DAFTAR PUSTAKA

Mia Haryati Wibowo dan Nur Fatimah, "Ancaman *phishing* terhadap pengguna sosial media dalam dunia cyber crime," JOEICT(jurnal Educ. Inf. Commun. Technol., vol. 1, pp. 1–5, 2017, [Online]. Available: http://jurnal.stkippgritulungagung.ac.id/index.php/joeict/article/view/69

D. Rachmawati, "*Phising* Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber," J. Ilm. Saintikom, Univ. Sumatera Utara, Medan, vol. 1978–6603, pp. 209–216, 2014

Atsuto Seko, Tomoya Maekawa, Koji Tsuda, and Isao Tanaka 2014 "*Machine Learning* with *system*atic density-functional theory calculations: Application to melting temperatures of single- and binary-component solids" Phys. Rev. B 89,054303 https://journals.aps.org/prb/abstract/10.1103/PhysRevB.89.054303

Defiyanti, S. & Pardede, C., 2010. Perbandingan Kinerja Algoritma ID3 dan C4.5 dalam Klasifikasi Spam-Mail. Proceeding Seminar Ilmiah Nasional Komputer dan Sistem Intelijen (KOMMIT 2010), (ISSN: 1411-6286). http://repository.gunadarma.ac.id/ 964/

Rahardja, U., Lutfiani, N., & Rahmawati, R. (2018). APTISI Student Perception to the News on The APTISI Website. Jurnal Ilmiah SISFOTENIKA, 8(2), 117–127.

Al Ghifari, M. A. G., Hananto, B., & Wahyono, B. T. (2022, August). Implementasi Ekstensi Google Chrome Dalam Mendeteksi Situs Web *Phishing* Menggunakan Algoritma Random Forest. In Prosiding Seminar Nasional Mahasiswa Bidang Ilmu Komputer dan Aplikasinya (Vol. 3, No. 2, pp. 640-649).

Devan, K P K and R, Adithya Nagaraj and P, Kamaleshwaran and S, Karthick. (February 22, 2023). Detection of *Phishing* Websites Using *Machine Learning*. Proceedings of the International Conference on Innovative Computing & Communication (ICICC) 2022.

Putri, N. B., & Wijayanto, A. W. (2022). Analisis Komparasi Algoritma Klasifikasi Data Mining Dalam Klasifikasi Website *Phishing*. Komputika: Jurnal Sistem Komputer, 11(1), 59-66.

Rahul, M. (2023). Pengembangan Aplikasi Deteksi *Phising* Menggunakan Algoritma *Decision Tree* Berbasis Website (Doctoral dissertation, UIN Ar-Raniry Banda Aceh).

Razaque, A., Frej, M. B. H., Sabyrov, D., Shaikhyn, A., Amsaad, F., & Oun, A. (2020, October). Detection of *phishing Website*s using *Machine Learning*. In 2020 IEEE Cloud Summit (pp. 103-107). IEEE.

Herho, S. H. S. (2017). Tutorial Pemrograman Python 2 Untuk Pemula. WCPL Press, 1– 140

Hamzan, M. A., Nrartha, I. M. A., & Wiryajati, I. K. (2022). Rancang Bangun Sistem Pemantauan Daya Listrik Berbasis Android Menggunakan Teknologi React Native. Dielektrika, 9(1), 42–50. http://www.dielektrika.unram.ac.id/index.php/dielektrika/article/view/29

Agung, Leo. 2012. Aplikasi Pemrograman Javascript untuk Halaman Web. Yogyakarta: Andi Offset

Heriani, Fitri Novia (28 April 2021). *"Jadi Korban Phising Lewat Mass Tagging Pornografi? Pengguna Bisa Tuntut Platform"*. Hukum Online. *Diakses tanggal 2 Desember 2021*.

Faisal lutfi. Mengenal Node.js. Codepolitan.com (2017) https://codepolitan.com/blog/mengenal-nodejs-5880234fe9ae3.

