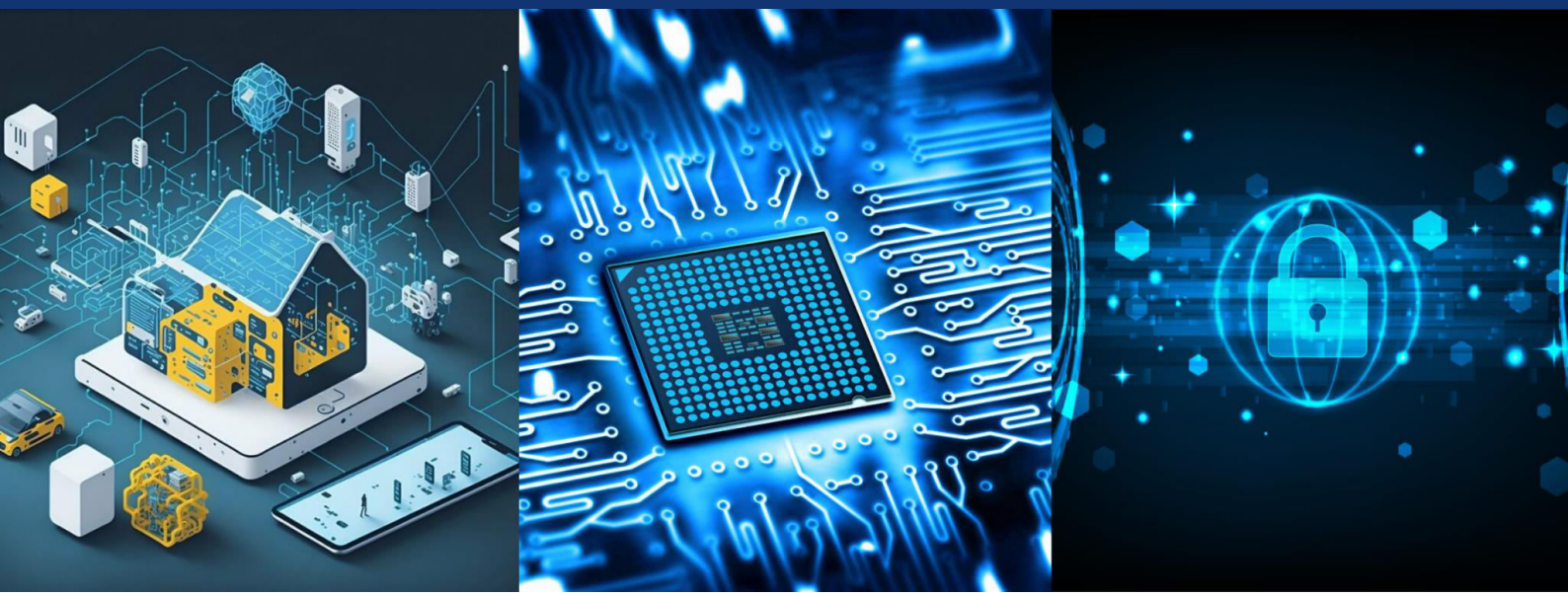
IJIRCCE

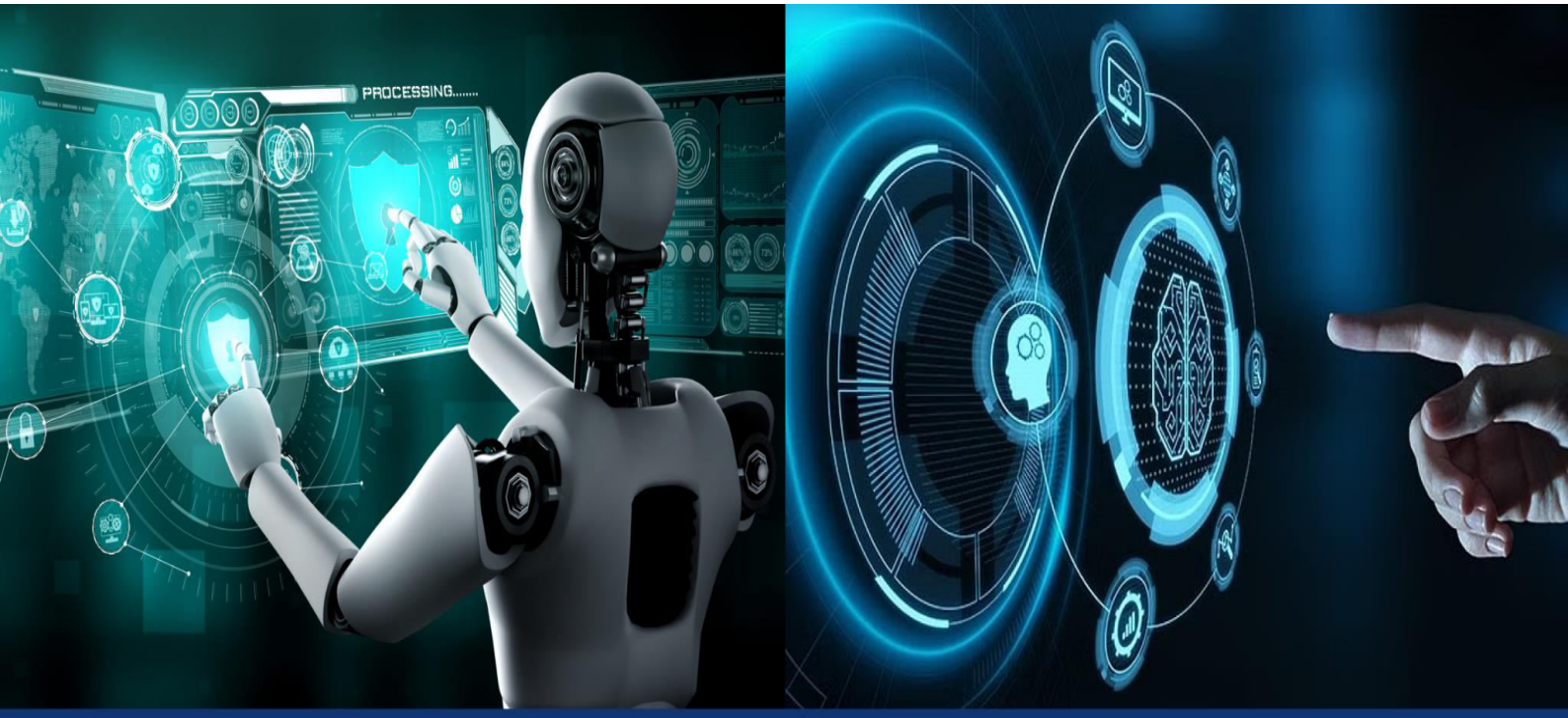
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

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



Impact Factor: 9.927

Volume 14, Issue 7, July 2026

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407015

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

Machine Learning-Augmented Cyber Forensics for Phishing Threat Detection and Attribution

Kutukanur Pramod Reddy, Dr. M. Nagaratna

Post-Graduate Student, Cyber Forensics and Information Security, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Hyderabad, India

Professor, Department of Computer Science Engineering, Jawaharlal Nehru Technological University, Hyderabad, India

ABSTRACT: Most existing phishing detection systems primarily rely on traditional rule-based filters, blacklists, and conventional machine learning models that analyze email content, URLs, and sender reputations to identify malicious activities. However, these approaches often fall short in effectively addressing the dynamic and increasingly sophisticated nature of phishing attacks, typically resulting in limited accuracy rates and a high number of false positives. They also tend to struggle with real-time detection and adaptability to novel phishing techniques.This project introduces a next-generation phishing detection framework using a hybrid deep learning architecture, RNT-J, which combines ResNeXt for advanced feature extraction and Gated Recurrent Units (GRU) for capturing temporal and sequential dependencies in data. Unlike conventional models, RNT-J employs ,enhances feature representation using ensemble learning techniques that integrate Autoencoders and ResNet (EARN), and uses Isolation Forests for effective anomaly detection. This comprehensive approach enables