INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ORIGINAL ARTICLE

# Using Ensemble Model for Classifying Network Traffic Flow and Identifying Attacks in Smart City

**Sujata N Bhosle**[1]*, **Jayshri D Pagare**[2]

**1** Jawaharlal Nehru Engineering College, MGM University, Chh.Sambhajinagar, Maharashtra, India
**2** Jawaharlal Nehru Engineering College, MGM University, Chh.Sambhajinagar, Maharashtra, India

OPEN ACCESS

**Received:** 19/12/2025
**Accepted:** 26/01/2026
**Published:** 08/02/2026

**Citation:** Bhosle SN, Pagare JD (2026) Using Ensemble Model for Classifying Network Traffic Flow and Identifying Attacks in Smart City. Indian Journal of Science and Technology 19(5): 262-269. https://doi.org/10.17485/IJST/v19i5.1991

* **Corresponding author**.

magaresujata@rediffmail.com

**Funding:** None

**Competing Interests:** None



Published By Indian Society for Education and Environment (iSee)

**ISSN**
Print: 0974-6846
Electronic: 0974-5645

## Abstract

**Objectives:**Smart City generates the vast amount of data through sensors and actuators. Smart city consist of diverse data that rely on IoT which demands the effective intrusion detection system. Paper focuses on key mechanism of Quality of Service to provide the security. This study aims to provide light-weight solution to classify the network attack categories using a robust approach. **Methods**: To detect the exact type of attack we have employed the Multi-class classification on the NF-TON-IOT-v2 dataset. This is a critical area of research in network traffic classification, particularly for enhancing IoT security. Random Forest, KNN and Ensemble models have been applied to this dataset, demonstrating significant advancements in accuracy and efficiency. **Findings**: The proposed Ensemble Model approach offers efficient and accurate traffic classification to detect attacks on the network. System gives 96.45% results with Ensemble algorithm, whereas Random Forest and KNN gives the accuracy of 96.15% and 95.15% respectively. **Novelty:** Proposed Ensemble model were trained on only 14 features out of 43, which were identified by the hybrid feature importance method. Unlike other existing deep learning studies, our study minimized the overburden of model by reducing the dimensions while providing promising result for Multiclass Classification.

**Keywords:** Attack Detection; NF-TON-IoT; Traffic Classification; QoS; Security Mechanism; Ensemble Model; Net-flow; Intrusion Detection System

## 1 Introduction

Smart city generates vast amout of data through sensors, actuators and from multiple services. Data is in the heterogeneous form. Various interconnected devices are there in smart city networking. Thedata is flown in alsmost every sector like educational institute, smart grid, smart heathcare system, life style, shipment and fleet tracking. These data needs to be kept in secure environment[(1)]. Network Traffic classification is one way to analyze the malicious activity on the network. Multiple investigations have been done on IoT intrusion detection using the TON_IoT dataset and its variants;

however, a critical evaluation shows the existence of major constraints related to model generalizability, computational efficiency, and the support of multiclass attacks.

Authors[2] have proposed AdaBoost and RuSBoost models for two class classification on TON-ToT dataset.to detect DDoS attacks The AdaBoost classifier achieved a higher accuracy of 99.7% but with a slower prediction speed compared to RUSBoost (99.3%). Both classifiers were evaluated using the ToN-IoT dataset, which contains wide and diverse network data. The study focused on only DDoS Attack detection, this study needs extention to work on other attack categories.

The Paper[3] discusses a multiclass classification approach using XGBoost and CatBoost for category wise intrusion detection, They have used SHAP technique to identify and describe important features and oversampling techniques to handle imbalanced data.The result achieved using XGBoost with 0.8 variance threshold and SVM-SMOTE gives higher accuracy than other classifiers. They have identified Src_Port and Flow_Duration as important features using SHAP analysis. Apart from achieving good accuracy, proposed model can be partial towards synthetic samples due to their heavy oversampling approach.

The Paper[4] created TON_IoT dataset, which includes various normal and attack flows trapped for Telementary data, Operating system log data and Network traffic data for diverse IoT/IIoT services, evaluated using SVM, kNN, NB, RF, CART, Logistic Regression and LDA methods. They have evaluated result of ML methods for attack detection using IIoT datasets and introduced the medium-scale testbed for dataset generation.

