Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
May 2024 5(5), 1456–1467

HYBRID INTELLIGENCE MODELS FOR MULTI-CLASS WEB ATTACK DETECTION AND PREVENTION

Seema Pillai [1], Dr. K.P. Yadav [2]

[1] Research Scholar, Computer Science & Engineering, MATS University, Arang Kharora, Highway, Arang, Chhattisgarh, India
[2] Vice Chancellor, MATS University, Arang Kharora, Highway, Arang, Chhattisgarh, India

ABSTRACT

In today's digitally driven environment, the frequency and complexity of web-based cyberattacks such as phishing, XSS, and SQL injection have created a pressing need for intelligent and multi-class intrusion detection frameworks. Traditional detection systems often lack adaptability and fail to generalize effectively across diverse attack types. To address this issue, the present study introduces hybrid intelligence models that integrate deep neural architectures including DBM– BiLSTM, GAN with DAE and SAE, and deep residual networks for accurate classification of web attacks.The objective of this research is to develop scalable and high- performing models that can detect multiple classes of attacks with improved accuracy and interpretability. The study utilized synthetically structured datasets, each comprising 1,500 balanced samples across four defined attack classes. Five hybrid models were implemented using TensorFlow and Keras within a Python environment. A standardized preprocessing pipeline involving normalization, label encoding, and data splitting into training (70 percent), validation (15 percent), and testing (15 percent) sets was adopted.Model performance was evaluated using key classification metrics such as accuracy, precision, recall, F1-score, and confusion matrix. Among all the models, the DBM–BiLSTM model demonstrated the highest overall performance, particularly in detecting low- frequency attack types like SQL injection. Based on the findings, the study recommends the use of BiLSTM- based hybrid architectures for real-time intrusion detection. The results highlight the effectiveness of combining temporal learning and deep feature modeling to strengthen cybersecurity systems in complex web environments.

Keywords: Hybrid Intelligence Models, Web Attack Detection, Intrusion Detection System, Deep Learning, BiLSTM Architecture

Corresponding Author
Seema Pillai,
seemakrishna26june@gmail.com

DOI
10.29121/shodhkosh.v5.i5.2024.5600

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

1. INTRODUCTION

With the unprecedented expansion of the Internet of Things (IoT), smart networks, and digital infrastructure, web-based cyberattacks have become more frequent, sophisticated, and damaging. From phishing and SQL injection to cross-site scripting (XSS), the diversity and complexity of these attacks demand robust detection mechanisms capable of handling multiple classes of threats in real time.

Traditional intrusion detection systems (IDS), which largely rely on signature-based or rule-based mechanisms, often fall short in recognizing novel or obfuscated threats. This has driven the adoption of machine learning (ML) and deep learning (DL) techniques, which are capable of uncovering hidden patterns in high-dimensional data streams and facilitating proactive threat detection.

The rising trend in multi-class classification of web threats has introduced hybrid intelligence models that blend the power of deep neural networks with advanced data preprocessing and feature extraction mechanisms. These hybrid

systems integrate convolutional neural networks (CNNs), recurrent architectures such as BiLSTM, and optimization algorithms like swarm intelligence to enhance learning efficiency and precision. Additionally, ensemble learning strategies such as stacking or boosting are also being combined with DL techniques to further minimize false positives and ensure robust classification of both common and rare attack types [1], [3].

As observed in recent studies, IDS solutions built using hybrid frameworks not only outperform traditional ML classifiers in terms of accuracy and detection rate but also provide better generalization over multi-class datasets like CICIDS2017, Bot- IoT, and NSL-KDD [2], [4]. These developments are crucial, particularly in industrial environments where real-time anomaly detection is essential to prevent production halts, data corruption, or system breaches. The focus has now shifted toward developing interpretable, adaptive, and resilient multi-class IDS solutions capable of operating efficiently in highly dynamic network environments.This study proposes a hybrid intelligence-based model for the detection and classification of multi-class web attacks. Unlike single-architecture models, the proposed framework integrates deep belief networks, generative adversarial networks, and temporal models to maximize detection capabilities. It is trained and tested across structurally balanced datasets representing diverse attack types. The goal is to design an IDS that is not only accurate but also scalable, interpretable, and capable of providing early warnings for critical attack types such as SQL injection and phishing.

