ASEC 2025 Conference
The 6th International Electronic Conference on Applied Sciences
09–11 December 2025 | Online
MDPI

Spatial and Temporal Feature Fusion for Enhanced Phishing Attack Detection in Web Environments

Abdullahi Raji Egigogo, Idris Ismaila, Morufu Olalere, Barira Hamisu, Abisoye Opeyemi Aderiike, Ojeniyi Adebayo Joseph

Department of Cyber Security Science, School of Information Communication Technology, Federal University of Technology, Gidan Kwanu, P.M.B 65, Minna, Niger State, Nigeria, Department of Software Engineering and Cyber Security, College of Computing and Information Systems, Al-Qalam University, Tafawa Balewa Way, Dutsin-ma, Road PMB 213, Kastina, Nigeria

INTRODUCTION & AIM

Rapid growth in AI, cloud computing, and IoT has expanded global digital ecosystems (Terpylo, 2024). Increased connectivity has led to a parallel surge in cyber threats, especially phishing attacks aimed at stealing sensitive information (Snehi & Bhandari, 2021).

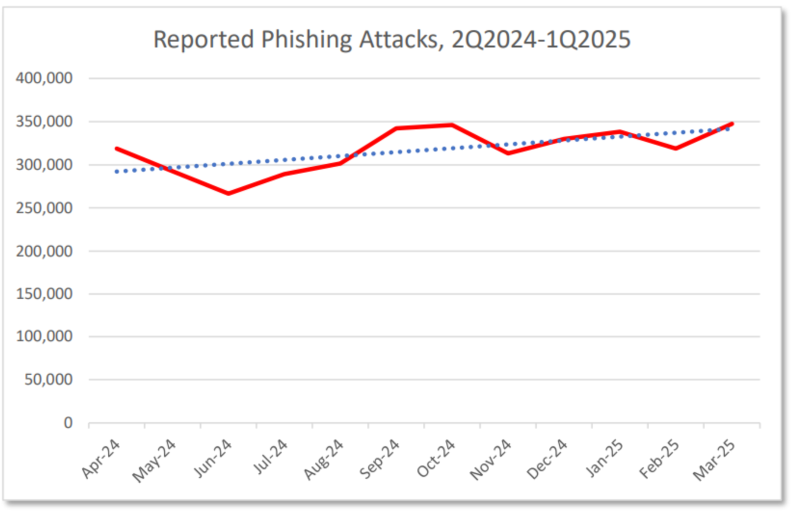

Figure 1: Phishing Activity Trends Report from 2nd Quarter 2024 to 1st Quarter 2025 (APWG, 2025)

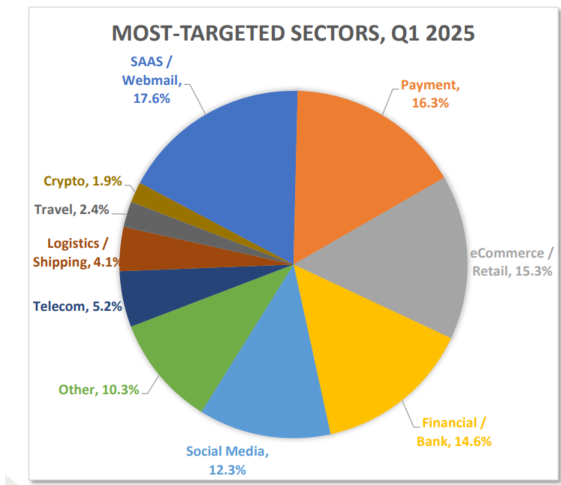

Figure 2: Most Targeted Sectors in 1st Quarter 2025 (APWG, 2025)

Existing detection systems that rely on manual feature design and rigid rules have become increasingly ineffective (Gupta et al., 2021; Do et al., 2021).

The study is structured around three primary objectives:

i. To design a dual-pathway feature extraction mechanism combining CNN and BiGRU for analyzing phishing website data.
ii. To develop a hybrid algorithm that encapsulates two algorithms for phishing website classification
iii. To evaluate the algorithm's performance using standard metrics, including accuracy, precision, recall, specificity, and F1 score.

METHOD

This study proposed a hybridized deep learning model using a Convolutional Neural Network (CNN) and Bidirectional Gated Recurrent Unit (BiGRU) for the detection of phishing websites.

