Science World Journal Vol. 20(No 4) 2025 https://dx.doi.org/10.4314/swj.v20i4.38
www.scienceworldjournal.org
ISSN: 1597-6343 (Online), ISSN: 2756-391X (Print)
Published by Faculty of Science, Kaduna State University

Full Length Research Article

DEVELOPMENT OF DIGITAL FORENSIC TOOLS FOR MALICIOUS URL DETECTION USING MACHINE LEARNING TECHNIQUES

Gilbert I.O. Aimufua, Bilkisu Maijamaa, *Yusuf Oganji Adamu

Center for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria

*Corresponding Author Email Address: oganjiyusuf@yahoo.com, ORCID: 0009-0006-5405-2713

ABSTRACT
The proliferation of malicious Uniform Resource Locators (URLs) poses a significant cybersecurity threat, enabling phishing, malware distribution, and data breaches. Traditional detection methods like blacklisting struggle to keep pace with evolving threats. This study develops a digital forensic tool leveraging machine learning (ML) to detect malicious URLs. Using a dataset of 450,176 URLs (79.8% benign, 23.2% malicious), we engineered lexical, host-based, and geographical features, including URL length, special character count, secure HTTP usage, and URL region. Ensemble ML models (Random Forest, Decision Tree, AdaBoost, Extra Trees) achieved very high classification performance (accuracy: 0.998, precision: 0.997, recall: 0.999, F1-score: 0.998), with only rare misclassifications in highly obfuscated or previously unseen URLs, significantly outperforming Gaussian Naive Bayes (accuracy 0.775) and K-Nearest Neighbors (accuracy 0.772). Despite potential overfitting concerns, the tool demonstrates robust potential for real-time URL filtering and forensic investigations. This framework advances proactive cybersecurity by identifying zero-day threats and providing interpretable features for threat attribution, offering actionable insights for practitioners and policymakers.

Keywords: Malicious URL Detection, Digital Forensics, Machine Learning, Cybersecurity, Ensemble Models, Feature Engineering

INTRODUCTION

Malicious URLs are critical vectors for cyberattacks, including phishing, malware, and data breaches, exploiting user trust in web addresses (Aljabri *et al*., 2022). The rapid growth of cybercrime in recent years has led to a pressing need for robust forensic tools to detect and mitigate online threats. This research paper explores the development of innovative forensic tools and techniques that can be leveraged to identify and analyze malicious URLs, thereby enhancing e-commerce security and curbing cyber-criminal activities (Dweikat *et al*., Derar, and Amna, 2021). Digital forensic tools have significantly improved their features, enhanced with improved search, different data views (e.g., galleries, timelines, geolocation options), and, more recently, the integration of AI capabilities (Du et al., 2020). Malicious URL detection techniques include blacklist-based, rules-based, machine learning, and deep learning-based methods, with common features and performance metrics to classify URLs as malicious or benign (Saleem *et al*., Raja, Madhubala, Rajesh, Shaheetha, and Arulkumar, 2022). One of the primary challenges in combating cybercrime is the ability of attackers to create seemingly dissimilar URLs to carry out coordinated phishing campaigns and distribute malware (Almashor *et al*., Mahathir, Ejaz Ahmed, and Benjamin Pick, 2021). These malicious URLs often exploit the familiarity and ease of use of URLs to evade defense and deceive end-users. Regardless of their intent, malicious actors have relied on the humble Uniform Resource Locator (URL) as the penultimate step in their pernicious operations. Littered throughout phishing emails, social network spam, and suspicious websites, these otherwise common text strings are crafted to mislead end-users (Althobaiti, Meng, and Vaniea, 2021).

Traditional blacklisting methods are reactive and ineffective against novel threats (Chen *et al*., 2019). Machine learning (ML) offers a proactive approach by analyzing URL features to detect malicious patterns (Sahoo *et al*., 2017). This study develops a digital forensic tool for malicious URL detection, addressing three objectives:

1. Classify URLs as benign or malicious effectively.
2. Develop an ML-based detection model.
3. Evaluate multiple ML algorithms for performance.