The paper[5] focuses on a recent dataset, the TON_IoT network dataset, and that the stacking-ensemble model achieves a MCC score of 0.9909 and 0.9971 for multiclass classification and Two-class classification respectively.This approach has insufficient multiclass granularity. Authors have not explicitly interpreted the feature importance techniques used it their proposed work

The paper[6] employs a public dataset for IoT devices, specifically focusing on multi-class classification. It evaluates various machine learning classifiers, ultimately demonstrating that a meta-ensemble classifier using soft voting of the top three classifiers yields superior performance. Meta-ensemble classifier outperforms other models tested. Authors primary focus was on device identification and not the intrusion detection.

The study in[7] develops a multi-class classification model to identify newly added IoT devices, demonstrating effectiveness on a public dataset, achieving high accuracy, precision, recall, F1 score, and FPR values, thus enhancing attack detection and cyber security measures. This study classifies the IoT devices, authors have focused on sensitive devices only, ignoring the acual traffic flow for attack detection.

Authors[8] focuses on a multi-class classification approach using a deep ensemble model applied to the UNSW 2018 and IoT Botnet dataset for detecting IoT attacks. Their Deep ensemble model achieves 98.4% accuracy in detecting IoT attacks. They have evaluated model using F1 score, recall, and precision under ROC curve.Using an deep ensemble approach makes it computationally cost expensive which is not suitable for edge and fog nodes that are deployed in smart city.

## 2 Methodology

### 2.1 Data Collection

We have used NF-TON-IOT-V2 dataset[9] for our research purpose. Reason behind selecting it is that it consists of latest attacks related with the smart city and IOT devices and therefore this dataset is most suitable for our study. Dataset has records with normal and attack category distribution as shown in Figure 1. There are 9 attack categories in the dataset, consisting 95,34,597 records. Remaining 36,01,284 record are categorised as normal records. Our research is intended to classify network flow in the either normal or exact attack category. This dataset consist of variour heterogeneous and high dimensional data flow and such data flow needs to handle global patterns as well as local irregularities in the network flow. Global patterns can influence the network performance.

```
Attack
Benign        3601284
scanning      3002169
xss           2449955
ddos          1746590
password       993718
injection      660467
dos            654359
backdoor        16259
mitm             7723
ransomware       3357
Name: count, dtype: int64
```

**Fig 1.** NF-TON-IOT-V2 dataset statistic

## 2.2 Feature Importance and Identification

Feature Identification is the preliminary stage where we can select right attributes for our classification model, which will reduce overburden of irrelevant feature training that do not contribute in the classification. As the dataset is very large in the size, first we have calculated spearman correlation to find out correlated features and then applied SHAP method on the features identified by the spearman correlation..

### *2.2.1. Using Correlation Analysis*

To find out most correlated features, we have calculated spearman correlation. We have set value as 0.8 for correlated features. Based upon spearman corr, 23 features were dropped and stored in separate parquet file which is 83.1 in MB in size.

### *2.2.2. Using SHAP Method (Figure 2)*

To check the contribution of each feature in the classification process, we have then used SHAP method on 18 features excluding label. With the result of SHAP method we have identified 14 features that will improve accuracy of the classification and dropped the features having less contribution in the classification, namely 'RETRANSMITTED_OUT_PKTS', 'ICMP_IPV4_TYPE', 'DNS_TTL_ANSWER', 'FTP_COMMAND_RET_CODE'.