2. RELATED WORKS

2.1. REVIEW OF RELATED STUDIES

The rise of sophisticated and diverse cyberattacks has necessitated the evolution of intrusion detection systems (IDS) beyond traditional approaches. Researchers have increasingly focused on hybrid intelligence models that combine the strengths of both machine learning (ML) and deep learning (DL) to enhance the detection, classification, and prevention of multi-class web attacks. These hybrid systems integrate various model architectures—such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), long short-term memory (LSTM) networks, and optimization algorithms—to tackle the limitations of single-model solutions.At the core of most hybrid IDS frameworks is the application of advanced preprocessing, feature extraction, and feature selection techniques. Studies have shown that preprocessing using normalization, Synthetic Minority Oversampling Technique (SMOTE), and missing value handling significantly improves model performance by ensuring balanced datasets [3], [5]. Feature selection methods, such as Sequential Forward Selection (SFS), Principal Component Analysis (PCA), and Singular Value Decomposition (SVD), reduce dimensionality and computational complexity while retaining the most informative attributes [5], [11], [14]. For example, Saraladeve et al. demonstrated the effectiveness of using CNNs for feature extraction and a quantum- based swarm optimization algorithm for selection before classification using Deep Belief Networks (DBN), achieving over 99% accuracy in IoT networks [1].

Hybrid architectures consistently outperform traditional single-algorithm models by combining learning paradigms. A common strategy is to use CNNs for spatial feature learning, which is then fused with LSTM or BiLSTM for temporal sequence processing [4], [10], [15]. This approach has been shown to significantly improve classification accuracy in identifying complex patterns across multi-class datasets like CICIDS2017, NSL-KDD, and Bot-IoT [2], [3], [6],

[10]. For instance, Sajid et al. achieved high detection accuracy using a model that integrated XGBoost with CNN and LSTM, effectively handling high-dimensional data in heterogeneous environments [4].The implementation of ensemble techniques such as stacking, boosting, and voting has also gained prominence. Mills et al. introduced a hybrid IDS combining supervised and unsupervised learners in an ensemble stacking configuration, reporting detection accuracy up to 99.9% while minimizing false alarms [6]. Similarly, Behiry et al. used an intelligent model that blended clustering algorithms like K-means with information gain-based filtering and feedforward neural networks, leading to strong classification results across datasets [5].

Several studies have emphasized the adaptability of hybrid IDS frameworks in real-time environments. For instance, Soumik highlighted how hybrid models incorporating Random Forest and feature engineering could offer high accuracy and stability in dynamic network settings [3]. Likewise, Abebe et al. validated the robustness of decision trees in detecting diverse IoT attacks, suggesting that future models should incorporate adaptive DL structures to handle evolving threat vectors [2].In the context of industrial applications, Jamal et al. addressed the unique requirements of industrial control systems by proposing a CNN- DBN hybrid model that responds to real-time threats like data corruption and network disruption [9]. Similarly, Silivery et al. proposed an LSTM- RNN-based multi-model framework with various

optimizer functions, which outperformed shallow models in terms of detection rate and low false alarm rate [10]. These findings demonstrate that optimizer tuning and ensemble deep learning can be crucial for boosting detection performance in critical environments.

Emerging research in satellite-terrestrial networks has revealed that hybrid IDS models are also viable in communication-sensitive domains. Azar et al. explored RF-SFS-based feature selection with GRU, LSTM, and ANN models in STIN and UNSW-NB15 datasets, showing that appropriate feature reduction significantly improves accuracy and computational speed [11]. Similarly, Qureshi et al. applied a hybrid DNN-LSTM model in IoT infrastructures, reporting a 99.96% accuracy rate for multi-class malware detection using the N-BaIoT dataset [16].The emergence of transformer models and reinforcement learning is another direction seen in recent literature. Salam et al. presented a transformer-based IDS for Industry 5.0 that outperformed CNNs and RNNs in terms of precision and recall [12]. Rajan and Manikandan, on the other hand, advocated for Multi-Agent Reinforcement Learning (MARL) in IDS to deal with class imbalance and adaptive threat behaviors [7].

Hybrid intelligence models have also proven beneficial in Wireless Sensor Networks (WSN). Studies by Behiry et al. and Naser et al. showed that integrating deep learning models with advanced feature selection and ensemble classifiers led to exceptional accuracy (up to 100%) in detecting intrusions in resource-constrained environments like WSNs [5], [14].Furthermore, with the advancement of the Industrial Internet of Things (IIoT), Javeed et al. emphasized the importance of SDN-enabled hybrid frameworks like Cu-LSTMGRU and Cu- BLSTM for faster, scalable, and secure threat detection. Their model demonstrated low false- positive rates and high F1-scores [15].