the framework to accurately and efficiently identify phishing attempts in real time, adapt to evolving attack patterns, and provide support for cybercrime forensics. The synergy of these components addresses critical shortcomings in existing systems by enhancing detection robustness, reducing false positives, and improving operational efficiency, positioning RNT-J as a powerful tool for countering phishing threats in today's complex cybersecurity landscape

KEYWORDS: Phishing Detection, Cyber Forensics, Machine Learning, Deep Learning, ResNeXt, GRU, Ensemble Learning, Autoencoder, ResNet, Isolation Forest, Anomaly Detection, Cybersecurity, Threat Attribution, Real-Time Threat Detection

I. INTRODUCTION

Over time, phishing attacks have grown increasingly complex. In order to make malicious URLs appear authentic, attackers now employ strategies like domain impersonation, URL obfuscation, redirection, shortened links, and dynamically generated websites. Conventional phishing detection techniques primarily rely on pre-established security rules, known signatures, and blacklists. These techniques are helpful for identifying threats that have already been identified, but they frequently fall short when dealing with recently created phishing URLs or attack patterns that are constantly changing.

Phishing attacks have gotten more sophisticated over the years. Today, attackers use tactics like domain impersonation, URL obfuscation, redirection, shortened links, and dynamically generated websites to make malicious URLs look legitimate. Traditional phishing detection methods depend heavily on black lists, known signatures and predefined security rules. These methods are useful for detecting already identified threats, but they often fail to detect newly created phishing URLs or frequently changing attack patterns.