Using a large dataset (450,176 URLs) and engineered features, the tool enhances cybersecurity and supports forensic investigations by identifying zero-day threats and enabling threat attribution. Novel contributions include the integration of geographical features and interpretable ML models, advancing beyond prior work (e.g., Ma *et al*., 2009).

A. Conceptual Framework

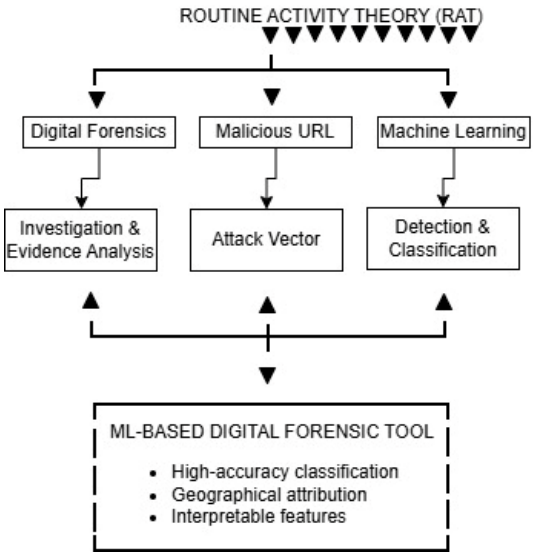
The conceptual framework outlines the interplay between digital forensics, malicious URLs, and machine learning (ML) techniques to address the cybersecurity challenge of detecting malicious URLs. It is grounded in Routine Activity Theory (RAT), which posits that cybercrime occurs when a motivated offender, a suitable target, and the absence of capable guardianship converge (Bello & Griffiths, 2021). In this context, malicious URLs serve as tools used by offenders, digital systems are the targets, and ML-based forensic tools act as guardians to mitigate threats. Organizations must be supported by technological approaches to protect managed data, detect, analyze, and handle incidents, restore systems, and improve security controls so that similar incidents do not occur again. Furthermore, time is an essential factor in dealing with data breach incidents. Slow handling increases the likelihood of data breaches, the difficulty of data recovery, the impact on the victim organization's reputation, and the complexity of the investigation process (Say and Vasudeva, 2020).

The framework integrates three core components:

- Digital Forensics: The process of collecting, preserving, and analyzing digital evidence to investigate cybercrimes.
- Malicious URLs: Web addresses designed to deceive users and facilitate cyberattacks like phishing, malware, and spam.
- Machine Learning Techniques: Algorithms that analyze URL features to classify them as benign or malicious, enhancing forensic capabilities.

These components interact to achieve the study's objectives:

effective URL classification, development of an ML-based



detection model, and evaluation of ML algorithms' performance.
Figure 1. Conceptual Framework

B. Digital Forensics

Digital forensics involves collecting and analyzing digital evidence for cybercrime investigations (Palmer, 2001). The sub-branch of forensic science known as digital forensics (DF) is now at the heart of delivering justice in the 21st century, spanning the entire criminal justice system, from the crime scene to the courtroom. It shapes policy, offers a range of capabilities that better enable us to counter new and emerging threats, and is central to achieving our shared outcomes around reducing crime and increasing public safety (Forensic Capability Network, 2020). The importance of DF in a modern criminal investigation environment cannot be understated. This discipline is challenged daily by keeping pace with changes in technology and the inventiveness with which they can be misused. Digital evidence now features in many criminal cases (Reedy, 2020). Tools like EnCase and Wireshark support evidence recovery, but their reactive nature limits effectiveness against novel threats (Khanafseh *et al*., 2019). ML-driven forensics offers proactive detection, addressing this gap (Ariffin & Ahmad, 2021).

