International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

# AI-BASED PHISHING URL & CYBER THREAT DETECTION PLATFORM

[1] D Shirisha, [2] M Srija, [3] M Manjula, [4] B Keerthi, [5] K Venkata Naga Ganesh
[1]AssistantProfessor, [2345]Students
Department of ECE
Siddhartha Institute of Technology & Sciences, Narapally
shirishadubbaka.ece@siddhartha.co.in, 23tq1a0427@siddhartha.co.in, 23tq1a0444@siddhartha.co.in, 23tq1a0438@siddhartha.co.in, 23tq1a0420@siddhartha.co.in,

## Abstract

The AI-Based Phishing URL & Cyber Threat Detection Platform is an intelligent cybersecurity system designed to identify and detect potentially malicious URLs and common cyber threats. Phishing attacks frequently use deceptive websites and URLs to trick users into revealing sensitive information such as usernames, passwords, financial details, and personal data. Traditional detection methods that depend only on static blacklists or predefined rules may fail to identify newly created or modified phishing URLs. The proposed system uses Artificial Intelligence (AI), Machine Learning (ML), and URL feature analysis to improve the detection process.

The platform allows users to enter or scan a URL, which is then analyzed using features such as URL length, domain characteristics, special characters, suspicious keywords, HTTPS usage, redirection behavior, and other relevant indicators. A trained machine-learning model evaluates these features and classifies the URL as legitimate, suspicious, or phishing/malicious, depending on the system's defined categories. The platform can display a risk score and explain important factors contributing to the detection result.

The system can also maintain a detection history, threat reports, alerts, and security analytics for monitoring purposes. An administrator dashboard can be used to manage datasets, detection records, users, and system configurations. The platform can be enhanced to analyze additional cyber-threat indicators and provide real-time alerts when suspicious activity is detected.

## I. Introduction

The AI-Based Phishing URL & Cyber Threat Detection Platform is an intelligent cybersecurity application designed to identify potentially harmful URLs and protect users from phishing and other online threats. With the rapid growth of internet services, cybercriminals increasingly use deceptive websites and malicious links to steal sensitive information. Phishing attacks can make a website appear similar to a legitimate service and trick users into entering usernames, passwords, banking details, or other confidential information.

Traditional phishing detection systems often depend on blacklists, predefined rules, and manually updated threat databases. Although these methods can detect known malicious websites, they may have difficulty identifying newly created phishing URLs or URLs that have been modified to avoid detection. Artificial Intelligence and

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Machine Learning can provide a more flexible approach by learning patterns from previously identified legitimate and malicious URLs.

The proposed system allows users to enter, scan, or analyze a URL through a simple interface. The system extracts relevant URL features such as URL length, domain structure, special characters, suspicious keywords, HTTPS usage, subdomains, redirects, and other security-related characteristics. These features are processed and provided to a trained machine-learning model for classification.

The prediction module can classify a URL as legitimate, suspicious, or phishing/malicious, depending on the categories defined during model development. A risk score can also be displayed to help users understand the potential threat level. The system can maintain detection history so users or authorized administrators can review previously analyzed URLs.

## II. Literature Survey

The AI-Based Phishing URL & Cyber Threat Detection Platform is based on research in cybersecurity, phishing detection, machine learning, URL analysis, and intelligent threat detection. The rapid growth of online services has increased the number of phishing attacks, creating a need for automated systems that can identify malicious websites before users interact with them. Researchers have therefore explored different techniques for detecting suspicious URLs and classifying websites as legitimate or malicious.

Early phishing detection systems mainly relied on blacklists containing previously identified malicious URLs. These systems were simple and effective for known threats, but they had limitations when attackers created new phishing websites or changed URLs frequently. Since a newly generated malicious URL may not immediately appear in a blacklist, researchers began investigating more dynamic detection approaches.

Rule-based detection techniques were also developed to identify suspicious characteristics in URLs. These methods examine features such as unusual domain names, excessive subdomains, special characters, suspicious keywords, URL length, and misleading domain structures. Although rule-based approaches can identify many suspicious patterns, attackers can modify URLs to bypass predefined rules.

