

A novel IOT intrusion detection system: Integrating features position encoder with a tab transformer deep learning model

Mohammad A. Alsharaiah^a, Mohammed Amin Almaiah^{a*}, Amer Alqutaish^{b*}, Udit Mamodiya^c, Rami Shehab^d and Mansour Obeidat^e

^aKing Abdullah II School for Information Technology, The University of Jordan, Amman, Jordan

^bDeanship of Development and Quality Assurance, King Faisal University, 31982, Al-Ahsa, Saudi Arabia

^cAssociate Professor & Association Dean (Research), Poornima University, Jaipur, India, Jaipur, Raj., India

^dVice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, 31982, Al-Ahsa, Saudi Arabia

^eApplied College, King Faisal University, Al-Ahsa, Saudi Arabia

CHRONICLE

Received October 12, 2025

Received in revised format

December 18, 2025

Accepted January 4 2026

Available online

January 4 2026

Keywords:

SMOTE

TabTransformer

Binary Classification

IoT

Positional encodings

ABSTRACT

Internet of Things (IoT) and Internet of Medical Things (IoMT) networks provide a massive amount of data. These types of data need a protection level, such as an intrusion detection framework. Deep learning models become a powerful tool for this purpose. Therefore, this work proposes an intrusion detection framework based on a deep learning technique which employs TabTransformer and self-attention mechanisms to imprison intricate dependencies among tabular features and detect abnormal attack behaviors. Precisely, each numerical feature is mapped into a learnable embedding vector and augmented with positional encodings to preserve feature identity and inter-feature relationships within the embedding space. The main task for the proposed model is to achieve binary classification tasks the model should classify the traffic data as either normal or abnormal. Furthermore, the model utilized a benchmark dataset such as the CICIoMT2024. Furthermore, this type of dataset faces issues, such as imbalance. So, the system integrates SMOTE-based data balancing, Stratified K-Fold Cross-Validation, and threshold optimization to ensure fairness and reproducibility to accomplish a binary classification task. As a consequence, experiments on the CICIoMT2024 dataset yield superior results, achieving a mean accuracy of 99.85. Through SHAP-based interpretability, key features influencing model predictions are identified, confirming the framework's transparency, robustness, and suitability for real-world ARP intrusion detection.

© 2026 by the authors; licensee Growing Science, Canada.

1. Introduction

Recently, most medical fields have adopted the Internet of Medical Things (IoMT) framework (Yadav et al., 2024). This integration faces significant cybersecurity vulnerabilities, for instance, spoofing attacks, wherein malicious parts pretend as authorized devices to access corporate data or compromise most of the operations in the systems (Al-Na'amneh, et al., 2025) and (Jaafar, Abed & Al-Shareeda, 2026), (Ang, Ho, Huy, & Janarthanan, 2026) and (Almarshood & Rahman, 2025) and (Ramesh et al., 2026). Particularly, the threat is the spoofing attack, which aims to exploit flaws in authentication protocols to permit adversaries to masquerade as legitimate medical sensors and devices (Jayaraj et al., 2024). This type of attack can corrupt patient data, medical services, and other issues (Davaran et al., 2024) and (Addula et al., 2025). Prominent techniques encompass IP, MAC, and biometric spoofing (Singh & Singh, 2022). In addition, the Address Resolution Protocol (ARP) is a fundamental protocol in local area networks that associates IP addresses with MAC addresses and facilitates basic host-to-host communication on Ethernet and Wi-Fi networks (Alshinwan et al., 2025) and (Albinhamad et al. (2025). The detection of ARP attacks is essential for network security and IDS (Newaz et al., 2021).

* Corresponding author

E-mail address: m.almaiah@ju.edu.jo (M. A. Almaiah) aalqutish@kfu.edu.sa (A. Alqutaish)

ISSN 2561-8156 (Online) - ISSN 2561-8148 (Print)

© 2026 by the authors; licensee Growing Science, Canada.

doi: 10.5267/j.ijds.2026.1.003

Therefore, researchers started to involve machine learning (ML) and deep learning (DL) models to develop intrusion detection systems (IDS) to solve spoofing threats (Mohammadpour et al., 2022). (ML) and (DL) empower NIDS by treating enormous datasets to uncover subtle anomalies and produce predictive insights that avoid manual analysis, thus producing a supplementary resilient and intelligent defense system (Zachos et al., 2021). For instance, typical algorithms such as Random Forest and SVM, to more complex deep learning designs, including CNNs and RNNs (Bhosale et al., 2021; Newaz et al., 2021; Zachos et al., 2021), function on packet or flow data. However, these types of data face several shortcomings. For instance, a dependence on manual feature engineering that supervises complicated feature relations; the application of CNNs and RNNs, which are inherently considered for spatial or sequential data, to the inherently tabular structure of network attributes; and assessment practices dependent on single train-test splits, which can produce overblown performance metrics on imbalanced or incomplete datasets (Abu Laila, 2025) and (Ali, 2024).

In this work, a proposed Tab Transformer-based intrusion detection framework is proposed for tabular ARP traffic data. The Tab Transformer architecture applies self-attention to feature embedding's to learn contextualized, interdependent representations of tabular inputs — an inductive bias well-suited to modelling the non-linear relationships among ARP features. To preserve feature identity while enabling rich interaction, each numeric feature is mapped to a learnable embedding and augmented with positional encodings that index feature columns. For robust, reproducible evaluation, we employ stratified K-fold cross-validation and report mean \pm standard deviation across folds; additionally, we perform validation-driven threshold optimization to maximize F1 score on imbalanced classes. Finally, we include model interpretability via SHAP explanations to identify the most influential features for the detector's decisions.

The structure of this paper is: (1) the first (to our knowledge) application of transformer-based tabular learning (TabTransformer) to ARP intrusion detection in IoT settings; (2) an architecture that combines per-feature learnable embeddings with positional encodings and multi-head self-attention to capture complex feature interactions; (3) a robust training and evaluation pipeline using stratified K-fold CV and threshold tuning to optimize F1 for imbalanced attacks; and (4) results discussions and (5) conclusion with future work.

2. Literature Review

The evolution of countermeasures for ARP spoofing and poisoning moved from static checks to statistical anomaly detection, and now focuses on data-driven methods. It can automatically learn feature hierarchies from less processed data, demonstrating promising performance gains (Newaz et al., 2021). Deep learning models (DNNs, CNNs, and LSTMs) are widely used and tested in Intrusion Detection Systems (IDS) (Zachos et al., 2021), showing a strong ability to learn complex features and temporal patterns in network traffic autonomously. Furthermore, the Transformer architecture has some advanced models, such as TabTransformer, this model is powerful in language processing (Sharma & Babbar, 2024). This model would be a pioneer in structured data. It uses self-attention to create better, contextualized representations of features, outperforming older deep learning baselines. However, transformer-based models have been successful in general tasks, including some cybersecurity fields, challenges can appear in numerical feature integration, computational cost, and data preprocessing. Crucially, their use in ARP spoofing detection is still a research gap (Saheed & Arowolo, 2021). The available approaches mainly use classical ML and CNN/RNN architectures (Majumder et al., 2025), overlooking the possibility of new transformer-based models that are inherently suitable for the tabular data structure of network features. Lately, DL models have been developed for ARP spoofing detection. For instance, the explainable ARP-PROBE model for IoT (Cabello-Solorzano et al., 2023) and an effective, pattern-aware DNN provided a high accuracy performance.