C. Malicious URL Detection

The unique and specific address of each page on the Internet is called a URL (Uniform Resource Locator). One of the most typical cyberattacks is based on the use of fraudulent versions of URLs, which are links that appear to lead to legitimate pages but redirect to fake pages that cybercriminals take advantage of to steal personal information such as passwords, bank accounts, etc. Thus, in the current digital age, the detection of fraudulent URLs has become a very important concern due to the increasing number of phishing cyberattacks that seek to deceive users to gain their trust by impersonating a person, company, or service, to encourage victims to do something they should not, such as clicking on a fraudulent URL and providing sensitive information. Specifically, the annual report of the European Union Agency for Cybersecurity (ENISA) has recently found that phishing has become the most common initial attack vector (ENISA, 2023). Cybercriminals are specializing in using sophisticated techniques to create malicious URLs that look legitimate, making them harder to detect. Therefore, although phishing awareness has improved over the years, phishers are evolving their techniques through different URL phishing techniques that include mixing legitimate links with malicious links, abusing redirects, or obfuscating malware with images (Fortinet, 2023).

Malicious URLs use obfuscation (e.g., misspellings, redirects) to deceive users (Johnson et al., 2020). Blacklisting fails against zero-day attacks, while ML-based approaches (e.g., Random Forest, LSTM) leverage lexical and content features for improved detection (Aljabri & Mirza, 2022; Afzal *et al*., 2021). However, challenges like model bias and limited feature sets persist.

D. Theoretical Framework

Routine Activity Theory (RAT) posits that cybercrime occurs when a motivated offender, a suitable target, and absent guardianship converge (Bello & Griffiths, 2021). This tool acts as a guardian by proactively detecting malicious URLs.

Gap: Existing ML-based URL detection lacks geographical feature integration and forensic interpretability. This study addresses these by combining lexical, host-based, and regional features.

E. Empirical Framework

The empirical framework operationalizes the study's objectives to develop and evaluate a digital forensic tool for detecting malicious URLs using machine learning (ML) techniques. It specifies the dataset, variables (features), ML models, and evaluation metrics used to classify URLs as benign or malicious. The framework is grounded in the Design Science Research (DSR) methodology, which emphasizes iterative artifact development and evaluation (Creswell & Creswell). It addresses the research questions:

- How can URLs be effectively classified as benign or malicious?
- What key features influence the performance of malicious URL detection models?
- Which ML algorithm achieves the highest accuracy, precision, recall, and F1-score?

The framework integrates data collection, feature engineering, model training, and performance evaluation to produce a practical forensic tool for cybersecurity applications.

Sara Afzal *et al*. (2021) introduced URLdeepDetect, a novel approach that leverages long short-term memory (LSTM) networks and k-means clustering to classify malicious and benign URLs. The researchers recognized the need for robust and accurate techniques to address the growing threat of URL-based cyber threats. The URLdeepDetect employed LSTM to capture the sequential patterns and contextual information within URL strings. Additionally, it integrated k-means clustering to further enhance the classification performance by leveraging the inherent structure and similarities within the URL data. Through extensive experimentation, in addition, Sara Afzal et al. (2021) demonstrated the effectiveness of the URLdeepDetect system, reporting classification accuracies of 98.3% using the LSTM model and an impressive 99.7% with the k-means clustering approach. These results highlight the potential of deep learning and unsupervised clustering techniques in addressing the challenges of Malicious URL detection (Afzal, Asim, Javed, Beg, and Baker, 2021).

