

وزارة
التعليم العالي والبحث العلمي
جامعة ميسان
كلية التربية الاساسية



مجلة ميسان للدراستات الأكاديمية

للعول الانسانية والاجتماعية والتطبيقية

**Misan Journal For Academic Studies
Humanities, Social and Applied Sciences**

ISSN (PRINT) 1994-697X

(Online)-2706-722X

ايلول 2026

العدد 59

المجلد 25

2026- SEP

59 Issue

25 vol

Misan Journal

مجلة ميسان للدراسات الأكاديمية

Misan Journal

مجلة ميسان للدراسات الاكاديمية
العلوم الانسانية والاجتماعية والتطبيقية
كلية التربية الاساسية/ جامعة ميسان

ايلول 2026

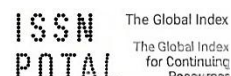
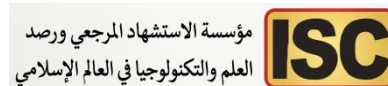
العدد 59

المجلد 25

2026 -SEP

59 Issue

25 Vole



رقم الايداع في المكتبة الوطنية العراقية 1326 لسنة 2009

journal.m.academy@uomisan.edu.iq

<https://www.misan-jas.com/index.php/ojs>

<https://iasj.rdd.edu.iq/journals/journal/view/298>

الصفحة	فهرس البحوث	ت
1_15	The Contrastive Values Between Voiced and Voiceless Sounds and Their Role in Ibn Arabi's Usage Enas Hamza Al-A'raji	1
16_41	Geographical Analysis of the Housing Crisis in Al-Maimouna City According to Population Growth: A Study of Causes and Remedies Aya Basim Saddam . Ahmed Syehood Hashim	2
42_64	Advertising and its Aesthetic and Expressive Vocabulary Ali Zair Rasan Al-Muzani , Muhsin Ali Hussein	3
65_76	A Reading of Polygamy between Islamic Legal Texts and Contemporary Transformations (An Analytical Study According to the Ja'fari School of Jurisprudence) Ali CHalloob Elalbl	4
77_91	The Representations of the Zionist Soldier in the Collection of Stories "My Short Stories" by Nachum Mendel Ammar Muhammad Hattab	5
92_107	The Relationship Between Genetic Mutations and Autism Spectrum Disorder: A Comprehensive Review Raghad Jabbar Abdul Sahib , Zahraa Qasim Mousa , Rehal Jehad Husain	6
108_121	The Reflection of Iraqi Reality in Feminist Poetry after 2003: A Study in Selected Models Hiba Salman Musa, Raad Hawir Sweilem	7
122_139	Humor and Seriousness in the Poetry of Ibn al-Mu'tazz Saja Jassim Mohammed	8
140_161	The Juristic Premises of Martyr Muḥammad Bāqir al-Sadr (A Study of the Most Significant Rijāl and Legal-Theoretical Opinions and Their Impact on Fatwā) Falah Abdul Hassan Hashem	9
162_175	The Mudarib's Entitlement to Expenses during Ḥaḍār: A Jurisprudential Study in Light of the Five Schools of Islamic Law Lamia Majid Dhahid Al-Hajjaji Ahmad Mortezaei Mohammad Amin-Fard	10
176_189	The Effect of Poetic Image Proliferation in the Diwan of Al-Khalidiyyayn Mahmoud Mohammed Allawi Jawad Al-Rawi	11
190_209	The Normative Level in Dr. Majid Al-Zamali's Al-Mustadrak 'alā Tadhkirat al-Kātib: An Analytical Study Murtadha Hamdan Ajib	12
210_229	The extent to which biology teachers possess TPACK skills and its relationship to their achievement motivation and future outlook Jaafar Khammat Jelow, Safaa Kamel Jaber, Mayada Abdel Sattar Abbas	13
230_248	Spatial and Temporal Variability of Groundwater Aquifer Properties in Eastern Maysan Governorate, Southern Iraq. Ahmed M. Hashoosh , Alaa M. Al-Abadi	14

