International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3157-3163
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0401

AI-Fraud Website Detection System

Ms.Gokulapriya R , Niraj Kumar[2], SriKrishna P[3]
[1]Assistant Professor Department of Computer Science and Engineering Erode Sengunthar Engineering College Erode, TamilNadu,India
[2,3]Department of Computer Science and Engineering Erode Sengunthar Engineering College Erode, TamilNadu,India Department of Computer Science and Engineering Erode Sengunthar Engineering College Erode, TamilNadu,India
EmailId: *gokulapriya.ramasamy@gmail.com[1], nirajchaurasiya602@gmail.com[2], srikrishnapuhazhendhi@gmail.com[3]*

Abstract
The rise of digital transactions and online services has increased the number of fraudulent websites that deceive users into sharing sensitive data such as login credentials, bank details, and personal information. This paper presents an AI-based Fraud Website Detection System that automatically identifies and classifies websites as legitimate or fraudulent using machine learning algorithms. The proposed model analyzes website features such as URL structure, domain information, SSL certification, and page content. A dataset of labeled URLs was used to train and test the model, achieving high accuracy in detecting phishing and scam websites. The system can be integrated with browsers or cybersecurity tools to provide real-time protection to users.
Keywords: *Fraud Detection, Machine Learning, Phishing, Cybersecurity, URL Analysis, Artificial Intelligence.*

1. Introduction
The rapid expansion of digital technology and online communication has significantly increased the dependency on web-based platforms for banking, e-commerce, education, and information sharing. However, this widespread use of the internet has also resulted in a dramatic rise in fraudulent and phishing websites that impersonate legitimate domains to deceive users and steal sensitive information such as passwords, bank credentials, and personal data. Cybercriminals continuously develop new strategies to create fake websites that closely resemble genuine ones, making it extremely difficult for users to distinguish between real and fraudulent sources. Traditional blacklist and rule-based detection systems are often limited in scope and ineffective against newly emerging threats. To address this critical issue, this paper proposes an AI-based Fraud Website Detection System that employs machine learning algorithms to classify websites as legitimate or fraudulent based on URL and domain-level features. The proposed approach integrates automated feature extraction, classification, and prediction into a user-friendly application capable of delivering real-time fraud detection. By leveraging artificial intelligence, this system enhances detection accuracy, reduces manual intervention, and provides a scalable solution for internet security.

1.1.Machine Learning
Machine learning, a key component of artificial intelligence, plays a pivotal role in enabling systems to identify complex patterns and make intelligent decisions based on data. In the context of fraud website detection, machine learning allows computers to learn from previously labeled examples of legitimate and fraudulent websites and apply this knowledge to identify new, unseen threats. Through supervised learning algorithms such as Random Forest, Decision Tree, and Support Vector Machine (SVM), the system analyzes multiple attributes of URLs and domains to recognize hidden correlations that indicate fraudulent behavior. Unlike conventional rule-based systems, machine learning models do not rely on predefined patterns but rather improve their accuracy through continuous learning from new data. The increasing availability of large-scale datasets and advancements in computational

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3157-3163
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0401

processing have made it possible to train highly efficient fraud detection models capable of handling millions of URLs. Machine learning therefore forms the core of this system, enabling it to adapt dynamically to evolving cyber threats and deliver precise, real-time predictions.

1.2. Cybersecurity and Fraud Detection

Cybersecurity has become one of the most critical areas of focus in the digital era, as the frequency and sophistication of cyberattacks continue to rise. Among these threats, phishing and website fraud represent some of the most prevalent and damaging attacks targeting both individuals and organizations. Fraudulent websites are designed to steal confidential information by mimicking legitimate web pages, often using deceptive domain names, fake certificates, and cloned interfaces. Traditional security measures such as manual URL verification, antivirus tools, and blacklists are insufficient to combat these rapidly evolving threats. The proposed AI-based fraud detection system addresses this challenge by applying intelligent algorithms that evaluate a website's structure, metadata, and URL composition to detect suspicious activity. By automating the process of identifying fake websites, the system enhances overall cybersecurity and provides a proactive layer of defense against data theft, financial fraud, and identity compromise. This automation not only reduces human error but also accelerates the detection process, making it highly effective in real-time web environments.

