iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: VI Month of publication: June 2025

DOI: https://doi.org/10.22214/ijraset.2025.71969

# An Intelligent System for Detecting Malicious Activity and Financial Fraud: A Programmatic Approach to Fraud Prevention

Ms. Sayali Parab[1], Mr. Chayan Bhattacharjee[2]
[1]Department of Information Technology, SES's L. S. Raheja College of Arts & Commerce, Mumbai, India
[2]Department of Information Technology, Chikitsak Samuha's Patkar Varde College, Mumbai, India

***Abstract:** In today's digital age, we are almost constantly connected to the internet and rely heavily on various websites for activities such as e-commerce, education, entertainment, and gaming. However, many users often overlook a critical aspect—whether the websites they interact with are genuinely secure. With the increasing number of online scams and fraudulent activities, it is essential to have tools that ensure safe browsing and transaction practices.*

***Our proposed solution is a smart website that assists users in identifying potentially harmful or fraudulent platforms, especially in high-risk sectors like e-commerce, banking, and fintech. The system will utilize advanced analysis of user behavior, access patterns, and historical data to detect malicious intent or fraud attempts. By leveraging these insights, our program will alert users in real time with warnings if they attempt to access suspicious websites.***

***This proactive approach aims to significantly reduce the risk of financial loss and enhance user trust in online platforms. By automatically providing suggestions and alerts, users are better equipped to avoid scams. Ultimately, our solution not only empowers individuals to browse safely but also acts as a critical tool in combating cyber fraud in an increasingly digital future.***

***Keywords:** Cyber-attacks, cybersecurity, Random Forest, Fraud Detection, online scammer.*

## I. INTRODUCTION

With the rise of digital technology, cyber-attacks have become a major concern for both individuals and organizations. Among the various threats, the rise of fake websites is particularly alarming. These fraudulent sites are designed to deceive users into revealing sensitive information such as login credentials, banking details, credit or debit card numbers, and personal data. Falling victim to such scams can result in significant financial losses and reputational harm.

This paper aims to explore how cybercriminals exploit users and organizations through fake websites, the consequences of such attacks, and effective strategies to mitigate these risks. Our focus is on identifying fake websites by analyzing specific characteristics, including domain names, spelling errors, misleading contact information, suspicious user reviews, flawed website design, and the age of the domain.

By examining these indicators, we aim to develop a method for early detection and prevention of such fraudulent platforms. Detecting and addressing these threats proactively is essential to safeguarding users and businesses from potential harm. As fake websites continue to evolve, creating robust detection systems will play a critical role in enhancing cybersecurity and ensuring a safer online experience for all.

Fake websites often mimic legitimate ones so convincingly that it becomes difficult for users to distinguish between the two. Cybercriminals may alter just a few letters in the domain name or replicate the layout and design of trusted websites to deceive users into sharing sensitive information. These deceptive tactics are increasingly effective in today's digital landscape, where internet usage continues to rise.

Traditionally, phishing websites were identified using blacklist-based approaches. Well-known platforms such as PhishTank, Norton Safe Web, VirusTotal, Google Safe Browsing, and SURBL maintain databases of known malicious websites. While useful, these methods are reactive; they rely on previously reported data and struggle to identify new threats in real time.

This project seeks to overcome the limitations of blacklist-based detection by leveraging machine learning and deep learning techniques. By training models on features extracted from website data, we aim to develop a system capable of predicting whether a website is malicious or legitimate. This real-time, intelligent approach enhances our ability to detect phishing attacks proactively, offering a more robust solution to combat evolving cyber threats and ensuring safer internet usage for all.

## II. LITERATURE REVIEW

*1)* Website scam detection is a crucial step towards countering online fraud.

This research highlights the most common techniques used by a scammers to steal sensitive information and exploit individuals. The study focuses particularly on phishing methods observed in recent times. To detect such an attacks, the researcher employed several techniques and conducted a detailed evaluation of various machine learning algorithms across multiple datasets. A key aspect of the study was identifying the most significant features within these datasets and assessing how classification performance changed when the data dimensions were reduced. The goal was to improve the efficiency and accuracy of phishing detection models. Statistical analysis of the results revealed that models like Random Forest and Artificial Neural Networks performed exceptionally well, achieving an accuracy rate of up to 97%. This research provides a comparative analysis of machine learning algorithms for phishing detection and website classification, demonstrating how intelligent models can effectively combat evolving cyber threats.