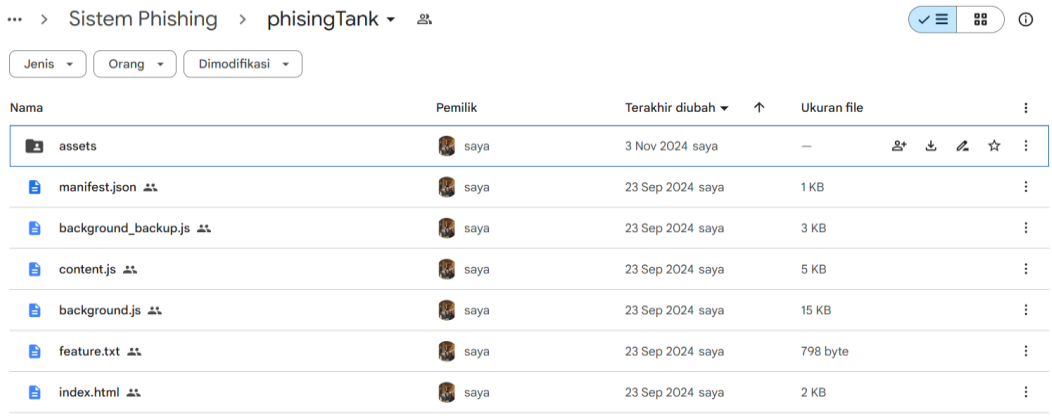
LAMPIRAN

Lampiran 1 Sistem Pendeteksi Phising

1. Link Google Drive Phising Tank Client

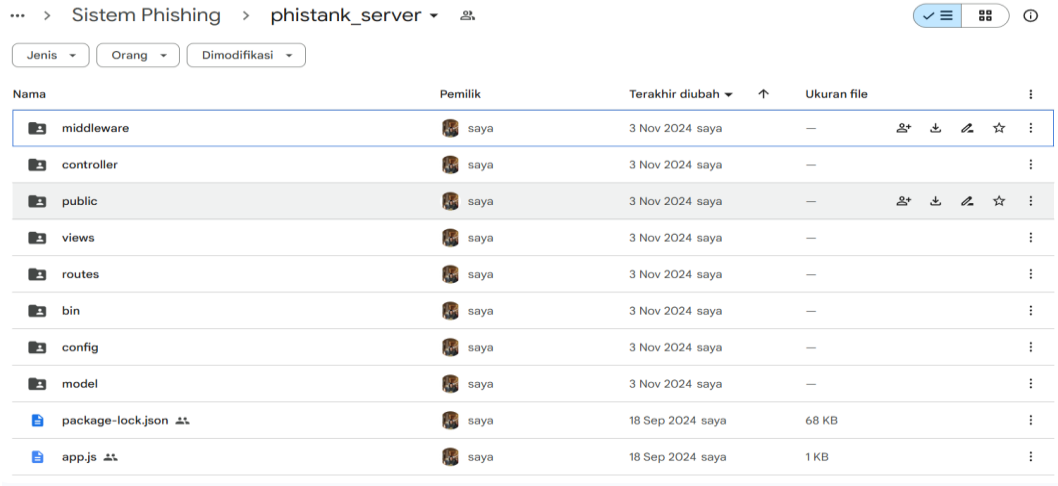
https://drive.google.com/drive/folders/1h4NRuQyMwZoiIZHVeGSL-3sQDH1RH5Ma?usp=sharing

iste



2. Link Google Drive Phising Tank Server

https://drive.google.com/drive/folders/1tZF7Hb33wCzs8bKURi9arhxUwLR873BU?usp=sharing