Machine learning has enhanced the detection of phishing, by allowing systems to learn from the patterns of lexical, structural and statistical properties of URLs. However, traditional machine learning models usually rely on manually selected features and may not reflect the complex relationships or sequential patterns in URLs. Deep learning models have better feature learning ability, and can discover hidden patterns that are hard to be found by traditional approaches.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

This paper presents a machine learning- enhanced cyber forensic framework to overcome these limitations by integrating GRU, ResNet, ResNeXt, Autoencoder and Isolation Forest models. Every model adds its own contribution to the detection process. GRU is able to capture the sequential relationships of URL patterns and ResNet and ResNeXt are able to capture the complex relationships of the extracted phishing-related features. Anomaly detection capabilities are provided by Autoencoder and Isolation Forest to help identify unusual patterns and unseen phishing behaviour.

The individual models' predictions are combined through a weighted ensemble decision method. Instead of using only the output of one model, the proposed approach takes into account the predictions of all models that are participating in the system. The models with the best classification performance have a larger impact on the final decision, while anomaly detection models give additional information on suspicious behavior. This combination improves the reliability of the final threat assessment, and overcomes the limitations associated with the use of a single detection technique.

The main contributions of this paper are summarised as follows:

- A cyber forensic framework with machine learning integration, using deep learning, anomaly detection and forensic analysis for phishing threat detection.
- A weighted ensemble decision mechanism of the GRU, ResNet, ResNeXt, Autoencoder and Isolation Forest model outputs to enhance the reliability of phishing detection.
- A cyber forensic analysis mechanism that captures suspicious URL indicators, model predictions, anomaly information and threat-related evidence to support the investigation of phishing incidents and analysis-oriented attribution.

II. RELATED WORK

Phishing detection has been studied extensively using various machine learning and deep learning techniques. Previous works mainly extracted useful information from URLs and website contents and trained classification models with these features .

Verma and Das [1] explored the use of lexical and structural features of URLs for malicious website detection. Their work demonstrated that useful information can be extracted directly from URL strings, without having to look at the entire content of the webpage. This approach reduced the detection time but its performance was very dependent on the quality of the selected features.

Jain and Gupta [2] proposed a client-side machine learning based approach for phishing website detection. Their system analysed various URL and website features and applied machine learning classifiers to differentiate phishing from legitimate websites. The research has shown that machine learning techniques can decrease the reliance on traditional blacklist-based systems and enhance the detection of unknown phishing websites.

Rao and Pais [3] proposed a feature-based phishing detection framework using the lexical, domain-related and webpage characteristics. They stressed the importance of choosing relevant features for improving classification performance. However, such methods still depend on human-designed features and may face difficulties in adapting to new phishing techniques introduced by attackers.

Deep learning for phishing detection was explored by Aljofey et al. [4] using a character-level Convolutional Neural Network (CNN). Instead of depending on hand-crafted features, the model learned useful patterns directly from URL character sequences. The results showed that deep learning models can learn complex URL patterns and achieve better detection capabilities to unseen phishing URLs.

Sahoo et al. [5] proposed a hybrid deep learning method that combined different learning strategies to identify phishing. Their work proved that the detection performance can be improved by using a combination of different models as different models learn different characteristics of phishing URLs. However, most existing hybrid approaches focus mainly on improving classification accuracy and have limited support for anomaly detection and cyber forensic investigation.

Based on the existing research, machine learning and deep learning techniques have significantly improved phishing detection. However, challenges still remain in detecting previously unseen attacks, combining different analytical

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407015

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

models, and providing useful forensic information after a phishing URL is detected. To address these limitations, the proposed framework combines GRU, ResNet, ResNeXt, Autoencoder, and Isolation Forest models using a weighted ensemble mechanism. The framework also incorporates cyber forensic analysis to record suspicious indicators, anomaly information, model predictions, and threat-related evidence that can support further investigation.