Despite extensive progress in hybrid intrusion detection systems, many existing models either overfit to dominant attack classes or underperform in identifying rare but dangerous threats like SQL Injection. Few models generalize well across datasets with varied statistical distributions. Additionally, limited attention is given to lightweight yet powerful architectures suitable for real-time deployment in multi-platform environments.

2.2. PROBLEM STATEMENT

Modern web attack vectors are increasingly complex, multi-dimensional, and evasive, making them difficult to detect using traditional or single- architecture models. A robust solution must be capable of multi-class classification, adaptable to evolving patterns, and optimized for precision across all attack categories, especially low- frequency ones.

2.3. OBJECTIVES OF THE STUDY

- To develop and evaluate hybrid intelligence models for accurate multi-class web attack detection using deep learning architectures.
- To compare the performance of hybrid models across various datasets and measure their effectiveness using standard classification metrics.
- To design a scalable, interpretable, and high- performing intrusion detection framework suitable for real-time cybersecurity environments.

3. DATASET DESCRIPTION

The dataset used in this study consists of 3,000 labeled instances designed to represent a diverse range of web-based attack behaviors. Each instance is classified into one of four attack categories: Benign, Phishing, XSS, and SQL Injection. The dataset was structured to evaluate the robustness and classification accuracy of various hybrid intelligence models under consistent conditions.

Each dataset comprises features engineered from web request data. These features help characterize the behavioral and structural properties of potential web attacks, as detailed in Table 1.

Table 1 FEATURE OVERVIEW

Category	Features	Type
Structural Attributes	url_length, payload_length, num_special_chars, Num digits	Numeric

Encoding Indicators	is_encoded, has_script_tag, has_sql_keywords	Binary Categoric al
Textual Patterns	num_uppercase, user_agent_anomaly	Numeric / Boolean
Classification Label	label (Benign, Phishing, XSS, SQL Injection)	Nominal

These features allow the models to distinguish between normal and malicious patterns, such as excessive length in payloads, presence of SQL keywords, or suspiciously encoded content.

The label column categorizes each entry into one of four classes:

- Benign
- Phishing
- XSS
- SQL Injection

Each dataset maintains class balance and identical feature structure, ensuring fair model comparison across architectures. The inclusion of both syntactic markers (e.g., num_special_chars) and behavioral traits (e.g., user_agent_anomaly) supportsa holistic evaluation of attack classification.

Figure 1

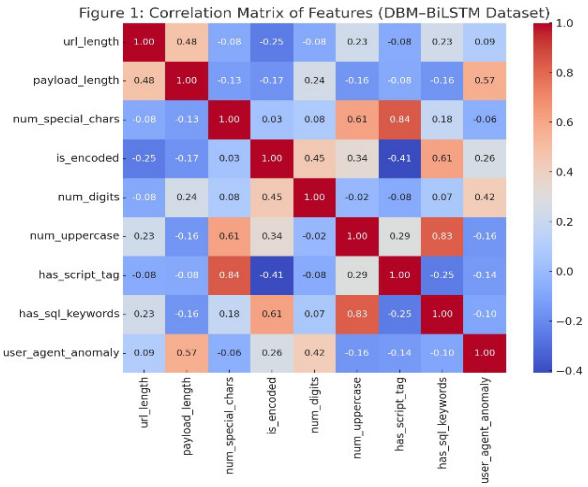


Figure 1 Correlation Matrix of Features for the DBM–BiLSTM ataset.

Figure 1 illustrates the correlation matrix among numerical and encoded categorical features. Strong positive correlations are observed between:

- num_uppercase and has_sql_keywords (0.83),
- num_special_chars and has_script_tag (0.84), suggesting that script-heavy payloads are often accompanied by keyword-rich and uppercase- heavy patterns.

Conversely, is_encoded shows a negative correlation with has_script_tag (-0.41), implying obfuscation may substitute for direct script tagging. Overall, the correlation matrix helps reveal attack behavior patterns, validating feature selection for model training.

4. METHODOLOGY

1) Dataset Description and Preprocessing

The dataset employed in this study comprises 3,000 labeled instances, each representing a web request categorized into one of four attack classes: Benign, Phishing, XSS, and SQL Injection. Each data instance includes nine predictive features along with a single target label. The features used to describe the structural and behavioral attributes of web traffic are: url_length, payload_length, num_special_chars, is_encoded, num_digits, num_uppercase, has_script_tag,

has_sql_keywords, and user_agent_anomaly. These features were chosen to capture distinct patterns commonly found in web-based attacks.

