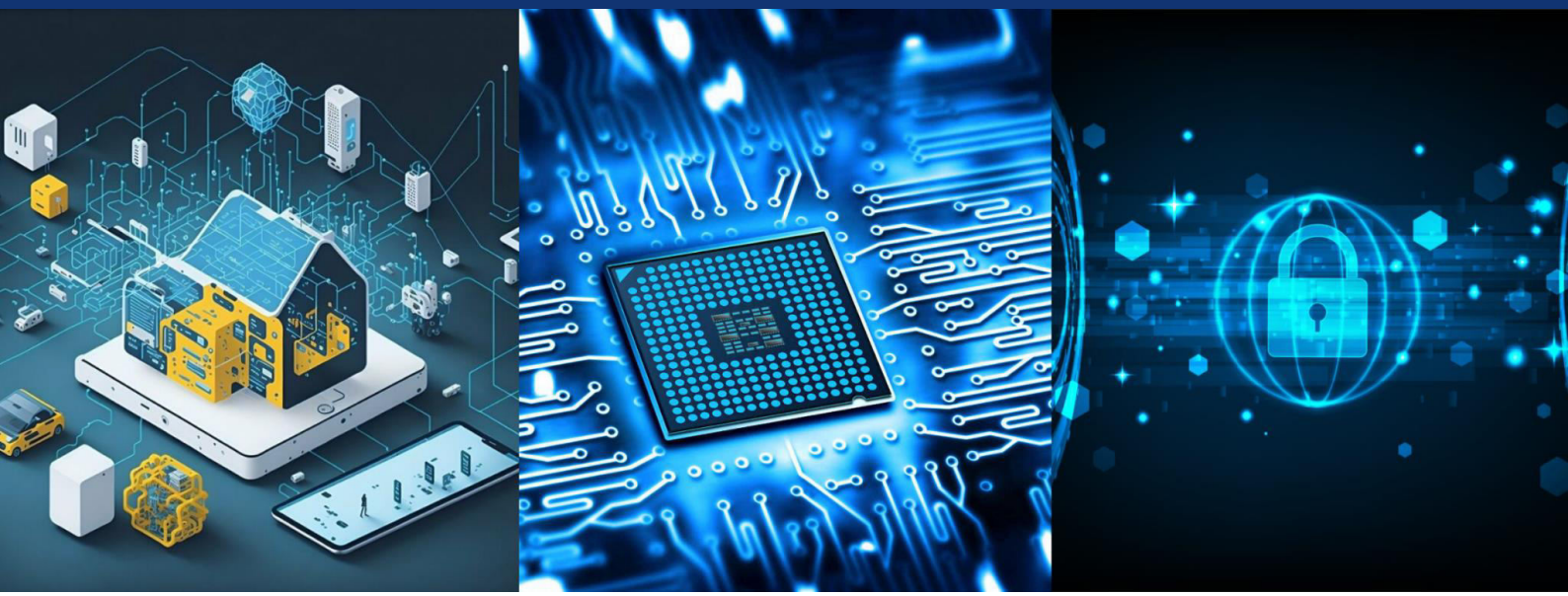
IJIRCCE

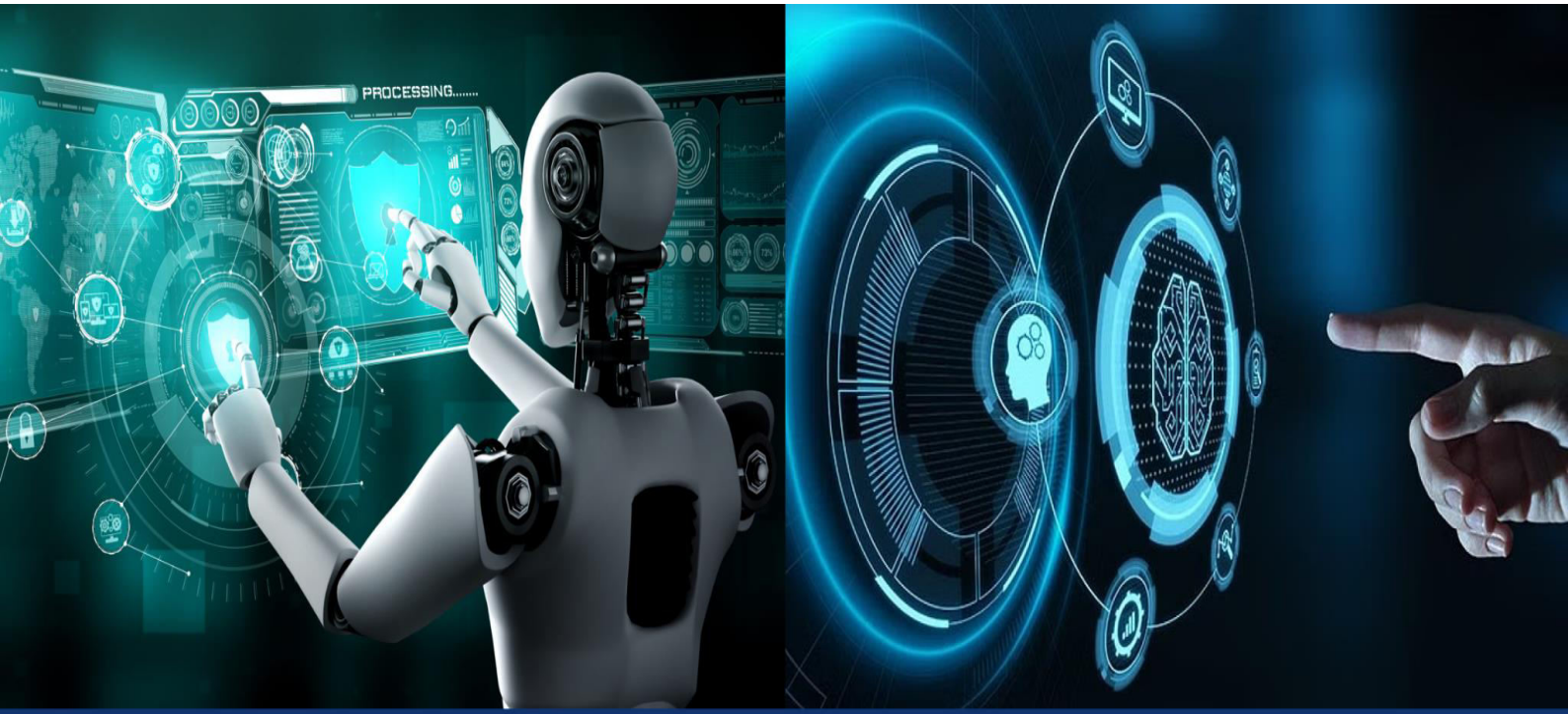
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.625

Volume 13, Issue 1, January 2025

© 2025 IJIRCCE | Volume 13, Issue 1, January 2025| DOI: 10.15680/IJIRCCE.2025.1301066

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Phishing Website Detection using AIML

Mr. Harish Kumar H C[1], Lohith H[2], Mahesh[3], Rahul P M[4], Sudarshan[5]

Associate Professor, Department of Computer Science and Engineering, Dr. Ambedkar Institute of Technology, Bangalore, Karnataka, India[1]

Students, Department of Computer Science and Engineering, Dr. Ambedkar Institute of Technology, Bangalore, Karnataka, India [2,3,4,5]

ABSTRACT: Phishing attacks continue to be a significant threat to online security, where attackers deceive users into disclosing sensitive information through fraudulent websites. Traditional detection methods often fail to adapt to rapidly evolving phishing techniques. This paper explores the use of Artificial Intelligence (AI) and Machine Learning (ML) in the detection of phishing websites. By analyzing various features such as domain characteristics, URL patterns, website content, and SSL certification, machine learning models can accurately classify websites as phishing or legitimate. The study highlights the application of supervised learning techniques, including decision trees, random forests, support vector machines (SVM), and deep learning approaches, to build an effective phishing detection system. The proposed system leverages feature extraction methods such as URL analysis, textual content examination, and visual element recognition to detect anomalies and suspicious behaviors. The evaluation of these models demonstrates their ability to identify phishing websites with high accuracy and low false-positive rates. The findings suggest that AIML-based approaches can be a valuable tool in combating phishing attacks, enabling real-time detection and response to potential threats.