Lampiran 2 Kode Pengujian Sistem dengan Metode Decision Tree

```
from google.colab import drive
drive.mount('/content/drive')


import pandas as pd
from sklearn.tree import DecisionTreeClassifier
from sklearn.model_selection import cross_val_predict, cross_val_score
from sklearn.metrics import f1_score, precision_score, recall_score,
confusion_matrix, classification_report
from imblearn.over_sampling import SMOTE
from sklearn.preprocessing import StandardScaler


# Path file dataset di dalam My Drive
file_path = '/content/drive/My Drive/LAMPIRAN
PENELITIAN/dataset_phising.csv'


# Memuat dataset
df = pd.read_csv(file_path)


# Tampilkan beberapa baris pertama dataset
df.head()


# Ubah label 'F' dan 'T' menjadi numerik
df['Label Asli'] = df['Label Asli'].replace({'F': 0, 'S':0,'T': 1}) # Change 'data' to
'df'


# Jika ada kolom lain yang juga berisi label, ubah juga ke numerik
```

```
for column in df.columns: # Change 'data' to 'df'
    if df[column].dtype == 'object': # Change 'data' to 'df'
        df[column] = df[column].replace({'F': 0, 'S':0,'T': 1}) # Change 'data' to 'df'

# Tampilkan data setelah diubah
print(df.head()) # Change 'data' to 'df'
# Definisikan fitur dan label
X = df.drop(columns=['Label Asli','Website Link'])  # Pastikan untuk mengganti dengan nama kolom yang benar
y = df['Label Asli']

# Gunakan SMOTE untuk oversampling jika data tidak seimbang

smote = SMOTE()
X_resampled, y_resampled = smote.fit_resample(X, y)

# Normalisasi data fitur
scaler = StandardScaler()
X_resampled_scaled = scaler.fit_transform(X_resampled)

# Buat model Decision Tree
model = DecisionTreeClassifier(max_depth=3, min_samples_split=5, min_samples_leaf=5)

# Gunakan cross-validation dengan 5 fold untuk mendapatkan prediksi
y_pred = cross_val_predict(model, X_resampled_scaled, y_resampled, cv=5)

# Hitung metrik evaluasi berdasarkan hasil cross-validation
```

```
f1 = f1_score(y_resampled, y_pred)
precision = precision_score(y_resampled, y_pred)
recall = recall_score(y_resampled, y_pred)
conf_matrix = confusion_matrix(y_resampled, y_pred)
class_report = classification_report(y_resampled, y_pred)

# Tampilkan hasil dari cross-validation
scores = cross_val_score(model, X_resampled_scaled, y_resampled, cv=5)
print(f'Akurasi Rata-rata dari Cross-Validation: {scores.mean() * 100:.2f}%')
print(f'Akurasi dari tiap fold: {scores}')

# Tampilkan metrik evaluasi
print(f'\nF1 Score: {f1:.2f}')
print(f'Precision: {precision:.2f}')
print(f'Recall: {recall:.2f}')
print(f'Laporan Klasifikasi:\n{class_report}')

# Import necessary libraries
import matplotlib.pyplot as plt
import seaborn as sns

# Set up the matplotlib figure
plt.figure(figsize=(6, 4))

# Plot the heatmap dengan desain berwarna
sns.heatmap(conf_matrix, annot=True, fmt="d", cmap="Blues", cbar=True,
annot_kws={"size": 16})
```

```
# Add labels, title, and ticks
plt.title('Confusion Matrix', fontsize=18)
plt.xlabel('Predicted Label', fontsize=14)
plt.ylabel('True Label', fontsize=14)
plt.xticks([0.5, 1.5], ['F', 'T'], fontsize=12)
plt.yticks([0.5, 1.5], ['F', 'T'], fontsize=12)

# Show the plot
plt.tight_layout()
plt.show()
```

Lampiran 3. Surat Penugasan

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET DAN TEKNOLOGI
UNIVERSITAS HASANUDDIN
FAKULTAS TEKNIK
Poros Malino Km.6Bontomarannu(92172) Gowa, Sulawesi Selatan 92172, Sulawesi Selatan
Telp. (0411) 586015, 586262 Fax (0411) 586015
http://eng.unhas.ac.id, Email : teknik@unhas.ac.id