III. PROPOSED METHODOLOGY

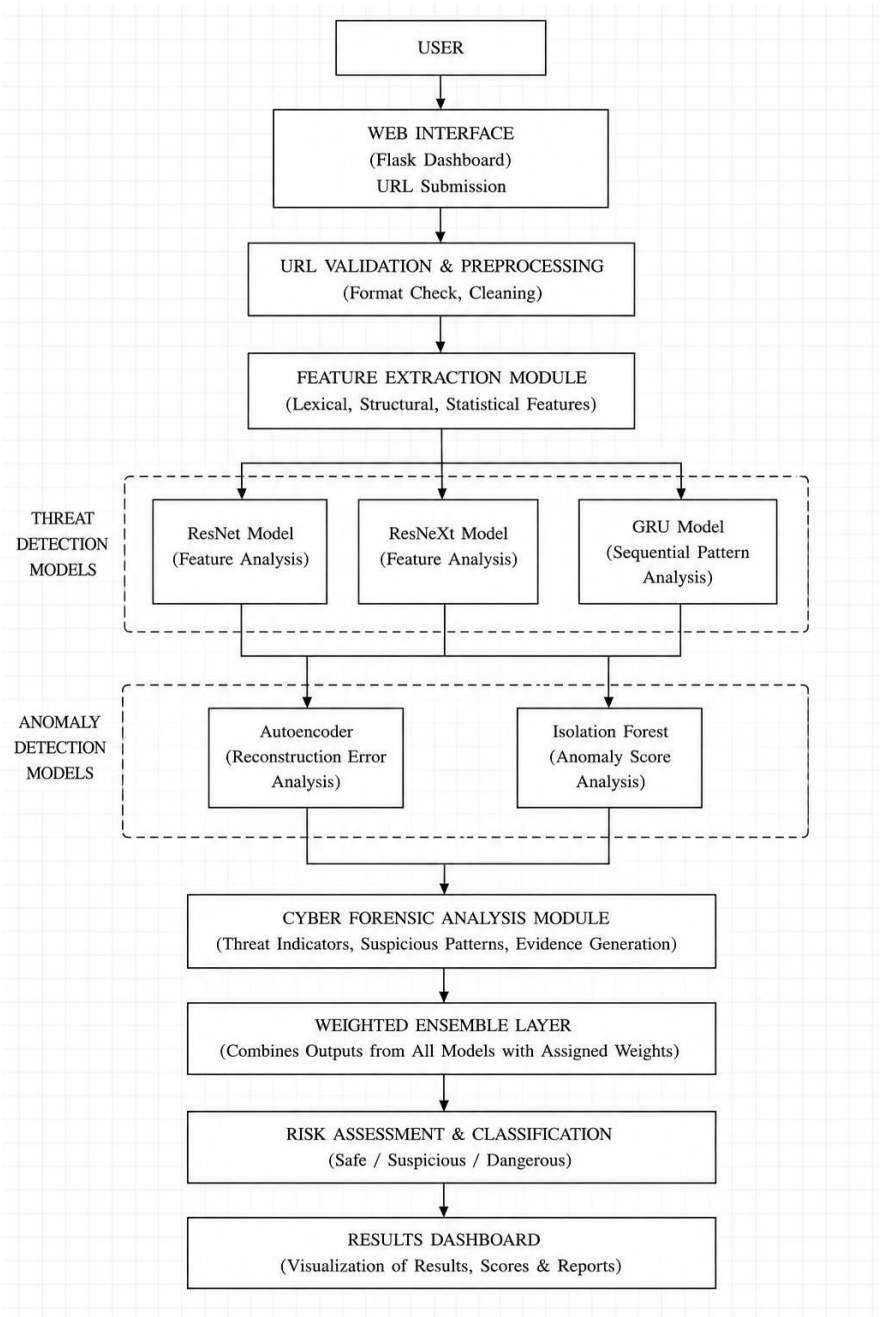


Figure 1: Architecture

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407015

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

A. System Architecture

The architecture of the proposed machine learning augmented cyber forensic framework is given in Figure 1. Firstly, the submitted URL is processed to extract lexical, structural and statistical features. This preprocessed data is then subjected to analysis using GRU, ResNet, ResNeXt, Autoencoder and Isolation Forest models.

The models each view the URL from a different perspective. GRU learns sequential URL patterns, ResNet and ResNeXt learn complex feature relationships and Autoencoder and Isolation Forest identify anomalous behaviour. The outputs of these models are combined with a weighted ensemble mechanism to produce the final risk score and classify the URL as Safe, Suspicious or Dangerous. The cyber forensic layer logs the results and the indicators of suspicion for future investigation.

B. Feature Extraction and Preprocessing

The submitted URL is transformed into numerical features that represent URL length, domain properties, subdomains, special characters, digits, HTTPS usage, obfuscation indicators and other phishing-related characteristics.

The extracted features are normalised before being fed to ResNet, ResNeXt, Autoencoder and Isolation Forest. For GRU-based analysis, URL characters are transformed to numerical sequences, which are padded or truncated to a fixed length.

C. GRU-Based Sequential Analysis

GRU is used to find sequential patterns in the URL strings. The tokenised URL is passed into an embedding layer and GRU network to learn relationships between characters and URL components.The learned representation is then input into a classification layer to output a phishing probability score.The use of update and reset gates enables GRU to retain important sequential information while maintaining lower computational complexity than conventional RNNs.

D. ResNet and ResNeXt Feature Analysis

Complex associations between the collected URL features are learned using ResNet and ResNeXt. ResNet reduces deterioration during training and enhances information flow via deeper networks by using residual connections.

ResNeXt enables the concurrent learning of several feature representations by extending residual learning through grouped transformations. For the ensemble framework, both models produce separate phishing probability scores.