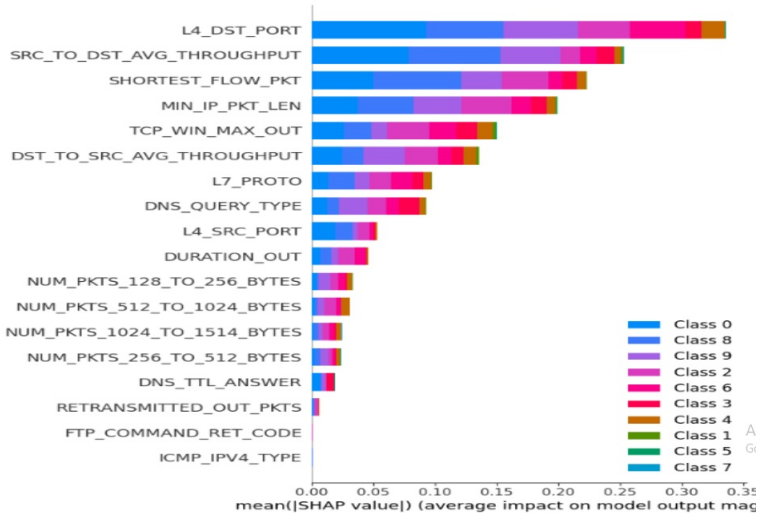


**Fig 2.** Feature Extraction using SHAP Analysis.

## 2.3 Proposed Methodology

In our earlier study[10], we have classified network flow in the Binary classification i.e. Benign and Attack category. Here we have extended our work to detect the exact attack category from netflow. The proposed model for multi-class classification is shown in the Figure 3. The proposed Ensemble model, Random Forest and KNN, is implemented to detect the attack category with 70:30 ratios of training and testing.

### *2.3.1. Random Forest Model*

The reason behind selecting Random Forest model is that it has robustsness to handle noisy, outlier data and high dimensional data as well as it has strong generalization capabilities. Random Forest does the strong multiclass discrimination due to improved generalization. This model reduces the overfitting issues by using Bagging and feature randomness. It can efficiently handle heterogeneous features without requiring substantial preprocessing.

### *2.3.2. k-Nearest Neighbor Classifier*

k-NN model complements RF model by handling local data structure. Class imbalance is there in the selected dataset where certain attack categories have less netflow, kNN will outperforms with such minority classes by focusing on neighborhood

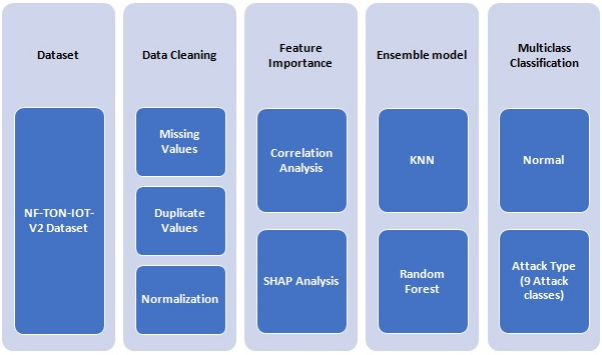


**Fig 3.** Proposed Methodology for Multiclass Classification.

similarity. kNN does not assume any prior statistical distribution and this nature will be helpful to deal with the irregular data flows.

### *2.3.3. Ensemble Model Classifier*

Random Forest lacks performance with the borderline data or minority data which are inadequately represented whereas k-NN model can be sensitive towards noisy data but it is computationaly very high. This gives us motivation to integrate these two model. Ensemble model of RF and knn can handle majority and minory classes by complementing each other.

## 2.4 Evaluation Metrics

To validate the performance of proposed model, accuracy alone is not sufficient evaluation metric. Our study is assessed based on Accuracy which provides the correctness, Precision which is false Alarm control, Recall which captures the actual positives and F1 score, which is balanced metric.

### *2.4.1. Precision*

Precision is the measure which ensures that model accuratelty indifies the type of attack. Figure 4 shows the comparison of precision of all three methods. Here, ensemble model gives the high precision rate than kNN. For MITM attack, KNN, RF and Ensemble model scores 0.69, 0.94 and 0.96 respectively. For ransomware attack KNN, RF and Ensemble model scores 0.84, 0.98 and 0.96 respectively. Ensemble model gives high precision score for Benign, backdoor, dos, injection and password category than kNN and RF model.