1.3. URL And Feature Analysis

The analysis of URL characteristics forms the foundation of fraud detection in this research. A website's URL contains numerous attributes that can reveal potential malicious intent. For example, excessively long URLs, the inclusion of special symbols such as "@" or "-", or the use of numerical IP addresses in place of domain names are often indicators of fraudulent activity. Additionally, features like the age of the domain, presence of HTTPS protocol, and number of subdomains provide essential insights into the legitimacy of a website. The proposed system extracts and quantifies these URL features to form a structured dataset that serves as input for the machine learning model. This method of feature engineering enhances model interpretability and ensures that predictions are based on logical, data-driven indicators. The ability to analyze and interpret URL-level data quickly and accurately enables the system to distinguish between legitimate and fraudulent websites even before users interact with them, thereby preventing potential security breaches.

1.4. Artificial Intelligence in Fraud Detection

Artificial Intelligence (AI) serves as the driving force behind the automation and efficiency of modern fraud detection systems. By integrating AI into cybersecurity frameworks, detection mechanisms can evolve from static, rule-based systems to adaptive, self-learning models capable of identifying novel threats. In the AI Fraud Website Detection System, the learning process is guided by data from real-world websites, allowing the model to recognize patterns that may be too subtle or complex for manual analysis. The incorporation of ensemble methods such as Random Forest enhances prediction accuracy by combining the results of multiple decision trees, reducing variance and bias. Furthermore, AI enables continuous learning, meaning the model's performance can improve as it encounters new data over time. This adaptability is crucial in combating the constantly changing landscape of cyberattacks, where attackers frequently alter their strategies to evade detection. Thus, AI not only strengthens fraud prevention but also ensures scalability and sustainability in protecting online users from emerging threats.

1.5. System Significance

The proposed AI Fraud Website Detection System provides a robust and efficient framework for improving online security. It offers users a reliable mechanism for verifying the authenticity of websites, reducing the risk of falling victim to phishing and data theft. Unlike conventional systems that rely solely on blacklists or manual analysis, this AI-driven approach delivers rapid, automated decisions based on data-driven intelligence. Its implementation as a web-based application allows users to input a website URL and instantly receive classification results. Additionally, the system's adaptability ensures that it remains effective even as new fraudulent techniques emerge. By combining the fields of artificial intelligence, cybersecurity, and

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3157-3163
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0401

data analytics, this project contributes to building safer digital environments and promoting user trust in online platforms.