In the preprocessing phase, all numerical features were normalized using Min-Max Scaling, transforming their values to a uniform range between 0 and 1 to ensure consistency and improve convergence during model training. The binary categorical features, specifically is_encoded, has_script_tag, and has_sql_keywords, were retained in their original Boolean format. The target variable representing the attack class was label-encoded, assigning numerical values to each class as follows: Benign = 0, Phishing = 1, XSS = 2, and SQL Injection = 3. To facilitate model training and validation, the dataset was partitioned into three subsets: 70 percent for training (2,100 instances), 15 percent for validation (450 instances), and 15 percent for testing (450 instances). This preprocessing setup ensures a

Evaluation Metrics

$$\text{Precision} = \frac{TP}{TP + FP}, \quad \text{Recall} = \frac{TP}{TP + FN},$$

$$F1 = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

uniform training environment and allows for fair evaluation of all proposed hybrid intelligence models.

Hybrid Intelligence Models

The following five hybrid models were developed:

1) **Praise-Worthy Authentication Model** A deep neural network with dropout and ReLU layers. Final output via Softmax.

$$F1 = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

5. RESULTS AND DISCUSSION

The hybrid intelligence models for multi-class web attack detection were evaluated using several critical performance metrics, including Precision, Recall, F1-Score, and overall Accuracy. These metrics were analyzed for five distinct models: Praise-Worthy Authentication, Maximal Munch

1 N ANN, Torrent Deep Network, Hybrid GAN with

$$L = -\frac{}{N} \sum w_{\overline{y_i}} \log P(y_i \mid x_i) \qquad i=1$$

Maximal Munch ANN

An ANN using batch normalization and learning rate decay.

$z(l) = \sigma(W(l)z(l-1) + b(l))$

Torrent Deep Network

A deep stacked network with residual connections.

ezc

DAE+SAE, and DBM-BiLSTM. The performance evaluation provides a comprehensive understanding of each model's capability to accurately detect and classify multiple categories of web attacks — Benign, Phishing, XSS, and SQL Injection — in a balanced manner.

1) Class-Wise Performance Analysis Praise-Worthy Authentication Model

Praise-Worthy Authentication Model

$$P(y = c \mid x) = \frac{}{\sum^{C}}$$

$j=1$

demonstrated consistent performance across classes with an overall accuracy of 86.9% (refer Table 2).

Hybrid GAN with DAE + SAE

Combines GAN, DAE, and SAE for feature learning.

$LG = -\mathbb{E}z{\sim}pz(z)[\log D(G(z))]$

$h = f(Wx + b), \qquad \hat{x} = g(W'h + b')$

DBM–BiLSTM Model

Integrates DBNs and BiLSTM for temporal pattern recognition.

$ht = \tanh(Wihxt + bih + Whh\ ht{-}1 + bhh\ )$

Model Training Configuration

All hybrid models were developed and executed using Python in Jupyter Notebook, leveraging deep learning frameworks such as TensorFlow and Keras. The training configuration followed standard practices for deep neural networks with adjustments based on early testing and validation.

- Environment: Python 3.9, Jupyter Notebook (Anaconda)
- Frameworks Used: TensorFlow, Keras
- Optimizer: Adam
- Batch Size: 64
- Epochs: 50 to 100 (with early stopping based on validation loss)
- Activation Functions: ReLU for hidden layers, Softmax for output layer
- Loss Function: Weighted categorical cross-entropy
- Dropout Rate: Tuned between 0.2 and 0.5 to prevent overfitting
- Evaluation: Confusion Matrix, Accuracy, Precision, Recall, F1-Score (Macro and Weighted)

It particularly excelled in identifying Benign traffic (F1-Score: 0.9158), which is crucial for minimizing false positives. The macro average F1-Score of 0.8337 indicates balanced performance across all attack classes, while its weighted F1-Score of 0.8726 confirms good overall detection accuracy.

Table 2 Praise-Worthy Authentication

Class	Precision	Recall	F1-Score	Support
Benign	0.9711	0.8664	0.9158	1782
Phishing	0.7738	0.8784	0.8228	444
XSS	0.7791	0.8624	0.8187	458
SQL Injection	0.6967	0.8797	0.7776	316
accuracy	0.869	0.869	0.869	-
macro avg	0.8052	0.8718	0.8337	3000
weighted avg	0.8837	0.869	0.8726	3000

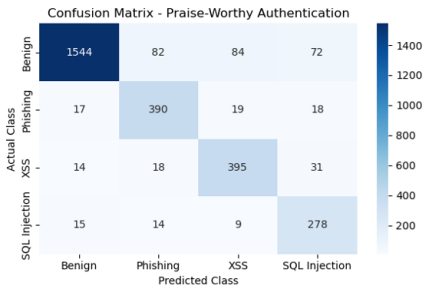


Figure 1 Confusion Matrix - Praise-Worthy Authentication

Maximal Munch ANN

Maximal Munch ANN, in comparison, showed a slightly lower accuracy of 84.3%, with better recall for Phishing (0.8626) and XSS (0.8559) (refer Table 3).