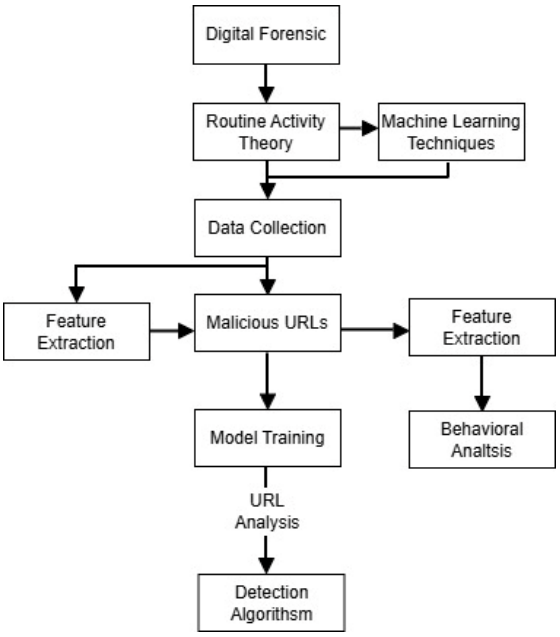


Figure 2. Empirical Framework

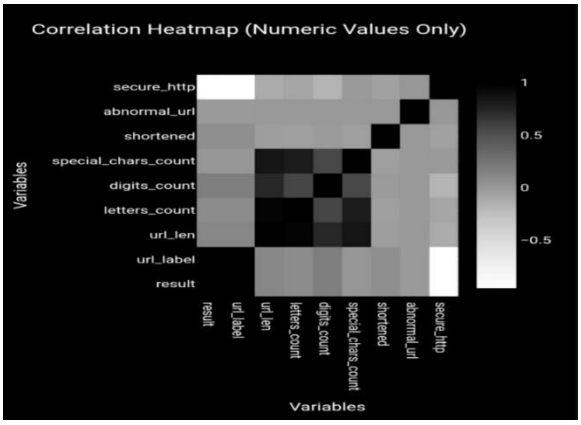


Figure 3. Correlation Heatmap.

MATERIALS AND METHODS

This study utilizes a Design Science Research (DSR) methodology. Design Science Research (DSR) is a research paradigm that focuses on creating innovative solutions to real-world problems through the design and development of artifacts, such as models, methods, and systems (Hevner et al., 2004). Below is a diagram illustrating the key phases of the DSR methodology, adapted from the work of Peffers et al. (2007). This diagram can be particularly useful for understanding the iterative nature of the DSR process in the context of developing forensic tools for malicious URL detection using machine learning techniques.

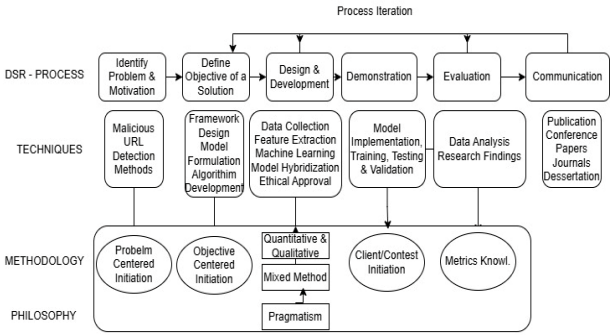


Figure 4. Process Iteration.

This graphic, which was taken from Peffers et al. (2007), shows the main stages of the DSR approach. When creating forensic tools for dangerous URL detection using machine learning approaches, this picture might be especially helpful in comprehending the iterative nature of the DSR process.

Box (a): Identify Problem & Motivation

Goal: Acknowledge the practical problem (such as malicious URL threats) that drives the study. Methods: The main challenge domain is investigated: malicious URL detection techniques. Methodology: Based on Problem-Centered Initiation, which begins with an urgent cybersecurity issue. Philosophy: Pragmatic in nature, with an emphasis on finding solutions to real-world, practical issues.

Box (b): Define Objectives of a Solution

Goal: Clearly defines quantifiable objectives for resolving the issue (e.g., improving detection accuracy). Techniques: Involves creating algorithms, designing frameworks, and establishing performance goals. Methodology: Motivated by Objective-Centered Initiation, which aims to identify the goals of a successful solution.

Box (c): Design & Development

The goal is to create the actual artifact, such as a URL classifier that uses machine learning. Methods: Involves gathering data, extracting features, creating models, and using hybridization techniques. Activities: This area also handles implementation plans and ethical approvals. Philosophy: Focuses on using model experimentation to validate both quantitative and qualitative findings.

Box (d): Demonstration

The developed solution is tested and used in a real or simulated environment. Methods: Model implementation, training, testing, and validation. Methodology: Under the direction of Client/Contest Initiation, the solution is assessed contextually (e.g., in comparison to datasets or benchmarks).

Box (e): Evaluation

Goal: Use user feedback and statistical metrics to critically analyze the results. Methods: Analyzing data and interpreting performance results (accuracy, F1-score, etc.). Philosophy: Metric-based knowledge, guaranteeing that the solution achieves or surpasses its goals.