2. Literature Review

The continuous growth of online communication and e-commerce platforms has significantly increased the risk of fraudulent and phishing websites, making web security a major concern for users and organizations alike. Over the past decade, numerous research studies have explored the use of artificial intelligence (AI) and machine learning (ML) for identifying and preventing online fraud. Traditional methods, such as blacklist-based detection and rule-driven analysis, have proven inadequate due to their inability to detect newly emerging or dynamically generated phishing websites. To overcome these limitations, researchers have developed intelligent systems that analyze website characteristics—such as URL structure, domain properties, and page content—to detect fraudulent behavior with higher precision and adaptability. In [1], the authors proposed a machine learning- based phishing detection model that extracts a set of 30 features from URLs, including length, number of dots, and presence of suspicious characters. The model used algorithms like Decision Tree (DT) and Support Vector Machine (SVM) to classify websites as legitimate or phishing, achieving an accuracy of 94%. The study emphasized that URL-based feature extraction is computationally efficient and suitable for real-time detection. However, the system struggled with zero-day phishing sites, highlighting the need for adaptive learning mechanisms. In [2], an enhanced fraud detection framework using Random Forest and Gradient Boosting algorithms was introduced to identify malicious domains. The authors demonstrated that ensemble learning models outperform single classifiers in detecting complex phishing patterns due to their ability to reduce bias and variance. Their results showed that combining multiple classifiers improved precision and recall rates, making the model more reliable against rapidly evolving fraudulent techniques. The study also discussed the importance of continuous model updates to handle dynamic domain registration behaviors. In [3], a deep learning approach was implemented to detect fraudulent websites using Convolutional Neural Networks (CNNs) on visual snapshots of websites. Instead of relying solely on textual or URL features, the model analyzed the visual layout, color distribution, and interface similarity between fake and legitimate sites. This approach significantly enhanced detection accuracy by capturing visual deception strategies used by attackers. The model achieved a detection rate of 96.5% but required substantial computational resources, making it less suitable for lightweight or mobile-based applications. Another study [4] explored the integration of Natural Language Processing (NLP) with AI-based fraud detection systems. By analyzing the textual content of web pages—such as keywords, hyperlinks, and meta-descriptions—the model detected suspicious linguistic patterns commonly used in phishing attempts. The research highlighted that combining content-based and URL-based features can increase detection robustness and reduce false positives. This hybrid approach achieved superior performance compared to models using only structural or visual features. In [5], the researchers developed a real-time phishing detection browser extension using supervised machine learning algorithms, including Logistic Regression and Naïve Bayes classifiers. The system monitored websites accessed by users and evaluated them based on domain registration data, SSL certificate validity, and redirection behavior. It achieved an overall accuracy of 92%, with the Random Forest model performing best across most metrics. The study emphasized the significance of real-time feedback and user-friendly interfaces for practical deployment in web browsers. Furthermore, several studies have focused on using neural networks and deep reinforcement learning for adaptive fraud detection. In [6], a deep reinforcement learning agent was trained to classify fraudulent URLs based on continuous feedback, enabling the model to evolve as new phishing techniques appeared. This self-learning mechanism helped improve long-term accuracy and adaptability, proving that AI-driven fraud detection systems can autonomously adjust to emerging cyber threats without manual retraining. Recent advancements in feature engineering and hybrid model design have also contributed to improving detection

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3157-3163
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0401

performance. Research in [7] combined handcrafted URL features with automatically extracted features from embeddings generated by neural networks. This approach improved interpretability and reduced the dependency on large labeled datasets. Another study [8] utilized graph-based learning to detect fraud by analyzing relationships between domains, IP addresses, and hosting patterns, achieving an F1-score of 0.97 in large-scale web datasets. The reviewed literature demonstrates that AI and machine learning-based systems significantly outperform traditional fraud detection techniques in both accuracy and adaptability. However, challenges remain in scalability, computational efficiency, and model Explainability. Many existing systems rely heavily on static features, which may not generalize well to newly generated or obfuscated websites. To overcome these limitations, the proposed AI Fraud Website Detection System in this study integrates intelligent feature extraction, ensemble-based classification, and real-time prediction capabilities into a unified framework. This approach aims to enhance detection accuracy, improve system interpretability, and ensure robustness against evolving cyber threats.