*2)* Sohail Ahmed Khan 1, Wasiq Khan2, Abir Hussain3, The University of Sheffield, Sheffield S102TN, UK sohailahmedkhan173@gmail.com

This study focuses on detecting malicious websites through URL classification and presents a comparative analysis of existing phishing detection methods. With phishing accounting for a significant portion of cyber-attacks, the research emphasizes the importance of understanding the strategies used by attackers to deceive users into trusting harmful websites or emails. The study explores common system vulnerabilities that cybercriminals exploit and how they manipulate users into revealing sensitive information such as credentials or financial details. It highlights various machine learning and deep learning techniques used to classify URLs and examines how these models can be trained using different datasets. By comparing the performance of these algorithms, the research aims to optimize their effectiveness in accurately detecting phishing URLs. The findings contribute to the ongoing development of more secure and intelligent systems that can protect users from evolving online threats, making URL-based detection a key area in cybersecurity defense.

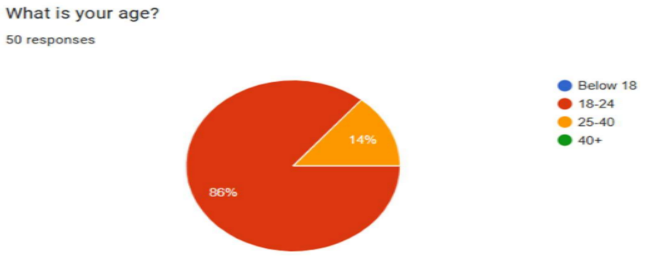
*3)* Maurya, S., & Jain, A. (2022).: Malicious Website detection based on URL Classification: A comparative analysis. In Lecture notes in networks and systems (pp. 249–260). https://doi.org/10.1007/978-981-19-1142-2_19

In today’s technology-driven world, the global communication and business landscape heavily relies on constant internet availability. Among the most severe cyber threats is the Distributed Denial of Service (DDoS) attack, which can cause substantial damage to both individuals and organizations. This study investigates two unsupervised neural network (NN) learning algorithms applied to weblog analysis as a means of detecting such threats. The primary objective was to gain deeper insights into visitor types and their browsing behavior on a public website. The research focused not only on identifying differences between user groups but also on uncovering similarities—particularly between malicious web crawlers and legitimate, non-malicious users.

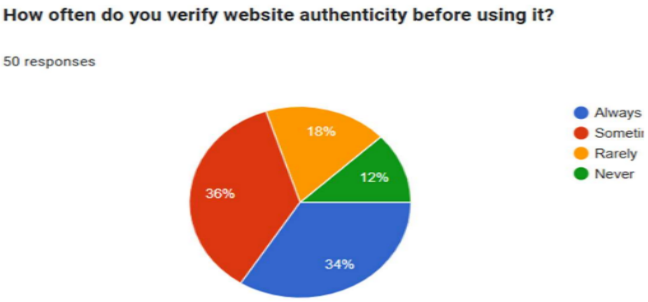
A key finding of the study revealed that 52% of malicious web crawlers mimic human-like browsing patterns, making them increasingly difficult to detect. This behavior presents a growing challenge for website security systems and emphasizes the need for more advanced detection mechanisms in the future.

## III. SURVEY AND ANALYSIS

A survey on malicious website detection was conducted, primarily targeting individuals aged 18–24, with some responses from the 25–40 age group. The results suggest that increasing awareness among these age groups can significantly reduce the risk of falling victim to online scams. Educating users about identifying suspicious websites and encouraging cautious browsing behavior can help prevent cyber-attacks. This highlights the importance of proactive awareness campaigns to minimize the impact of malicious websites and promote safer internet usage.

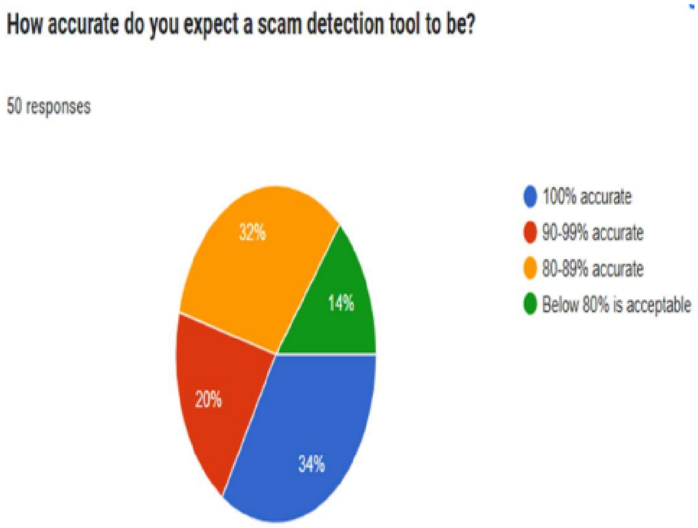


The survey revealed that only 34% of individuals consistently verify a website before using it, despite being aware of the risks associated with malicious sites. Interestingly, a slightly larger group of 36% reported checking a website's authenticity only when it appears suspicious. These findings suggest that while some awareness exists, it is not always translated into consistent behavior. With improved education and awareness campaigns, more users could be encouraged to verify websites regularly, ultimately reducing the risk of online fraud and enhancing overall cybersecurity awareness.