KEYWORDS: Phishing Detection, Artificial Intelligence, Machine Learning, Cybersecurity, URL Analysis, Supervised Learning, Deep Learning, Feature Extraction, Real-Time Detection, Phishing Classification

I. INTRODUCTION

Phishing attacks have become one of the most prevalent and dangerous cyber threats in the digital age. These attacks involve cybercriminals impersonating legitimate organizations or entities to deceive individuals into providing sensitive information such as usernames, passwords, credit card numbers, or personal identification details. Phishing is typically executed through fraudulent websites that appear to be authentic, often replicating the look and feel of legitimate websites with the goal of tricking users into sharing confidential information.

The increasing sophistication of phishing techniques poses a significant challenge for traditional detection methods. Manual identification of phishing websites is time-consuming and often fails to adapt to the ever-changing tactics employed by attackers. Moreover, phishing websites can bypass conventional security measures, making it difficult for users to distinguish between real and malicious sites. As a result, there is an urgent need for advanced, automated solutions to detect and prevent phishing attacks in real-time.

Artificial Intelligence (AI) and Machine Learning (ML) have shown tremendous promise in enhancing the accuracy and efficiency of phishing detection. By leveraging large datasets and learning from historical examples of phishing and legitimate websites, AI-based systems can identify patterns, behaviors, and features that are indicative of phishing attempts. These systems are capable of analyzing website URLs, content, and other relevant characteristics to classify websites as either phishing or legitimate.

By combining the power of machine learning algorithms with domain-specific knowledge, this research aims to contribute to the development of advanced phishing detection systems that can offer enhanced security for internet users and reduce the risk of phishing-related cybercrimes

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. RELATED WORK

Phishing detection has been a significant area of research, with various approaches developed to address the growing complexity of phishing attacks. Early methods largely relied on heuristic-based systems that utilized predefined rules to identify suspicious website characteristics, such as URL patterns, domain names, and the presence of SSL certificates. While these methods provided a basic level of protection, they struggled to keep up with the evolving tactics used by attackers.

As phishing techniques became more sophisticated, machine learning (ML) began to be incorporated into detection systems. Researchers such as Mohammad et al. (2016) and Aburrous et al. (2010) explored the use of decision trees, random forests, and support vector machines (SVM) to classify websites, leveraging features like URL length, special characters, and domain age. These approaches demonstrated improved accuracy over traditional heuristic methods. More recently, deep learning models, such as those used by Zhang et al. (2019), have gained traction for their ability to learn complex patterns from large datasets, allowing them to detect more advanced phishing techniques. By employing models like convolutional neural networks (CNNs) and deep neural networks (DNNs), researchers were able to automate feature extraction and improve detection accuracy, even for previously unseen phishing websites.

In addition, hybrid and ensemble learning methods, which combine multiple models to improve prediction robustness, have also shown success in enhancing phishing detection rates, as demonstrated by studies from Rani et al. (2021) and Abdullahi et al. (2020). Furthermore, feature extraction methods, including the analysis of URL, HTML content, and textual elements using Natural Language Processing (NLP), have become essential in identifying phishing sites based on their content and structure. Real-time phishing detection has also been a key focus, with systems being integrated into web browsers or mobile devices to alert users of potential threats while browsing. Despite the progress, phishing detection remains an ongoing challenge, with the need for continuous model updates and improvements to stay ahead of ever-changing attack strategies.

III. PROPOSED SYSTEM

The proposed system aims to enhance the detection of phishing websites by leveraging Artificial Intelligence (AI) and Machine Learning (ML) techniques, specifically supervised learning models, to automatically classify websites as either phishing or legitimate. The system is designed to analyze multiple features of websites, including URL structure, domain characteristics, content analysis, and other elements commonly associated with phishing attacks. By incorporating a combination of feature extraction techniques and advanced machine learning models, the system can identify phishing websites in real-time with high accuracy and low false-positive rates. The system's architecture can be divided into the following key components:

1. Data Collection and Preprocessing

The first step in the system involves collecting a large dataset consisting of both legitimate and phishing websites. The dataset can be sourced from public repositories such as PhishTank or other reliable cybersecurity datasets. Preprocessing is performed to clean and structure the data, which may involve:

- Removing unnecessary or irrelevant data.
- Converting raw HTML data into structured features.
- Normalizing numerical features, such as URL length or the number of subdomains.
- Tokenizing and encoding text features, such as the textual content of web pages, using methods like TF-IDF (Term Frequency-Inverse Document Frequency) or word embeddings.