Table 1

Models overview

Reference	Proposed Scheme	Dataset	Key Findings	Limitations
Zachos et al. (2021)	Anomaly-based IDS for IoMT using Random Forest, Decision Tree, KNN	Simulated IoMT dataset	96% accuracy, strong feature importance analysis	Limited scalability to real-time IoMT
Faruqui et al. (2023)	CNN-LSTM hybrid IDS	Custom IoMT dataset	97.63% accuracy, captures spatial + temporal patterns	Overfitting risk, high resource cost
Nazir et al. (2024)	Hybrid CNN-LSTM for IoT threats	IoT benchmark dataset	98% accuracy, strong temporal modeling	No focus on spoofing types
Iqbal et al. (2024)	Deep Learning GNSS spoof detection	GNSS spoof dataset	Robust to real-time spoofing	Domain-specific, not IoMT
Awotunde et al. (2024)	RNN with feature selection for keylogger detection	IoT dataset	High accuracy via feature reduction	No spoofing-specific evaluation
Ayo et al. (2024)	Ontology-based layered NIDS	Synthetic & real traffic	Strong rule-based reasoning	Lacks deep learning adaptability

Table 1 explores a comparative analysis of modern intrusion detection methods applied to IoT and IoMT environments, stressing some of the points such as their datasets, performance, and limitations. Initial anomaly-based methods, like (Zachos et al., 2021), accomplished admirable accuracy using typical ML classifiers such as Random Forest and KNN, they faced scalability issues when extended to real-time IoMT situations. Following developed models, Faruqui et al. (2023) and Nazir

et al. (2024). Presented hybrid CNN-LSTM architectures that effectively combined spatial and temporal learning, and they achieved accuracies above 97%. Nevertheless, these models faced some issues, such as high computational overhead and overfitting risks. As a consequence, they become less feasible for resource-constrained IoT devices. Further research, such as Iqbal et al. (2024), employed deep learning for GNSS spoofing detection, signifying robustness in domain-specific applications but absent generalization to IoMT contexts. Likewise, Awotunde et al. (2024) accomplished robust performance through RNN models with feature selection, although Ayo et al. (2024) suggested an ontology-driven layered IDS stressing rule-based reasoning but deprived of deep learning adaptability. On the other hand, the recommended TabTransformer model integrates data augmentation, efficiently addressing class imbalance and spoofing-specific tasks. Verified on the CICIOMT2024 dataset, it reached a 99.85% accuracy, surpassing previous models in both robustness and generalization.

3. Proposed Methodology

In this part, a detailed overview of the research methodology is presented. Also, it includes dataset description, data preprocessing, and preparation procedures undertaken before model training. Also, it explains the techniques and strategies implemented in constructing the proposed model. A comprehensive outline of the architectural framework and operational characteristics of the proposed system.

3.1 ICIOMT2024 dataset and Preprocessing phase

The CICIOMT2024 benchmark dataset has been used in this study to evaluate the Cybersecurity mechanism in the healthcare sector (Gheni & Al-Yaseen, 2024). It's mainly a public dataset with 46 distinct features across 18 categories of cyber threats, also including ARP spoofing, totaling 16,047 traffic instances. Established to endorse research and performance assessment in Internet of Medical Things (IoMT) security, CICIOMT2024 provides an essential foundation for testing the accuracy and robustness of ML and DL based intrusion detection systems (IDS) against spoofing-related attacks. Mainly, a One-Hot Encoder was applied to change categorical label values in numerical values to apply a binary classification task (Lv, Ding, Wang, & Zou, 2021). Features like timestamp, flow ID, and destination IP were dropped as they were deemed non-essential. Variations in feature scales can present biases in results. Therefore, a data standardization technique was engaged to normalize numbers around the mean (μ) with a unit standard deviation (σ). Consider Eq. (1) as follows,

$$X' = \frac{X - \mu}{\sigma} \quad (1)$$

Besides, Preprocessing techniques like data normalization (Cabello-Solorzano, Ortigosa de Araujo, Peña, Correia & Tallón-Ballesteros, 2023) are engaged to realize reliable analysis. This step was maintained using the method outlined in Equation 2. Following, categorical data were changed into numeric values, and all attack types in the dataset were categorized as either 1 for abnormal instances or 0 for normal instances. Data normalization: Input data is standardized to confirm uniformity and facilitate model convergence through Eq. (2) as follows,

$$X_{Normalized} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (2)$$

Fig. 1 shows the efficiency of the Synthetic Minority Oversampling Technique (SMOTE) in detecting the imbalanced class that is present in the dataset (Amirruddin et al., 2022). However, before applying SMOTE, the majority class (Class 0) comprised approximately 97.3% of the samples, while the minority class (Class 1) represented only 2.7%. This explores the imbalance state and could bias the learning process toward the dominant class, causing poor detection of rare but critical anomalies. Concerning the imbalanced data set, the SMOTE (Synthetic Minority Oversampling Technique) has been engaged since this technique is valuable in supervising imbalanced datasets Elreedy et al. (2024). It is a method to up-sample the smaller classes while crossover overfitting. It does this by producing novel synthetic instances close to the other points. So, SMOTE addresses the problem of data shortage in the minority class by creating synthetic examples that bridge the gap between minority class occurrences in feature space.

By utilizing SMOTE, the minority class was synthetically augmented through interpolation between existing minority samples, resulting in an evenly balanced distribution (50%–50%). This resampling not only reduces model bias but also improves its sensitivity to minority patterns, thereby improving recall and F1 performance in subsequent evaluations. SMOTE provides a more fit learning environment. It ensures the capture of both normal and anomalous network behaviors in ARP traffic classification and intrusion detection. This bar chart displays the original class imbalance in the dataset. Class 0 (normal traffic) signifies 97.3% of samples, while Class 1 (anomalous traffic) only accounts for 2.7% (428 samples). The imbalance can bias the model's majority class, with poor detection of the minority (attack) and low recall. After employing SMOTE, the classes are balanced (50%–50%). It generates synthetic trials for the minority class by inserting between existing minority

instances, rather than merely duplicating them. This makes the model to learn the minority class patterns more successfully, refining its recall, F1-score, and complete generalization on unobserved data.