Machine-learning techniques have become an important research area for phishing URL classification. Algorithms such as Decision Trees, Random Forest, Support Vector Machines, Logistic Regression, Naive Bayes, and K-Nearest Neighbors have been used to classify URLs based on extracted features. These models can learn patterns from datasets containing both legitimate and phishing URLs and use those patterns to classify previously unseen URLs.

Researchers have investigated URL lexical features as an effective source of information for machine-learning models. Features such as URL length, number of dots, hyphens, digits, special characters, suspicious words, and domain structure can

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

help distinguish malicious URLs from legitimate ones. These features can often be extracted without visiting the potentially dangerous website, making them useful for safer preliminary analysis.

Another research direction involves host-based and domain-based features. Information about domain registration, DNS records, domain age, hosting characteristics, and related properties can provide additional evidence about whether a website may be suspicious. Combining URL-based features with domain information can improve detection performance, although some features may require external threat-intelligence or domain-information services.

Researchers have also explored deep-learning approaches for phishing detection. Neural networks can automatically learn complex patterns from large amounts of URL and website data. Techniques involving recurrent neural networks, convolutional neural networks, and transformer-based models have been investigated for identifying malicious URL patterns. However, deep-learning models generally require suitable datasets, computational resources, and careful validation.

Browser-based and real-time phishing detection systems have been developed to provide protection while users browse the internet. These systems can analyze URLs when users attempt to access websites and provide warnings when suspicious activity is detected. Such approaches can reduce the time between threat identification and user notification.

Another important area is threat-intelligence integration. Security platforms can combine machine-learning predictions with external databases containing information about known malicious domains, URLs, IP addresses, and other indicators of compromise. Combining multiple sources can provide a broader view of potential cyber threats and improve detection capabilities.

Research has also emphasized explainable phishing detection. Instead of simply displaying that a URL is malicious, an intelligent system can identify important indicators that contributed to the prediction, such as suspicious domain structure, unusual URL length, or the presence of misleading keywords. Explainable results can improve user awareness and help security analysts understand automated predictions.

Despite advances in phishing detection, challenges remain regarding false positives, evolving attack techniques, dataset quality, class imbalance, and zero-day phishing attacks. A legitimate website may sometimes exhibit characteristics similar to suspicious URLs, while attackers continually develop new methods to evade detection. Therefore, detection systems require regularly updated datasets, appropriate model evaluation, and multiple complementary detection techniques.

Based on these research areas, the proposed AI-Based Phishing URL & Cyber Threat Detection Platform combines URL feature extraction, machine-learning classification, risk scoring, detection history, threat analytics, and security alerts in a centralized platform. The system can classify URLs into categories such as legitimate, suspicious, or phishing/malicious based on the trained model and selected features.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

## III. System Analysis

System analysis is an important stage in developing the AI-Based Phishing URL & Cyber Threat Detection Platform. The system is designed to identify potentially malicious and phishing URLs using Artificial Intelligence and Machine Learning techniques. Users can enter a URL through a simple and user-friendly interface for security analysis. The system extracts important features such as URL length, number of special characters, domain structure, subdomains, suspicious keywords, and HTTPS usage. These features are processed and provided to a trained machine-learning model for classification. The model analyzes the URL and predicts whether it is legitimate, suspicious, or potentially malicious. The system can generate a risk score to indicate the potential threat level of the analyzed URL. Detection results can include important indicators that contributed to the prediction. The application can store previous scan results in a database for future reference and analysis. An administrator can manage users, datasets, threat records, and system configurations. Security alerts can be provided when a potentially dangerous URL is detected. Overall, the system analysis defines the functional and technical requirements for developing an intelligent phishing and cyber-threat detection platform.