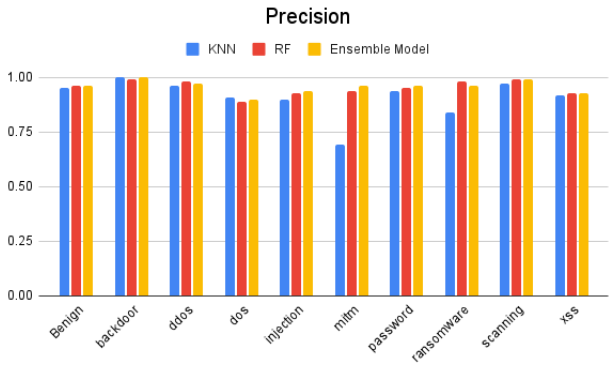


**Fig 4.** Precision comparison

### 2.4.2. Recall

Recall is he measure which identify the actual positive attack types classified by the model. To check the Figure 5 shows the comparison of KNN, RF and Ensemble method for Recall. In this figure we can analyze that kNN scores low in recall metric. Random forest and Ensemble model are good enough to score racall in almost every attack category except MiTM. For MiTM attack kNN, RF and Ensemble model scores 0.17, 0.33 and 0.31 respectively. .

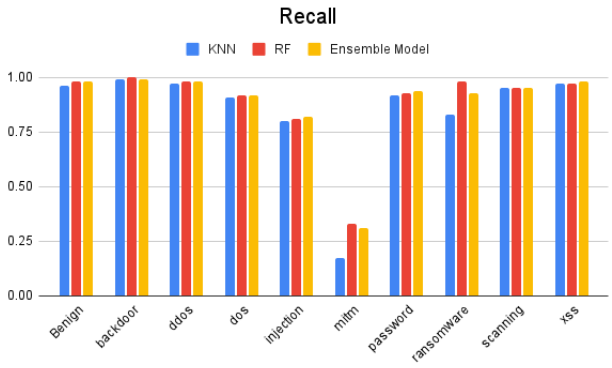


**Fig 5.** Recall comparison

### 2.4.3. F1-Score

F1-score is the measure which balances the precision and recall. Model's preciseness and comprehensiveness is ensured with the good F1-score. Figure 6 shows the comparison of KNN, RF and Ensemble method for F1-score.Ensemble model and RF model both got the f1-score as 1 for backdoor attack, 0.97 for benign, 0.98 for ddos, 0.91 for dos, 0.97 for scanning and 0.95 for xss attack whereas kNN scores low than both models.

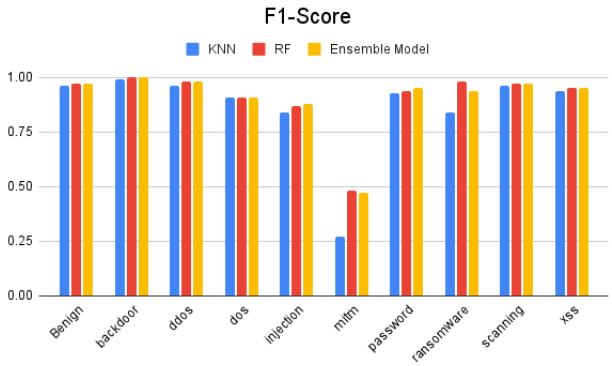


**Fig 6.** F1-score comparison

## 3 Results and Discussion

Experiment was conducted on the system 12th Gen Intel(R) Core(TM) i5 with a base frequency of 3.00 GHz, 16GB Ram and Jupyter notebook to do the Multiclass Classification on NF-TON-IOT-V2 dataset. This experiment identifies the exact type of Attack. In this study we have employed K-NN and Random Forest classifier. For Random Forest algorithm is generated with the 100 trees and depth of 20 which resulted in accuracy of 96.15%. For KNN classifier 13 neighbors with 20 jobs were selected for the classification. We have achieved the 95.15% accuracy for the KNN classifier.

Our study has implemented an Ensemble model of KNN and Random forest classifier. Ensemble classification Model achieved the Train accuracy of 96.45% and 95.90% Test Accuracy. The proposed system completed the build process in 1391

seconds. This Ensemble soft voting approach leverages the strengths of both algorithms Hybrid model votes for the best model while classifying in the attack category.