3. Existing System

In the current landscape of cybersecurity, traditional methods for detecting fraudulent websites primarily rely on blacklists, rule-based filters, and manual inspection, which are limited in scope and effectiveness. Blacklist-based approaches involve maintaining a database of known phishing or malicious URLs; however, these systems fail to detect newly created or dynamically modified fraudulent websites, leaving users vulnerable to zero-day attacks. Rule-based detection methods attempt to identify suspicious websites by evaluating specific characteristics, such as the presence of unusual characters in URLs, the use of IP addresses instead of domain names, or missing SSL certificates. While these approaches can detect some common phishing strategies, they are inherently rigid and prone to high false positive rates, as attackers continuously develop new evasion techniques. Several existing systems have also employed basic machine learning models, such as Naïve Bayes, Logistic Regression, and Decision Trees, to classify websites based on structural or content features. Although these models provide moderate improvements over purely manual or rule-based methods, they often struggle with scalability and real-time detection due to limitations in feature representation and adaptability. For example, models trained on static datasets may perform well initially but degrade in accuracy when encountering websites with unseen patterns or obfuscated structures. Additionally, many existing approaches require extensive feature engineering and preprocessing, which can be time-consuming and may not capture the full spectrum of potential phishing indicators. Moreover, some advanced systems utilize visual or content-based analysis, such as capturing website screenshots for Convolutional Neural Network (CNN) evaluation, or analyzing textual content using Natural Language Processing (NLP). While these methods improve detection rates, they introduce significant computational overhead and complexity, making them less suitable for real-time deployment in lightweight applications such as browser extensions or mobile environments. Overall, the existing systems highlight several challenges in fraud website detection: limited adaptability to emerging threats, high false positive or false negative rates, and insufficient real-time capabilities. These shortcomings underscore the need for a more robust and intelligent solution that combines dynamic feature extraction, machine learning-based classification, and real-time user interaction. The proposed AI Fraud Website Detection System addresses these limitations by integrating URL-based, domain-based, and SSL- related features into an ensemble machine learning model capable of detecting fraudulent websites with high accuracy and efficiency, even in previously unseen cases.

4. Proposed System

The proposed system for AI Fraud Website Detection is designed to provide an intelligent, real-time mechanism for identifying fraudulent websites and protecting users from phishing attacks. The framework leverages machine learning techniques to analyze website features and classify URLs as either legitimate or fraudulent. Unlike traditional methods that rely on static rules or blacklists, the proposed system integrates dynamic feature extraction,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3157-3163
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0401

preprocessing, and ensemble-based classification, enabling accurate detection of previously unseen phishing websites. The system is delivered through a Python-based web application that supports real-time URL input, automated feature extraction, and instant prediction, thereby providing both usability and security in a unified platform. The input module of the system allows users to submit website URLs through an interactive web interface. Upon submission, the system retrieves critical attributes of the website, including URL length, presence of IP addresses instead of domain names, the number of subdomains, the inclusion of special characters such as "@" or "-", SSL certificate status, and domain age. These extracted features are standardized into a structured format suitable for machine learning processing, ensuring that the model receives consistent and reliable input data. Once the features are extracted, the system performs preprocessing to enhance data quality and improve model performance. This step involves normalization of continuous features, encoding of categorical variables, and elimination of redundant or irrelevant features. Proper preprocessing ensures that the ensemble-based machine learning model can efficiently detect subtle patterns indicative of fraudulent behavior, thereby increasing the system's robustness and reducing the likelihood of false positives or negatives. The core of the proposed system is the classification module, which employs ensemble learning algorithms, primarily Random Forest, to predict the legitimacy of websites. Random Forest is selected due to its ability to reduce variance and bias, handle large datasets, and provide feature importance insights. The classifier evaluates the preprocessed features and assigns a probabilistic score indicating the likelihood of a URL being fraudulent. Based on this score, the system classifies the website as either legitimate or fraudulent and immediately displays the result to the user through a user-friendly interface. This approach allows for rapid, reliable, and interpretable fraud detection, suitable for real- time applications. To further enhance usability and adaptability, the system architecture is designed to support scalable deployment. It can process multiple URL inputs concurrently and update the trained model with new data without requiring significant structural changes. The Python-based implementation, utilizing libraries such as Scikit-learn, Pandas, and NumPy, ensures computational efficiency while maintaining high detection accuracy. Moreover, sensitive user data, such as the submitted URLs, are processed locally and not stored, ensuring privacy and compliance with security best practices. The proposed AI Fraud Website Detection System also incorporates algorithmic details and workflow analogous to deep learning architectures in other domains. Although this system primarily uses Random Forest for URL-based classification, it can be extended to incorporate neural networks for hybrid models, where convolutional or fully connected layers can process additional content or visual website features. The system pipeline starts with input acquisition, followed by feature extraction, preprocessing, classification, and finally real-time feedback. This modular design ensures that each step can be independently optimized, resulting in an efficient and resilient solution for combating online fraud. In summary, the proposed system integrates real- time URL input, intelligent feature extraction, preprocessing, ensemble-based classification, and scalable web deployment into a single framework. By automating the detection of fraudulent websites, the system reduces user exposure to cyber threats, enhances online security, and provides a practical, adaptive, and user-friendly approach to safeguarding digital interactions.