### Existing System

In the existing system, phishing and malicious websites are commonly detected using blacklists, predefined security rules, browser warnings, and manually maintained threat databases. Blacklists contain previously identified malicious URLs and domains that can be blocked or flagged. Although this approach is useful for known threats, it may not effectively identify newly created phishing websites. Rule-based systems analyze predefined characteristics of URLs to determine whether they appear suspicious. Attackers can modify URL structures and domain names to bypass some predefined rules. Users may also depend on antivirus software or browser security features that provide limited information about why a URL is considered dangerous. Traditional systems may not provide detailed risk scores or explainable detection results. Manual analysis of suspicious URLs can require technical knowledge and considerable time. Some systems also depend heavily on frequently updated external databases. Detection records and security analytics may not be available to ordinary users. Therefore, an intelligent system that learns patterns from phishing and legitimate URLs can provide a more flexible approach to detecting evolving threats.

### Disadvantages of Existing System

- Mainly depends on known URL blacklists.
- Newly created phishing URLs may not be detected immediately.
- Rule-based systems can be bypassed by attackers.
- Limited ability to detect evolving phishing techniques.
- Manual URL analysis can be time-consuming.
- Requires frequent database updates.
- Limited personalized risk assessment.
- May provide limited explanation for detection results.
- Some systems require technical cybersecurity knowledge.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

- Limited integration of machine-learning-based analysis.

**Proposed System**

The proposed AI-Based Phishing URL & Cyber Threat Detection Platform uses Artificial Intelligence and Machine Learning to provide intelligent URL security analysis. Users can enter or scan a URL through the application to determine whether it appears legitimate or potentially dangerous. The system extracts relevant lexical and structural features from the URL without requiring the user to manually inspect it. Features such as URL length, special characters, domain structure, suspicious keywords, subdomains, and HTTPS usage are analyzed. The extracted features are passed to a trained machine-learning model for classification. The system can categorize URLs as legitimate, suspicious, or phishing/malicious based on the model's defined output. A risk score can be displayed to communicate the potential threat level to the user. The platform can provide key indicators that contributed to the detection result to improve security awareness. Previous scan results can be stored securely in a database for monitoring and analysis. Administrators can manage datasets, users, threat records, and system configurations. The platform can also generate alerts when potentially harmful URLs are identified. Overall, the proposed system provides a proactive, automated, and user-friendly approach to phishing URL and cyber-threat detection.

**Advantages of Proposed System**

- Provides AI-based phishing URL detection.
- Can identify suspicious patterns beyond simple blacklists.
- Automates URL feature analysis.
- Provides risk scores for analyzed URLs.
- Supports legitimate, suspicious, and malicious classifications.
- Reduces the need for manual URL inspection.
- Can analyze previously unseen URL patterns.
- Provides useful security indicators.
- Maintains detection history.
- Supports threat analytics and reporting.
- Can provide real-time security alerts.
- Can be extended with external threat-intelligence sources.

## IV. Methodology

The methodology begins with collecting a suitable dataset containing both legitimate and phishing or malicious URLs. The collected dataset is cleaned to remove duplicate, incomplete, or invalid records before model development. Relevant URL features are extracted, including URL length, number of dots, special characters, subdomains, digits, suspicious keywords, domain structure, and HTTPS-related characteristics. The extracted features are converted into a structured format suitable for machine-learning algorithms. The dataset is divided into training and testing sets to develop and evaluate the detection model. Suitable classification algorithms such as Random Forest, Decision Tree, Support Vector Machine, or Logistic Regression can be trained