SURAT PENUGASAN
No. 486/UN4.7.1/TD.06/2024

Dari : Dekan Fakultas Teknik Universitas Hasanuddin

Kepada : Dr.Eng. Ady Wahyudi Paundu, ST., M.T

I s I : 1. Berdasarkan Surat Ketua Departemen Teknik Informatika Fakultas Teknik Nomor. 044/UN4.7.7./TD.06/2024 tanggal 8 Januari 2024 tentang usulan DOSEN PEMBIMBING MAHASISWA, maka dengan ini kami menugaskan Saudara untuk membimbing penulisan Skripsi/Tugas Akhir mahasiswa Teknik Informatika Fakultas Teknik Universitas Hasanuddin di bawah ini :

N a m a :	No. Stambuk :
Muh. Naufal Febriantama	D121 18 1021

Judul Skripsi/Tugas Akhir :

" Sistem Pendeteksi Phising Menggunakan Algoritma Decision Tree Berbasis Ekstensi Web Browser "

2. Surat penugasan pembimbing ini mulai berlaku sejak tanggal ditetapkannya dan berakhir sampai selesainya penulisan Skripsi/Tugas Akhir mahasiswa tersebut.

3. Agar penugasan ini dilaksanakan sebaik-baiknya dengan penuh rasa tanggung jawab.

Ditetapkan di Gowa
Pada tanggal 8 Januari 2024
a.n. Dekan,
Wakil Dekan Bidang Akademik dan Kemahasiswaan
Fakultas Teknik Unhas

Dr. Amil Ahmad Ilham, ST., M.IT
NIP. 197310101998021001

Tembusan :
1. Dekan FT-UH,
2. Ketua Departemen Teknik Informatika FT-UH,
3. Mahasiswa yang bersangkutan

Lampiran 4 Berita Acara Seminar Hasil

KEMENTERIAN PENDIDIKAN , KEBUDAYAAN
RISET DAN TEKNOLOGI
UNIVERSITAS HASANUDDIN
FAKULTAS TEKNIK
DEPARTEMEN TEKNIK INFORMATIKA
Kampus FakultasTeknikUnhas, Jl. Poros Malino, Gowa
http://eng.unhas.ac.id/informatika, Email : informatika@unhas.ac.id

BERITA ACARA SEMINAR HASIL

Pada hari ini **Rabu,** tanggal 6 November **2024** Pukul **10.30 WITA - Selesai** bertempat di **Ruang Lab. UBICON Departemen Teknik Informatika**, telah dilaksanakan Seminar Hasil bagi Saudara :

Nama : Muh.Naufal Febriantama
No. Stambuk : D121181021
Fakultas/Departemen : Teknik/Teknik Informatika
Judul Skripsi : **"Sistem Pendeteksi Phishing Menggunakan Algoritma Decision Tree Berbasis Ekstensi Web.Browser"**

Yang dihadiri oleh Tim Penguji Seminar Hasil sebagai berikut :

No.	Nama	Jabatan	Tanda tangan
1.	Dr.Eng.Ady Wahyudi Paundu, ST.,M.T	Pemb I/Ketua	1.....
2.	Adnan,ST.,M.T.,Ph.D	Anggota	2.....
3.	Iqra Aswad,ST.,M.T	Anggota	3.....

Hasil keputusan Tim Penguji Seminar Hasil : **Lulus / Tidak lulus** dengan nilai angka ..... dan huruf .....

Gowa, 6 November 2024

Ketua/Sekretaris Panitia Ujian,

Dr.Eng.Ady Wahyudi Paundu, ST.,M.T

Lampiran 5 Surat Izin Ujian Skripsi

KEMENTERIAN PENDIDIKAN KEBUDAYAAN,
RISET DAN TEKNOLOGI
UNIVERSITAS HASANUDDIN
Jalan Perintis Kemerdekaan Km. 10, Makassar 90245
Telepon (0411) 586200, (6 Saluran), 584200, Fax (0411) 585188
Laman: www.unhas.ac.id

SURAT IZIN UJIAN SKRIPSI
Nomor 53539/UN4.1.1.1/PK.03.02/2024

Berdasarkan Peraturan Rektor Universitas Hasanuddin tentang Penyelenggaraan Program Sarjana Nomor 29/UN4.1//2023 tanggal 17 Oktober 2023, dengan ini menerangkan bahwa:

Nama	:	MUH. NAUFAL FEBRIANTAMA
NIM	:	D121181021
Tempat/Tanggal Lahir	:	BONE, 6 FEBRUARI 2001
Fakultas	:	TEKNIK
Program Studi	:	TEKNIK INFORMATIKA

Telah memenuhi syarat untuk Ujian Skripsi Strata I (S1). Demikian Surat Persetujuan ini dibuat untuk digunakan dalam proses pelaksanaan ujian skripsi, dengan ketentuan dapat mengikuti wisuda jika **persyaratan kelulusan/wisuda telah dipenuhi**. Terima Kasih.