2. Feature Extraction

In this phase, a variety of features are extracted from the URLs and content of the websites to create a feature vector that represents each website. Common features include:

- **URL Features:** Length of the URL, the number of subdomains, the presence of special characters (e.g., "@", "-", "www"), and domain age.
- **SSL/TLS Certificate Information:** Whether the website uses HTTPS (Secure HyperText Transfer Protocol) or not.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- **Content Features:** Textual analysis of the webpage using Natural Language Processing (NLP) to identify phishing-related keywords (e.g., "urgent action required" or "verify your account").
- **HTML Structure:** The presence of suspicious HTML tags or forms that ask for sensitive information (e.g., login forms, credit card details).
- **Visual Features:** Detection of anomalies in the visual design of the site, such as logos that appear distorted or mismatched with the official brand.
- **External Links:** Number of external links, especially links leading to suspicious or non-trusted domains.

3. Model Training and Classification

The system uses supervised machine learning algorithms to train a model on the extracted features. The choice of model can vary depending on the dataset and its complexity. Commonly used models for phishing detection include:

- **Decision Trees** and **Random Forests:** These models can handle both categorical and numerical data effectively, providing a clear understanding of the decision-making process.
- **Support Vector Machines (SVM):** Known for their ability to perform well with high-dimensional data and complex classification tasks.
- **Deep Learning Models:** Convolutional Neural Networks (CNNs) or Multi-Layer Perceptrons (MLPs) can be employed to learn intricate patterns in both structured data (URL and content features) and unstructured data (text and visual elements).
- **Ensemble Learning:** The system may also integrate multiple models to create an ensemble that aggregates predictions to improve classification accuracy.

Once the models are trained on labeled datasets (phishing and legitimate websites), they are validated using metrics such as accuracy, precision, recall, and F1-score to ensure robust performance.

4. Real-Time Detection

After training, the system can be deployed to analyze websites in real-time. When a user navigates to a website, the system can automatically extract the relevant features and input them into the trained model for classification. If the website is detected as phishing, the system can generate an alert to warn the user. Real-time detection can be integrated into various platforms, such as:

- **Browser Extensions:** Users receive immediate warnings while browsing.
- **Network Security Tools:** The system can be integrated into firewalls or Intrusion Detection Systems (IDS) to block access to phishing sites.
- **Mobile Applications:** The system can be embedded into mobile security apps to protect users on smartphones.

5. Continuous Learning and Model Improvement

To keep the system up-to-date with emerging phishing techniques, continuous learning is incorporated into the workflow. New phishing websites and tactics can be incorporated into the training dataset, allowing the model to adapt and improve over time. Additionally, the system can include feedback loops where users or administrators can manually verify flagged websites, providing labeled data to further train and refine the model.

6. User Interface and Alerts

The proposed system also includes a user-friendly interface to present real-time phishing alerts and provide detailed information about the detected phishing attempts. Alerts can be categorized based on the level of threat, with more severe phishing attempts being flagged as high-risk. Additionally, users may be provided with recommendations on how to protect themselves from phishing attacks, such as verifying the legitimacy of a website or avoiding entering sensitive data on suspicious sites.

IV. SYSTEM ARCHITECTURE

The system architecture of the blockchain-based Land Registration System is designed to address the inefficiencies of traditional land registration processes by integrating modern technologies. It ensures transparency, security, and automation through a layered approach.

© 2025 IJIRCCE | Volume 13, Issue 1, January 2025| DOI: 10.15680/IJIRCCE.2025.1301066

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

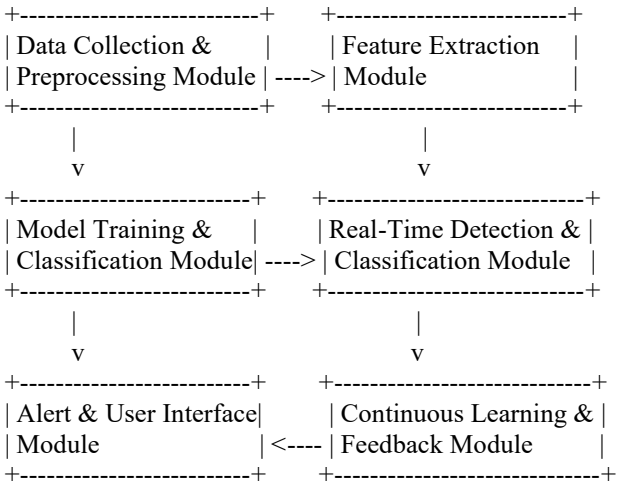
International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A. **Overview of Architecture**

