karakteristik yang umum dimiliki URL phishing.

### Rumusan Masalah

Kekhawatiran terhadap keamanan siber mendorong pengembangan berbagai metode perlindungan. Salah satu metode yang sering digunakan oleh browser adalah blacklisting, tetapi pendekatan ini kurang efektif dalam mendeteksi situs phishing yang baru dan sering kali dapat diakali. Oleh karena itu, diperlukan metode yang lebih canggih untuk mendeteksi situs phishing dengan lebih akurat dan cepat. Penelitian ini bertujuan untuk mengembangkan aplikasi web yang mendeteksi situs phishing menggunakan metode Long Short-Term Memory (LSTM), yang terkenal dalam memproses data urutan waktu.

## 2. METODE PENELITIAN

Program ini dirancang sebagai aplikasi web yang menggunakan machine learning untuk mendeteksi situs phishing. Aplikasi ini menerima input berupa URL dari pengguna, yang kemudian diproses oleh model LSTM (Long Short-Term Memory) yang telah dilatih sebelumnya. Proses pelatihan model mencakup beberapa tahap penting, seperti normalisasi URL, tokenisasi, dan representasi numerik menggunakan embedding, seblum akhirnya dijadikan input dalam pelatihan model LSTM. Selain itu, akan dilakukan ekstraksi fitur seperti panjang url, nama domain, dan banyak symbol dalam URL. Fitur-fitur ini akan diumpan ke dalam beberapa jaringan dense layer. Hasil dari keseluruhan proses ini akan digabungkan dan melalui satu lapisan dense layer terakhir untuk klasifikasi. Setelah selesai dengan tahap pelatihan, akan dilakukan evaluasi model menggunakan teknik hyperparameter tuning serta memanfaatkan confusion matrix untuk menemukan model dengan akurasi paling tinggi.

**Pengumpulan data**

Pengumpulan data dilakukan dari dua sumber utama: Kaggle, platform yang menyediakan berbagai dataset gratis, dan PhishTank, sebuah komunitas anti-phishing yang menyediakan dataset URL situs phishing dan situs sah. Data yang dikumpulkan terdiri dari tautan URL dari situs phishing dan situs sah yang telah dikonfirmasi.

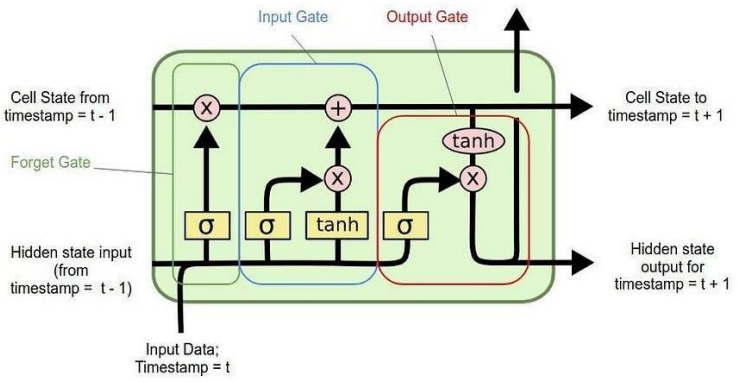
**Pra-pemrosesan**

Pengumpulan data dilakukan dari dua sumber utama: Kaggle, platform yang menyediakan berbagai dataset gratis, dan PhishTank, sebuah komunitas anti-phishing yang menyediakan dataset URL situs phishing dan situs sah. Data yang dikumpulkan terdiri dari tautan URL dari situs phishing dan situs sah yang telah dikonfirmasi.

**LSTM**

LSTM yang pertama kali diperkenalkan oleh Hochreiter dan Schmidhuber pada tahun 1997, merupakan jenis *Recurrent Neural Network* yang telah dimodifikasi untuk mengatasi kekurangan dalam perihal ingatan yang mengakibatkan turunnya kemampuan klasifikasi dalam jangka waktu yang lebih lama. Modifikasi ini dilakukan dengan cara menambahkan sel memori, yang memungkinkan LSTM untuk menyimpan informasi dalam jangka waktu yang lama, sehingga menjadi jauh lebih efektif dalam memproses dan mengklasifikasikan data sekuensial. *Long short term memory* (LSTM) adalah salah satu variasi dari *recurrent neural network* (RNN). RNN dikenal dengan kemampuannya yang sangat baik dalam menangkap informasi dari data sekuensial.