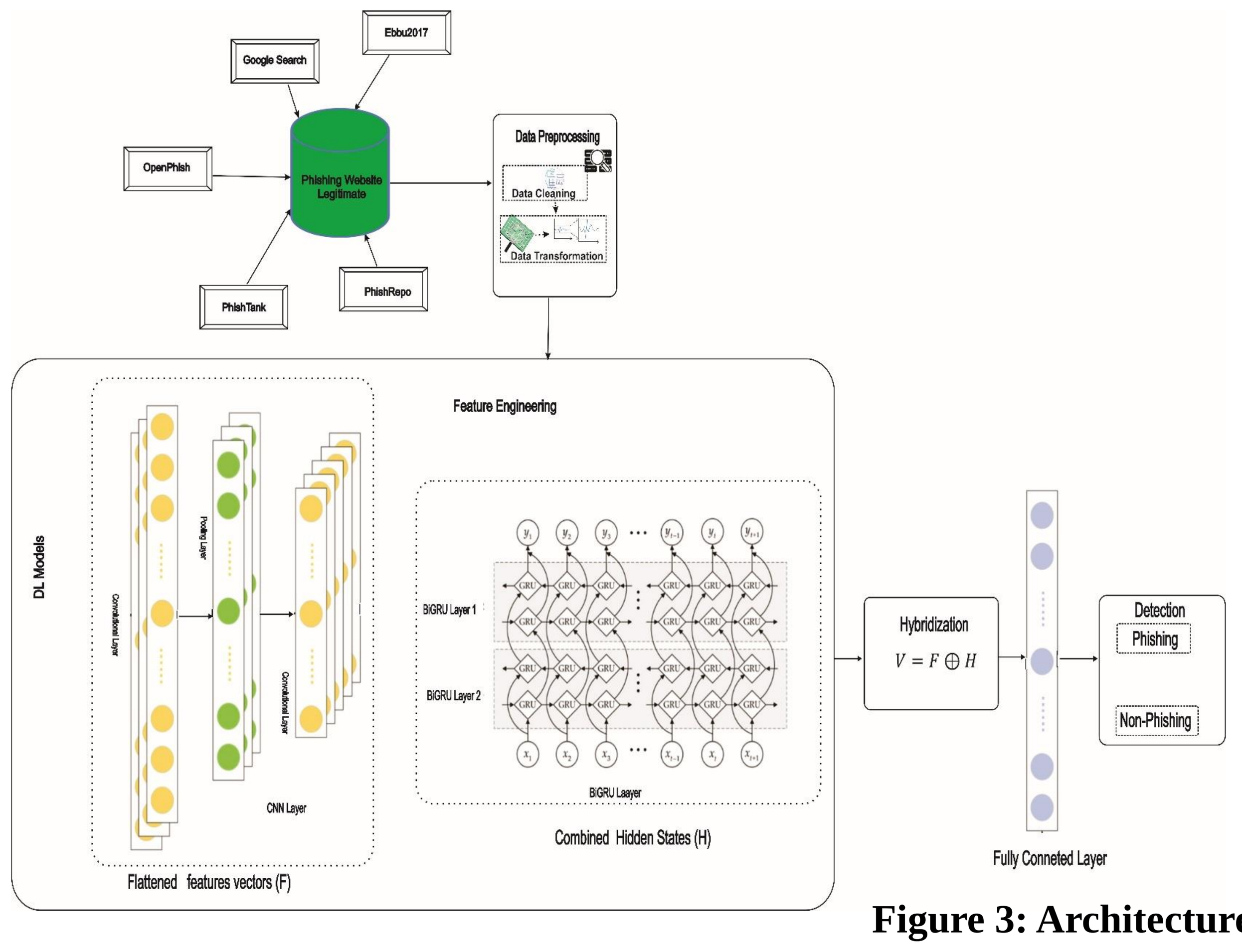

Figure 3: Architecture of the proposed model

Feature Engineering and Feature Extraction

- In this phase, feature engineering was performed using two deep learning algorithms.
- CNN for spatial and BiGRU for temporal feature extraction, which is presented in
- Tables 2 and 3 as follows:

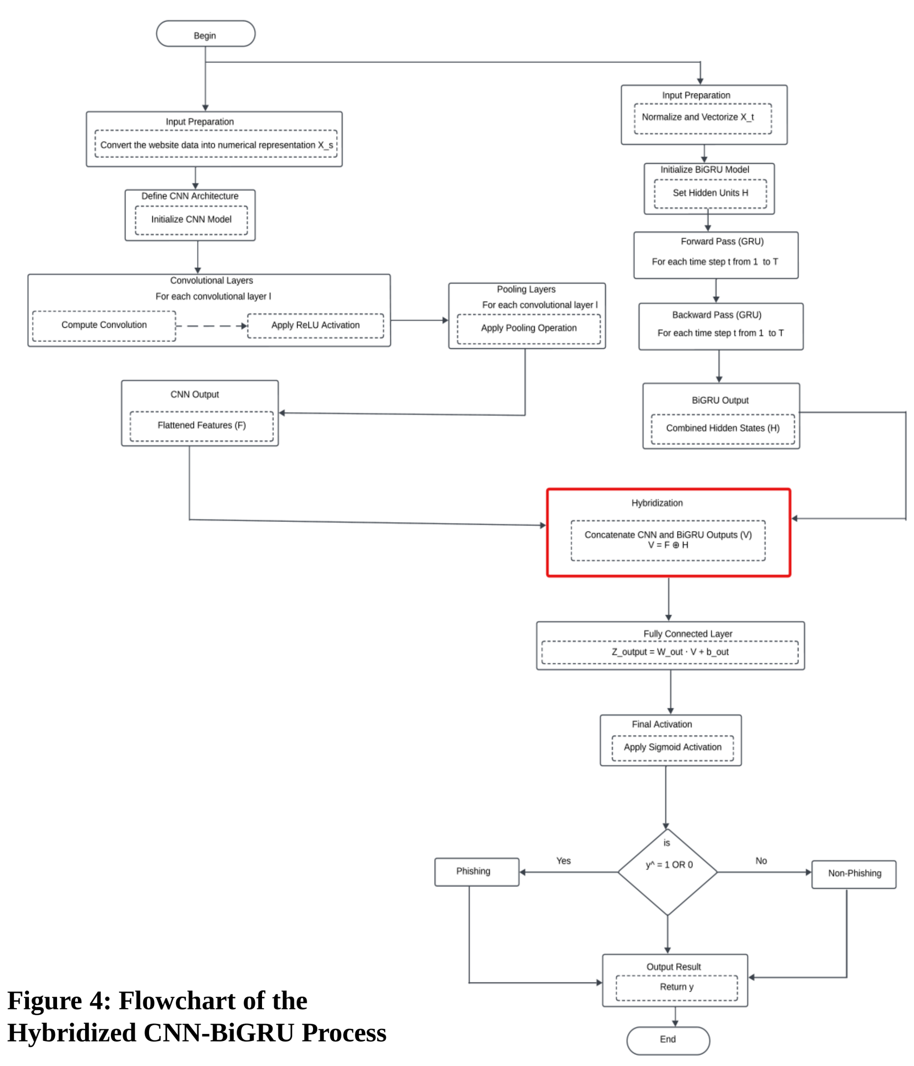

Figure 4: Flowchart of the Hybridized CNN-BiGRU Process

Table 5: Hybridized CNN-BiGRU Algorithm

Hybridized CNN-BiGRU Algorithm

Input: Input: Website {x1, x2, x3, …, xL}, L = length of website
Output: Phishing or Non-Phishing (Y), where Y = 0 for Non-Phishing and Y = 1 for Phishing
Steps

1	Begin
2	Input Preparation: Convert the website data X into numerical representations for spatial features X, and temporal features X_t
3	CNN Component:
3.1	For each Convolutional Layer L : Compute the output: $Z_i - W_i * A_{l-1} + b_l$
3.2	Apply the activation function (ReLU): $A_l = \max(0, Z_l)$
4	For each Pooling Lays L : Reduce dimensionality: $P_l = \text{pool}(A_t)$
5	Flatten the pooled output: $F = \text{Flatten}(P)$
6	BiGRU Component:
6.1	Initialize hidden states: $h_{t-1}^{(f)}$ and $h_{t+1}^{(i)}$
6.2	For each time step 1 Compute forward GRU hidden state: $h_i^{(f)} - \text{CRU}\left(A_t, h_{i-1}^{(f)}\right)$
6.3	Compute backward GRU hidden state: $\hat{h}_t^{(\theta_i'} - \text{GRU}\left(A_t, h_{t+1}^{(0)}\right)$
6.4	Combine forward and backward hidden states $h_t - h_z^{(n)} \oplus h_i^{(s)}$
7	Hybridization:
7.1	Concatenate outputs from CNN and BiGRU: $V = F \oplus H$
7.2	Fully connected layer computation: $Z_{\text{outpet}} = W_{\text{out}} \cdot V + b_{\text{eat}}$
8	Final Detection Apply the sigmoid activation function $\hat{y} - \sigma(Z_{\text{output}}) - \frac{1}{1+\epsilon}$
9	Output Result: Return y (Phishing or Non-Phishing)
10	End

RESULTS & DISCUSSION

Feature selection with CNN (spatial) and BiGRU (temporal)

- **CNN (Spatial Features)**
  - PCA shows clear separation between legitimate and phishing sites, indicating strong spatial feature extraction
- **BiGRU (Temporal)**
  - PCA also reveals distinct class clusters, showing effective temporal feature learning.