249_260	Influence of Boswellic Acid on Enamel Microhardness in Initial Caries Lesions: An in Vitro Study Roa'a Jamal Abdulameer , Nada Jafer Mohammed Hassan Radhi	15
261_278	A Comparative Analysis of Sedentary Behavior and Dietary Behavior in Relation to Dental Caries Among Resistance Trained Men Sarah Bassil Abdulwhid , Alhan Ahmed Qasim	16
279_284	Semantic Challenges in Translating Road Signs Falah Hussein Hanoon Al-Sari	17
285_299	Macroeconomic Indicators: Iraq and the Dynamics of Oil and Conflict in the Arabian Gulf the Impact of Regional Wars (1950–2000) Dhifaf Mahdi Hasson	18
300_320	Characterization and Classification of Soils in Al-Muwafaqiyah and Al-Dujaili Areas within Al-Kut District, Wasit Governorate, and Evaluation of Their Agricultural Suitability Hasanain Mohammed Mahmood Alabooda	19
321_332	Deciphering the Unfamiliar: Generational Conflict and Cultural Transformation in the Novels of Jhumpa Lahiri Hussein Mnahi Munshid	20
333_355	Neuro-Symbolic and Federated Learning for Privacy-Preserving Intrusion Detection Marwah Najm Mansoor, Manar Hasan Ali Al-Malik, Hanan Falah Mohammed Taif talal Alwakeel	21
356_380	The Error Analysis two-dimension nonlinear convection diffusion problem by using Crank- Nicolson Petrov Weak Galerkin Wafaa S. Mohammed	22
381_400	Green Spectrophotometric and RP-HPLC Methods for the Quantification of Cefdinir in Pharmaceutical Formulations: A Comprehensive Review Abdalrhman Saad Abdaljaber Lamya A. Sarsam	23
401_415	Comparative evaluation of the efficiency of Endophytic Aspergillus and Penicillium spp. for gold nanoparticles biosynthesis Azhar Mohammed Alewi	24

ISSN (Print) 1994-697X
ISSN (Online) 2706-722X

DOI: <https://doi.org/10.54633/2333-025-059-021>

Received:2/May/2026
Accepted:22/June/2026
Published online:30/Sep/2026



MJAS: Humanities, Social and Applied
Sciences
Publishers
The university of Misan.
College of Basic Education This article is an
open access article distributed under the terms
and conditions of the Creative Commons
Attribution

(CC BY NC ND 4.0)
<https://creativecommons.org/licenses/by-nc-nd/4.0/>

Neuro-Symbolic and Federated Learning for Privacy-Preserving Intrusion Detection

Marwah Najm Mansoor ^{1*}, Manar Hasan Ali Al-
Maliki ², Hanan Falah Mohammed ³ Taif talal
Alwakeel ⁴

¹Graduate Studies Department, Research and Development
Division, Ministry of Higher Education and Scientific Research,
Baghdad, Iraq.

¹Email: marwah.najim@moheer.edu.iq <https://orcid.org/0009-0009-9475-1457>.

²Department of Communications Engineering, College of
Engineering, University of Information Technology and
Communications, Baghdad, Iraq.

²Email: manar.hassan@uoitc.edu.iq

³Graduate Studies Department, Research and Development
Division, Ministry of Higher Education and Scientific Research,
Baghdad, Iraq.

³Email: hanan.falah@moheer.edu.iq

⁴Graduate Studies Department, Research and Development
Division, Ministry of Higher Education and Scientific Research,
Baghdad, Iraq.

⁴Email: taifalwakeel118@gmail.com

Abstract

The concept of artificial intelligence (AI) has established itself as a foundation of contemporary intrusion detection systems because it can examine the network traffic on a large scale and detect sophisticated attack patterns. Nevertheless, the issues of data privacy, interpretability, and class imbalance still remain as the hindrances to

the efficiency of the available solutions. The paper performs a detailed experimental analysis of six AI-based intrusion detection models, Logistic Regression (LR), Decision Tree (DT), Random Forest (RF), Artificial Neural Networks (ANN), Federated Learning (FL) and Neuro-Symbolic Artificial Intelligence (NSAI) on the CICIDS2017 dataset within a single framework of pre-processing and evaluation. The findings show that the tree-based models (RF and DT) exhibit the highest overall performance (0.9985), which is why they are appropriate in resource-limited and high-speed settings. The Artificial Neural Networks are suitable in the nonlinear pattern of traffic with a precision of about 0.9880. On competitive performance ([0.9838]), Federated Learning achieves competitive performance and obtains data privacy only with decentralized training, which is suitable in collaborative and

privacy-conscious environments. Importantly, Neuro-Symbolic AI model has a high accuracy/interpretability/robustness balance, as it has better recall and F1-score with the minority and complex attack classes. These results suggest that there is no universally best model but instead the option of intrusion detection methodology depends on specific operational needs such as detection reliability, computing efficiency, and privacy limits. The research is practically applicable in choosing AI-based models of intrusion detectors in the actual world of cybersecurity.

Keywords: Artificial Intelligence (AI), Intrusion Detection Systems (IDS), Federated Learning (FL), Neuro-Symbolic Artificial Intelligence (NSAI), Data Privacy, Cybersecurity.