| | precision | recall | f1-score | support |
|---|---|---|---|---|
| Benign | 0.95 | 0.96 | 0.96 | 756712 |
| backdoor | 1.00 | 0.99 | 0.99 | 3360 |
| ddos | 0.96 | 0.97 | 0.96 | 367721 |
| dos | 0.91 | 0.91 | 0.91 | 137356 |
| injection | 0.90 | 0.80 | 0.84 | 138211 |
| mitm | 0.69 | 0.17 | 0.27 | 1561 |
| password | 0.94 | 0.92 | 0.93 | 208689 |
| ransomware | 0.84 | 0.83 | 0.84 | 690 |
| scanning | 0.97 | 0.95 | 0.96 | 629370 |
| xss | 0.92 | 0.97 | 0.94 | 514865 |
| accuracy | | | 0.95 | 2758535 |
| macro avg | 0.91 | 0.84 | 0.86 | 2758535 |
| weighted avg | 0.95 | 0.95 | 0.95 | 2758535 |

**Fig 7.** Classification Report of KNN Model

| | precision | recall | f1-score | support |
|---|---|---|---|---|
| Benign | 0.96 | 0.98 | 0.97 | 756712 |
| backdoor | 0.99 | 1.00 | 1.00 | 3360 |
| ddos | 0.98 | 0.98 | 0.98 | 367721 |
| dos | 0.89 | 0.92 | 0.91 | 137356 |
| injection | 0.93 | 0.81 | 0.87 | 138211 |
| mitm | 0.94 | 0.33 | 0.48 | 1561 |
| password | 0.95 | 0.93 | 0.94 | 208689 |
| ransomware | 0.98 | 0.98 | 0.98 | 690 |
| scanning | 0.99 | 0.95 | 0.97 | 629370 |
| xss | 0.93 | 0.97 | 0.95 | 514865 |
| accuracy | | | 0.96 | 2758535 |
| macro avg | 0.95 | 0.89 | 0.90 | 2758535 |
| weighted avg | 0.96 | 0.96 | 0.96 | 2758535 |



**Fig 8.** Classification Report of Random Forest Model

| | precision | recall | f1-score | support |
|---|---|---|---|---|
| Benign | 0.96 | 0.98 | 0.97 | 756712 |
| backdoor | 1.00 | 0.99 | 1.00 | 3360 |
| ddos | 0.97 | 0.98 | 0.98 | 367721 |
| dos | 0.90 | 0.92 | 0.91 | 137356 |
| injection | 0.94 | 0.82 | 0.88 | 138211 |
| mitm | 0.96 | 0.31 | 0.47 | 1561 |
| password | 0.96 | 0.94 | 0.95 | 208689 |
| ransomware | 0.96 | 0.93 | 0.94 | 690 |
| scanning | 0.99 | 0.95 | 0.97 | 629370 |
| xss | 0.93 | 0.98 | 0.95 | 514865 |
| accuracy | | | 0.96 | 2758535 |
| macro avg | 0.96 | 0.88 | 0.90 | 2758535 |
| weighted avg | 0.96 | 0.96 | 0.96 | 2758535 |

**Fig 9.** Classification Report of Ensemble Model

Figure 7, Figure 8 and Figure 9 show the classification report of KNN, RF and Ensemble model respectively. Here, we can analyze category wise precision improvement using Ensemble method. Macro average is the unweighted arithmetic mean of each class score. It provides the generalized performance of model.Weighted average shows the real world model performance with the imbalanced data. It is weighed with the frequency of instances or flows.Ensemble and RF model got the balanced and good weighted average. kNN model got the macro average 0.91,0.84 and 0.86 for precision, recall and f1 score respectively. Random Forest scores macro average as 0.95, 0.89 and Ensemble model scores macro average 0.96, 0.88 for precision and recall

respectively. Both RF and Ensemble model got 0.90 macro average for f1-score. kNN achieved 0.95 weighted average score which is lower than Rf and Ensemble model i.e. 0.96.

It necessary to validate models performance with existing studies. Table 1 shows the comparative result analysis of proposed model with existing studies. Table 2 compares TON-IOT datasets.