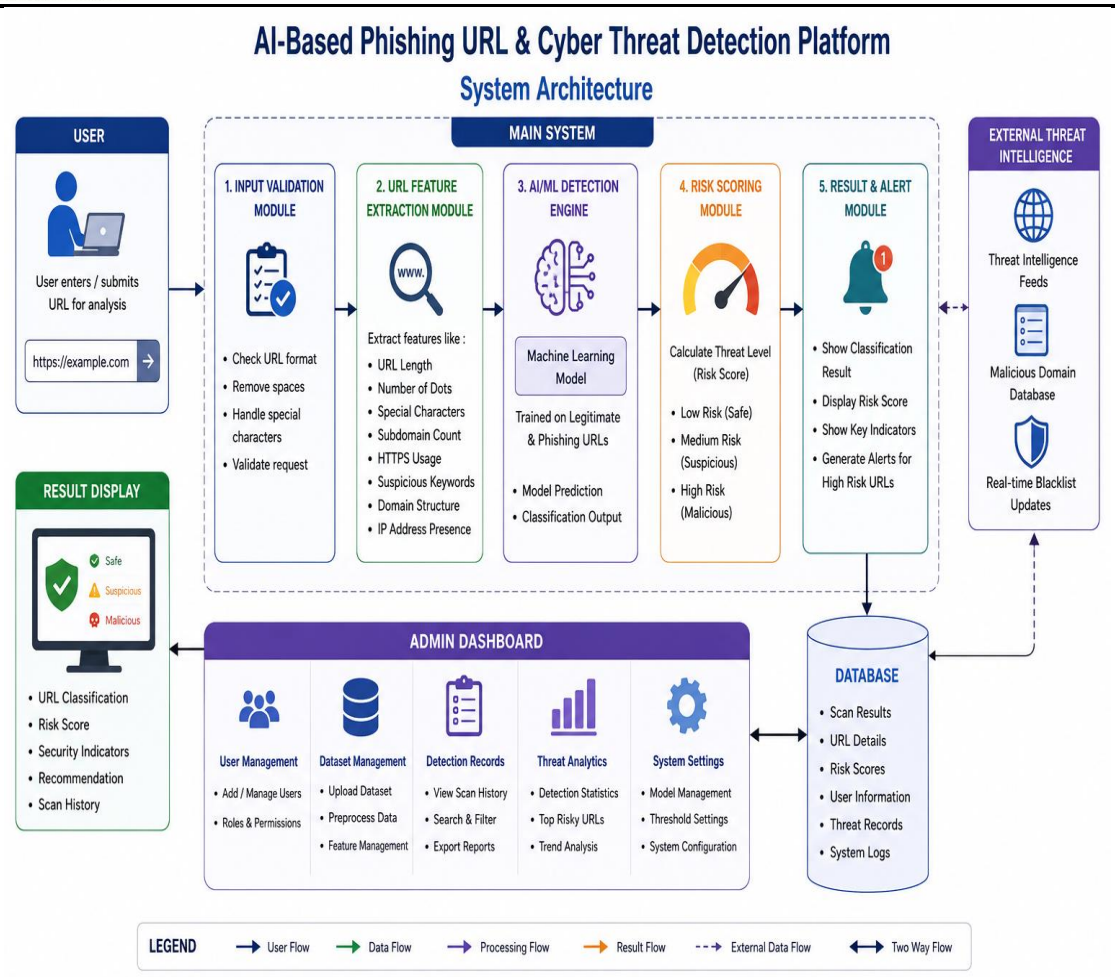
International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

and compared using appropriate evaluation metrics. The selected model is integrated into the backend of the detection platform. When a user submits a URL, the system validates the input and extracts the required features automatically. The trained model analyzes these features and generates a classification and risk score. The result is displayed through the frontend along with relevant security indicators and recommendations. Scan details can be stored in a database for future analysis and reporting. Finally, the platform is tested for detection accuracy, response time, input validation, security, usability, and reliability.