1. Introduction

The digital infrastructure and network technologies have rapidly evolved, and the complexity of cyberattacks as well as their frequency has increased dramatically (Li *et al.*, 2020). Network systems in modern organization are becoming more susceptible to advanced cyberattacks to exchange data and deliver services (Hasan, Al-Maliki and Jasim, 2022). The old fashioned intrusion detection can be based on signatures or fixed rules, failing to identify new attacks or advanced attacks (Devlin, Parkin and Janssen, no date). For this reason, AI technology has become a vital tool for cyber security purposes owing to its capability of handling large amounts of network information and recognizing sophisticated behavior patterns. Recent studies have shown that machine learning and deep learning can increase the efficiency of intrusion detection systems. For instance (Al-Hammash, M. S. H., & Maarouf, 2024) developed a network threat detection model that incorporates machine learning and feature selection to simplify data analysis, and this technique works effectively with tabled data structures. The use of artificial neural networks has also gained broad usage since it reveals nonlinear relations between network data. The usage of these models, however, presents an issue of privacy of data, since it would involve the collection and integration of sensitive data through several sources (Sharafaldin, Lashkari and Ghorbani, 2018).

Unified learning has appeared to be a new approach to privacy protection since it is possible to train models collaboratively with multiple parties without sharing raw data (Marra, 2024). This method will be based on the training model at the local entity level and then integrating the weights to have a complete one (Wan *et al.*, 2024). Although this approach has some benefits in terms of data protection, it has been faced with a number of challenges ; unequal spread of data among the clients, the different nature of the data, and the cost of communication between the involved parties (Chen *et al.*, 2024). Symbolic neural artificial intelligence is another developing trend which is a combination of neural learning and symbolic inference. Neural networks have high ability to derive patterns and features in data whereas symbolic inference makes the decisions more interpretable as well as better in predicting them using logical rules and domain knowledge (Hitzler *et al.*, 2022). Research has indicated that such a combination can work well in identifying rare or unbalanced attacks in network data. Nonetheless, there are limited studies, which experimentally compare symbolic neural models with traditional models and unified learning in a standardized testing setup (Renkhoff *et al.*, 2024). In spite of numerous works devoted to machine learning, deep learning, unified learning, and symbolic neural intelligence independently, the quantity of works giving a comprehensive comparative analysis of these methods. However, when identical data are used, the range of possible preprocessing methods and metrics is still constrained. Additionally, it will be essential to explore the correlation between the interpretability of a particular model, its

ability to detect any possible threats, and the applied protective measures within IDS (Tarek & Abdelrahman, 2025). On the other hand, it has been shown by (Younus, Y. M., Ibraheem, A. S., Tuama, M. H., & Mashloosh, 2025) that a properly set machine learning model can be used to forecast DoS attack scenarios; hence, a need for framework analysis emerges.

The outputs of this study are as follows: Offering a single comparative platform to assess the traditional machine learning models, neural networks, unified learning, and symbolic neural intelligence on the basis of the same preprocessing environment and benchmarks. Compiling the association among detection accuracy, model interpretability and privacy protection of intrusion detection systems. Comparing the capacity of symbolic neural intelligence to identify the occurrence of rare attacks and assessing the capacity of generalization in comparison to centralized and distributed models. The study is organized into the following sections: Section 2 will review the past research on intrusion detection systems and privacy preserving learning techniques; Section 3 will detail the research methodology, dataset, pre-processing processes, and model architecture; Section 4 will present the experimental findings; Section 5 will include a discussion and analysis and finally, Section 6 will give its conclusion and research suggestions.

○ Research Problem

Even though the techniques of artificial intelligence have made great advancements for intrusion detection systems, yet some issues have not been resolved yet. The research work done till now has mostly emphasized either machine learning, or deep learning, or federated learning or neuro-symbolic techniques independently. But the issue is that no comparative experiment has been conducted in an equal setting till now. Moreover, the datasets used for intrusion detection like CICIDS2017 are known to have problems of class imbalance since there are attack classes that appear only infrequently in the dataset. In addition to this problem, balancing between accuracy of the intrusion detection models, interpretability of the machine learning algorithm, computational cost, and privacy is another huge challenge in today's intrusion detection systems. Therefore, the research focuses on evaluating the differences between traditional machine learning algorithms, deep learning algorithms, federated learning, and neuro-symbolic artificial intelligence based on their effectiveness in detection, preserving the privacy, and their interpretability, using one common experimental environment and CICIDS2017 dataset.

1.2 Research Theories

The development of these hypotheses relied on the past research that showed that models vary in terms of their capacity to achieve accuracy, interpretability, and privacy protection.

First Hypothesis: The hypothesis of this study is that deep learning models that are implemented using artificial neural networks (ANNs) perform better than their traditional machine learning counterparts in identifying complex attack patterns as measured using common performance measures like accuracy, recall and F1.

Second Hypothesis: The hypothesis in this study is that a federated learning model can reach the level of performance comparable to that of centralized learning models, at the same time being able to preserve data privacy as a result of training the model in a distributed fashion without exchanging the raw data between participating entities.

