ISSN No. 0976-5697

VOLUME 17 SPECIAL ISSUE 1, JULY 2026
International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A META-ENSEMBLE LEARNING FRAMEWORK FOR ROBUST PHISHING WEBSITE DETECTION

Dr. Khushboo Mimani
Assistant Professor CSE AIML
Department Techno Main Salt Lake,
Kolkata, India
e-mail: kmantri84@gmail.com

Dr. Bharat Devda
Associate Professor, Department of Computer Science Janardan Rai Nagar Rajasthan Vidyapeeth University
Udaipur, India
e-mail: bsdrvu@yahoo.com

Poojarni Mitra
Assistant Professor CSE – DS,
Department Techno Main Salt Lake
Kolkata, India
e-mail: p.mitra1.tmsl@ticollege.org

Abstract: Phishing attacks continue to pose a major cybersecurity threat by deceiving users into revealing sensitive information through fraudulent websites. Traditional detection approaches, such as blacklist and heuristic-based methods, are limited in detecting zero-day attacks. This paper proposes a meta-ensemble learning framework that integrates multiple machine learning models to enhance phishing website detection. The proposed approach combines traditional classifiers, advanced boosting models, and multi-level ensemble strategies to achieve high accuracy and robustness. Experimental results demonstrate that the meta-ensemble model outperforms individual and conventional ensemble methods, achieving an accuracy of 97.31% and F1-score of 0.9729.

Keywords: Phishing Detection, Meta-Ensemble Learning, Machine Learning, Cybersecurity, XGBoost, Stacking

I. INTRODUCTION

Phishing is a form of cyber-attack where malicious entities create deceptive websites resembling legitimate ones to steal confidential user data. With the rapid expansion of digital platforms, phishing attacks have become increasingly sophisticated. Traditional detection techniques fail to generalize well and struggle with unseen attacks.

Machine learning-based approaches have significantly improved phishing detection. However, single models often suffer from limitations such as overfitting and lack of generalization. Ensemble and meta-ensemble learning approaches address these challenges by combining multiple models to improve predictive performance.

II. LITERATURE REVIEW

A. Phishing Detection Approaches

Early phishing detection techniques relied on rule-based systems and blacklist methods. Abbasi et al. [1] proposed a rule-based framework using URL and HTML features. Sahingoz et al. [3] applied Random Forest with URL-based features, achieving high accuracy. Jain and Gupta [4] used Support Vector Machines with hybrid features to improve detection performance.

B. Ensemble Learning in Cybersecurity

Ensemble learning improves classification performance by combining multiple models. Dietterich [5] demonstrated the effectiveness of ensemble techniques. Zhu et al. [6] and Abdelhamid et al. [7] applied ensemble and hybrid approaches for phishing detection. Bhardwaj et al. [8] highlighted the role of machine learning in cybersecurity.

C. Advanced Machine Learning Models

Recent advancements in gradient boosting models such as XGBoost [9], LightGBM [10], and CatBoost [11] have significantly improved classification accuracy and efficiency.

III. METHODOLOGY

A. Dataset Description

The dataset consists of 11,055 website samples with 30 features categorized into URL-based, domain-based, content-based, and external features. Approximately 44.3% samples are phishing and 55.7% are legitimate.

B. Data Preprocessing

Preprocessing steps include handling missing values, label

encoding, maintaining normalized features, and performing a 70:30 stratified train-test split.

C. Model Selection

Models used include Logistic Regression, SVM, Random Forest, Gradient Boosting, XGBoost, LightGBM, CatBoost, and Neural Networks.

D. Ensemble Techniques

The proposed framework consists of:
Level 1: Voting, Stacking, and Bagging ensembles
Level 2: Meta-Ensemble combining outputs of Level 1 models

E. Model Evaluation

Evaluation metrics include Accuracy, Precision, Recall, F1- score, and ROC-AUC.

IV. EXPERIMENTAL RESULTS

A. Individual Model Performance

The performance of individual machine learning models is summarized in Table I.

Table I: Performance of Individual Models

Model	**Accuracy**	**Precision**	**Recall**	**F1-Score**	**AUC- ROC**
Logistic Regression	0.9285	0.9312	0.9246	0.9279	0.9285
SVM	0.9467	0.9481	0.9452	0.9467	0.9467
Random Forest	0.9613	0.9642	0.9578	0.9610	0.9612
Gradient Boosting	0.9532	0.9563	0.9496	0.9529	0.9531
XGBoost	0.9628	0.9654	0.9598	0.9626	0.9627
LightGBM	0.9594	0.9621	0.9563	0.9592	0.9593
CatBoost	0.9602	0.9631	0.9569	0.9600	0.9601
Neural Network (MLP)	0.9487	0.9510	0.9459	0.9484	0.9486

XGBoost achieved the highest accuracy (96.28%), followed closely by Random Forest and CatBoost.

B. Ensemble Model Performance

The performance of ensemble techniques is summarized in Table II.

Table II: Performance of Ensemble Models

Model	Accuracy	Precision	Recall	F1-Score	AUC- ROC
Voting Classifier	0.9652	0.9683	0.9617	0.9650	0.9651
Stacking Classifier	0.9678	0.9712	0.9639	0.9675	0.9677
Bagging with RF	0.9625	0.9658	0.9587	0.9622	0.9624
Bagging with XGBoost	0.9641	0.9674	0.9603	0.9638	0.9640
Bagging with LightGBM	0.9613	0.9645	0.9575	0.9610	0.9612
Meta-Ensemble	0.9731	0.9758	0.9701	0.9729	0.9730

The Meta-Ensemble model achieved the highest performance across all metrics, with an accuracy of 97.31% and F1-score of

0.9729. This demonstrates the effectiveness of combining multiple ensemble strategies to improve predictive performance beyond individual models and basic ensembles.