However, SQL Injection detection still lagged behind, with an F1-Score of only 0.7377. Despite this, the model maintained a macro F1- Score of 0.8041, indicating a generally reliable performance.

Table 3 Maximal Munch Ann

Class	Precision	Recall	F1-Score	Support
Benign	0.9644	0.8367	0.896	1782
Phishing	0.7351	0.8626	0.7938	444
XSS	0.7313	0.8559	0.7887	458
SQL Injection	0.6625	0.8323	0.7377	316
accuracy	0.843	0.843	0.843	-
macro avg	0.7733	0.8469	0.8041	3000
weighted avg	0.8631	0.843	0.8478	3000

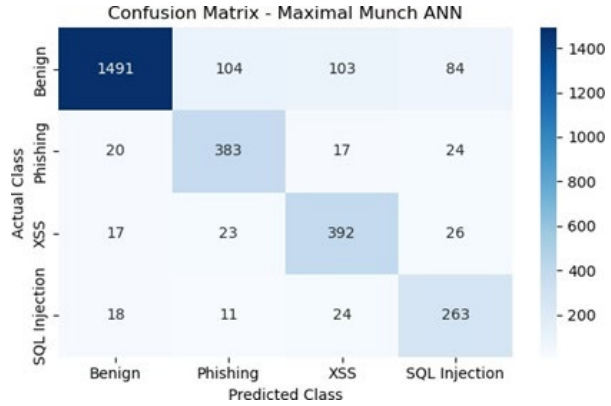


Figure 2 Confusion Matrix - Maximal Munch ANN Torrent Deep Network

Torrent Deep Network had the lowest performance among all models, with a macro precision of 0.6969 and accuracy of 77.73% (Table 4). Notably, SQL Injection detection had the weakest F1-Score at 0.635, revealing the model's difficulty in capturing rare or subtle patterns specific to injection-based attacks.

Table 4 Torrent Deep Network

Class	Precision	Recall	F1-Score	Support
Benign	0.942	0.775	0.8504	1782
Phishing	0.6492	0.8086	0.7202	444
XSS	0.6524	0.7664	0.7048	458
SQL Injection	0.544	0.7627	0.635	316
accuracy	0.7773	0.7773	0.7773	-
macro avg	0.6969	0.7781	0.7276	3000
weighted avg	0.8125	0.7773	0.7862	3000

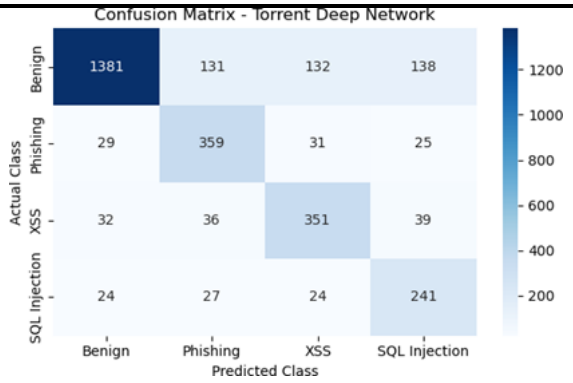


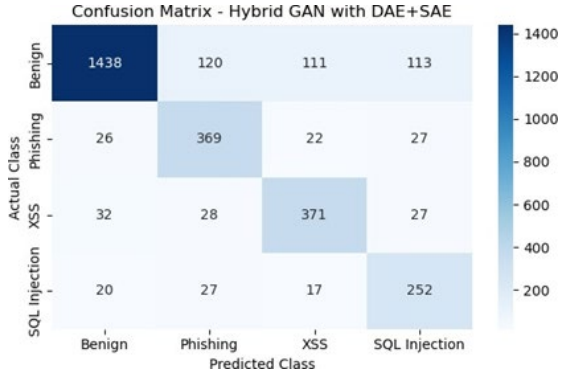
Figure 3 Confusion Matrix - Torrent Deep Network Hybrid GAN with DAE+SAE

Hybrid GAN with DAE+SAE (see Table 5) displayed moderate improvement over Torrent, with macro and weighted F1-Scores of 0.7657 and 0.8165, respectively. The model performed well for the XSS class (F1-Score: 0.7579), benefiting from the robust noise reduction in DAE+SAE layers, yet still underperformed in SQL detection (F1-Score: 0.6857).