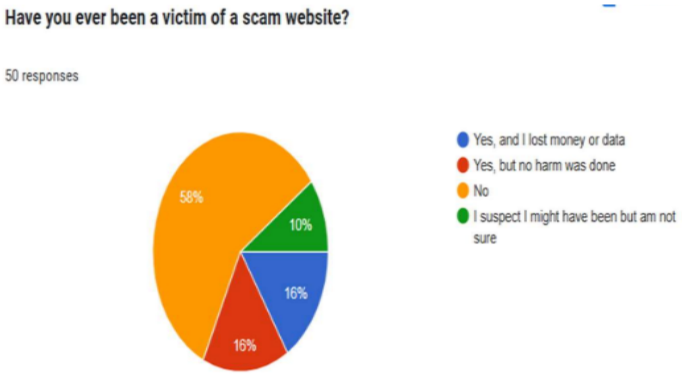


Approximately 30% of people rarely or never verify websites before accessing them, which significantly increases their vulnerability to cyber-attacks. Among these, 18% and 12% represent smaller but notable groups with similar risky behaviors. These individuals often fall prey to fake websites created by scammers, who trick them into sharing sensitive information such as bank details, credit or debit card numbers, and personal photos. In some cases, simply clicking on a malicious site allows attackers to gain control of their devices, including smartphones and laptops. Through this access, cybercriminals can steal critical personal data, leading to financial losses, identity theft, or severe damage to the victim's reputation. This highlights the urgent need for greater awareness and caution when browsing online.

The pie chart reveals that 54% of users expect the tool to deliver 90-100% accuracy to trust it fully and browse websites without fear of deception. This high demand for precision reflects the importance of reliability in cybersecurity tools. Meanwhile, 46% of users are comfortable with an accuracy range of 80-90%, valuing other features alongside accuracy. These insights highlight the varying user expectations regarding tool performance and emphasize the need to balance accuracy with additional functionalities to meet diverse user preferences.



The pie chart indicates that the majority of respondents, 58%, have not been affected by scams, suggesting a good level of awareness and caution among these users. Additionally, 26% reported either experiencing an attempted scam with no harm done (16%) or suspecting they might have been targeted without facing any actual damage (10%). This group remains uncertain about the full impact of these incidents. However, 10% of people admitted to suffering some form of harm due to scams, emphasizing the critical need for increased awareness and protective measures. This highlights the importance of tools and resources designed to help users identify and avoid malicious websites, underscoring how such solutions could significantly benefit those at risk



## IV. IMPLEMENTATION AND DESCRIPTION

### *A. Installing Dependencies*

```
pip install pandas scikit-learn
```

(i) pandas: This provides powerful data structures for data manipulation and analysis. It is used to create and handle the dataset of URLs and can also perform feature extraction and organize data in tabular form.

(ii) scikit-learn: This is a robust machine learning library in Python. It is used to build and evaluate the machine learning model (Random Forest) and provides tools for train-test split, classification, and metrics.

### *B. Dummy code implementation*

```
import pandas as pd
from sklearn.ensemble import RandomForestClassifier
from sklearn.model_selection import train_test_split
from sklearn.metrics import classification_report
import re

# Sample dummy dataset (URLs and Labels: 1 = Fraud, 0 = Legit)
data = {
    'url': [
        'http://secure-login-paypal.com',
        'https://www.amazon.com',
        'http://update-account-info.ru',
        'https://www.google.com',
        'http://bankofamerica-login.com',
        'https://www.wikipedia.org'
    ],
    'label': [1, 0, 1, 0, 1, 0]
}

df = pd.DataFrame(data)

# Feature extraction from URL
def extract_features(url):
    return {
        'url_length': len(url),
        'has_https': int(url.startswith('https')),
        'has_at_symbol': int('@' in url),
        'has_hyphen': int('-' in url),
        'num_dots': url.count('.'),
        'suspicious_words': int(bool(re.search(r'(login|update|secure|account)', url.lower())))
    }

# Apply feature extraction
features = df['url'].apply(lambda x: pd.Series(extract_features(x)))
X = features
y = df['label']

# Train-test split
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.3, random_state=42)

# Model
model = RandomForestClassifier(n_estimators=100, random_state=42)
model.fit(X_train, y_train)

# Predict and evaluate
y_pred = model.predict(X_test)
print("Classification Report:\n", classification_report(y_test, y_pred))

# Test on a new website
test_url = 'http://secure-update-login.com'
test_features = pd.DataFrame([extract_features(test_url)])
prediction = model.predict(test_features)[0]

print(f"\nTest URL: {test_url}")
print("Prediction:", "Fraudulent" if prediction == 1 else "Legitimate")
```