Makassar, 18 November 2024
a.n. Direktur Pendidikan
Kepala Subdirektorat Administrasi
Pendidikan,

Susy Asteria Irafany, S.T., M.Si.
NIP. 197403132009102001

Keterangan online wisuda:

User	:	D121181021
Password	:	2166603
Alamat Web	:	http://wisuda.unhas.ac.id

Lampiran 6 Berita Acara Ujian Sidang

KEMENTERIAN PENDIDIKAN , KEBUDAYAAN
RISET DAN TEKNOLOGI
UNIVERSITAS HASANUDDIN
FAKULTAS TEKNIK
DEPARTEMEN TEKNIK INFORMATIKA
Kampus FakultasTeknikUnhas, Jl. PorosMalino, Gowa
http://eng.unhas.ac.id/informatika, Email : informatika@unhas.ac.id

BERITA ACARA UJIAN SKRIPSI

Pada hari ini Kamis, tanggal 28 November 2024 Pukul **09.00 WITA - Selesai** bertempat di **Lab. IOT Departemen Teknik Informatika Gowa** , telah dilaksanakan Ujian Skripsi bagi Saudara :

Nama : Muh.Naufal Febriantama
No. Stambuk : D121181021
Fakultas/Departemen : Teknik /Teknik Informatika
Judul Skripsi : **"Sistem Pendeteksi Phishing Menggunakan Algoritma Decision Tree Berbasis Ekstensi Web Browser"**

Yang dihadiri oleh Tim Penguji Ujian Skripsi sebagai berikut :

No.	Nama	Jabatan	Tanda tangan
1.	Dr.Eng.Ady Wahyudi Paundu, ST.,M.T	Pemb I/Ketua	1.
2.	Adnan,ST.,M.T.,Ph.D	Anggota	2.
3.	Iqra Aswad,ST.,M.T	Anggota	3.

Hasil keputusan Tim Penguji Ujian Skripsi/Tugas Akhir : **Lulus / Tidak lulus** dengan nilai angka ……74…… dan huruf ……B……

Gowa, 28 November 2024

Ketua/Sekretaris Panitia Ujian,

Dr.Eng.Ady Wahyudi Paundu, ST.,M.T

Lampiran 7 Log Book

KARTU BIMBINGAN SKRIPSI

Prodi S1 Teknik Informatika Universitas Hasanuddin

Stb.	Nama Mahasiswa
D121181021	Muh. Naufal Febriantama

Pembimbing	Nama Pembimbing	Paraf & Tgl Persetujuan Ujian Akhir
I	Dr-Eng. Ady Wahyudi Paundu, S.T., M.T.	25/11/24
No. SK Pemb : No. 486/UN4.7.1/TD.06/2024		

Judul Skripsi	Sistem Pendeteksi *Phising* Menggunakan Algoritma *Decision Tree* Berbasis Ekstensi *Web Browser*

No	Tanggal Bimbingan	Uraian Kegiatan Bimbingan	Paraf Pemb.
1	02 Oktober 2023	Konsultasi Judul Pertama mengenai enkripsi	
2	9 November 2023	Penggantian Topik dari enkripsi ke Deteksi Phising	
3	21 November 2023	Review Draft Proposal Sistem Deteksi Phising	
4	27 November 2023	Perbaikan FlowChart dan evaluasi sistem	
5	07 Desember 2023	Review Bab 1-3 Persiapan seminar Proposal	
6	21 Desember 2023	Tanda tangan Form Revisi Proposal	
7	06 Juni 2024	Diskusi Draft TA Bab 4-5	
8	10 Oktober 2024	Review Sistem dan Penulisan bab 4-5	
9	11 Oktober 2024	Penambahan metode evaluasi sistem Pada draft TA	
10	14 Oktober 2024	Finalisasi draft skripsi dan Acc Hasil	
11	25 November 2024	Bimbingan revisi Hasil dan Acc Tutup	
12			
13			
14			
15			
16			