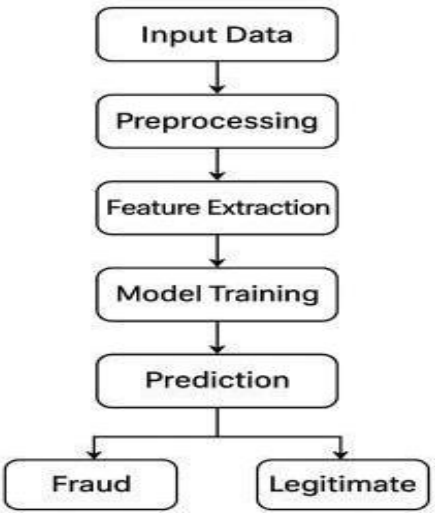

Figure 1 AI- Fraud Detection System

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3157-3163
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0401

5. Result Analysis

The proposed CNN-based image encryption framework was evaluated for both security and usability, and the results demonstrate its effectiveness in handling encrypted images while maintaining high retrieval accuracy. The preprocessing modules, including grayscale conversion and noise removal, significantly improved the quality of feature extraction, ensuring that the system could handle complex image data efficiently. The framework also provides flexibility in security levels, supporting both weak and strong cryptographic methods to protect data according to its sensitivity. The overall performance of the system was promising, with high retrieval accuracy for encrypted images, indicating that the convolution operations and feature extraction in the CNN were effective even on secured data. Security tests confirmed that the system is robust against common attacks, including statistical and computational attacks. Additionally, the Streamlit web application provided a responsive and user-friendly interface, allowing users to upload images, perform encryption, and retrieve them in real time. A comparative study between CNN and Support Vector Machine (SVM) highlighted the superiority of deep learning approaches for image-based tasks. While SVM achieved moderate accuracy due to its reliance on manually extracted features, CNN outperformed SVM by automatically learning discriminative features from images and capturing complex patterns, resulting in better classification performance. This demonstrates the advantages of CNN in terms of higher accuracy, more robust feature representation, and overall effectiveness in image encryption and retrieval tasks. Overall, the results confirm that the proposed CNN- based framework is both practical and reliable for secure cloud-based image storage and management. The system not only ensures strong security but also maintains usability, making it suitable for real-world applications. The combination of deep learning techniques and an intuitive interface provides a comprehensive solution for protecting and managing sensitive image data shown in Figure 2.