The system architecture of the proposed phishing website detection solution is designed to efficiently and accurately classify websites as phishing or legitimate in real-time. It integrates multiple components to provide seamless phishing detection, including data collection, feature extraction, model training, real-time detection, user alerts, and continuous learning. Below is an overview of each key module in the architecture:

1. **Data Collection and Preprocessing Module:**
2. **Feature Extraction Module:**
3. **Model Training and Classification Module:**
4. **Real-Time Detection and Classification Module:**
5. **Alert and User Interface Module:**
6. **Continuous Learning and Feedback Module:**



B. **Components of System Architecture**

∟ **Data Collection Module:** Collects raw data from phishing databases or web crawlers, including both phishing and legitimate websites.

∟ **Data Preprocessing Module:** Cleans and structures the raw data by handling missing values, tokenizing text, and normalizing numerical features for analysis.

∟ **Feature Extraction Module:** Extracts key features from websites, such as URL structure, SSL certification, content analysis, and external links, to represent each website's characteristics.

∟ **Model Training and Classification Module:** Trains machine learning models using the extracted features to classify websites as phishing or legitimate based on labeled data.

∟ **Real-Time Detection and Classification Module:** Analyzes websites in real-time as users visit them, extracts features, and uses the trained model to classify the site.

∟ **Alert and User Interface Module:** Provides notifications and alerts to users when a phishing site is detected, with details and recommendations for protection.

∟ **Continuous Learning and Feedback Module:** Updates and improves the model by incorporating new phishing data and user feedback to adapt to evolving phishing techniques.

∟ **Integration and Deployment Module:** Ensures the system is integrated into web browsers, mobile apps, or security tools, offering scalable real-time protection across different platforms.

C. **Data Flow in Architecture:**

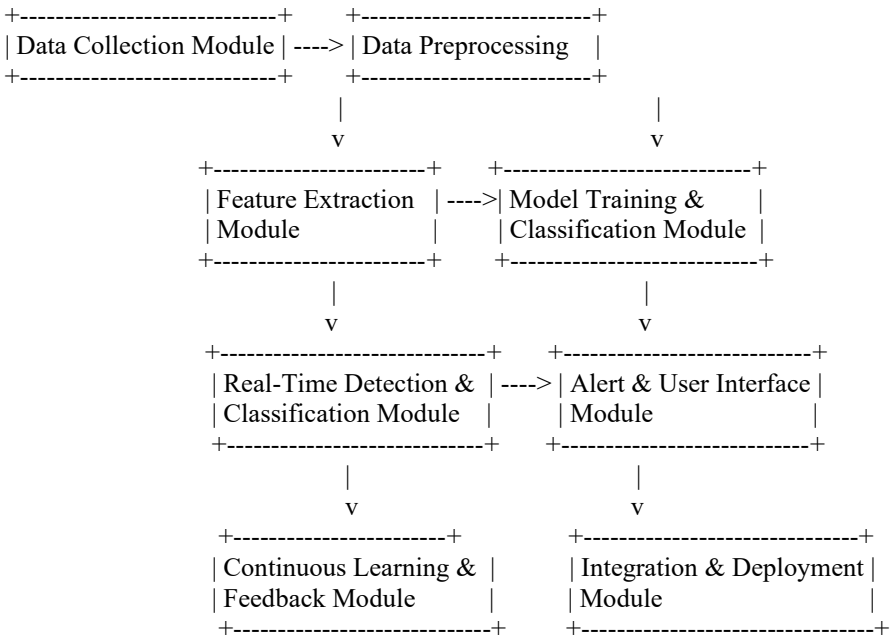
- **Data Collection:** The system gathers raw website data (URLs, content) from sources like phishing databases or web crawlers.
- **Data Preprocessing:** The raw data is cleaned, normalized, and structured for analysis (handling missing values, encoding text, etc.).