E. Autoencoder and Isolation Forest Anomaly Detection

By reconstructing input samples, the Autoencoder learns typical feature representations. Reconstruction error is used to quantify the difference between the original and reconstructed features. A larger reconstruction error indicates unexpected behaviour and adds to the anomaly score.

Based on how simple it is to distinguish problematic URLs from typical samples, Isolation Forest finds them. In general, fewer divisions are needed to separate anomalous findings.

F. Weighted Ensemble Decision Framework

A weighted ensemble technique is used to blend the results produced by each model. Higher contribution weights are given to models that perform better in classification, and anomaly detection models offer more proof of anomalous URL behaviour.

The final risk score is computed as:

$$RiskScore=(w1\times ResNet)+(w2\times ResNeXt)+(w3\times GRU)+(w4\times Autoencoder)+(w5\times IsolationForest)$$

Where:

- w1,w2,w3,w4,w5are the assigned model weights.
- The sum of all weights equals 1.
- The generated RiskScore is used for final classification.

Based on predefined thresholds, the final risk score classifies the submitted URL as Safe, Suspicious, or Dangerous.

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407015

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

G. Cyber Forensic Analysis

Suspicious URL attributes, individual model predictions, anomaly indicators, final risk score, threat classification, and scan history are all recorded by the cyber forensic layer.

These results can help security analysts analyse suspicious behaviour and carry out extra forensic research. They also offer more context regarding phishing attacks that have been identified.

IV. PSEUDO CODE

Algorithm: Machine Learning-Augmented Phishing Detection and Cyber Forensic Analysis

Step 1: Initialize the trained GRU, ResNet, ResNeXt, Autoencoder, and Isolation Forest models.
Step 2: Accept the URL submitted by the user.
Step 3: Validate the URL format.
If the URL is invalid or empty,
Return an error message and stop the analysis.
Step 4: Extract lexical, structural, and statistical features from the submitted URL.
Step 5: Normalize the extracted feature values and prepare the URL character sequence for GRU analysis.
Step 6: Generate the phishing probability score using the GRU model.
Step 7: Generate independent phishing probability scores using the ResNet and ResNeXt models.
Step 8: Calculate the reconstruction error using the Autoencoder and convert it into a normalized anomaly score.
Step 9: Generate the anomaly score using the Isolation Forest model.
Step 10: Combine the prediction and anomaly scores using the weighted ensemble mechanism.
$RiskScore=(w1\times ResNet)+(w2\times ResNeXt)+(w3\times GRU)+(w4\times Autoencoder)+(w5\times IsolationForest)$
Step 11: Determine the final threat classification.
If (Risk Score ≥ Dangerous Threshold)
Classify the URL as **Dangerous**.
Else If (Risk Score ≥ Suspicious Threshold)
Classify the URL as **Suspicious**.
Else
Classify the URL as **Safe**.
Step 12: Generate cyber forensic findings using suspicious URL features, individual model scores, anomaly indicators, final risk score, and threat classification.
Step 13: Store the submitted URL, analysis results, forensic findings, and scan history.
Step 14: Display the final threat assessment and cyber forensic findings to the user.
Step 15: End.

V. SIMULATION RESULTS

The proposed machine learning-augmented cyber forensic framework was evaluated and compared with the individual GRU, ResNet, ResNeXt, Autoencoder, and Isolation Forest models. The experiments were carried out to examine the performance of the models in phishing URL detection and to evaluate the improvement achieved by combining multiple detection models through the proposed weighted ensemble framework. Accuracy, Precision, Recall, and F1-score were used as the main evaluation metrics.

A. Accuracy Analysis

Accuracy represents the overall ability of a model to correctly classify phishing and legitimate URLs. Figure 2 compares the accuracy achieved by GRU, ResNet, ResNeXt, Autoencoder, Isolation Forest, and the proposed weighted ensemble framework.

As shown in Figure 2, the proposed weighted ensemble framework achieves the highest accuracy of 99.88%, followed by GRU with 99.78%, ResNeXt with 99.50%, and ResNet with 99.49%. The Autoencoder achieves 96.02% accuracy, while Isolation Forest obtains 79.87% accuracy. The improved performance of the proposed framework is achieved by combining the outputs of multiple models, allowing the final decision to benefit from sequential learning, deep feature analysis, and anomaly detection.

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407015

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

B. Precision Analysis

Precision measures the proportion of URLs classified as phishing that are actually phishing URLs. Higher precision indicates that the detection system produces fewer false alarms by avoiding the incorrect classification of legitimate URLs as phishing.

As illustrated in Figure 3, the proposed weighted ensemble framework achieves the highest precision of 99.73%. GRU obtains 99.67% precision, while ResNet and ResNeXt achieve 99.31% and 99.22%, respectively. The Autoencoder records 94.42% precision, whereas Isolation Forest achieves 78.00%. These results show that the weighted ensemble mechanism improves the reliability of phishing predictions and reduces false positive classifications.