Third Hypothesis: This paper has a hypothesis that symbolic neural AI can strike a balance between the detection rate and interpretability, and it is likely to work better at detecting infrequent attacks than other neural networks.

2. Literature Review

A systematic review of machine learning models, offering effective and balanced solutions to the challenges and obstacles facing various aspects of modern cybersecurity (Tarek and Abdelrahman, 2025). A comprehensive analysis of the model demonstrated superiority in achieving high detection accuracy, ensuring robust privacy protection, and enhancing resilience against hostile threats. Therefore, leveraging the strengths of hybrid AI systems is crucial for translating the potential of quantitatively enhanced machine learning into widespread cybersecurity solutions (Moussaoui and Kmiti, 2025).

The surge in research activity since 2020, reflecting a growing recognition of the importance of integrating symbolic approaches to enhance AI's and reasoning capabilities. The paper identifies current gaps in the symbolic AI literature, finding that most research between 2020 and 2024 concentrated on learning and reasoning, with a significant portion also dedicated to logic, inference, and knowledge representation (Colelough and Regli, 2024).

A comprehensive overview of decentralized symbolic neural cognitive systems, outlining their foundations, concepts, structure, and operation. First, they offer a systematic design of layered structures representing cognitive interfaces, causal guidance, cognitive capsules, cognitive registers, and memory systems, demonstrating how neural and symbolic elements can interact securely. Second, they introduce governance innovations: the Neuro conflict resolution protocol and a "no-knowledge" validation mechanism that ensures auditability, transparency, and normative integrity. Third, they demonstrate how these principles can be implemented in areas such as finance and healthcare. Fourth, they highlight the system's relative advantages in terms of robustness, scalability, and interpretability compared to traditional models, demonstrating their success in providing a model for transformative and responsible artificial intelligence (Oyebode, 2025).

This study stratifies some algorithms to the CICIDS 2017 dataset. According to the results, random forests outperformed decision trees with an accuracy of 99%, while neural networks were particularly good at spotting intricate assault patterns. Class imbalance issues were noted since the volume of attack instances was lower than the volume of typical traffic (Chavan and Alone, 2025). Another study along similar lines have been carried out by (Agheeb Al-Hamdawae, 2025), who suggested an intrusion detection system for IoT-based networks based on machine learning classification techniques coupled with feature selection algorithms such as RFE and PSO. From the results, it can be noted that feature selection techniques significantly improved the performance of the classifier in terms of accuracy as well as model complexity.

As shown

in table 1 which summarized previous studies.

TABLE 1. SUMMARY OF FL-BASED IDS STUDIES

Authors & Year	Dataset	Algorithms / Technique	Key Findings	Challenges / Notes
J. Moussaoui et al.,2025	Multiple	A comprehensive, integrated analysis of hybrid models combining FL, ML, and DL, focusing on evaluation metrics such as specificity, accuracy, robustness, scalability, and interpretability.	The results showed that hybrid models achieve higher performance compared to single-model models.	The systematic review was limited to articles between 2015–2024, and this limits generalization.
B.Colelough et al.,2025	Multiple	Analysis of 1,428 research papers in areas such as reasoning, learning, and logic using a systematic analysis (PRISMA).	The majority of the research focused on reasoning and learning.	It recommends a deep integration of learning, logic, transparency, and knowledge for effective progress.
2025	Multiple	federated cognitive capsules	Architectural Framework for an AI System that Integrates Connectivity, Symbolism, and Learning with Governance	Architectural Challenges of More Autonomous Systems in Symbolic-Neural AI
P.V. Chavan et al., 2025	CICIDS2017	Logistic Regression, Decision Tree, Random Forest, ANN	Random Forest achieved 99% accuracy; ANN performed well in detecting complex attack patterns	Class imbalance: normal traffic much higher than attack types
D.M.Jimenez, et al., 2025	Multiple	FL, Personalized Learning, Differential Privacy	Explains core principles of mobile and federated learning; multiple applications	Non-IID data; device & system heterogeneity; communication costs
M.Tarek, et al.,2025	CICIDS2017	Random Forest, Decision Tree	High accuracy and consistent performance	Some minor attacks not detected well; class