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- **Feature Extraction:** Key features (URL structure, content, SSL certificates) are extracted to create a structured feature vector for each website.
- **Model Training:** The extracted features are used to train machine learning models to distinguish between phishing and legitimate websites.
- **Real-Time Detection:** When a user visits a website, the system extracts real-time features and passes them to the trained model for classification (phishing or legitimate).
- **User Alerts:** If a phishing website is detected, the system triggers an alert, notifying the user with recommendations for safety.



V. RESULTS

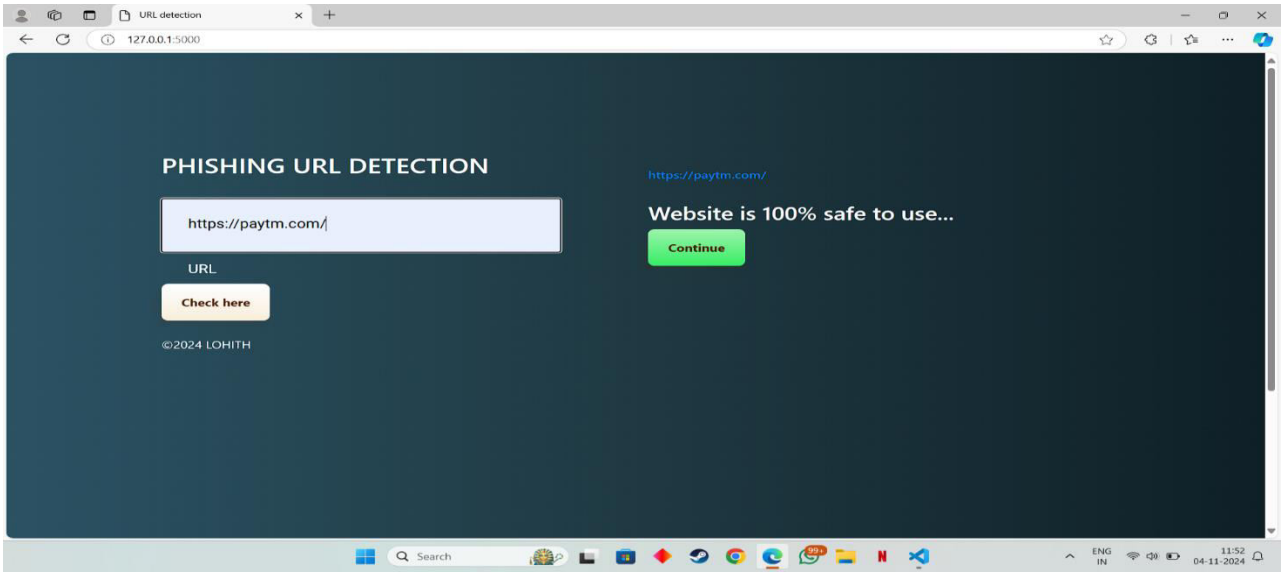


Fig. 1. Website Is Secure to Use

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

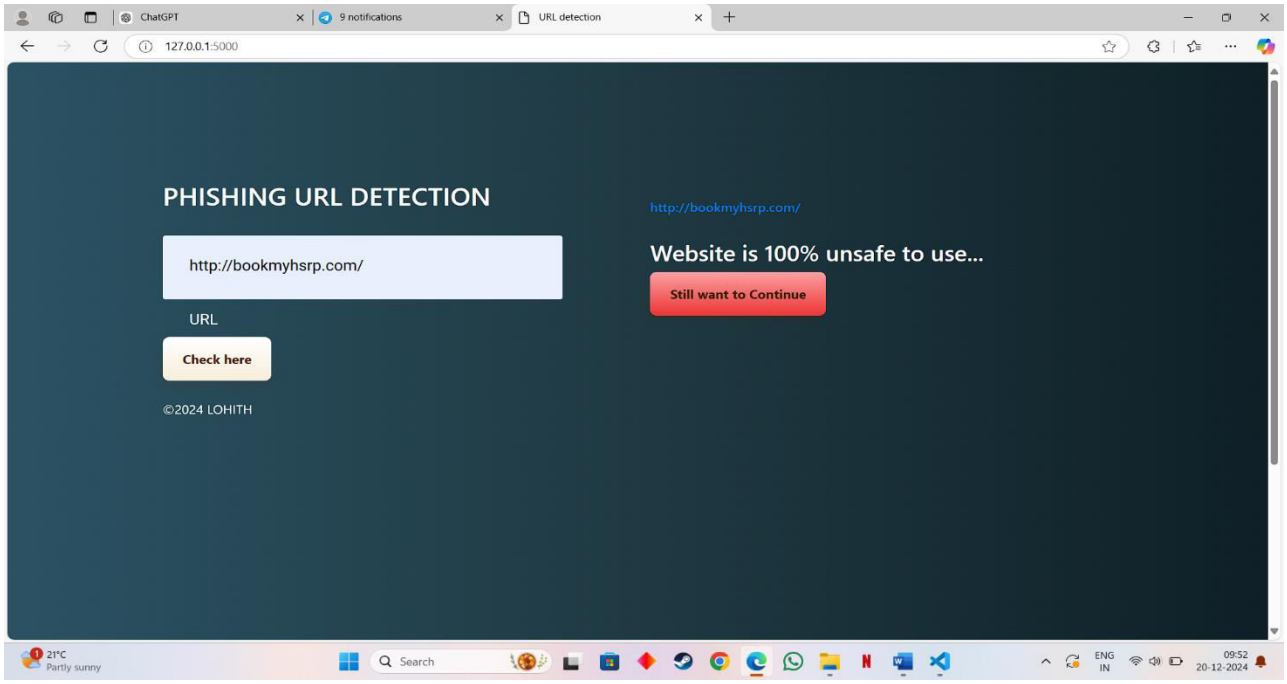


Fig. 2. Website Is Not Secure

The screenshots depict a phishing URL detection web application designed to help users identify whether a website is safe or potentially harmful. The interface includes an input field where users can enter a website URL and a "Check here" button to initiate the analysis. Based on the entered URL, the application classifies the website as either safe or unsafe. If the website is deemed safe, a green message appears, stating "Website is 100% safe to use," along with a "Continue" button for further navigation. Conversely, if the website is identified as unsafe, a red message warns that the "Website is 100% unsafe to use," and a "Still want to Continue" button is displayed, cautioning users about potential risks.

The application likely operates using a backend mechanism that evaluates URLs through a machine learning model or a rule-based system. It analyzes factors such as URL length, the presence of suspicious keywords, HTTPS usage, and domain reputation to make its decision. Hosted locally on a Flask development server (127.0.0.1:5000), the app provides users with a straightforward and intuitive interface that uses color-coded feedback to highlight safe or unsafe websites. This tool is an essential resource for preventing phishing attacks by helping users assess potentially malicious links before accessing them.