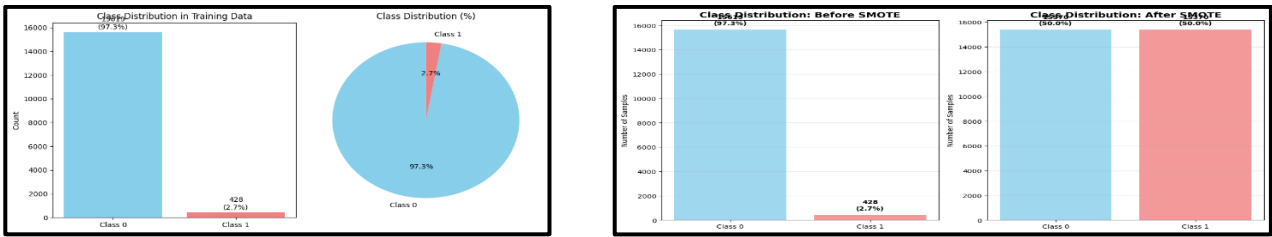


Fig. 1. Class Distribution: Before SMOTE and after SMOTE.

Furthermore, a comparative visualization of different SMOTE (Synthetic Minority Oversampling Technique) has been applied to explain the effects of class distribution. Fig. 2 illustrates the effect of the SMOTE on balancing the dataset. The standard and “only minority” SMOTE variants resulted in a fully balanced dataset, efficiently offsetting class domination and exploiting equality among normal and anomalous samples. However, the full balancing may present redundant synthetic patterns and an increase in overfitting risk, particularly when the original minority data are sparse. On other hand, the partial resampling strategies (80% and 60% of the majority class) created reasonable balancing levels, allowing the model to retain a further realistic class distribution while still refining minority representation, as shown in Fig. 2. These organized configurations are mainly beneficial when computational efficiency or generalization stability is a concern. Inclusive, the results show that SMOTE provides smooth balancing strategies that can be adjusted depending on the trade-off between performance robustness and overfitting in ARP traffic anomaly detection, where together sensitivity and reliability are important for precise system behavior modeling.

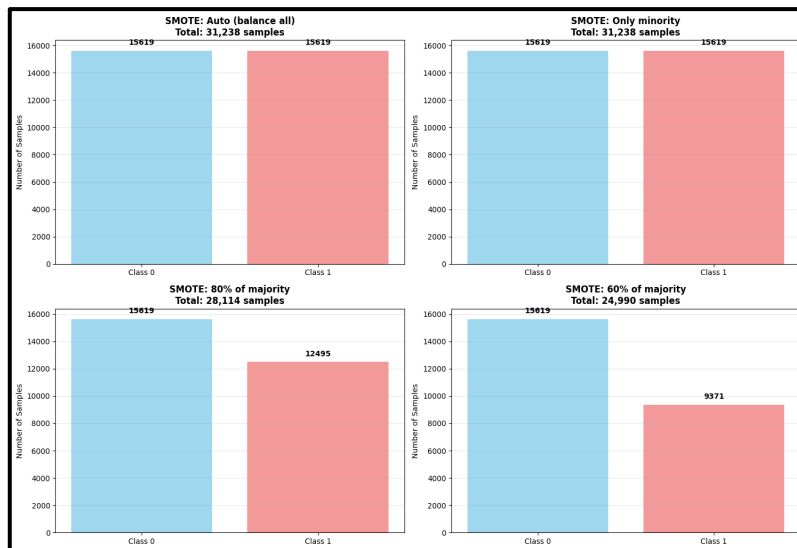


Fig. 2. comparative visualization of different SMOTE

During data encoding, categorical values are transformed into numerical representations using a one-hot encoder. The feature scaling phase ensures normalization using a standardization scaling approach. Finally, the dataset is partitioned into 75% training and 25% testing subsets.

3.2 Classification Metrics

3.2.1 Accuracy

Provides the proportion of precise predictions made by the model out of all predictions (Huang et al., 2021). It depends on 4 factors. For instance, the instances in spoofing attacks are correctly identified called true positives (TP). The legitimate network traffic is precisely recognized as a normal named true negative (TN). If the normal traffic is identified incorrectly as an attack while this is known as a false positive (FP) while a false negative (FN) indicates the spoofing attack would be undetected, as represented in Eq. (3).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (3)$$

3.2.2 Recall and Precision

Further analysis for the classification task would be provided by Recall and Precision (He & Zhang, 2023). Recall indicates the sensitivity and evaluates the model's performance to detect actual spoofing threats. It reduces the probabilities of missing attacks, see Eq. (4). Precision: Signifies the fraction of properly identified spoofing attempts out of all identified attacks. See Eq. (5).

$$Recall = \frac{\text{True Positive}}{\text{True Positive} + \text{False Negative}} \quad (4)$$

$$Precision = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}} \quad (5)$$

3.2.3 F1-Score

This metric indicates an effective trade-off between accurate threat recognition and decreasing misclassification errors (Fourure et al., 2021). See Eq. (6).

$$F\text{-Measure} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (6)$$

3.2.4 Confusion Matrix

This metric provides a structured interpretation of correct and incorrect predictions (Hairani et al., 2024) as shown in Fig. 3, and helps in performance tuning, and it consists of TP, TN, FN, and FP, as mentioned before.

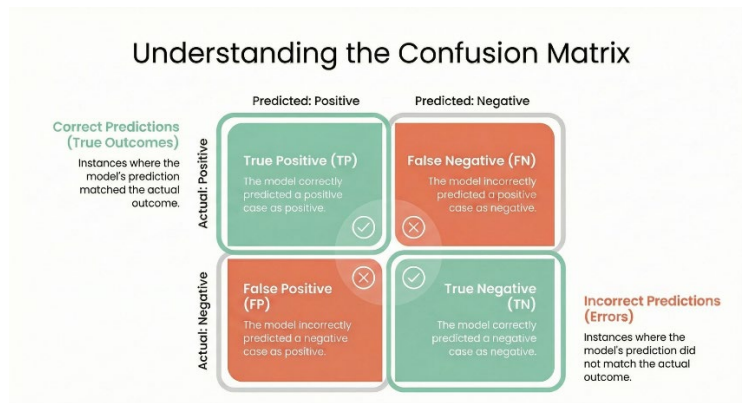


Figure 3. Confusion matrix

3.3 Main Method

The pipeline starts with a data preprocessing and preparation step that makes all the input features clean, normalized, and structurally compatible for Transformer learning. For example, the pipeline includes a full cleaning step to manage missing data and Null values. Then, the pipeline separates the feature set (X) and target variable (y). The features are normalized by mean and variance scaling (StandardScaler of scikit-learn library) (Testas, 2023). This normalization technique results in each real-valued feature having a mean of zero and a standard deviation of one, which is an important step for stabilizing gradient-based optimization as well as making features competitive. The dataset has categorical features and the TabTransformer model creates dense embedding projections, which involves changing the categorical tokens into continuous vector representations before feeding them into the Transformer encoder layers Lippi et al. (2025) and Alboalebrah and Al-augby, (2025). In this way, the model can learn rich feature interactions through categorical and numerical attributes to be a unified latent space Almedires et al. (2025) and Frederick and Ali (2024).