				imbalance needs addressing
B.B.S, 2025	UNSW-NB15, CSE-CIC-IDS2018	Random Forest, Deep Neural Networks	RF accuracy; DNN better for complex patterns	Difficult to interpret DNN; requires precise hyperparameter tuning
A.Mathur, et al.,2025	Multiple	FL, LoRA, Adapters	Better balance between performance and efficiency with subcomponent adaptation	Privacy & security issues not fully addressed; limited practical healthcare implementations
Huynh T. T. Tran et al., 2025	CICIDS2017 & other IDS datasets	Neuro-Symbolic AI + Transfer Learning	Transfer learning improves detection accuracy, especially on incomplete/unbalanced data; allows generalization across networks	Requires careful tuning of transfer strategies; longer training time
Huynh T. T. Tran et al., 2025	CICIDS2017	Neuro-Symbolic AI + Feature Extraction + XGBoost	Hybrid approach enhances reliability, generalization, and accuracy on rare or complex attacks	High computational resources; complex architecture for large-scale datasets
B.Liu, et al., 2024	Multiple	Federated Learning	Train shared model while preserving privacy	Privacy vulnerabilities; potential compromise of client data
F.Adjewa, et al., 2024	Multiple, 5G Edge Data	Federated Learning, BERT	97.79% accuracy; model size reduced 28.74% with 0.02% accuracy loss	Non-IID data handling; optimized for resource-limited edge devices
K.Daly, et al.,	CICIDS20	Federated Learning	Performance close	Data

2024	17, Edge-IoTset		to centralized models while preserving privacy	distribution & heterogeneity affect training speed & accuracy
A. Piplai et al., 2023	Cybersecurity datasets (simulated /real	Neuro-Symbolic AI	Combines deep neural networks with symbolic reasoning; improves interpretability and decision reliability in IDS	High computational cost; increased complexity with more symbolic rules
G.Cascavilla, et al.,2021	NSL-KDD, UNSW-NB15, CICIDS2017	Federated Learning, Random Forest	Federated model outperformed local RF models per client	Managing multiple datasets & local client variations
N.Gupta, et al.,2021	CICIDS2017	Federated Learning	Performance close to centralized models while preserving privacy	Communication between users & building a federated system

The study looks at the general architecture of mobile learning and communication protocols, covering important problems such non-independent and identically distributed data (non-IID), privacy concerns, device and system heterogeneity, and connectivity costs. The paper investigates a range of federated learning (FL) and personalized learning (PL) strategies with various applications, encompassing quantum computing and reinforcement learning. Additionally, it examines real-world applications, reference datasets, and important assessment criteria (Jimenez-Gutierrez *et al.*, 2025).

This research paper reviews some successful applications of federated learning and focuses on its importance as a valuable and distinctive tool for preserving privacy by training a model without sharing the original data. It also highlights the current vulnerabilities of these attacks and identifies the circumstances under which client privacy can be compromised (Liu *et al.*, 2024).

In this paper, the researchers used RF and DT algorithms on the CICIDS2017 dataset after selecting important features. The results demonstrated the need to address data imbalance. The results also demonstrated high accuracy and consistent performance, but some small numbers of attacks were not well identified.

In this paper, the researchers used Random Forest and Deep Neural Networks algorithms on the UNSW-NB15 and CSE-CIC-IDS2018 datasets. Random Forest achieved an accuracy of 98–99%, while neural networks performed better in recognizing complex patterns, but were difficult to interpret and required precise hyperparameter tuning(S, 2025).

This study systematically classifies research on federated learning models according to the model cycle, encompassing training, modification, and deployment. The researchers classified the

approaches in this work according to technical criteria encompassing complexity, efficiency, and scalability. They eventually established that techniques involving the adaptation of model subcomponents yield a superior equilibrium between performance and efficiency in comparison to comprehensive model training. They also disclosed deficiencies with privacy and security that remain inadequately addressed in existing methodologies, and there is a scarcity of practical implementations of experimental models within the healthcare sector (Mathur, Gupta and Das, 2025). This research discusses a neuro-symbolic AI architecture designed for network intrusion detection and demonstrates how selective learning can enhance the system's threat detection efficiency, particularly in contexts with unbalanced or insufficient data. This paper offers a neuro-symbolic artificial intelligence system that mixes deep pooling for feature extraction with symbolic inference via XGBoost. The study explains how the combination can improve the system dependability (Tran *et al.*, 2025).

This study presents a potent intrusion detection system (IDS). The concept was based on the BERT paradigm, which is intended to detect harmful network activities. The model has been refined. There are two different environments: (1) a space-centric environment, where an inference accuracy of around 97.79% was attained; and (2) federated learning employing dispersed, non-independent, non-identical (non-IID) data. The model's size was reduced by 28.74% and its accuracy 0.02% based on the findings. Large models like BERT are suitable for edge scenarios in 5G networks that leverage federated learning while preserving high efficiency and privacy (Adjewa, Esseghir and Merghem-Boulahia, 2024).