C. Recall Analysis

Recall represents the ability of the detection system to correctly identify phishing URLs from all the actual phishing samples. A higher recall value indicates that fewer phishing attacks remain undetected.

As shown in Figure 4, the proposed weighted ensemble framework achieves the highest recall of 99.96%. GRU achieves 99.95% recall, followed by ResNeXt with 99.91% and ResNet with 99.80%. The Autoencoder achieves 98.89% recall, while Isolation Forest obtains 90.25%. The high recall achieved by the proposed framework demonstrates its ability to detect phishing URLs effectively and reduce the number of missed phishing attacks.

D. F1-Score Analysis

F1-score represents the balance between Precision and Recall and provides a useful measure of the overall detection performance of the models. A higher F1-score indicates that the model maintains both accurate phishing detection and a low number of false predictions.

As illustrated in Figure 5, the proposed weighted ensemble framework achieves the highest F1-score of 99.85%, followed by GRU with 99.81%. ResNet and ResNeXt both achieve an F1-score of 99.56%, while the Autoencoder obtains 96.60% and Isolation Forest achieves 83.68%. The results demonstrate that the proposed ensemble framework provides a better balance between Precision and Recall than the individual models.

E. Overall Performance Comparison

The overall performance comparison evaluates the models using Accuracy, Precision, Recall, and F1-score together. Figure 6 compares the complete performance of the individual detection models and the proposed weighted ensemble framework.

As shown in Figure 6, the proposed weighted ensemble framework consistently achieves the best overall performance across all evaluation metrics. Among the individual models, GRU produces the strongest classification results, while ResNet and ResNeXt also provide high detection performance. Although Autoencoder and Isolation Forest show comparatively lower standalone classification results, they provide complementary anomaly detection information that supports the identification of unusual and previously unseen phishing patterns.