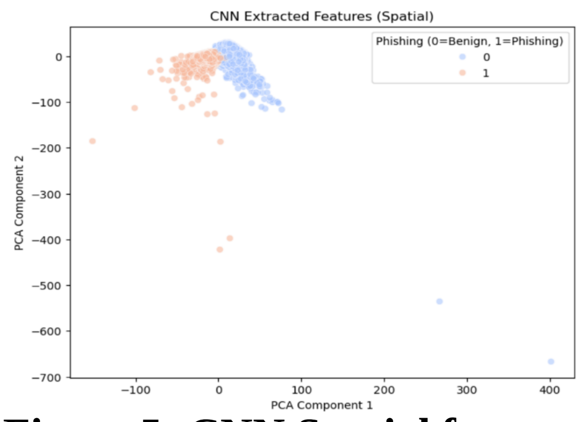

Figure 5: CNN Spatial features

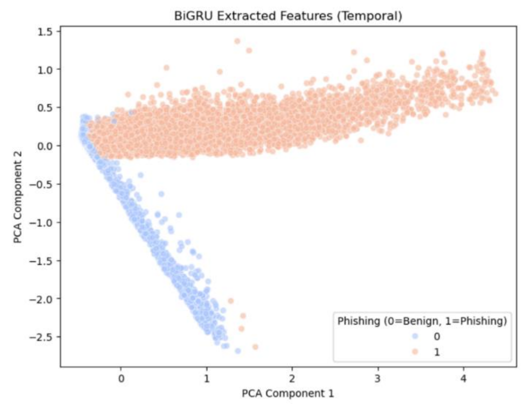

Figure 6: BiGRU Temporal Features

Train-Test Split

- The performance of the proposed algorithms was evaluated using the train-test split technique.
- The dataset was divided into 80% for training and 20% for testing

Table 7: Performance Result of Hybridized CNN-BiGRU Algorithm

Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	Specificity
99.97	99.97	99.98	99.98	99.96

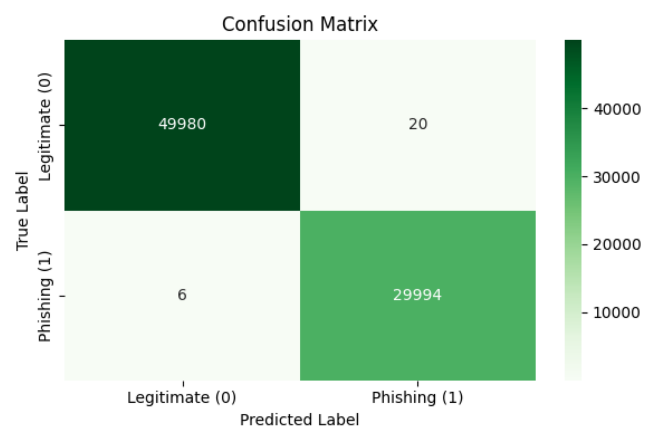

Figure 7: Confusion Matrix

Cross-validation

- A stratified fold cross-validation technique was employed with 5k folds on the same baseline dataset.
- The study was evaluated on a different publicly available dataset that was collected from IEEE DataPort.