Sebuah sel LSTM terdiri ari beberapa bagian yang disebut dengan *gate*. Pertama adalah *forget gate* yang berfungsi untuk menentukan banyak informasi yang perlu disimpan dan dilupakan dari sel LSTM sebelumnya. Kedua, *input gate* memiliki fungsi untuk menyaring informasi baru yang dianggap penting dan relevan untu disimpan. Ketiga adalah *output gate*, yang merupakan *gate* terakhir yang berfungsi untuk meneruskan informasi ke sel LSTM berikutnya. Struktur dari sebuah sel LSTM dapat dilihat pada Gambar 1.




Gambar 1. Struktur sel LSTM Sumber

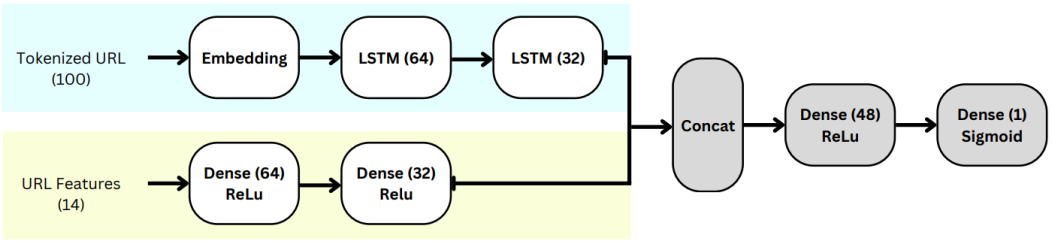
Gambar: https://medium.com/

## 3. HASIL DAN PEMBAHASAN

Rancangan arsitektur yang digunakan dalam penelitian ini melibatkan kombinasi antara model Long Short Term Memory (LSTM) dan dense layer. LSTM digunakan untuk menganalisa dan mempelajari pola yang ditemukan dalam suatu URL dan menggunakan kemampuannya untuk mempelajari data secara kontesktual, sementara jaringan dense memiliki tugas untuk memproses fitur tambahan dalam URL yang relevan terhadap keamanan situs. Fitur-fitur tambahan yang digunakan dalam pemrosesan jaringan dense, antara lain:

1. Panjang URL
2. Penggunaan IP address dalam domain
3. Tingkat entropi URL
4. Karakter punycode
5. Rasio huruf dan angka dalam URL
6. Banyak titik dalam URL
7. Banyak simbol '@' dalam URL
8. Banyak simbol '-' dalam URL
9. Banyak TLD (top level domain) dalam URL
10. Penggunaan angka dalam domain
11. Banyak subdomain dalam URL
12. Tingkat entropi karakter non-alfanumerik
13. Tautan dalam subdirektori URL
14. Umur domain

Model ini dirancang untuk menggabungkan kombinasi dari dua pendekatan yang berbeda. Dengan memanfaatkan kelebihan dari setiap pendekatan, diharapkan model ini dapat menangkap pola dan karakteristik yang lebih kompleks di dalam URL untuk memperoleh hasil prediksi yang lebih akurat.




Gambar 2. Rancangan arsitektur model pendeteksi URL phishing

Dalam tahap pelatihan dan pengujian model menggunakan teknik hyperparameter tuning untuk menemukan kombinasi optimizer dan fungsi aktivasi dengan performa paling baik. Semua proses pelatihan model menggunakan jumlah epoch yang sama, yaitu sebanyak 60 epoch. Hasil pengujian model menggunakan dataset Kaggle dapat dilihat pada Tabel 1.

Tabel 1. Hasil pelatihan model dengan hyperparameter tuning

| | **Optimizer** | **Fungsi Aktivasi** | **Akurasi Validasi** | **Loss Validasi** |
|---|---|---|---|---|
| Model 1 | Adam | Relu | 99,95% | 0,21% |
| Model 2 | SGD | Tanh | 97,00% | 9,58% |
| Model 3 | Adam | Sigmoid | 98,63% | 6,86% |
| Model 4 | SGD | Relu | 93,47% | 17,92% |
| Model 5 | Adam | Tanh | 98,04% | 9,97% |
| Model 6 | SGD | Sigmoid | 97,00% | 10,21% |

Setiap model juga dilakukan kalkulasi terhadap presisi, recall, dan F-1 Score yang dapat dilihat pada Tabel 2.

Tabel 2. Hasil klasifikasi model

| | **Presisi** | **Recall** | **F-1 Score** |
|---|---|---|---|
| Model 1 | 99,96% | 99,94% | 99,95% |
| Model 2 | 95,39% | 98,78% | 97,05% |
| Model 3 | 98,37% | 98,91% | 98,64% |
| Model 4 | 91,54% | 95,82% | 93,63% |
| Model 5 | 97,69% | 98,42% | 98,08% |
| Model 6 | 98,86% | 95,07% | 96,93% |

Dari hasil pengujian model dapat dilihat bahwa Model 1, dengan kombinasi antara optimizer Adam dan fungsi aktivasi Relu memiliki performa paling baik dalam mendeteksi URL phishing dengan akurasi sebesar 99,95%.