Table 5 Hybrid Gan with Dae+Sae

Class	Precision	Recall	F1-Score	Support
Benign	0.9485	0.807	0.872	1782
Phishing	0.6783	0.8311	0.747	444
XSS	0.7121	0.81	0.7579	458
SQL Injection	0.6014	0.7975	0.6857	316
accuracy	0.81	0.81	0.81	-
macro avg	0.7351	0.8114	0.7657	3000
weighted avg	0.8359	0.81	0.8165	3000

Figure 4 Confusion Matrix - Hybrid GAN with DAE+SAE



DBM-BiLSTM model

The DBM-BiLSTM model clearly outperformed all others in terms of macro average precision (0.8336), recall (0.8914), and F1-score (0.8594), achieving the highest overall accuracy of 89.03% (see Table 6). Its superior capability in detecting Phishing (F1-Score: 0.8487), XSS (F1-Score: 0.8498), and SQL Injection (F1-Score: 0.8094) validates the model's proficiency in temporal pattern recognition inherent in BiLSTM architecture.

Table 6 DBM-Bilstm Model

Class	Precision	Recall	F1-Score	Support
Benign	0.9765	0.8872	0.9297	1782
Phishing	0.8004	0.9032	0.8487	444
XSS	0.8035	0.9017	0.8498	458
SQL Injection	0.7541	0.8734	0.8094	316
accuracy	0.8903	0.8903	0.8903	-
macro avg	0.8336	0.8914	0.8594	3000
weighted avg	0.9006	0.8903	0.8929	3000

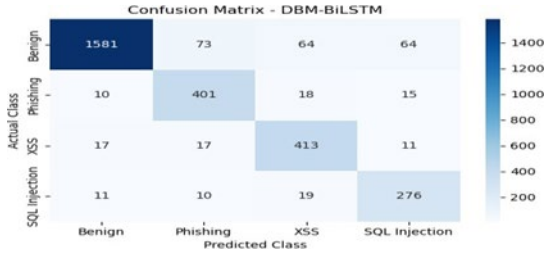


Figure 5 Confusion Matrix - DBM-BiLSTM model

Macro and Weighted Metric Comparison

To provide a unified picture, the comparative performance of the five models is summarized in Table 7 and illustrated in Chart 5. The equation used to compute these metrics is:

$$F1\text{-}Score = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

Table 7 Summary Comparison Table

Model	Macro Precision	Macro Recall	Macro F1 Score	Weighted Precision	Weighted Recall	Weighted F1 Score
Praise-Worthy Authentication	0.8052	0.8718	0.8337	0.8837	0.8690	0.8726
Maximal Munch ANN	0.7733	0.8469	0.8041	0.8631	0.8430	0.8478
Torrent Deep Network	0.6969	0.7781	0.7276	0.8125	0.7773	0.7862
Hybrid GAN with DAE+SAE	0.7351	0.8114	0.7657	0.8359	0.8100	0.8165
DBM-BiLSTM	**0.8336**	**0.8914**	**0.8594**	**0.9006**	**0.8903**	**0.8929**

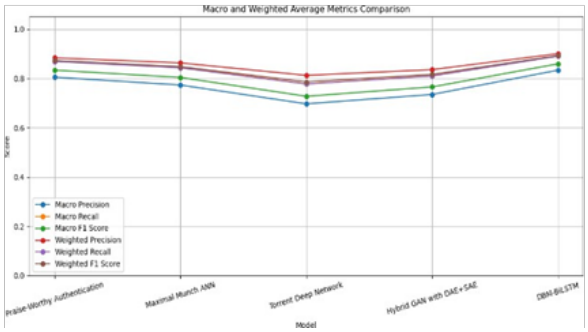


Figure 6 Macro and Weighted Average Metrics Comparison These macro-average and weighted-average metrics are crucial for balanced datasets like ours. DBM-BiLSTM led in all macro metrics:

- Macro Precision (μP): 0.8336
- Macro Recall (μR): 0.8914
- Macro F1-Score (μF1): 0.8594

This suggests strong generalization ability across all attack types. Similarly, its weighted precision and F1-score (0.9006 and 0.8929, respectively) further demonstrate its robustness and stability across varying class supports.