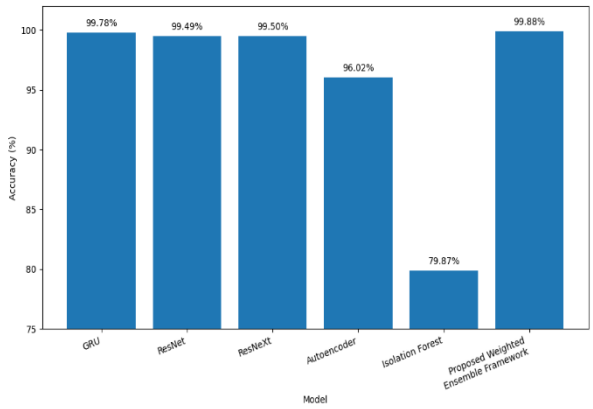


Fig.2. Accuracy Comparison

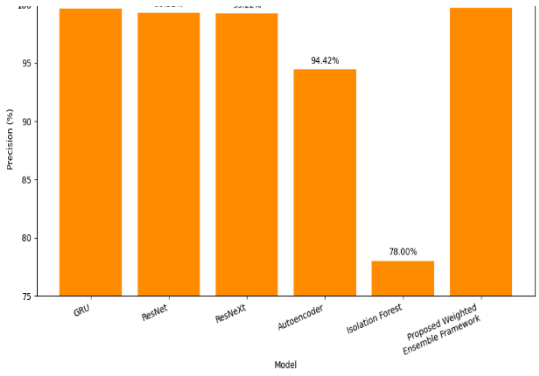


Fig. 3. Precision Comparison

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407015

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

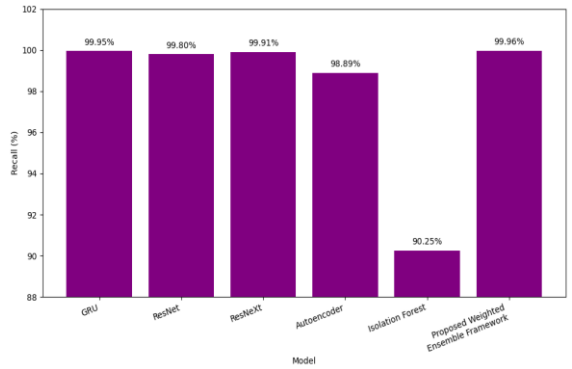


Fig. 4. Recall Comparison

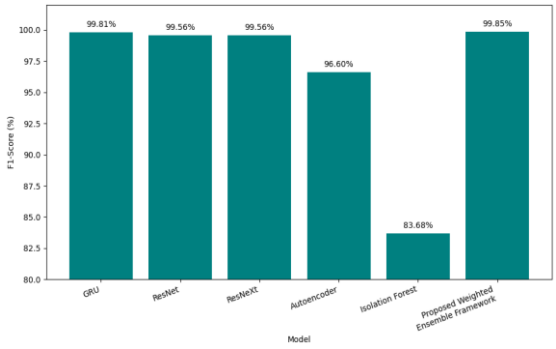


Fig 5. F1 Score Comparison

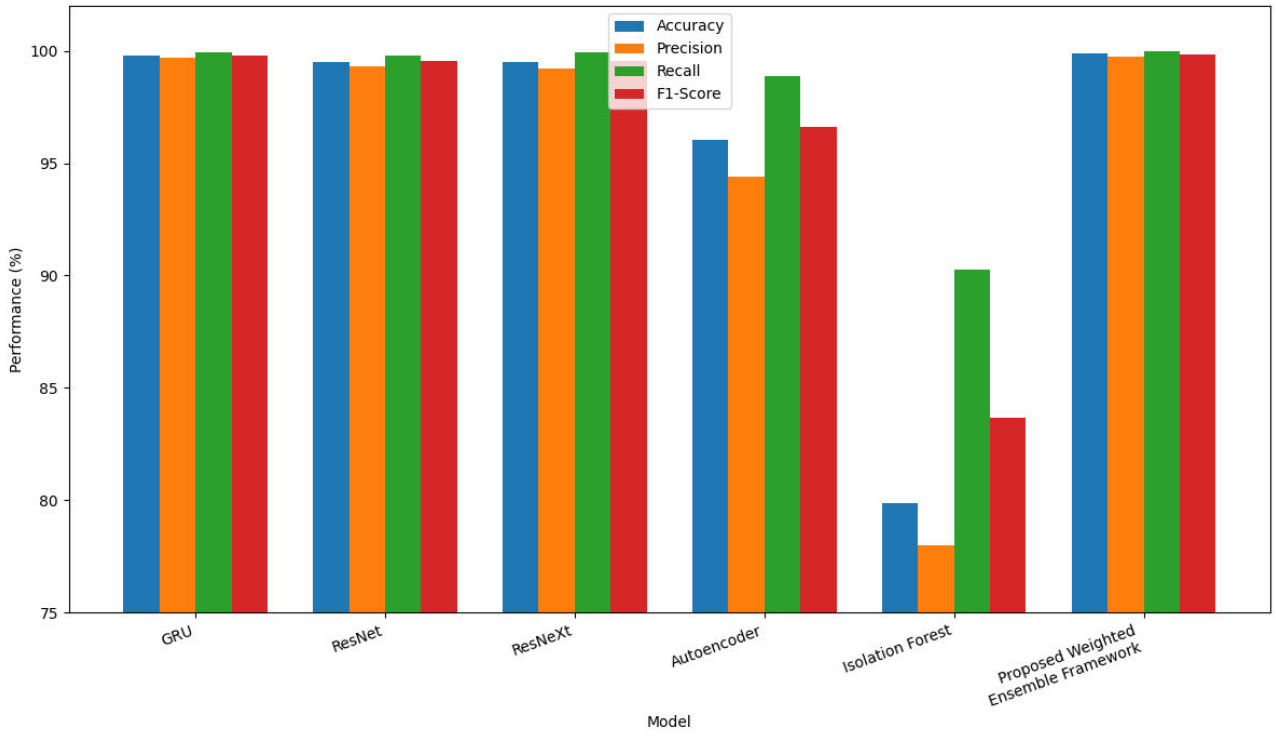


Fig. 6. Overall Performance Comparison

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407015

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

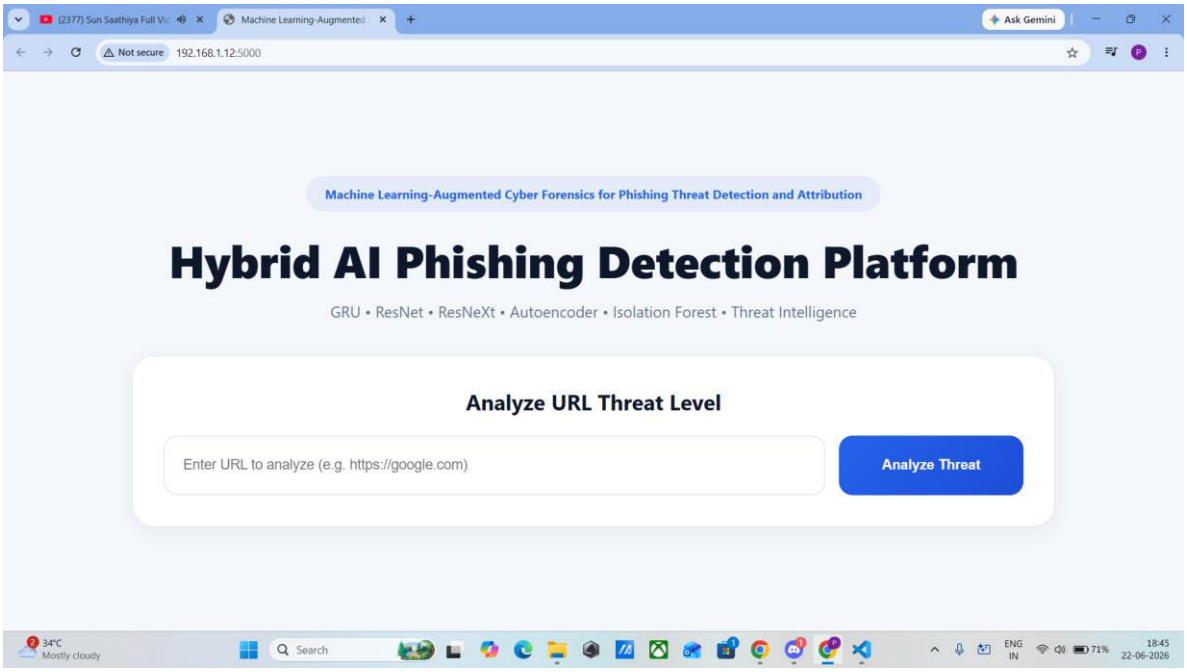


Fig. 7. Machine Learning-Augmented Cyber Forensics for Phishing Threat Detection and Attribution Model

VI. CONCLUSION AND FUTURE WORK

This paper presented a machine learning-augmented cyber forensic framework for phishing threat detection by integrating GRU, ResNet, ResNeXt, Autoencoder, and Isolation Forest models with a weighted ensemble decision mechanism. The proposed framework analyses sequential URL patterns, complex feature relationships, and anomalous behaviour, while the cyber forensic layer records suspicious URL characteristics, individual model predictions, anomaly indicators, risk scores, and threat-related findings to support further investigation. Experimental results demonstrated that the proposed weighted ensemble framework achieved 99.88% accuracy, 99.73% precision, 99.96% recall, and 99.85% F1-score, outperforming the individual detection models and providing a more reliable phishing threat assessment. By combining deep learning-based classification with anomaly detection and forensic analysis, the proposed framework reduces dependence on a single detection technique and improves the identification of both known and previously unseen phishing patterns. Future work will focus on extending the framework to detect phishing threats from emails, QR codes, shortened URLs, and social media platforms, integrating real-time threat intelligence and explainable AI techniques, and deploying the proposed system in large-scale real-world environments for continuous phishing detection and automated cyber forensic investigation.