The researchers used the CICIDS2017 and Edge-IoT set datasets, with Federated Learning. The challenges were the variety and distribution of data among clients, which affected training time and accuracy while protecting data privacy (Daly *et al.*, 2024). The research indicates that combination enhances the capacity to manage unexpected circumstances, and improves the accuracy of judgment in challenging circumstances (Piplai *et al.*, 2023). The studies were conducted using four KDD datasets (NSL-KDD, UNSW-NB15, and CIC-IDS-2017). The findings demonstrated that in tasks involving both detection and classification, the federated model performed better for each client than the locally built Random Forest models (Cascavilla *et al.*, 2021). The researchers applied federated learning primarily to the CICIDS2017 dataset. The main challenges were communication between participating users and the complexity of developing a federated system (Gupta, Jindal and Bedi, 2022), (Tran *et al.*, 2025). Fewer research has fully evaluated federated, deep learning, and conventional techniques under the same experimental settings. The goal of this study is to close that gap.

3. Methodology

This section explains the dataset and the kind of the attacks that were resorted to during the experiments. The pre-processing part gives the procedure utilized in the transformation of the data to be challenges and segments so that it fits the machine learning models. The models used are also described in detail, such as the traditional machine learning models, neural networks, federated learning and the neural symbolic AI model. Lastly, the evaluation metrics which are applied to measure and compare the model performances in an experimental setting are explained part highlights the way of description dataset preparation procedures, model architectures, and training procedures. Additionally, comprehensive comparison of each model's effectiveness in detecting network intrusions, experimental conditions and performance evaluation criteria are supplied.

3.1 Design of Research

A comparative experimental study of AI-based intrusion detectives' model on the CICIDS2017 data. The models that have been assessed are logistic regression, decision tree, random forest, artificial neural networks, federated learning, and neuro-symbolic AI. Federated learning is conducted in a simulated setting in order to test its privacy-preserving training property as opposed to an actual distributed implementation.

This study compares and contrasts the level of detection of these models, under unified experimental conditions. All models are trained and assessed with the help of the same dataset and preprocessing steps so that the comparison is not biased and unfair. Figure 1 represents the general workflow of the research.

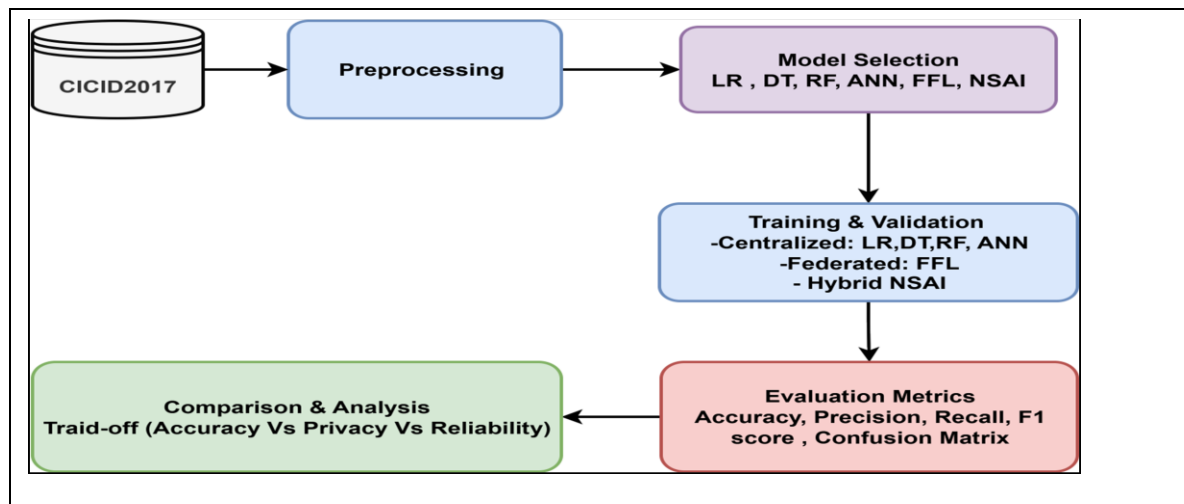


Figure 1. Methodology Flowchart.

3.2 Description of the Dataset

The CICIDS2017 dataset was used in this study as one of the most widely used datasets for evaluating network intrusion detection systems. This dataset contains over 2.8 million network flows, and a wide range of statistical and behavioral characteristics were extracted from each flow, such as flow duration, number of packets, packet lengths, transmission rates, and protocol indicators, more than 50 numerical characteristics. The dataset includes both normal traffic and various types of cyberattacks, such as denial-of-service (DoS) and DDoS attacks, brute-force attacks, port scanning attacks, web attacks, and bot attacks. In this study, a multi-class classification setup was adopted with the aim of evaluating the ability of models to distinguish between normal traffic and different types of attacks. This dataset was chosen due to its realism and the diversity of attack patterns it encompasses, making it suitable for evaluating the effectiveness of AI models in modern network environments preprocessing of Data

- **Data Cleaning:** There were no missing data and superfluous duplicate entries. The cases were eliminated by removing incomplete samples.
- **Target Variable Separation:** The attack type (Attack Type) was isolated and made the target variable in the classification exercise.