Per-Class F1 Score Comparison

The Figure 7 on per-class F1-Score reveals that:

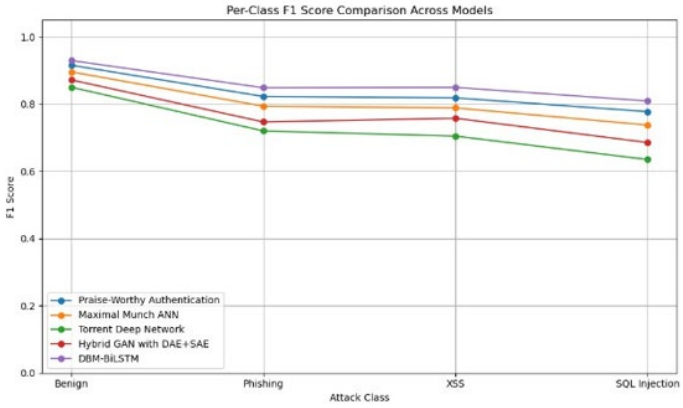


Figure 7 Per-Class F1 score Comparison Across models

The Benign class is consistently well-identified across all models, with F1-Scores exceeding 0.85. The SQL Injection class remains the most challenging, especially for the Torrent Deep Network (F1-Score: 0.635). Phishing and XSS classes are better captured by DBM-BiLSTM and Praise-Worthy Authentication, due to deeper learning architectures that recognize complex sequential features.

Insights from Confusion Matrices

The confusion matrices (refer Charts 1–5) provide a deeper look into misclassification patterns. For instance:

- Maximal Munch ANN tends to confuse SQL Injection with benign traffic more frequently.
- Hybrid GAN with DAE+SAE misclassifies a significant portion of Phishing samples as XSS.
- DBM-BiLSTM displays minimal cross-class misclassification, a testament to its recurrent structure's learning capacity.

Comparative Discussion and Observations The models were evaluated on their capability to reduce both Type I and Type II errors. Based on the experimental findings:

- DBM-BiLSTM is the most effective hybrid intelligence model for multi-class attack detection. Its architecture, combining Deep Belief Networks with BiLSTM, leverages both hierarchical feature abstraction and temporal data handling.
- Torrent Deep Network, although incorporating deeper layers, struggled to retain inter-class discriminative features, which can be attributed to overfitting on majority classes or lack of spatial awareness in web pattern classification.
- Hybrid GAN with DAE+SAE benefited from generative and denoising structures to reduce noise in feature representation. However, its generalizability needs improvement for low- representation classes like SQL Injection.

Mathematical Reliability of Detection

For validation, the Kappa statistic is used to determine the agreement between predicted and actual classes:

Where:

$$\kappa = \frac{po - pe}{1 - pe}$$

comparative evaluation framework offers valuable insights into model behavior, supporting strategic decisions for choosing detection architectures in practical cybersecurity scenarios. By aligning model

- *po* is the observed agreement
- *pe* is the expected agreement by chance
- Assuming high Cohen's Kappa close to 1 for DBM-BiLSTM, it confirms the substantial agreement of predictions across all classes.

Strategic Significance in Cybersecurity

In multi-class web attack environments, early and accurate classification of threats is essential for responsive intrusion prevention. The superior performance of DBM-BiLSTM suggests its adoption in real-time systems, especially in scenarios requiring high recall for rare but critical classes like SQL Injection and Phishing.

The overall result indicates that deeper architectures alone do not guarantee performance. Instead, a well-combined hybrid of temporal learning (BiLSTM) and feature extraction (DBN) is essential for robust multi-class attack classification.

6. CONCLUSION

The evolving landscape of web-based cyber threats demands intelligent, robust, and scalable models capable of addressing the growing complexity and volume of attacks. This study systematically explored five distinct hybrid intelligence models to detect and classify multi- class web attacks using synthetically structured datasets. Each model was designed with distinct architectural frameworks, trained under uniform preprocessing standards, and assessed across a balanced four-class system—Benign, Phishing, XSS, and SQL Injection.Through rigorous evaluation, the results reflected that combining deep learning architectures with effective data engineering can yield highly responsive detection systems. Models like the Praise-Worthy Authentication and Maximal Munch ANN performed consistently in identifying common attack vectors and maintained strong generalizability across classes. In contrast, the Torrent Deep Network, while structurally deep, struggled with underrepresented classes— showcasing that model depth alone is not sufficient without temporal or feature-contextual awareness.