Lampiran 8 Lembar Perbaikan Skripsi

LEMBAR PERBAIKAN SKRIPSI

"SISTEM PENDETEKSI *PHISING* MENGGUNAKAN ALGORITMA *DECISION TREE* BERBASIS EKSTENSI WEB BROWSER "

OLEH:

MUH. NAUFAL FEBRIANTAMA
D121181021

Skripsi ini telah dipertahankan pada Ujian Akhir Sarjana tanggal 28 November 2024. Telah dilakukan perbaikan penulisan dan isi skripsi berdasarkan usulan dari penguji dan pembimbing skripsi.

Persetujuan perbaikan oleh tim penguji:

	Nama	Tanda Tangan
Ketua	Dr. Eng. Ady Wahyudi Paundu, S.T., M.T.	
Anggota	Adnan, S.T., M.T., Ph.D	
	Iqra Aswad, S.T., M.T.	

Persetujuan Perbaikan oleh pembimbing:

Pembimbing	Nama	Tanda Tangan
1	Dr. Eng. Ady Wahyudi Paundu, S.T., M.T.	

Revisi oleh Pak Adnan, S.T., M.T., Ph.D

1. **Perbedaan antara Phising dan Spoofing secara spesifik**

Jawaban :

Menurut (Heriani, Fitri Novia 2021), *phishing* berasal dari kata dalam bahasa Inggris "fishing" (memancing), yang dianalogikan dengan "memancing" korban untuk memberikan informasi sensitif secara sukarela melalui rekayasa sosial (social engineering). Sebagai contoh, Seorang *hacker* yang mengirimkan sebuah email yang berisikan link/tautan *phising* yang kemudian meminta mereka menekan tautan tersebut sehingga membuat korban memberikan informasi pribadinya kepada *hacker*.

Tautan tersebut kemudian mengarahkan korban ke situs web palsu yang dirancang menyerupai situs asli yang resmi, dan ini disebut *spoofing*. Dalam situasi ini, *phishing* berperan dalam menarik perhatian korban dan memanipulasi mereka secara psikologis, sementara *spoofing* mendukung serangan dengan menyamarkan situs palsu agar terlihat meyakinkan. Kombinasi keduanya sering digunakan untuk mencuri informasi login atau data penting lainnya dari korban.

2. **Menambahkan Penjelasan Mengapa Model Harus di Proses di Server**

Jawaban :

Dalam konteks sistem deteksi *phishing*, pemrosesan di server-side menggunakan Javascript lebih menguntungkan dibandingkan dengan client-side.

Pemrosesan di server memungkinkan pemanfaatan sumber daya yang lebih besar tanpa membebani perangkat pengguna, yang mungkin memiliki keterbatasan komputasi seperti memori dan prosesor. Dalam hal ini juga dapat diperhatikan bahwa setiap user tidak semuanya memiliki *device* yang mumpuni untuk melakukan proses komputasi yang kompleks. Dalam hal *sharing data* karena database kita berada di sisi server , data-data website seperti *safe,phising,* dan *suspicious* itu bisa diakses semua user yang menggunakan ekstensi ini. Pemrosesan Model yang dilakukan di sisi server-side juga bermanfaat agar *user experience* atau kenyamanan pengguna tidak terganggu saat mengakses ekstensi tersebut. Karena jika pemrosesan model ini di proses di sisi client-side, user akan terganggu dengan proses lain yang harusnya berada di sisi server-side.

Revisi oleh Pak Iqra Aswad, S.T., M.T.