Selain pengujian dengan teknik hyperparameter tuning, dilakukan juga pengujian ketika hanya menggunakan jaringan LSTM dan hanya menggunakan jaringan dense.

Tabel 3. Perbandingan akurasi model berdasarkan arsitektur

| | **Akurasi Latih** | **Loss Latih** | **Akurasi Validasi** | **Loss Validasi** |
|---|---|---|---|---|
| LSTM + Dense | 99,94% | 0,20% | 99,95% | 0,21% |
| LSTM | 98,40% | 5,59% | 95,67% | 17,44% |
| Dense | 89,86% | 15,22% | 99,75% | 1,49% |

Selain itu, dilakukan juga perbandingan pengujian dari Model 1 menggunakan dataset Ebbu2017 yang dapat dilihat pada Tabel 4.

Tabel 4. Perbandingan akurasi model berdasarkan sumber dataset

| Dataset | Jumlah Data | Akurasi |
|---|---|---|
| Kaggle | 20.000 | 99,95% |
| Ebbu2017 | 73.575 | 52,03% |

Dari perbandingan hasil pengujian dataset Kaggle dan dataset Ebbu2017, dapat dilihat perbedaan yang cukup signifikan dalam akurasi. Hal ini dapat disebabkan dataset Ebbu2017 yang terdiri dari URL lama yang sudah tidak akttif, sehingga tidak dapat dilakukan ekstraksi terhadap fitur umur domain. Kegagalan dalam ekstraksi fitur ini menjadi kendala yang cukup besar, dikarenakan fitur yang digunakan dalam pelatihan tidak ditemukan dalam dataset pengujian.

## 4. KESIMPULAN DAN SARAN

Dari hasil perancangan dan pengujian arsitektur LSTM dan jaringan dense, diperoleh kesimpulan bahwa model ini bisa diandalkan dalam mendeteksi URL phishing dengan akurasi 99,95%. Namun, terlihat penurunan yang cukup signifikan ketika dilakukan pengujian menggunakan dataset Ebbu2017 tanpa adanya fitur umur domain yang bisa diekstrak.

Saran yang bisa diberikan untuk penelitian berikutnya adalah menambahkan dataset pelatihan yang lebih banyak beragam untuk memperkaya informasi yang dimiliki model dalam pengenalan pola-pola dalam URL. Selain itu, dapat dilakukan penambahan fitur lainnya yang relevan dalam mengenali fitur phishing, atau bahkan melakukan scraping ke dalam konten dari website itu sendiri.

**Ucapan Terima Kasih** (*Acknowledgement*)

Penulis juga tidak lupa memberikan ucapan terima kasih bagi seluruh pihak yang turut membantu dalam penelitian ini, terutama kepada Ibu Viny Christianti Mawardi dan Bapak Manatap Dolok Lauro selaku pembimbing penelitian, pihak yang menyediakan dataset yang digunakan dalam penelitian ini, dan tema-teman yang ikut memberikan dukungan, serta pihak-pihak lainnya yang tidak disebutkan yang ikut membantu penyelesaian penelitian ini baik secara langsung atau tidak langsung.

**REFERENSI**


Kevin Marcello, J. (2020). "Perbandingan Kinerja Algoritma Naïve Bayes dan C4.5 untuk mendeteksi pengelabuan Uniform Resource Locator (Phishing URL)". Jurnal Ilmu Komputer & Sistem Informasi (JIKSI), 8, 116-120.

Santoso, S. (2018). "Memperkuat Pertahan Siber Guna Meningkatkan Ketahanan Nasional".

Jurnal Lemhannas RI, 6, 43-48.

Sanjiban Sekhar, R. (2022). "Multimodel phishing url detection using lstm, bidirectional lstm, and gru models". *Future Internet*, *14*, 340.

Gopali, S. (2024)." The Performance of Sequential Deep Learning Models in Detecting Phishing Websites Using Contextual Features of URLs". *Computers and Structures.* 1064-1066.

Koray Sahingoz, O. (2019). "Machine learning based phishing detection from URLs". *Expert Systems with Applications, 117,* 345-357.

Ozcan, A., Catal, C., Donmez, E., & Senturk, B. (2023). "A hybrid DNN–LSTM model for detecting phishing URLs". *Neural Computing and Applications*, 1-17.

Hochreiter, S. (1997). "Long Short-term Memory". *Neural Computation MIT-Press*.

Ebubekirbbr**.** (2017). *PDD* [Source code]. GitHub. https://github.com/ebubekirbbr/pdd.