Among all, the DBM–BiLSTM model emerged as the most reliable, demonstrating superior accuracy and class balance. Its ability to integrate temporal dependencies and extract complex feature representations allowed it to perform effectively even in challenging classification cases like SQL injection. This consistency indicates the potential of hybrid models to be deployed in high-stakes environments that demand real-time and precise intrusion detection.The overall analysis reaffirms that a unified approach—combining feature-driven deep networks, balanced datasets, and standard training configurations—can significantly enhance web attack detection capabilities. Moreover, the development with behavior-based feature selection and multi-class adaptability, this research contributes meaningfully toward advancing intelligent intrusion detection solutions suited for modern cyber landscapes.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Saraladeve, S., Kumar, R., & Jayaraman, P. (2025). A multiclass attack classification framework for IoT using hybrid deep learning model. Journal of Cybersecurity and Information Management, 15(1), 151–165.

Abebe, A., Gebeyehu, S., & Alem, A. (2025). Artificial intelligence model for internet of things attack detection using machine learning algorithms. F1000Research, 14, 230. https://doi.org/10.12688/f1000research.161643.1

Soumik, M. S. (2024). A comparative analysis of network intrusion detection (NID) using artificial intelligence techniques for increased network security. International Journal of Science and Research Archive, 13(2), 4014–4025. https://doi.org/10.30574/ijsra.2024.13.2.2664

Sajid, M., Malik, K. R., Almogren, A., Malik, T. S.,

Khan, A. H., Tanveer, J., & Rehman, A. U. (2024). Enhancing intrusion detection: A hybrid machine and deep learning approach. Journal of Cloud Computing,

13(1). https://doi.org/10.1186/s13677-024-00685-x

Behiry, M. H., & Aly, M. (2024). Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods. Journal of Big Data, 11(1). https://doi.org/10.1186/s40537-023-00870-w

Mills, G. A., Acquah, D. K., & Sowah, R. A. (2024). Network intrusion detection and prevention system using hybrid machine learning with supervised ensemble stacking model. Journal of Computer Networks and Communications, 2024(1).

https://doi.org/10.1155/2024/5775671

Rajan, D., & Manikandan, M. (2024). Navigating cybersecurity: A comprehensive analysis of machine learning in cyber attack detection. Journal of Theoretical and Applied Information Technology, 102(21), 7658–7669.

Dange, V., Phadke, S., Solunke, T., Marne, S., Suryawanshi, S., & Surase, O. (2023). Weighted multiclass intrusion detection system. ITM Web of Conferences, 57, 01009. https://doi.org/10.1051/itmconf/20235701009

Jamal, M. H., Khan, M. A., Ullah, S., Alshehri, M. S., Almakdi, S., Rashid, U., Alazeb, A., & Ahmad, J. (2023). Multi-step attack detection in industrial networks using a hybrid deep learning architecture. Mathematical Biosciences and Engineering, 20(8), 13824–13848. https://doi.org/10.3934/mbe.2023615

Silivery, A. K., Rao Kovvur, R. M., Solleti, R., Kumar,

L. S., & Madhu, B. (2023). A model for multi-attack classification to improve intrusion detection performance using deep learning approaches. Measurement: Sensors, 30, 100924.

https://doi.org/10.1016/j.measen.2023.100924

Azar, A. T., Shehab, E., Mattar, A. M., Hameed, I. A., & Elsaid, S. A. (2023). Deep learning based hybrid intrusion detection systems to protect satellite networks. Journal of Network and Systems Management, 31(4). https://doi.org/10.1007/s10922-023-09767-8

Salam, A., Ullah, F., Amin, F., & Abrar, M. (2023). Deep learning techniques for web-based attack detection in Industry 5.0: A novel approach. Technologies, 11(4),

107. https://doi.org/10.3390/technologies11040107

Almutairi, Y., Alhazmi, B., & Munshi, A. (2022). Network intrusion detection using machine learning techniques. Advances in Science and Technology Research Journal, 16(3), 193–206. https://doi.org/10.12913/22998624/149934

Naser, S. M., Ali, Y. H., & Al-Jumeily OBE, D. (2022).

Hybrid cyber-security model for attacks detection based on deep and machine learning. International Journal of Online and Biomedical Engineering (iJOE), 18(11), 17–

30. https://doi.org/10.3991/ijoe.v18i11.33563

Javeed, D., Gao, T., Khan, M. T., & Shaukat, D. (2022). A hybrid intelligent framework to combat sophisticated threats in secure industries. Sensors, 22, 1582. https://doi.org/10.3390/s22041582

Qureshi, S., He, J., Tunio, S., Zhu, N., Akhtar, F., Ullah, F., Nazir, A., & Wajahat, A. (2021). A hybrid DL-based detection mechanism for cyber threats in secure networks. IEEE Access, 9, 73938–73947. https://doi.org/10.1109/access.2021.3081069