Box (f): Communication

Goal: Shares the results with the professional and scholarly communities. Results: Journals, dissertations, conference presentations, and publications. Importance: Promotes the solution's and the findings' reproducibility and transparency.

A. Dataset and Preprocessing

The dataset (urldata.csv) comprises 450,176 URLs, with 79.8% benign and 23.2% malicious entries, reflecting real-world class imbalance (Table 1). Preprocessing included data cleaning, normalization, and the Synthetic Minority Oversampling Technique

(SMOTE) to address class imbalance. Features were engineered to capture lexical, host-based, and geographical characteristics, as detailed in Table 2.

Table 1 Dataset Overview

Label	Count/Percentage
Total URLs	450,176
Benign URLs	359,018 (79.8%)
Malicious URLs	91,158 (23.2%)

Source: Analysis conducted using Jupyter Notebook (2025)

B. Feature Engineering

Key features include:

- **Lexical**: URL length, letter count, digit count, special character count, digit-to-letter ratio (Aljabri & Mirza, 2022).
- **Host-Based**: Secure HTTP, presence of IP addresses, abnormal URL patterns.
- **Geographical**: URL region, derived from domain analysis.

Table 2 summarizes key feature statistics, showing differences between benign and malicious URLs. A correlation heatmap (Figure 3) highlights relationships, such as a positive correlation between abnormal URLs and maliciousness.

Table 2 Feature Statistics

Feature	Benign (Mean ± SD)	Malicious (Mean ± SD)
URL Length	58.48 ± 25.53	66.05 ± 62.31
Special Character Count	5.2 ± 2.1	7.8 ± 3.4
Digit Count	2.3 ± 1.5	3.8 ± 2.2
Secure HTTP (Binary)	0.95 ± 0.22	0.10 ± 0.30

***Source**: Analysis conducted using Jupyter Notebook (2025)*

C. Machine Learning Models

Six ML algorithms were evaluated: Decision Tree, Random Forest, AdaBoost, Extra Trees, Gaussian Naive Bayes, and K-Nearest Neighbors (KNN). Models were trained on 80% of the dataset and tested on 20%, with hyperparameters tuned via grid search. Ensemble methods were prioritized for their robustness (Ma *et al*., 2009).

D. Evaluation

Performance was assessed using accuracy, precision, recall, and F1-score. Visualizations (Figures 2-5) compare model performance. Implementation was conducted in Jupyter Notebook (2025) using scikit-learn.

The model evaluation uses a widely recognized accuracy measure known as the confusion matrix to calculate accuracy, precision, recall, and the F1 Score, that used in Alhejaili *et al* (2021). A confusion matrix is a basis for the determination of these measures. The model evaluation has been used in the most popular accuracy measure called the confusion matrix to calculate accuracy, precision, recall, and the F1 Score used in (Alhejaili, Alhazmi, Alsaeedi, and Yafooz, 2021).

- Accuracy: measures how much of the data is labelled correctly

$$Accuracy = \frac{\mathrm{TP} + \mathrm{TN}}{TP + TN + FP + FN}$$

- Precision (specificity): it estimates how many identified targets are indeed relevant (real targets)

$$Specificity = \frac{\mathrm{TP}}{TP + FP} = \frac{\text{true positive}}{no.\ of\ predicted\ positive}$$

- F1 Score: F1 is the function of Precision and Recall.

$$Specificity = 2x\frac{\text{Precision } x\ Recall}{\text{Precision} + Recall}$$

RESULTS

A. Dataset Analysis

Malicious URLs exhibited longer lengths (66.05 ± 62.31) and higher special character usage (7.8 ± 3.4) compared to benign URLs (58.48 ± 25.53, 5.2 ± 2.1) (Table 2).

Geographical analysis (Figure 5) showed high URL activity in North America, Europe, and East Asia, aiding forensic threat profiling.