**Table 1.** Comparative result analysis of existing studies with different NIDS datasets

| Study | Dataset | Classification Approach | Result | Remarks |
|---|---|---|---|---|
| Nazir et al. [11] | CICIoT, IoT-23, N-BaIoT | Binary & Multiclass | Achieved accuracy: IoT23: 95% BaIoT: 99.9% CICIDS2017: 99.9% | Expensive Computation |
| Lilhore et al. [12] | Custom Smart City Dataset | Multiclass | Autoencoder model achieved 95% accuracy | Sensor network fusion is required |
| Zhao [13] | IoT23, Malimg | Binary | Achieved 96.1% accuracy | -Limited Explicability<br>-Low record in the dataset |
| Maasaoui et al. [14] | Mixed IoT Traffic | Binary & Multiclass | F1-score nearly 95% | Emphasizes scalability |
| El-Sayed et al. [15] | ACI Dataset | Multiclass | 99.85% accuracy | -Used Hybrid classifier<br>-Dataset Specific Tuning<br>-High computation complexity |
| Hooshmand et al. [16] | Smart Grid Traffic | Binary | 98.75% accuracy | It focuses on smart grid domain only |
| Shukla et al. [17] | NSL-KDD | Binary & Multiclass | Acc 97.37%<br>Precision 82%<br>Recall 77% | Used old dataset, model has to be validatde with the recent dataset |
| Proposed Ensemble of RF–KNN model | NF-TON-IoT-V2 | Multiclass | 96.45% accuracy | Computationally low cost,edge friendly and light-weight ensemble model |

**Table 2.** Comparative Result analysis on TON-IOT dataset

| Study | Accuracy | No. of records for Evaluation | No. of Selected Features | Observations |
|---|---|---|---|---|
| Poposed Ensemble Model | 96.45% | 39,40,765 | 14 | Provided Multiclass Classification with Class wise accuracy<br>Used Sufficient Records<br>Reduced number of features |
| Gad et al. [18] | 98.3% | 1,38,313 | 43 | Provided Multiclass Classification accuracy.<br>Class wise accuracy is not available<br>Used less number of records<br>Number of features are greater than our proposed study |
| M. Awad [19] | 98% | 44,18,916 | 17 | Provided Multiclass Classification accuracy.<br>Class wise accuracy is not available<br>Used Sufficient Records<br>Number of features are greater than our proposed study |

## 4 Conclusion

This study proposed a computationally efficient and robust Ensemble approach for classifying modern smart city network attacks using NF-TON-IOT-V2 dataset. Feature Extraction using Spearman correlation followed by SHAP analysis, identified the most important features that contributed in classifying cyber attacks and strengthen the classification. Random Forest and kNN together captures the global and local behavior of the traffic flow. An Ensemble model outperforms with the accuracy of 96.45% involving the classified flow in the exact attack category with the hybrid multiclass classifier. Comparative result

analysis as shown in Table 2 proves that proposed model's performs better than individual classifier and recent approaches. In the existing studies most of the authors have classified the result in binary class i.e. Normal and Abnormal flow.

Future study can be focused on improving the detection rate of MiTM attack, which will also contribute in achieving the higher accuracy of the model. Researcher should use Multiclass classification instead of simply classifying Normal and Abnormal Traffic. To tackle the cyber attacks, it is necessary that network admin should understand the type and behaviour of the attack. Although models are precise but attacks are growing day by day with the variance in the nature, there will be always need for network flow classification with recent data. In future, with the use of recent diverse-nature dataset such light weight ensemble model solution should be proposed. Feature Importance techniques plays the major role in dimensionality reduction. The proposed study is capable of protecting the data leakage of Smart cities.

## 5 Acknowledgements

The authors would like to thank the Jawaharlal Nehru Engineering College, MGM University for providing the infrastructure for this research.