REFERENCES

1. R. Verma and A. Das, “What’s in a URL: Fast feature extraction and malicious URL detection,” in *Proceedings of the 3rd ACM International Workshop on Security and Privacy Analytics (IWSPA)*, Scottsdale, AZ, USA, 2017, pp. 55–63.
2. A. K. Jain and B. B. Gupta, “Towards detection of phishing websites on client-side using machine learning based approach,” *Telecommunication Systems*, vol. 68, no. 4, pp. 687–700, 2018.
3. R. S. Rao and A. R. Pais, “Detection of phishing websites using an efficient feature-based machine learning framework,” *Neural Computing and Applications*, vol. 31, no. 8, pp. 3851–3873, 2019.
4. A. Aljofey, Q. Jiang, Q. Qu, M. Huang, and J.-P. Niyigena, “An effective phishing detection model based on character level convolutional neural network from URL,” *Electronics*, vol. 9, no. 9, Art. no. 1514, 2020.
5. D. Sahoo, C. Liu, and S. C. H. Hoi, “Malicious URL detection using machine learning: A survey,” arXiv preprint arXiv:1701.07179, 2017.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

6. A. Blum, B. Wardman, T. Solorio, and G. Warner, "Lexical Feature Based Phishing URL Detection Using Online Learning," in *Proceedings of the 3rd ACM Workshop on Artificial Intelligence and Security (AISec)*, Chicago, IL, USA, 2010, pp. 54–60.
7. W. Zhang, H. Lu, B. Xu, and H. Yang, "Web Phishing Detection Based on Page Spatial Layout Similarity," *Informatica*, vol. 37, no. 3, pp. 231–244, 2013.
8. W. Chen, W. Zhang, and Y. Su, "Phishing Detection Research Based on LSTM Recurrent Neural Network," in *Proceedings of the International Conference on Computer and Communications (ICCC)*, Chengdu, China, 2018, pp. 2199–2203.
9. M. A. Adebowale, K. T. Lwin, E. Sánchez, and M. A. Hossain, "Intelligent Web-Phishing Detection and Protection Scheme Using Integrated Features of Images, Frames and Text," *Expert Systems with Applications*, vol. 115, pp. 300–313, 2019.
10. A. A. Orunsolu, A. S. Sodiya, and A. T. Akinwale, "A Predictive Model for Phishing Detection," *Journal of King Saud University – Computer and Information Sciences*, vol. 34, no. 2, pp. 232–247, 2022.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details