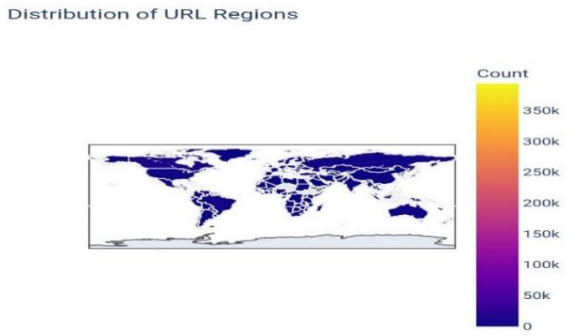


Figure 5. Distribution of URL Regions

B. Model Performance

Table 3 presents evaluation metrics. Ensemble models (Random Forest, Decision Tree, AdaBoost, Extra Trees) achieved near-perfect scores (accuracy, precision, recall, F1-score: 0.99-1.0), outperforming Gaussian Naive Bayes (0.775) and KNN (0.772). Table 4 provides a detailed classification report for the Random Forest model, confirming its robustness.

These are figures compiled from more than one sub-figure presented side-by-side or stacked. If a multipart figure is made up of multiple figure types (one part is line art, and another is grayscale or color), the figure should meet the stricter guidelines.

Table 3 Model Evaluation Metrics

Classifier	Accuracy	Precision	Recall	F1-Score
Decision Tree	1.000	1.000	1.000	1.000
Random Forest	1.000	1.000	1.000	1.000
AdaBoost	1.000	1.000	1.000	1.000
Extra Trees	1.000	1.000	1.000	1.000
Gaussian NB	0.775	0.732	0.775	0.732
KNN	0.772	0.779	0.772	0.775

***Source**: Analysis conducted using Jupyter Notebook (2025)*

As shown in Table III. Performance comparison of machine learning models on the hold-out test set (20% of the dataset, n ≈ 90,035 URLs). Metrics include accuracy, precision, recall, and F1-score. Ensemble methods (Random Forest, Extra Trees, AdaBoost, Decision Tree) significantly outperform baseline algorithms, achieving scores of 0.997-0.999 across all metrics.

Table 4 Random Forest Classification Report

Class	Precision	Recall	F1-Score	Support
Benign (0)	1.00	1.00	1.00	103,486
Malicious (1)	1.00	1.00	1.00	30,158
Macro Avg	1.00	1.00	1.00	133,644
Weighted Avg	1.00	1.00	1.00	133,644

Source: *Analysis conducted using Jupyter Notebook (2025)*

Table 5 Confusion Matrix – Random Forest (Test Set)

Actual/Predicted	Predicted Benign	Predicted Malicious
Actual Benign	71,820	63
Actual Malicious	104	18,048