After that, the data is fed into a Stratified K-Fold Cross-Validation (CV) (Prusty, Patnaik & Dash, 2022) procedure to ensure fair and balanced evaluation through numerous subsets of the data. Then, each fold preserves the innovative label spreading since it's important during interaction with imbalanced classes, such as ARP traffic data. The model is trained and validated

with each fold in an independent form. This makes the calculation of stable and generalizable performance metrics. Mainly, the CV process is parameterized by the number of folds, the validation ratio, and the random seed to ensure reproducibility. The CV process is parameterized by the number of folds, the validation ratio, and the random seed to ensure reproducibility. The architecture for the proposed TabTransformer model is designed based on tabular data, as shown in Figure 4. It started with a feature projection layer to transform the input features into an embedding space of a fixed dimension (e.g., 48).

The positional encoding mechanism is employed to preserve the column order and feature relationships, mimicking the positional embedding used in sequence models. Mainly, the core consists of multiple Transformer encoder blocks, and each one comprises multi-head self-attention mechanisms and feed-forward sublayers. The attention heads (typically four per block) enable the model to detect local and global dependencies among input features, learning higher-order interactions that traditional ML algorithms such as Random Forests cannot easily model. The output from the encoder is aggregated and moved by a dense classification head, which has batch normalization and dropout regularization to crossover overfitting. The final dense layer outputs class probabilities by a sigmoid activation function, based on whether the task is binary classification. The training stage uses the Adam optimizer with an adaptive learning rate (default value of 3×10^{-4}) and employs early stopping to handle the overfitting by monitoring the validation F1-score. Furthermore, this study implements a class-weighting mechanism to counteract the class imbalance, ensuring the minority attack classes receive adequate gradient updates throughout optimization. The model also supports hybrid resampling by SMOTETomek for synthetic oversampling of minority classes mixed with underdamping of overlapping examples. The number of epochs (typically 20) and batch size (128) were used through the training phase. it has an automatic checkpointing to keep the best-performing models over validation performance.

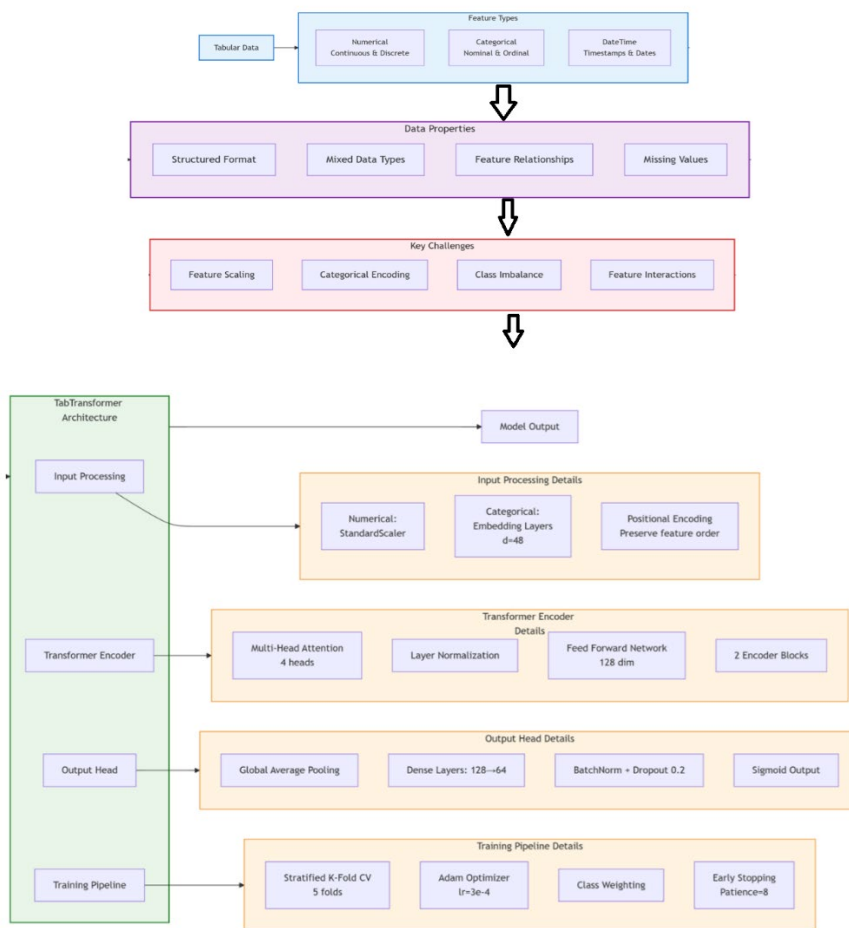


Fig. 4. The proposed model architecture.

Once the proposed model completes the cross-validation, the model is evaluated by some of the most popular performance metrics for each fold, such as accuracy, precision, recall, F1-score, and AUC, the maximization of F1-score can determine the optimal classification model. Furthermore, the model development supports explainability by SHAP-based on feature importance analysis, the analysis of model predictions among quantifying the contribution of every feature to the final classification output.

4. Result

Herein, the model performance to evaluate binary classification task, either spoofing attack or normal traffic. The quantitative results are reported based on some performance metrics that were mentioned above. Illustrate learning behavior through training/validation curves and a confusion matrix. This examination delivers a definitive assessment of the model's predictive competencies and error profile. The system configurations used for this research are presented in Table 2.

Table 2

System Environment

OS	Windows 11
Processor (CPU)	Intel Core i7-12700H (14 cores, 24MB cache)
Graphics Card (GPU)	NVIDIA RTX 3060 (6GB VRAM)
the Memory (RAM)	16GB DDR5 (4800 MHz)
The Environment	Anaconda, Python
The Frameworks	TensorFlow

Mainly, the proposed model shows a fruitful performance. For instance, the proposed model confirms an effective learning rate and robust generalization as demonstrated in Fig. 5.