- **Data Encoding:** Traditional machine learning models were encoded using label encoding and artificial neural networks and federated learning models using one-hot encoding.
- **Feature Normalization:** The numerical features were normalized using the Min-Max method in order to fit the values in the range $[0,1]$, which enhanced the training stability and convergence.
- **Data Splitting:** The training and testing set divisions were done on a 70/30 split with stratified sampling in order to maintain the original balance of classes. Reproducibility was provided using a fixed random state.
- **Data Balancing:** There was no application of data balancing method like SMOTE or under sampling in this research to assess the model performance in the default state of the class distribution, especially the rarely occurring attack categories.
- **Training Validation:** In the case of the artificial neural network, a validation split was used to use a portion of the training data to validate the model used during the training process, as 20 percent.

3.4 Model Implementation

CICIDS2017 dataset which comprises of Logistic Regression (LR), Decision Tree (DT), Random Forest (RF), Artificial Neural Networks (ANN), Federated Learning (FL), and Neuro Symbolic AI (NSAI). The dataset, preprocessing pipeline, and the experimental environment were used to implement all the models so that they would be fairly and consistently compared against each other.

- **Logistic Regression (LR):** The Logistic Regression was used as a baseline linear classifier to estimate the correlation between network features and attack types. The model was trained to 1000 maximum number of iterations to estimate the probabilities of the classes applying a logistic function. The performance measurement was based on the classification metrics.
- **Decision Tree (DT):** Decision Tree model was selected as it is able to represent hierarchical and conditional relationship in the network traffic data. The tree was trained on default parameters and a constant random seed so that the tree can be reproduced. Evaluation measures that are used to evaluate performance were applied to the model.
- **Random Forest (RF):** Random Forest is an ensemble learning algorithm, which uses a combination of many decision trees in order to enhance generalization and minimize overfitting. The model used in this research was trained on 100 trees using the random sampling of the features and bootstrap sampling. DE aggregation of the outputs of individual trees was used to obtain final predictions.
- **Artificial Neural Networks (ANN):** The artificial neural network with a multi-layer perceptron architecture was applied as a centralized one. This model is made up of three layers of hidden layers containing 128, 64, and 32 neurons respectively with ReLU activation functions and a multi-class Softmax output layer. The model was trained on 50 epochs with a batch size of 64 on the Adam optimizer and categorical cross-entropy loss. Training and validation loss curves were used to measure training stability.
- **Federated Learning (FLL):** The federated learning was applied in a simulated setting with the help of several virtual clients. The training dataset was divided into five subsets with each being sent to a local client. The local ANN models were trained by each client, each with three epochs, and FedAvg algorithm was used to combine the local model weights. This was repeated five times of communication. The last international model was tested with the centralized test set.

The FL setup deployed is a simulated privacy-preserving training set up not a real distributed deploy.

- **Neuro-Symbolic AI (NSAI):** Neuro-symbolic model combines two components, artificial neural network and symbolic reasoning. The ANN is first learned to learn feature representation and make initial predictions. This is followed by domain-specific symbolic rules which are used as a post-processing step to hone out the predictions, especially with respect to some attack patterns. The aim of this integration is to make the interpretation easier and detect rare or complicated attacks. The model also was tested based on accuracy, precision, recall, F1-score, and confusion matrix.

Table 2. Training Configurations and Hyperparameters for The Implemented Models.

Model	Architecture/ parameters	Optimiz er	Loss Function	Epochs	Batch Size	Notes
LR	Solver = lbfgs, Max iterations = 1000	-	Log-loss (internal)	-	-	Baseline linear classifier
RF	n_estimators = 100, Random state = 42	-	-	-	-	Ensemble of DTs
DT	Criterion = Gini, Random state = 42	-	-	-	-	Tree-based classifier
ANN	Dense-128 (ReLU), Dense-64 (ReLU), Dense-32 (ReLU), Output (Softmax)	Adam	Categoric al cross-entropy	50	64	Validation split = 0.2
FFL	Local model = ANN, Clients = 5, Rounds = 5, Local epochs = 3	Adam	Categoric al cross-entropy	3 × 5 rounds	32	FedAvg aggregation (simulated)
NSAI	Dense-64 (ReLU), Dense-32 (ReLU), Output (Softmax) + Symbolic Rules	Adam	Sparse categoric al cross-entropy	20	32	ANN with symbolic post-processing

3.4.1 Neuro-Symbolic AI Architecture

Neuro-symbolic artificial intelligence (NSAI) model is one that involves a combined approach using neural networks and rule-based symbolic reasoning. In the NSAI model used, the neural part comprises an MLP network having two hidden layers with 64 and 32 neurons in each of them. It is important to note that both layers utilize ReLU activation functions. In addition, the neural network learns from the CICIDS2017 dataset.