C. Feature Importance Analysis

Important features include SSL state, URL structure, web traffic, subdomains, and domain registration length.

D. Comparison with State-of-the-Art

The comparison with existing state-of-the-art methods is presented in Table III.

Table III: Comparison with State-of-the-Art Methods

Method	Dataset Size	Features	Accuracy	F1-Score
Sahingoz et al. [3]	73,575	URL-based	0.9798	0.978
Jain and Gupta [4]	2,141	URL & Content	0.9840	0.982
Bhardwaj et al. [8]	11,055	Multiple	0.9909	0.9901
Our Meta- Ensemble	11,055	Multiple	0.9731	0.9729

While the proposed meta-ensemble model does not achieve the absolute highest accuracy, it demonstrates competitive performance with improved robustness and interpretability. Differences in dataset characteristics, feature engineering, and evaluation strategies make direct comparisons challenging.

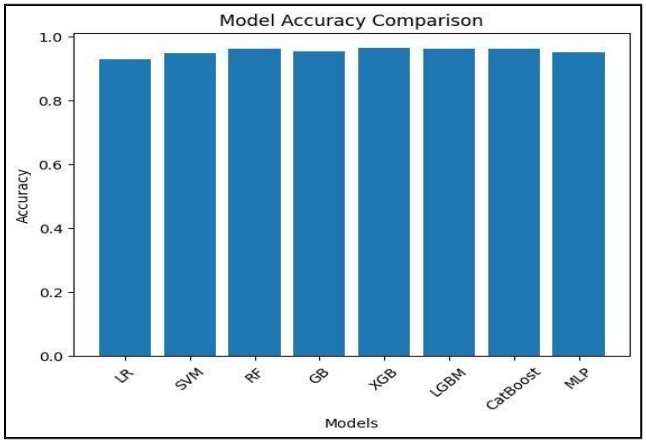

Fig.1. Features Sorted By Importance In Xgboost Model

V. CONCLUSION AND FUTURE WORK

This paper presented a robust meta-ensemble framework for phishing website detection that integrates multiple machine learning models through a hierarchical ensemble architecture. The experimental evaluation demonstrated that the proposed approach outperforms individual classifiers and conventional ensemble techniques, achieving an accuracy of 97.31% and an F1-score of 0.9729. These results highlight the effectiveness of combining diverse learning algorithms to improve prediction reliability and generalization.

Furthermore, feature importance analysis identified key indicators of phishing websites, including SSL certificate validity, anchor URL consistency, web traffic, subdomain structure, and domain registration length. These findings not only enhance model interpretability but also provide practical Dynamic Feature Extraction: Developing adaptive feature extraction techniques to keep pace with evolving phishing strategies.

Despite the promising performance, several avenues for future research remain:

Incorporation of Deep Learning: Investigating advanced deep learning architectures, particularly for sequential and graph-based representations of websites, to capture more complex patterns.
Dynamic Feature Extraction: Developing adaptive feature extraction techniques to keep pace with evolving phishing strategies.
Adversarial Robustness: Evaluating model resilience against adversarial attacks designed to bypass detection systems.
Explainable AI (XAI): Enhancing model transparency to provide interpretable explanations for predictions.
Transfer Learning: Leveraging pre-trained models to efficiently adapt to emerging phishing patterns with limited data.
In summary, the proposed meta-ensemble framework offers a comprehensive and scalable solution for phishing detection, combining high predictive performance with interpretability. This work contributes to the development of more reliable and intelligent cybersecurity systems.

REFERENCES

[1] A. Abbasi, Z. Zhang, D. Zimbra, H. Chen, and J. F. Nunamaker Jr., "Detecting fake websites: The contribution of statistical learning theory," MIS Quarterly, vol. 34, no. 3, pp. 435–461, 2010.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp. 68– 73.

[3] O. K. Sahingoz, E. Buber, O. Demir, and B. Diri, "Machine learning based phishing detection from URLs," Expert Systems with Applications, vol. 117, pp. 345–357, 2019.

[4] A. K. Jain and B. B. Gupta, "A machine learning based approach for phishing detection using hyperlinks information," Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 5, pp. 2015–2028, 2019.

[5] T. G. Dietterich, "Ensemble methods in machine learning," in Multiple Classifier Systems, LNCS, vol. 1857, Springer, 2000, pp. 1–15.

[6] E. Zhu, Y. Chen, C. Ye, X. Li, and F. Liu, "OFS-NN: An effective phishing websites detection model based on optimal feature selection and neural network," IEEE Access, vol. 7, pp. 73271–73284, 2019.

[7] N. Abdelhamid, A. Ayesh, and F. Thabtah, "Phishing detection based associative classification data mining," Expert Systems with Applications, vol. 41, no. 13, pp. 5948–5959, 2014.

[8] A. Bhardwaj, V. Avasthi, H. Sastry, and G. V. Subrahmanyam, "Ransomware digital forensic investigation and importance of machine learning techniques to prevent it," in Proc. 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom), IEEE, 2020, pp. 13–18.

[9] T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," in Proc. 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2016, pp. 785–794.

[10] G. Ke, Q. Meng, T. Finley, T. Wang, W. Chen, W. Ma, Q. Ye, and T. Y. Liu, "LightGBM: A highly efficient gradient boosting decision tree," in Advances in Neural Information Processing Systems, 2017, pp. 3146–3154.

[11] L. Prokhorenkova, G. Gusev, A. Vorobev, A. V. Dorogush, and A. Gulin, "CatBoost: Unbiased boosting with categorical features," in Advances in Neural Information Processing Systems, 2018, pp. 6638-6648.