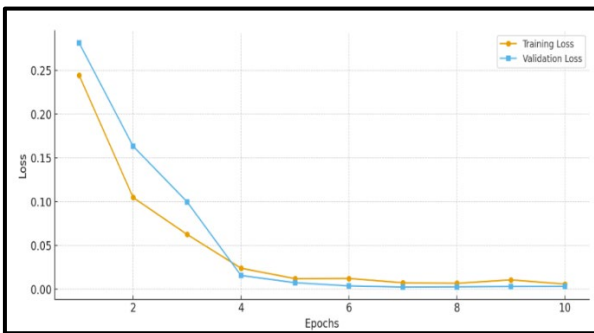


Fig. 5. The proposed Model Loss Exploration

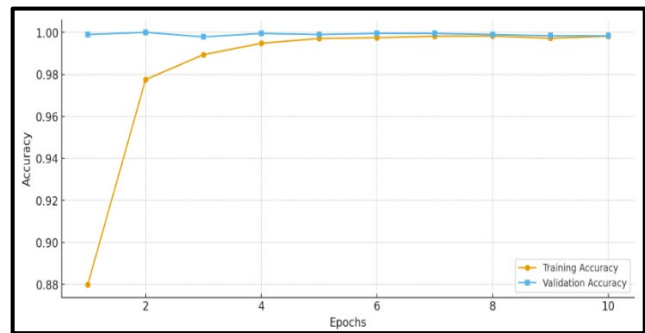


Fig. 6. The proposed Model Accuracy

The accuracy for the proposed model exceeds the 99.8% for training and validation. This demonstrates a stable and efficient learning. The model displays robustness by minimal fluctuation and no substantial overfitting as exposed in Fig. 6. Besides, the cross-validation outcomes are illustrated in Figure 6. It validates the strong generalization ability and robustness of the proposed model to the classification task. Across all folds, the model achieved exceptionally high scores in Accuracy, Precision, Recall, F1-score, and AUC, with mean values consistently exceeding 0.99 and minimal standard deviations. The high values (close to 1.0) indicate strong, stable model performance. As shown in Fig.7.

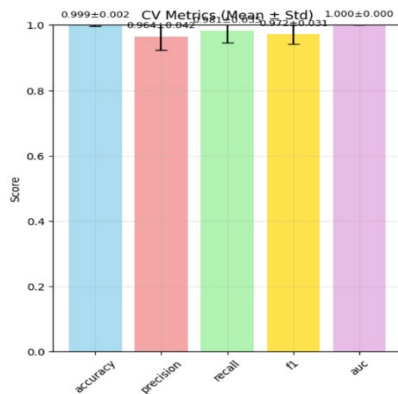


Fig. 7. average performance metrics across all folds of cross-validation, along with standard deviation error bars

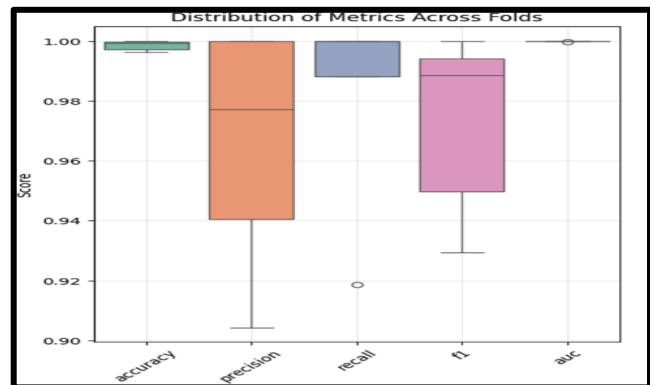


Fig. 8. Distribution of Metrics across Folds. The boxplot compares the variation of each metric across folds

The narrow boxes for accuracy and precision confirm low variability, suggesting that the model performs reliably across all subsets. As shown in Fig. 8. Slight variability in Recall or F1 could indicate mild differences in sensitivity to minority-class detection between folds as shown in Fig. 8. The narrow metric distributions and uniform heatmap patterns confirm that the model maintains stable predictive performance across data partitions, thereby reducing the risk of overfitting as illustrated in Fig. 9.

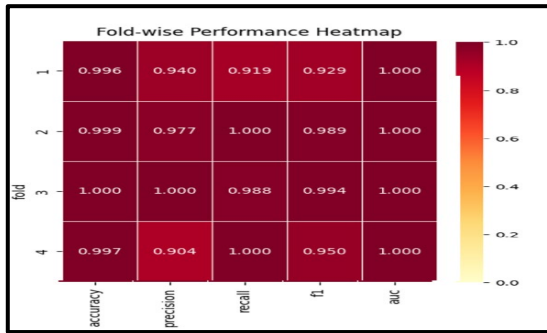


Fig. 9. Heatmap visualizes the per-fold values of each metric. Darker red shading corresponds to higher scores (near 1.0). All folds appear uniformly dark, reinforcing that each fold achieved excellent performance, and there are no weak folds

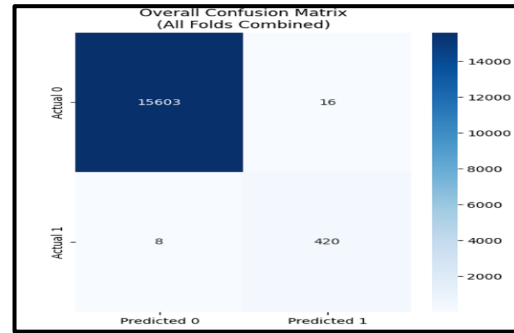


Fig. 10. Overall Confusion Matrix (All Folds Combined)

These results collectively indicate that the model effectively learns the distinguishing patterns of the data and generalizes well to unseen samples. Such performance dependability is mainly serious in security-sensitive field’s similar to ARP traffic analysis, where false negatives and false positives can have important effective influences. The combined confusion matrix illustrates a near-perfect separation among classes, with just some of misclassifications, the diagonal for the elements (true positives and true negatives) dominates, signifying very few misclassifications. Besides, the result shows the false positives (16) and false negatives (8) arise, providing high classification accuracy and balanced precision–recall trade-off as shown in Fig. 10. Also, the Receiver Operating Characteristic (ROC) curves for each fold are represented in Figure 11. Exploring the rates for the trade-off between true positive and false positive. Every curve closely follows the top-left corner, and the AUC values are near 1.0, showing exceptional discriminative ability. The steadiness through folds again validates robustness. So, the effectiveness and robustness of the proposed model for real-world deployment can be validated by the observed cross-validation performance.