## References

1) Magare SS, Dudhgaonkar AA, Kondekar SR. Security and Privacy Issues in Smart City: Threats and Their Countermeasures. In: Tamane SC, Dey N, Hassanien AE, editors. Security and Privacy Applications for Smart City Development;vol. 308 of Studies in Systems, Decision and Control. Cham. Springer. 2021. 10.1007/978-3-030-53149-2_3.
2) Chishti F, Rathee G. ToN-IOT Set: Classification and Prediction for DDoS Attacks using AdaBoost and RUSBoost. Greater Noida, India. 2023. 10.1109/ICACITE57410.2023.10183100.
3) Amierh Z, Hammad L, Qaddoura R, Al-Omari H, Faris H. A Multiclass Classification Approach for IoT Intrusion Detection Based on Feature Selection and Oversampling. In: Almomani I, Maglaras LA, Ferrag MA, Ayres N, editors. Cyber Malware. Security Informatics and Law Enforcement. Cham. Springer. 2024. 10.1007/978-3-031-34969-0_8.
4) Alsaedi A, Moustafa N, Tari Z, Mahmood A, Anwar A. TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems. *IEEE Access*. 2020;8:165130–165150. 10.1109/ACCESS.2020.3022862.
5) Guo G, Pan X, Liu H, Li F, Pei L, Hu K. An IoT Intrusion Detection System Based on TON IoT Network Dataset. Las Vegas, NV, USA. 2023. 10.1109/CCWC57344.2023.10099144.
6) Davrazos G, Panagiotakopoulos T, Kotsiantis S, Kameas A. IoT Device Identification Using a Meta-Ensemble Multi-Class Classifier. Volos, Greece. 2023. 10.1109/IISA59645.2023.10345911.
7) Wang H, Guo D, Wei J, Li J. A method of classifying IoT devices based on attack sensitivity. *Journal of Information Security and Applications*. 2024;82:103751. 10.1016/j.jisa.2024.103751.
8) Alrefaei A, Ilyas M. Ensemble Deep Learning Model based on Multi-Class Classification Technique to Detect Cyber Attacks in IoT Environment. Surakarta, Indonesia. 2024. 10.1109/SIML61815.2024.10578143.
9) Sarhan M, Layeghy S, Portmann M. Towards a Standard Feature Set for Network Intrusion Detection System. *Mobile Networks and Applications*. 2022;27(1-2):1–14. 10.1007/s11036-021-01843-0.
10) Bhosle SN, Pagare J. Detecting Network Attacks Using Decision Tree Classifier. 2025.
11) Nazir A, He J, Zhu N, Wajahat A, Ullah F, Qureshi S, et al. Empirical evaluation of ensemble learning and hybrid CNN-LSTM for IoT threat detection on heterogeneous datasets. *Journal of Supercomputing*. 2025;81:775. 10.1007/s11227-025-07255-1.
12) Lilhore UK, Simaiya S, Rahoof PP, Alroobaea R, Baqasah AM, Alsafyani M, et al. Advanced threat detection for smart cities through IoT sensor and network data integration with IoT-securefusion. *Journal of Wireless Communications and Networking*. 2025. 10.1186/s13638-025-02554-w.
13) Zhao Z. Digital security risk identification and model construction of smart city based on deep learning. *Scientific Reports*. 2025;15:25061. 10.1038/s41598-025-09894-z.
14) Maasaoui Z, Merzouki M, Battou A, Lbath A. A Scalable Framework for Real-Time Network Security Traffic Analysis and Attack Detection Using Machine and Deep Learning. *Platforms*. 2025;3:7. 10.3390/platforms3020007.
15) El-Sayed ME, Raj S, Vasudevan SK. Hybrid ensemble learning for flow-level IoT traffic classification using ACI dataset: Towards scalable and real-time threat detection. *Journal of Artificial Intelligence and Metaheuristics*. 2025;p. 1–18. 10.54216/JAIM.090201.
16) Hooshmand MK, Colleagues. Intrusion detection in smart grids using artificial intelligence-based ensemble modelling. *Cluster Computing*. 2025;28. Article 238. 10.1007/s10586-024-04964-9.
17) Shukla D, Bhushan K, Kant GS. Network traffic classification model using ensemble machine learning. *Journal of Information Systems Engineering and Management*. 2025;10(58s). Available from: https://jisem-journal.com/index.php/journal/article/view/12737?utm.
18) Gad A, Nashat A, Barkat T. Intrusion Detection System Using Machine Learning for Vehicular Ad Hoc Networks Based on ToN-IoT Dataset. *IEEE Access*. 2021;9:142206–142217. 10.1109/ACCESS.2021.3120626.
19) Awad M, Fraihat S, Salameh K, Redhaei AA. Examining the Suitability of NetFlow Features in Detecting IoT Network Intrusions. *Sensors*. 2022;22(16):6164. 10.3390/s22166164.