**System Architecture**

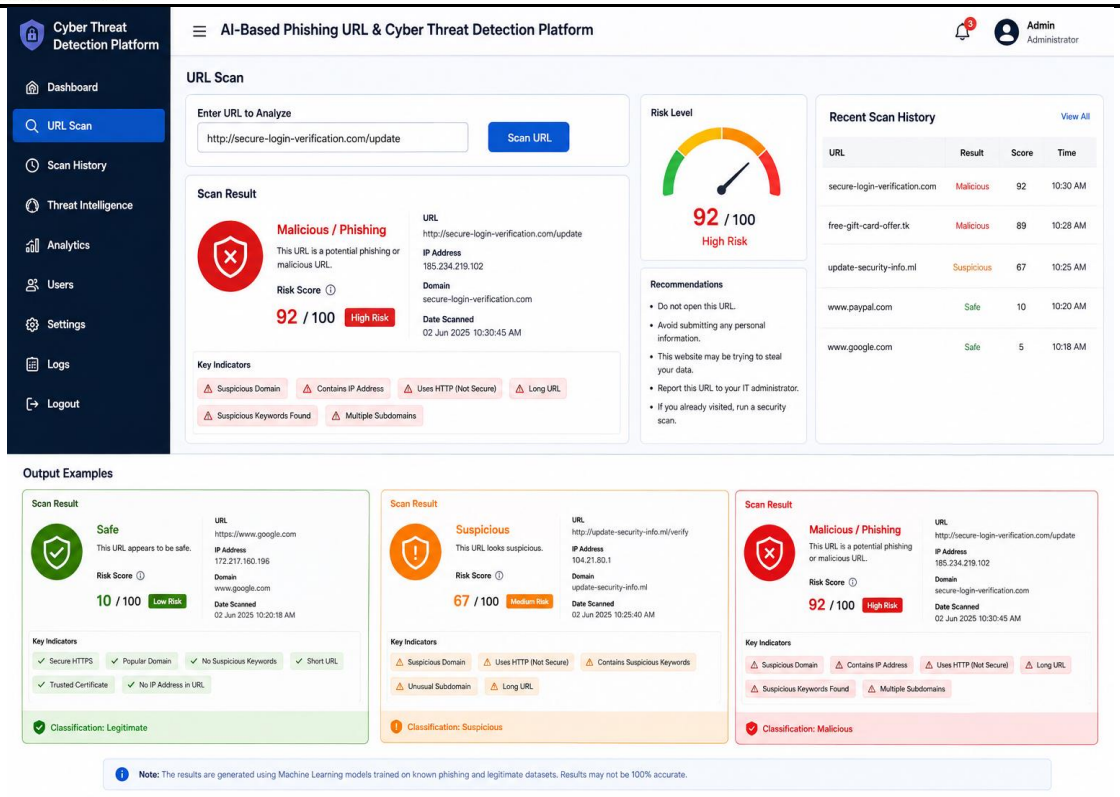
The system architecture represents the complete flow of information from URL submission to AI-based threat detection and result generation. The process begins when the user accesses the platform through a web-based interface and enters a URL for analysis. The URL is passed to the input validation module, which checks the format and prepares it for further processing. The validated URL is sent to the URL feature extraction module, which identifies characteristics such as length, domain structure, special characters, keywords, subdomains, and HTTPS usage. The extracted features are passed to the AI/ML detection engine, which contains the trained phishing classification model. The machine-learning model analyzes the features and predicts whether the URL is legitimate, suspicious, or potentially malicious. The risk-scoring module calculates an appropriate threat level based on the prediction and model output. The result is sent to the result and alert module, which displays the classification, risk information, and security indicators to the user. Scan details can be stored in a centralized database for detection history, reporting, and analytics. An administrator dashboard allows authorized administrators to manage datasets, users, detection records, and system configurations. The platform can also connect to external threat-intelligence sources to supplement the machine-learning prediction. Overall, the architecture follows the workflow **User → URL Input → Validation → Feature Extraction → AI/ML Detection Engine → Risk Scoring → Result & Alert → Database → Analytics & Admin Management**.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper




## V. Result and Output

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper




## VI. Conclusion

The AI-Based Phishing URL & Cyber Threat Detection Platform provides an intelligent and automated approach to identifying potentially harmful URLs and cyber threats. The system uses Artificial Intelligence, Machine Learning, and URL feature analysis to examine suspicious characteristics and classify URLs as legitimate, suspicious, or malicious.