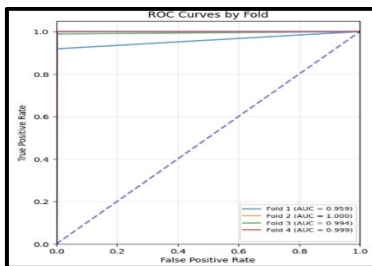


Fig. 11. ROC Curves by Fold

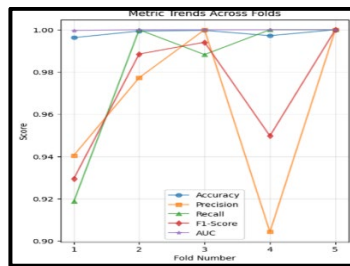


Fig. 12. Metrics Trends across Folds



Fig.13. The Cross-Validation per Fold

Fig. 12 shows the line chart that keeps track of the fluctuation for every metric through folds. The line projections are almost flat for the performance metrics such as Accuracy, Precision, and AUC. On the other hand, Recall and F1 confirm minor variations. These supplements illuminate model stability over different data splits. In addition, Fig. 13 explains the cross-validation metrics per Fold for the proposed model. The model established admirable overall performance through all assessed metrics, as represented in Table 3. It accomplished a high Recall of around 0.981, signifying its robust ability to suitably recognize positive cases, with a small standard deviation (Std) of 0.035. Also, Precision was robust at 0.964 std=0.041. These marks resulted in a joint F1-score of about 0.972, std=0.031. The model's discerning power is close to perfect, as presented by the mean AUC of 0.9999 with a remarkably tight std of 0.00015. Lastly, the mean of Accuracy was extremely high at 0.9985 std=0.0017, suggesting the model is greatly effective and consistent for the classification task.

Table 3
Cross-Validation Summary (Mean ± Std):

Index	mean	std
Recall	0.9813679890560876	0.0354536738496834
precision	0.9644008473795708	0.04150348901193609
f1	0.9723442044920134	0.031038788035094616
Auc	0.9999284914811591	0.0001495942293491638
accuracy	0.9985044787392157	0.0016690755906448376

In addition, both Table 4 and Fig. 14 demonstrate a comparison analysis between the proposed model and other models that are available in the literature.

Table 4
Performance metrics summarization among several models

Reference Number	Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
(Zachos et al., 2021)	Decision Tree, Random Forest, KNN	96.0	99.0	93.0	89.0
(Farooqui et al., 2023)	Hybridization (CNN-LSTM)	97.63	98.47	97.0	97.73
(Farooq et al., 2024)	CNN, RNN, LSTM, Fully Connected Networks	98.5	97.8	98.2	98.0
(Al-Hassani & Mohammed, 2023)	Gradient Boosting	96.5	96.0	96.0	95.0
(Prusty, Patnaik & Dash, 2022)	Support Vector Machine	95.85	95.0	95.0	94.78
(Kadhim & Al-Bahadili, 2024)	Deep Convolutional Neural (Deep-CNN1)	98.88	98.88	98.88	98.88
(Tauqeer et al., 2022)	Long Short-Term Memory (LSTM)	97.06	97.06	97.06	96.60
(Awotunde et al., 2024)	Deep learning + Feature Selection for Keylogger Detection	99.76	100	98.6	99.0
(Iqbal et al., 2024)	Deep Learning for GNSS Spoofing Detection (Real-time)	99.4	—	—	—
(Lourenço et al., 2025)	Ontology-based Layered Rule-based NIDS for Cybercrime	98.21	98.21	98.21	98.21
(Farooq et al., 2024)	Hybrid CNN-LSTM Architecture for IoT Threat Detection	99.0	—	—	—
—	The Proposed Model	99.85	96.33	98.13	97.22

Models analysis

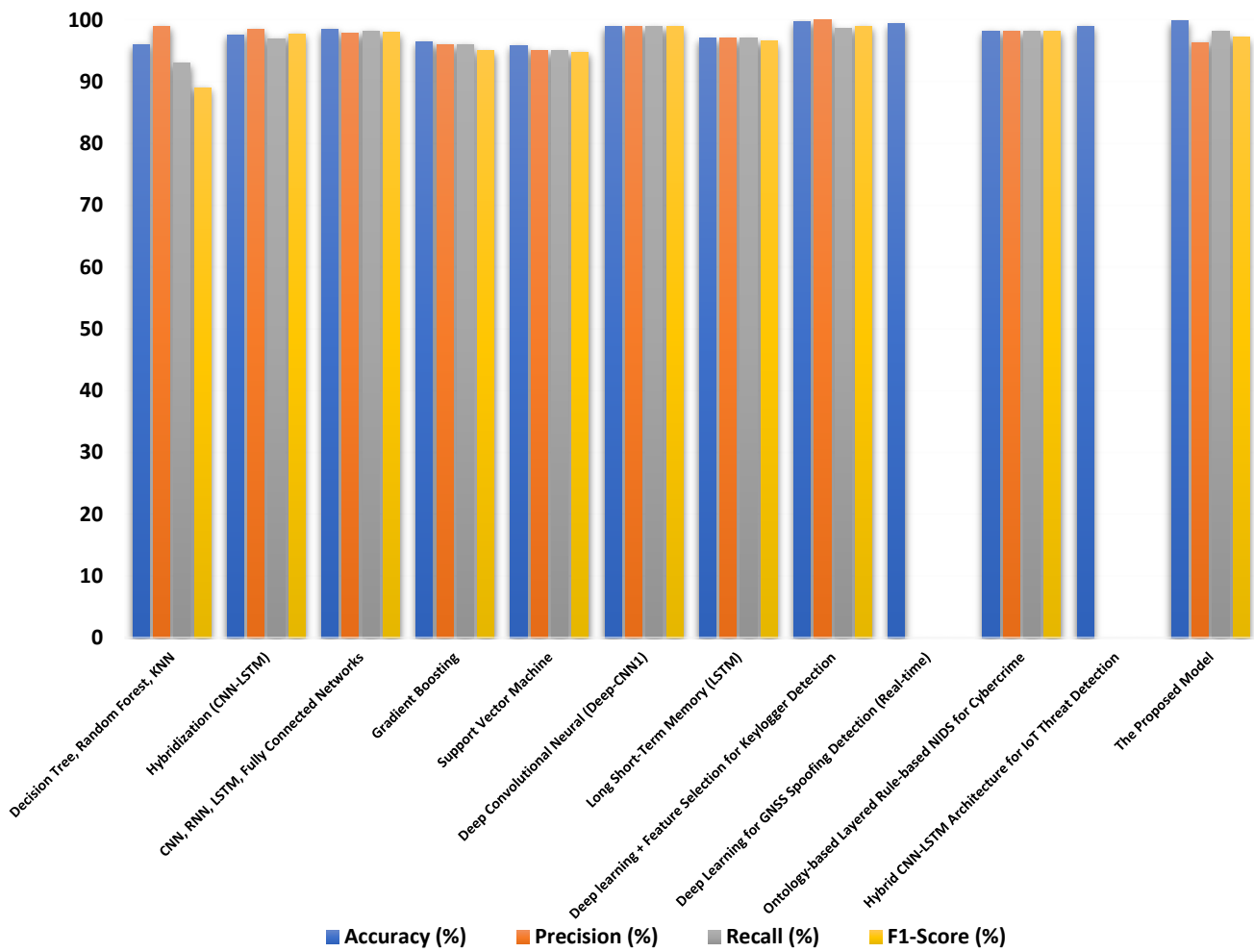


Fig. 14. Performance metrics visualization for several Models.