VI. CONCLUSION AND FUTURE WORK

A phishing URL detection web application powered by AI/ML provides an efficient and user-friendly solution for identifying malicious websites. By leveraging datasets, feature engineering, and machine learning models, the application can classify URLs as safe or unsafe based on specific characteristics like URL structure, domain reputation, and content analysis. Integrating this functionality into a web interface using frameworks like Flask ensures accessibility and ease of use for end users. This tool is a critical asset in enhancing online security, protecting users from phishing attacks, and promoting safe browsing practices.By combining the power of machine learning algorithms with domain-specific knowledge, this research aims to contribute to the development of advanced phishing detection systems that can offer enhanced security for internet users and reduce the risk of phishing-related cybercrimes

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

REFERENCES

1.Pressman, R. S. (2014). Software Engineering: A Practitioner's Approach. McGraw-Hill.
2.Breiman, L. (2001). Random Forests. Machine Learning, 45(1), 5–32.
3.Chawla, N. V., et al. (2002). SMOTE: Synthetic Minority Over-sampling Technique. Journal of Artificial Intelligence Research, 16, 321–357.
4.Provos, N., & Holz, T. (2007). Virtual Honeypots: From Botnet Tracking to Intrusion Detection. Addison-Wesley Professional.
5.OpenCV Documentation. (n.d.). Retrieved from https://opencv.org/
6.Python Software Foundation. (n.d.). Python Language Reference, version 3.9. Available at https://www.python.org/
7.PhishTank. (n.d.). Phishing URL Dataset. Retrieved from https://phishtank.org/
8.Chollet, F. (2018). Deep Learning with Python. Manning Publications.
9.Goodfellow, I., et al. (2016). Deep Learning. MIT Press.
10.Bishop, C. M. (2006). Pattern Recognition and Machine Learning. Springer.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details