The platform reduces the need for manual URL inspection by automatically analyzing features such as URL length, domain structure, special characters, suspicious keywords, subdomains, and HTTPS usage. It can also provide a risk score, security indicators, detection history, and alerts, helping users understand the potential threat associated with a URL.

The proposed system provides a proactive approach to cybersecurity and can help users identify potentially dangerous links before interacting with them. It can also assist administrators in monitoring detection records and analyzing cyber-threat patterns through a centralized dashboard.

Overall, the system demonstrates how AI and Machine Learning can be applied to improve phishing detection and cybersecurity awareness. Future enhancements can include real-time browser extensions, email phishing detection, threat-intelligence integration, deep-learning models, explainable AI, real-time domain monitoring, and automated security alerts.

## References

Received: 21-07-2026 | Accepted: 29-08-2026 | Published: 04-09-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

[1] Kumar, R. D., Prudhviraj, G., Vijay, K., Kumar, P. S., & Plugmann, P. (2024). Exploring COVID-19 through intensive investigation with supervised machine learning algorithm. In Handbook of Artificial Intelligence and Wearables (pp. 145-158). CRC Press.
[2] Swathi, B., Vijay, K., Sushanth Babu, M., & Dinesh Kumar, R. (2024, November). Machine Learning Techniques in Cloud Based Intrusion Detection. In The International Conference on Artificial Intelligence and Smart Environment (pp. 557-564). Cham: Springer Nature Switzerland.
[3] Sv satyakrishna, shirisha rangu ,bhargavi nalacheruve.(2024) Prospective investigation on colorectal cancer with SMOTE on machine learning Algorithm
[4] Dr.G.Vishnu Murthy, BhargaviNalacheruve 1Professor, Department of computer Science & engineering, Anurag University, TS, India. 2Student, Department of computer Science & engineering, Anurag University, TS, India.
[5] V. N. S. Manaswini, K. K, C. Nigam, S. S. Ali, R. Niranjana, and Suman, "Real-Time Object Detection in Drone Surveillance Using YOLOv5," in Proc. 2025 3rd Int. Conf. IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, 2025, pp. 1–6, doi: 10.1109/ICICAT68430.2025.11414670.
[6] B. Soundarya, V. N. S. Manaswini, M. Ayyakrishnan, R. D. Kumar, "Contextual Analysis of Big Data Analytics in Intelligent Transportation Frameworks," in Intersection of Artificial Intelligence, Data Science, and Cutting-Edge Technologies: From Concepts to Applications in Smart Environment, Lecture Notes in Networks and Systems, vol. 1353, Cham: Springer, 2025, doi: 10.1007/978-3-031-88304-0_79.
[7] R. D. Kumar, V. N. S.Manaswini, "Applications of blockchain in smart cities: detecting fake documents from land records using blockchain technology," in Blockchain for Smart Cities, Elsevier, 2021, pp. 105–117, doi: 10.1016/B978-0-12-824446-3.00017-X.
[8] Tejavath Veeramma, Badarla Anil, Guguloth Ravinder, "An advanced movie recommender using collaborative filtering and sentiment analysis," International Research Journal of Modernization in Engineering Technology and Science, vol. 7, no. 7, July 2025, doi: 10.56726/IRJMETS81618.
[9] Ravi Kumar Banoth, Ramana Murthy B V, "Automatic crop recommendation system using LightGBM and decision tree machine learning models," Journal of Machine and Computing, vol. 5, no. 1, pp. 343, Jan. 2025, doi: 10.53759/7669/jmc202505026.
[10] Ravi Kumar Banoth, Dr. B.V. Ramana Murthy, "Smart agriculture through IoT and machine learning for analyzing carbon footprints," in Proc. Int. Conf. Computer Science and Communication Engineering (ICCSCE), Apr. 2025.
[11] Ravi Kumar Banoth, B. V. Ramana Murthy, "Soil image classification using transfer learning approach: MobileNetV2 with CNN," SN Computer Science, vol. 5, art. no. 199, 2024, doi: 10.1007/s42979-023-02500-x.