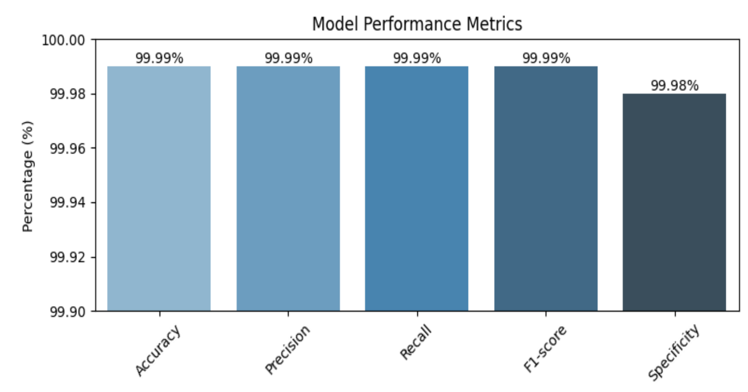

Figure 8: Cross-validation Performance of the algorithm

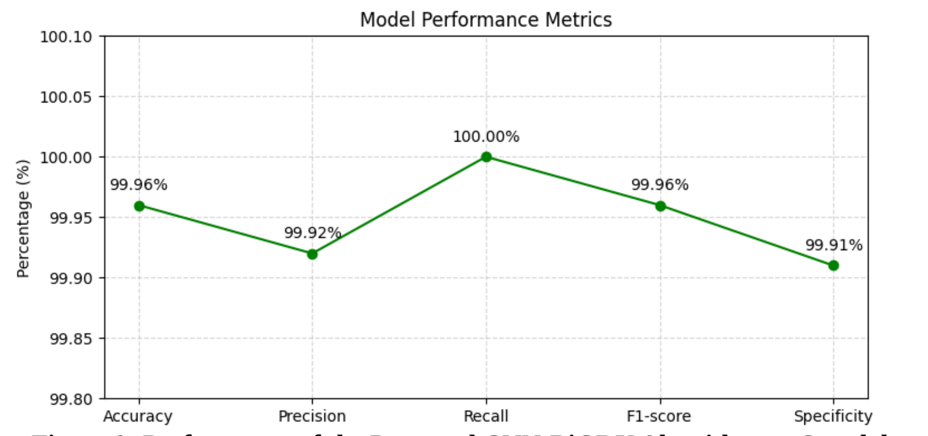

Figure 9: Performance of the Proposed CNN-BiGRU Algorithm on Standalone Data

Comparison of this Study with Existing Hybrid Deep Learning Algorithms

Table 8: Comparison of this Study with other Existing Hybrid Deep Learning Algorithms

Authors& Year	Algorithm(s)	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
Adebowale *et al*. (2020)	CNN-LSTM	93.20	93.30	93.27	93.21
Zhang *et al*. (2021)	CNN-BiLSTM	98.84	98.87	99.71	98.04
Alshingiti *et al*. (2023)	LSTM-CNN	97.60	96.90	98.20	97.60
Ujah-Ogbuagu *et al*. (2024)	CNN-LSTM	96.80	96.00	97.00	97.00
This Study	CNN-BiGRU	99.97	99.97	99.98	99.98

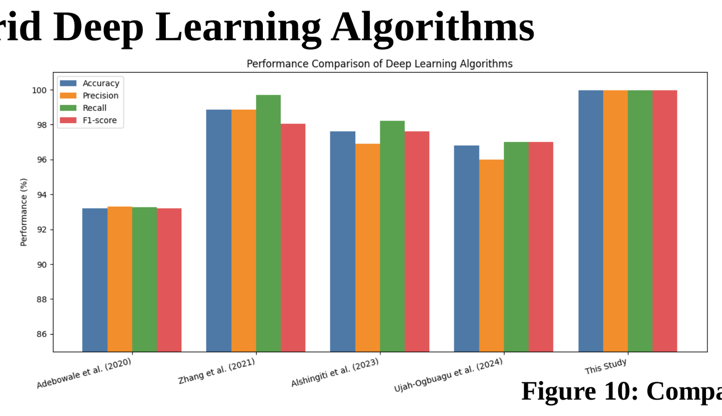

Figure 10: Comparison

CONCLUSION/ FUTURE WORK

The study shows that combining spatial and temporal features through a CNN-BiGRU model greatly improves phishing website detection. Extensive experiments on an 80,000-instance dataset and an external benchmark confirm the model's robustness and generalization, achieving near-perfect performance (Accuracy 99.97–99.99%, Precision 99.97–99.99%, Recall up to 100%, F1-score up to 99.99%, Specificity up to 99.98%). These gains consistently outperform prior hybrid approaches (CNN-LSTM, CNN-BiLSTM, LSTM-CNN), establishing feature fusion as a decisive advancement for phishing mitigation. with future work targeting real-time use, robustness against attacks, and adaptation to new phishing techniques..

REFERENCES

Alshingiti, Z., Alaqel, R., Al-Muhtadi, J., Haq, Q. E. U., Saleem, K., & Faheem, M. H. (2023). A Deep Learning-Based Phishing Detection System Using CNN, LSTM, and LSTM-CNN. *Electronics (Switzerland)*, *12*(1). https://doi.org/10.3390/electronics12010232

Maroofi, S., Korczynski, M., Holzel, A., & Duda, A. (2021). Adoption of Email Anti-Spoofing Schemes: A Large Scale Analysis. *IEEE Transactions on Network and Service Management*, *18*(3), 3184–3196. https://doi.org/10.1109/TNSM.2021.3065422