Conversely, although our binary classification method accomplishes robust overall detection performance, it does not differentiate between spoofing subtypes (e.g., IP, MAC, or biometric spoofing), which could exhibit different feature patterns. Future work will discover multiclass classification to address this granularity. While the TabTransformer provides robust detection performance, its routing-by-agreement process increases computational cost and memory use, which can limit scalability in real-time, resource-constrained IoMT systems. Future work will explore lightweight TabTransformer variants, compact routing repetitions, and optimization techniques like pruning and quantization to improve deployment feasibility

without compromising accuracy. Furthermore, the model would be employed in other fields such as (Al-Hassani & Mohammed, 2023) and (Kadhim & Al-Bahadili, 2024).

5. Conclusion

The proposed TabTransformer-based intrusion detection framework efficiently improves ARP spoofing detection. It employs positional encodings and self-attention mechanisms to model complex dependencies among network features. Over the incorporation of SMOTE-based data balancing and Stratified K-Fold validation, the model accomplishes exceptional performance, yielding a mean accuracy of 99.85% with robust consistency and minimal variance across folds. The employment for the SHAP interpretability explores the model's transparency and operational reliability, making it suitable for deployment in critical IoT and IoMT infrastructures. The inclusion of SHAP interpretability further establishes the model's transparency and operational reliability, so it becomes appropriate for utilization in critical IoT and IoMT infrastructures. Future research would employ this framework for multi-class spoofing detection to report diverse attack categories. Also, optimizing the computational efficiency of transformer layers through lightweight or quantized attention mechanisms will improve deployment feasibility on low-power IoT devices. Further research comprises temporal modeling of ARP traffic patterns and hybrid transformer-graph neural architectures to release contextual and relational dependencies, ultimately proceeding adaptive and intelligent intrusion detection systems for next-generation IoT ecosystems. The only existing drawback lies in its binary classification design, which can be extended to multi-class spoofing detection in future work.

Acknowledgment

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU260056).

References

- Abu Laila, D. (2025). Responsive Machine Learning Framework and Lightweight Utensil of Prevention of Evasion Attacks in the IoT-Based IDS. *STAP Journal of Security Risk Management*, 2025(1), 59–70.
- Addula, S. R., Norozpour, S., & Amin, M. (2025). Risk Assessment for Identifying Threats, vulnerabilities and countermeasures in Cloud Computing. *Jordanian Journal of Informatics and Computing*, 2025(1), 37-48.
- Adeniyi, A. E., Olorunfemi, B. O., Jimoh, R. G., Olagunju, M., & Awotunde, J. B. (2024). Integrating convolutional neural networks and long short-term memory for enhanced detection of glaucoma. In *Conference Organising Committee* (p. 350).
- Albinhamad, H., Alotibi, A., Alagnam, A., Almaiah, M., & Salloum, S. (2025). Vehicular Ad-hoc Networks (VANETs): A Key Enabler for Smart Transportation Systems and Challenges. *Jordanian Journal of Informatics and Computing*, 2025(1), 4-15.
- Alboalebrah, M. R., & Al-augby, S. (2025). Unveiling the causes of fatal road accidents in Iraq: An association rule mining approach using the Apriori algorithm. *Journal of Cyber Security and Risk Auditing*, 2025(2), 1-11.
- Al-Hassani, A., & Mohammed, S. (2023). A novel capsule network-based approach for detecting spoofing attacks in Internet of Medical Things systems. *Iraqi Journal for Computer Science and Mathematics*, 4, 45–56.
- Ali, A. (2024). Adaptive and Context-Aware Authentication Framework Using Edge AI and Blockchain in Future Vehicular Networks. *STAP Journal of Security Risk Management*, 2024(1), 45–56. <https://doi.org/10.63180/jsrm.thestap.2024.1.3>
- Almarshood, R., & Rahman, M. M. H. (2025). Enhancing Intrusion Detection Systems by Using Machine Learning in Smart Cities: Issues, Challenges and Future Research Direction. *STAP Journal of Security Risk Management*, 2025(1), 3–21.
- Almedires, M. A., Elkhilil, A., & Amin, M. (2025). Adversarial attack detection in industrial control systems using LSTM-based intrusion detection and black-box defense strategies. *Journal of Cyber Security and Risk Auditing*, 2025(3), 4-22.
- Al-Na'amneh, Q., Aljawarneh, M., Alhazaimeh, A. S., Hazaymih, R., & Shah, S. M. (2025). Securing Trust: Rule-Based Defense Against On/Off and Collusion Attacks in Cloud Environments. *STAP Journal of Security Risk Management*, 2025(1), 85–114. <https://doi.org/10.63180/jsrm.thestap.2025.1.5>
- Alshinwan, M., Memon, A. G., Ghanem, M. C., & Almaayah, M. (2025). Unsupervised text feature selection approach based on improved Prairie dog algorithm for the text clustering. *Jordanian Journal of Informatics and Computing*, 2025(1), 27-36.
- Amirruddin, A. D., Muharam, F. M., Ismail, M. H., Tan, N. P., & Ismail, M. F. (2022). Synthetic minority over-sampling technique (SMOTE) and logistic model tree-adaptive boosting algorithms for classifying imbalanced datasets. *Computers and Electronics in Agriculture*, 193, 106646.
- Ang, S., Ho, M., Huy, S., & Janarthanan, M. (2026). A Multi-Layered Adaptive Cybersecurity Framework for the Banking Sector Integrating Next-Gen Firewalls with AI-Driven IDPS. *STAP Journal of Security Risk Management*, 2026(1), 67–76. <https://doi.org/10.63180/jsrm.thestap.2026.1.4>
- Bhosale, K. S., Nenova, M., & Iliev, G. (2021). A study of cyber attacks in the healthcare sector. In *Proceedings of the Sixth Junior Conference on Lighting* (pp. 1–6). IEEE.