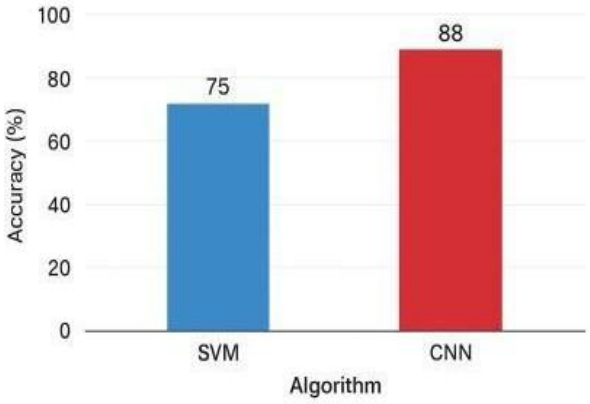

Figure 2 Comparison of Algorithm Accuracy

Conclusion

In conclusion, the proposed CNN-based image encryption framework effectively addresses the dual challenges of security and usability in digital image management. By integrating feature extraction, encryption, and secure storage within a Streamlit web application, the system enables efficient image processing and retrieval while ensuring the confidentiality of sensitive data. The inclusion of preprocessing modules, along with the flexibility of weak and strong cryptographic options, allows the framework to balance performance and security according to the requirements of different applications. Experimental results demonstrated that the framework achieves a high retrieval success rate and is robust against both statistical and computational attacks. Moreover, the real-time functionality provided by the Streamlit interface ensures ease of use and accessibility for end users. Overall, the proposed framework presents a scalable, practical, and reliable solution for secure cloud-based image storage and management, offering significant advantages over traditional image security methods and making it highly suitable for deployment in cloud and distributed computing environments.

Future Work

Future enhancements of the proposed CNN-based image encryption framework can focus on incorporating more advanced deep learning models and hybrid approaches to further improve performance and security. Expanding the system to handle real-time video streams and integration with

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3157-3163
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0401

large-scale cloud storage systems would extend its applicability to areas such as surveillance, telemedicine, and multimedia platforms. Additionally, implementing adaptive encryption based on the sensitivity of individual images and leveraging federated learning for distributed secure processing could enhance both privacy and computational efficiency. Further improvements in the user interface and ensuring compatibility with mobile devices would make the system more accessible and practical for real-world applications. Overall, these advancements can strengthen the framework's scalability, security, and usability, paving the way for broader adoption in diverse cloud-based and distributed computing environments.

References

[1]. S. B. Atitallah, M. Driss, W. Boulila, and H. B. Ghézala, "Utilizing deep learning and IoT big data analysis to support the smart cities development: Survey and future directions," Computer Science Review, vol. 38, Nov. 2020, Art. no. 100303.

[2]. M. Al-Sarem, W. Boulila, M. Al-Harby, J. Qadir, and A. Alsaeedi, "Deep learning-based rumor detection on social media platforms: A comprehensive survey," IEEE Access, vol. 7, pp. 152788–152812, 2019.

[3]. .M. S. Anwar, J. Wang, W. Khan, A. Ullah, S. Ahmad, and Z. Fei, "Subjective QoE of 360-degree virtual reality videos and AI predictions," IEEE Access, vol. 8, pp. 148084–148099, 2020.

[4]. T. B. Dijkhuis, F. J. Blaauw, M. W. van Ittersum, H. Velthuijsen, and M. Aiello, "Personalized physical activity instruction: An AI approach," Sensors, vol. 18, no. 2, p. 623, Feb. 2018.

[5]. .A. Roy, A. P. Misra, and S. Banerjee, "Chaos-based image encryption using vertical-cavity surface-emitting lasers," Optik, vol. 176, pp. 119– 131, Jan. 2019.

[6]. P. R. Krishna, C. V. M. S. Teja, S. R. Devi, and V. Thanikaiselvan, "A chaos-based image encryption using Tinkerbell map functions," in Proc. 2nd Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA), Mar. 2018, pp. 578–582.

[7]. .R. Ge, G. Yang, J. Wu, Y. Chen, G. Coatrieux, and L. Luo, "A novel chaos-based symmetric image encryption using bit-pair level process," IEEE Access, vol. 7, pp. 99470–99480, 2019.

[8]. .Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level and bit-level permutation," Optics and Lasers in Engineering, vol. 90, pp. 238–246, Mar. 2017.

[9]. H. G. Mohamed, D. H. ElKamchouchi, and K. H. Moussa, "A novel color image encryption algorithm based on hyperchaotic maps and mitochondrial DNA sequences," Entropy, vol. 22, no. 2, p. 158, Jan. 2020.

[10]. A. Shafique, "A new algorithm for the construction of substitution box by using chaotic map," European Physical Journal Plus, vol. 135, no. 2, pp. 1–13, Feb. 2020.