1. **Menambahkan Alasan Mengapa Sistem tidak konsisten saat melakukan proses deteksi phising**

Jawaban :

Pada pengujian sistem deteksi phishing, terdapat ketidakkonsistenan hasil deteksi, baik pada website asli maupun phishing, dengan dan tanpa penggunaan IP Addresss. Meskipun performa sistem cukup baik, beberapa faktor, seperti keterbatasan dataset, pemilihan fitur yang kurang optimal, serta pengaruh preprocessing dan evaluasi model, dapat mempengaruhi hasil deteksi. Bagian ini akan membahas faktor-faktor yang menyebabkan ketidakkonsistenan tersebut.

1. Dataset yang Terbatas dan Tidak Seimbang

Dalam sistem ini, dataset yang digunakan terbatas, hanya terdiri dari 20 situs web yang sah dan sejumlah situs phishing. Jumlah data yang sedikit, serta kurangnya variasi dalam jenis phishing yang digunakan, membuat model kesulitan dalam mendeteksi pola phishing yang lebih beragam. Jika dataset yang digunakan tidak cukup representatif atau tidak mencakup variasi serangan phishing yang cukup, hasil deteksi cenderung tidak konsisten, terutama ketika menghadapi serangan phishing yang lebih kompleks atau teknik yang belum dilatih sebelumnya.

2. Pemilihan Fitur yang Tidak Optimal

Pemilihan fitur merupakan faktor penting yang mempengaruhi kinerja sistem. Dalam sistem ini, jika hanya menggunakan fitur tanpa memerhatikan keselarasan antara model dan topik yang di teliti, model mungkin tidak dapat mendeteksi pola phishing yang lebih kompleks karena adanya ketidakselarasan tersebut. Oleh karena itu, pemilihan fitur yang lebih komprehensif dan lebih spesifik akan membuat model lebih akurat dan konsisten dalam mendeteksi berbagai jenis phishing. Dengan pemilihan fitur yang lebih baik, hasil deteksi dapat lebih konsisten.

3. Overfitting pada Dataset Pelatihan

Penyebab ketidakkonsistenan hasil deteksi lainnya adalah overfitting pada dataset pelatihan. Ketika model terlalu terfokus pada data pelatihan yang terbatas, model menjadi sangat sensitif terhadap pola-pola yang ada dalam data tersebut. Meskipun model dapat bekerja dengan baik pada data pelatihan, ia akan kesulitan untuk menggeneralisasi pada data baru atau serangan phishing yang belum pernah dilihat sebelumnya. Hal ini menyebabkan ketidakkonsistenan dalam hasil deteksi, terutama pada data uji atau serangan phishing yang berbeda, karena sistem ini lebih fokus pada link yang telah terdaftar dalam dataset, sehingga kesulitan mendeteksi link baru atau teknik phishing yang belum ada dalam database.

4. Pengaruh dari Teknik Preprocessing Data

Proses preprocessing data sangat penting dalam meningkatkan kinerja sistem. Dalam sistem ini, pelabelan dan normalisasi fitur telah dilakukan dengan baik. Namun, apabila ada kesalahan dalam preprocessing seperti penanganan label atau normalisasi fitur yang tidak memadai informasi penting bisa hilang, yang berdampak pada ketidakkonsistenan hasil deteksi. Oleh karena itu, meskipun preprocessing sudah dilakukan dengan baik, kesalahan dalam tahap ini tetap dapat memengaruhi kinerja model dan menyebabkan hasil deteksi tidak konsisten.

5. Keterbatasan dalam Evaluasi Model dengan Cross-Validation

Meskipun menggunakan teknik cross-validation, jika distribusi data dalam dataset pelatihan tidak cukup representatif atau data terlalu sedikit, model mungkin tidak dapat diuji secara menyeluruh pada berbagai jenis situs phishing. Ini berarti model tidak cukup robust dalam menghadapi variasi teknik phishing yang lebih luas, yang menyebabkan hasil deteksi tidak konsisten. Agar hasil deteksi lebih konsisten, diperlukan evaluasi yang lebih mendalam dengan dataset yang lebih variatif.