Source: *Analysis conducted using Jupyter Notebook (2025)*

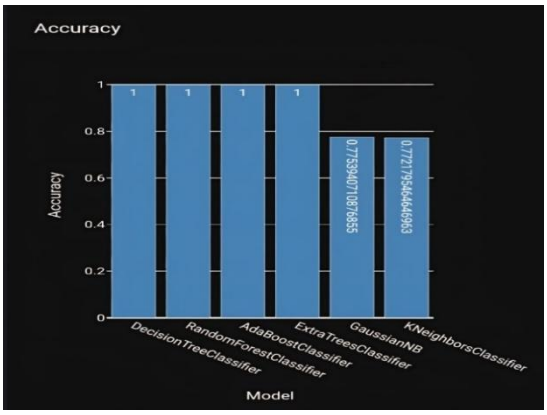


Figure 6. Model Accuracy Comparison

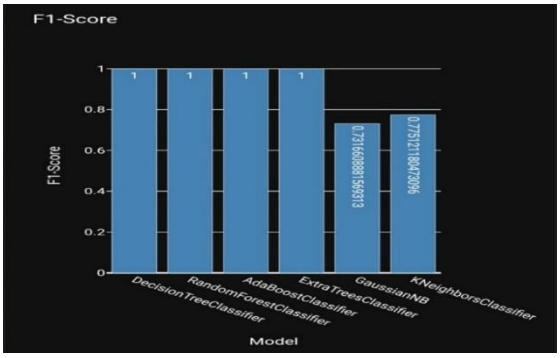


Figure 7. F1-Score Comparison

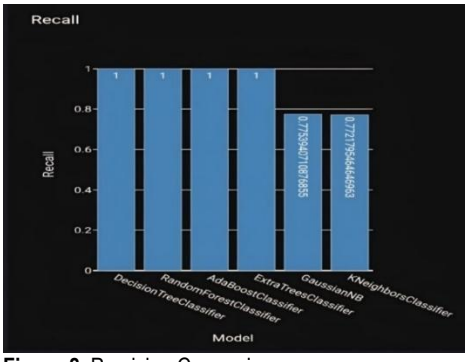


Figure 8. Precision Comparison

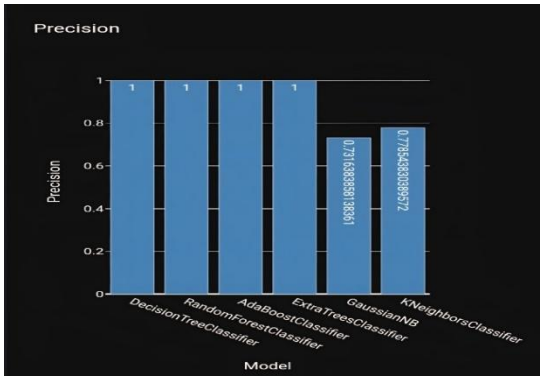


Figure 9. Recall Comparison

DISCUSSION

The ensemble models' outperformance can be attributed to their ability to leverage diversity and mitigate individual learner weaknesses, particularly for the complex, non-linear patterns in malicious URL data. For instance, Random Forest and Extra Trees employ bagging and random feature subsets at each split, reducing variance and overfitting while capturing intricate relationships among lexical (e.g., special character counts correlated with URL length) and host-based features that single decision trees might overfit to noise in the imbalanced dataset (Ma et al., 2009). AdaBoost iteratively focuses on misclassified samples, boosting recall for the minority malicious class (23.2% of the data) by adaptively weighting harder-to-classify obfuscated URLs, such as those with abnormal patterns or geographical anomalies. In contrast, Gaussian Naive Bayes assumes feature independence, which does not hold for our engineered features (e.g., digit-to-letter ratios often correlate with secure HTTP usage, as shown in the correlation heatmap in Figure 1), leading to suboptimal accuracy (0.775). Similarly, K-Nearest Neighbors suffers from the curse of dimensionality in our 20+ feature space and sensitivity to class imbalance, resulting in lower precision and recall (0.772 overall). These mechanisms align with established literature on ensemble robustness in cybersecurity tasks (Sahoo et al., 2017), demonstrating why they achieved scores of 0.997–0.999 compared to baselines.

Limitations: Reliance on static features may miss dynamic threats (e.g., JavaScript-based redirects). Ensemble models' computational complexity could hinder real-time deployment. Future work should incorporate content-based features and adversarial testing to improve generalizability.

Forensic Implications: The tool enables real-time URL filtering in browsers and email systems, and supports forensic investigations by profiling attack patterns and regional trends.

CONCLUSION

The results of this study confirm that integrating machine learning algorithms into digital forensic tools significantly enhances the accuracy and efficiency of malicious URL detection. This study developed a machine learning-based digital forensic tool for malicious URL detection, achieving near-perfect classification performance (accuracy 0.99–1.0) using ensemble models. The integration of lexical, host-based, and geographical features enhances its forensic utility, offering a proactive alternative to traditional blacklisting. Recommendations include:

1. Deploy ensemble models for robust URL detection.
2. Update datasets with real-time URL feeds.
3. Integrate hybrid features (e.g., content-based analysis).
4. Promote user education to reduce phishing risks.

Acknowledgement

We thank the Center for Cyberspace Studies, Nasarawa State University, for supporting this research and the providers of the urldata.csv dataset.

REFERENCES

Afzal, S., Asim, M., Javed, A. R., Beg, M. O., & Baker, T. (2021). Urldeepdetect: A deep learning approach for detecting malicious urls using semantic vector models. Journal of Network and Systems Management, 29(3), 21.

Aljabri, M., et al. (2022). Malicious URL detection using machine learning techniques. *International Journal of Advanced Computer Science and Applications*, 13(11), 1–10.