- Cabello-Solorzano, K., Ortigosa de Araujo, I., Peña, M., Correia, L., & Tallón-Ballesteros, A. J. (2023). The impact of data normalization on the accuracy of machine learning algorithms: A comparative analysis. In *International Conference on Soft Computing* (pp. 344–353). Springer.
- Davaran, A., Samual, J., Palansundram, K., & Ali, A. (2024). A Comprehensive Review of Machine Learning Approaches for Android Malware Detection. *Journal of Cyber Security and Risk Auditing*, 2024(1), 38–60.
- Elreedy, D., Atiya, A. F., & Kamalov, F. (2024). A theoretical distribution analysis of synthetic minority oversampling technique (SMOTE) for imbalanced learning. *Machine Learning*, 113(7), 4903–4923.
- Farooq, F., Mohammad, S. S., Nazir, N. A., & Shah, P. A. (2024). Happiness at work: A systematic literature review. *International Journal of Organizational Analysis*, 32(10), 2236–2255.
- Farooqui, M., Zaidat, O. O., Hassan, A. E., Quispe-Orozco, D., Petersen, N., Divani, A. A., & Ortega-Gutierrez, S. (2023). Functional and safety outcomes of carotid artery stenting and mechanical thrombectomy for large vessel occlusion ischemic stroke. *JAMA Network Open*, 6(3), e230736.
- Fourure, D., Javaid, M. U., Posocco, N., & Tihon, S. (2021). Anomaly detection: How to artificially increase your F1-score with a biased evaluation protocol. In *Joint European Conference on Machine Learning and Knowledge Discovery in Databases* (pp. 3–18). Springer.
- Frederick, N., & Ali, A. (2024). Enhancing DDoS Attack Detection and Mitigation in SDN Using Advanced Machine Learning Techniques. *Journal of Cyber Security and Risk Auditing*, 2024(1), 23–37.
- Gheni, H. Q., & Al-Yaseen, W. L. (2024). Using CICIoMT2024 dataset for improved intrusion detection. In *International Conference on Data Analytics & Management* (pp. 285–301). Springer Nature.
- Hairani, H., Widiyaningtyas, T., & Prasetya, D. D. (2024). Addressing class imbalance of health data: A systematic literature review on modified SMOTE strategies. *JOIV: International Journal on Informatics Visualization*, 8(3), 1310–1318.
- He, B., & Zhang, J. (2023). An association rule mining method based on named entity recognition and text classification. *Arabian Journal for Science and Engineering*, 48(2), 1503–1511.
- Huang, C., Li, S. X., Caraballo, C., Masoudi, F. A., Rumsfeld, J. S., Spertus, J. A., & Krumholz, H. M. (2021). Performance metrics for the comparative analysis of clinical risk prediction models employing machine learning. *Circulation: Cardiovascular Quality and Outcomes*, 14(10), e007526.
- Iqbal, A., Aman, M. N., & Sikdar, B. (2024). A deep learning-based induced GNSS spoof detection framework. *IEEE Transactions on Machine Learning in Communications and Networking*, 2, 457–478.
- Jaafar, H. S., Abed, A. A., & Al-Shareeda, M. A. (2026). A Secure Industrial Internet of Things (IIoT) Framework for Real-Time PI Control and Cloud-Integrated Industrial Monitoring. *STAP Journal of Security Risk Management*, 2026(1), 77–86. <https://doi.org/10.63180/jsrm.thestap.2026.1.5>
- Jayaraj, I. A., Shanmugam, B., Azam, S., & Thennadil, S. (2024). Detecting and localizing wireless spoofing attacks on the Internet of Medical Things. *Journal of Sensor and Actuator Networks*, 13(6), 72. <https://doi.org/10.3390/jsan13060072>
- Kadhim, R., & Al-Bahadili, H. (2024). Enhancing security in IoMT using deep learning: A capsule network framework for spoofing attack detection. *Iraqi Journal for Computer Science and Mathematics*, 5(1), 30–42.
- Kommisetty, P. D. N. K., Kuppala, B. M. S. R., & Buvvaji, H. V. (2022). Transforming cyber defense: Anomaly detection and predictive analytics for automated threat response. *International Journal of Engineering and Computer Science*, 11(8), 1–10.
- Lippi, G., Aljawarneh, M., Al-Na'amneh, Q., Hazaymih, R., & Dhomeja, L. D. (2025). Security and privacy challenges and solutions in autonomous driving systems: A comprehensive review. *Journal of Cyber Security and Risk Auditing*, 2025(3), 23–41.
- Lourenço, B., Adão, P., Ferreira, J. F., Marques, M. M., & Vaz, C. (2025). Structuring security: A survey of cybersecurity ontologies, semantic log processing, and LLM applications. *arXiv preprint arXiv:2510.16610*.
- Lv, Z., Ding, H., Wang, L., & Zou, Q. (2021). A convolutional neural network using dinucleotide one-hot encoder for identifying DNA N6-methyladenine sites in the rice genome. *Neurocomputing*, 422, 214–221.
- Majumder, S., Deb Barma, M. K., & Saha, A. (2025). ARP spoofing detection using machine learning classifiers: An experimental study. *Knowledge and Information Systems*, 67(1), 727–766.
- Mohammadpour, L., Ling, T. C., Liew, C. S., & Aryanfar, A. (2022). A survey of CNN-based network intrusion detection. *Applied Sciences*, 12(16), 8162.
- Newaz, A. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2021). A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. *ACM Transactions on Computing for Healthcare*, 2(3), 1–44. <https://doi.org/10.1145/3453175>
- Prusty, S., Patnaik, S., & Dash, S. K. (2022). SKCV: Stratified K-fold cross-validation on ML classifiers for predicting cervical cancer. *Frontiers in Nanotechnology*, 4, 972421.
- Rahmanzadehgervi, P., Nguyen, H. H., Liu, R., Mai, L., & Nguyen, A. T. (2025). TAB: Transformer attention bottlenecks enable user intervention and debugging in vision-language models. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*.
- Ramesh, H., Ismail, N., Abd Rahman, N. A., & Ali, A. (2026). PhishGuard: AI-Driven Graph-Based Analysis for Smarter Email Security. *STAP Journal of Security Risk Management*, 2026(1), 31–45. <https://doi.org/10.63180/jsrm.thestap.2026.1.2>
- Saheed, Y. K., & Arowolo, M. O. (2021). Efficient cyber attack detection on the Internet of Medical Things smart environment based on deep recurrent neural networks and machine learning algorithms. *IEEE Access*, 9, 161546–161554.

- Sharma, A., & Babbar, H. (2024). Preventing spoofing threats in IoT: Machine learning approaches for intrusion detection. In *Proceedings of the IEEE 3rd World Conference on Applied Intelligence and Computing (AIC)* (pp. 1267–1271). IEEE.
- Testas, A. (2023). Support vector machine classification with Pandas, scikit-learn, and PySpark. In *Distributed Machine Learning with PySpark* (pp. 259–280). Apress.
- Yadav, R., Pradeepa, P., Srinivasan, S., Rajora, C. S., & Rajalakshmi, R. (2024). A novel healthcare framework for ambient assisted living using the Internet of Medical Things (IoMT) and deep neural networks. *Measurement: Sensors*, 33, 101111. <https://doi.org/10.1016/j.measen.2024.101111>
- Zachos, G., Essop, I., Mantas, G., Porfyraakis, K., Ribeiro, J. C., & Rodriguez, J. (2021). An anomaly-based intrusion detection system for Internet of Medical Things networks. *Electronics*, 10(21), 2562.



© 2026 by the authors; licensee Growing Science, Canada. This is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (<http://creativecommons.org/licenses/by/4.0/>).