### *C. Dummy Output*

```
Classification Report:
            precision    recall  f1-score   support


         0       1.00      1.00      1.00         1
         1       1.00      1.00      1.00         1

   accuracy                          1.00         2
...

Test URL: http://secure-update-login.com
Prediction: Fraudulent
```

## V. LIMITATIONS

1) Binary Classification Only: The model predicts only two classes (fraudulent or legitimate). but in reality, fraud websites can be phishing, malware-spreading, scam sites, defacement pages, etc. This granularity is missing.
2) No Natural Language Analysis: The code does not analyze the actual content of the webpage (e.g., text, JavaScript, HTML structure). A site may have a legitimate-looking URL but suspicious on-page content, which this model will miss.
3) No Real-Time Threat Intelligence Integration: The model does not check against dynamic blacklists like Google Safe Browsing, PhishTank, or VirusTotal APIs.Any known phishing or scam sites are not instantly flagged if they’re not in the training data.
4) Static Model-No Continuous Learning: The model is trained once and does not adapt or learn from new threats. As cyberattack strategies evolve, the static model quickly becomes outdated.

## VI. CONCLUSIONS

In this study, we successfully examined various techniques and methodologies employed by scammers to carry out fraudulent activities. By applying our detection methods, we identified common scam patterns including fake reviews, fraudulent email addresses, transaction fraud, and fake contact numbers. Our approach involved implementing a multi-layered fraud detection system, which enhanced the overall accuracy of identifying malicious behavior while significantly reducing false positives. This comprehensive strategy allowed us to better distinguish genuine activities from deceptive ones, making the detection process more reliable. The results demonstrate that combining multiple detection techniques can strengthen defenses against scams and improve the effectiveness of fraud prevention efforts. This research contributes valuable insights for developing more robust security solutions to protect users from increasingly sophisticated fraudulent schemes. The implemented model demonstrates how simple URL-based features, when paired with a reliable machine learning algorithm like Random Forest, can effectively distinguish between legitimate and fraudulent websites.While the dummy dataset used here is minimal, the concept can be extended to large, real-world datasets forBuilding browser extensionsIntegrating with firewalls, Creating user alert systems**.** With real-world phishing data and more advanced features (like domain age, WHOIS info, or page content analysis), this approach can become a powerful tool in automated fraud detection systems.

## REFERENCES

[1] H. R, Upendra & Patil, Anusha & ., Mohana. (2023). Malicious URL Detection and Classification Analysis using Machine Learning Models. 470-476. 10.1109/IDCIoT56793.2023.10053422 Maurya, S., & Jain, A. (2022).

[2] Malicious Website detection based on URL Classification: A comparative analysis. In Lecture notes in networks and systems (pp. 249– 260). https://doi.org/10.1007/978-981-19-1142-2_19 Dusan Stevanovic, Natalija Vlajic, Aijun An Department of Computer Science and Engineering, York University, 4700 Keele St., Toronto, Ontario, M3J 1P3, Canada.

[3] Manjeri, A. S., Kaushik, R., Mnv, A., & Nair, P. C. (2019). A Machine Learning Approach for Detecting Malicious Websites using URL Features. In Proceedings of the 3rd International Conference on Electronics and Communication and Aerospace Technology, ICECA 2019 (pp. 555–561). Institute of Electrical and Electronics Engineers Inc.

[4] Saeid Sheikhi, Panos Kostakos, Safeguarding cyberspace: Enhancing malicious website detection with PSOoptimized XGBoost and firefly based feature selection, Computers & Security,Volume 142,2024,103885,ISSN 0167-408

[5] Vanhoenshoven, F., Napoles, G., Falcon, R., Vanhoof, K., & Koppen, M. (2017). Detecting malicious URLs using machine learning techniques. In 2016 IEEE Symposium Series on Computational Intelligence, SSCI 2016. Institute of Electrical and Electronics Engineers Inc.

[6] US Treasury. (2020). Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments. FinCen Advisory, 42(c), 1–8.

[7] Alghamdi, B., Watson, J., & Xu, Y. (2017). Toward detecting malicious links in online social networks through user behavior. In Proceedings - 2016 IEEE/WIC/ACM International Conference on Web Intelligence Workshops, WIW 2016 (pp. 5–8). Institute of Electrical and Electronics Engineers Inc.