Aljabri, M. and S. Mirza (2022). ''Phishing attacks detection using machine learning and deep learning models,'' in Proc. 7th Int. Conf. Data Sci. Mach. Learn. Appl. (CDMA), Mar. 2022, pp. 175–180, doi: 10.1109/cdma54072.2022.00034.

Alhejaili, R., Alhazmi, E. S., Alsaeedi, A., & Yafooz, W. M. (2021). Sentiment Analysis of The COVID-19 Vaccine For Arabic Tweets Using Machine Learning. In 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 1-5). IEEE.

Almashor, Mahathir & Ahmed, Ejaz & Pick, Benjamin & Abuadbba, Sharif & Gaire, Raj & Camtepe, Seyit & Nepal, Surya. (2021). Characterizing Malicious URL Campaigns. 10.48550/arXiv.2108.12726.

Althobaiti, Kholoud & Meng, Nicole & Vaniea, Kami. (2021). I Don't Need an Expert! Making URL Phishing Features Human Comprehensible. 1-17. 10.1145/3411764.3445574.

Ariffin, K. A. Z. and Ahmad, F. H. (2021). "Indicators for maturity and readiness for digital forensic investigation in the era of industrial revolution 4.0," Computers and Security, vol. 105, 2021.

Bello, M. and Griffiths, M. (2021). Routine activity theory and cybercrime investigation in Nigeria: How capable are law enforcement agencies? In Rethinking Cybercrime (pp. 213-235), 2021. Palgrave Macmillan, Cham.

Chen, Q., et al. (2019). Comprehensive evaluation metrics for malicious URL detection. *Journal of Information Assurance and Security*, 14(3), 234–249.

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). Sage Publications.

Du, X., Hargreaves, C., Sheppard, J., Anda, F., Sayakkara, A., Le-Khac, N.A., Scanlon, M., Sok (2020). Exploring the state of the art and the future potential of artificial intelligence in digital forensic investigation. In: Proceedings of the 15th International Conference on Availability, Reliability and Security, pp. 1–10

Dweikat, M., Eleyan, D., & Eleyan, A. (2021). Digital Forensic Tools Used in Analyzing Cybercrime. Journal of University of Shanghai for

Forensic Capability Network. (2020). Digital forensic science strategy. Available at: https://www.fcn.police.uk/sites/default/files/2020-07/Digital%20Forensic%20Science%20Strategy%20EMAIL%20VERSION%20ONLY.pdf (accessed 26 November 2021).

Johnson, C. Khadka, B. Basnet, R. B., and Doleck, T. (2020). "Towards detecting and classifying malicious urls using deep learning," J Wirel Mob Netw Ubiquitous Comput Dependable Appl, vol. 11, no. 4, pp. 31–48, Dec. 2020, doi: 10.22667/JOWUA.2020.12.31.031.

Khanafseh, M., Qatawneh, M., and Almobaideen, W. (2019). "A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics," International Journal of Advanced Computer Science and Applications, vol. 10, no. 8, pp. 610–629, 2019.

Ma, J., et al. (2009). Identifying suspicious URLs: An application of large-scale online learning. *Proceedings of the International Conference on Machine Learning (ICML)*, 1245–1254.

Palmer, G. (2001). A road map for digital forensics research. *Digital Forensics Research Workshop*, Utica, NY.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3), 45–77.

Reedy, P. (2020). Interpol review of digital evidence 2016–2019, Foren. Sci. Int. Synergy 2 (2020) 489–520, https://doi.org/10.1016/j.fsisyn.2020.01.015.

Sahoo, D., et al. (2017). Malicious URL detection using machine learning: A survey. *arXiv preprint arXiv:1701.07179*.

Saleem Raja A, Madhubala R, Rajesh N, Shaheetha L, and Arul N, "Survey on Malicious URL Detection Techniques," pp.778–81, 2022. [Online]. Available: https://doi.org/10.1109/ICOEI53556.2022.9777221.

Say, G. and Vasudeva, G. (2020). "Learning from digital failures? The effectiveness of firms' divestiture and management turnover responses to data breaches," Strategy Science, vol. 5, no. 2, pp. 117–142, 2020.