For improved decision making, there is use of symbolic reasoning as an additional step after processing. Symbolic reasoning is based on cybersecurity rules defined by experts who have knowledge about network behaviors. The layer focuses on making predictions in cases where the attacks' classes are highly similar or hard to classify using neural models.

Symbolic analysis entails the evaluation of neural outputs against the rule conditions that have been generated from the traffic attributes, such as flow dynamics and anomalies. In case there is a deviation between a prediction and rule conditions, then there is a revision of the prediction. Final outcome of classification is obtained through combining the results of neural network prediction with symbolic validation process. Such combination brings about greater interpretability, prevents classification errors for imbalanced data sets, and increases robustness in intrusions detection applications.

3.5 Experimental Setup

Python 3.10 and the TensorFlow 2.x and scikit-learn packages were used to do all experiments. Google Colab, with the use of a GPU, was used to conduct the experiments to make them efficient in terms of model training.

3.6 Preparation and Preprocessing of The Dataset.

Within the simulation of the federated learning approach, the dataset was divided among five simulated clients and trained their own artificial neural network (ANN). This model aggregation took place using FedAvg method, while evaluation of these models was carried out using the same centralized test set. Data was split using stratified random sampling in order to ensure that every client had an equal representation of all the attack classes and thus ensuring that the data was approximately IID distributed. Even though there was no strict non-IID requirement, slight class differences were experienced due to the random splitting of the data.

3.7 Assessment Measures

All of the models were assessed in terms of several quantitative and qualitative indicators to have a complete evaluation.

- Accuracy: This is the ratio of accurate samples in a sample
- Precision, Recall, and F1-score: These are applied to determine the performance of class-level detection, especially in imbalanced categories of attacks.
- Confusion Matrix: It is employed to examine the classification outcomes and the misclassification patterns of the various types of attacks.
- AUC: Requested threshold-based performance evaluation of a select models and significant categories of attacks.
- Training Time and Prediction Time: To determine the efficiency of computations of each model and its practical usefulness.

3.8 Reproducibility

All suitable models and data splitting procedures were randomized with the fixed seed of randomness (random_state = 42) to achieve higher levels of reproducibility. The preprocessing procedures, model architectures and training parameters are clearly written down. The experimental scripts and settings are maintained in order to enable the reporting results to be replicated.

4. RESULT

Here, the experimental results of the analysis of six artificial intelligence models that include (LR), (DT), (RF), (ANN), (FL), and (NSAI) and were tested on the CICIDS2017 dataset are presented. The training and testing of all the models were achieved in the same experimental conditions to make a fair comparison.

The models were evaluated by various measures of the model performance namely accuracy, precision, recall, F1-score, analysis of confusion matrix, training time and prediction time. These metrics give a complete insight on the effectiveness of classification and effectiveness of computation.

4.1 Comprehensive Model Efficacy

This sub-subsection will provide a detailed analysis of the performance of (ANN), Random Forest (RF), (DT), (FL), (LR) and (NSAI) in a classification study based on the CICIDS2017 test data. All the models were tested on the same test so as to ensure consistency and fairness in comparison. As explains in table3.

Table 3. Comparison of Model Performance on The CICIDS2017 Test Set.

Model	Accuracy	Precision	Recall	F1-score	Training Time(s)	Prediction Time(s)
LR	0.9573	0.9569	0.9573	0.9555	225.120622	0.099787
DT	0.9984	0.9984	0.9984	0.9984	126.038251	0.129263
RF	0.9985	0.9985	0.9985	0.9985	750.021611	6.473585
ANN	0.9880	0.9877	0.9880	0.9874	2266.356740	39.327270
FL	0.9838	0.9854	0.9838	0.9851	1610.973785	33.568341
NSAI	0.9878	0.9875	0.9878	0.9872	2580.97	24.97

Accuracy, precision, recall, and F1-score, were taken into account to find out the most effective intrusion detection model. All the models have their final results compared in Table 3.

4.2 Training Accuracy Compared to Test Accuracy

Figure 2 and Figure 3 shows the training and testing accuracy of the LR, DT, RF, ANN, and FL models. gives the per-attack F1-score comparison among various categories of attack.

The findings indicate that the majority of the centralized models are slightly more accurate in training than they are in test accuracy which is a sign of low overfitting. Also, the Federated Learning model has shown the comparatively equal performance in the various types of attacks especially on the minority classes. It can be noted that the Neuro-Symbolic AI model is also stable in the performance across the types of attacks, which demonstrates the efficiency of the neural learning with the symbolic rules.

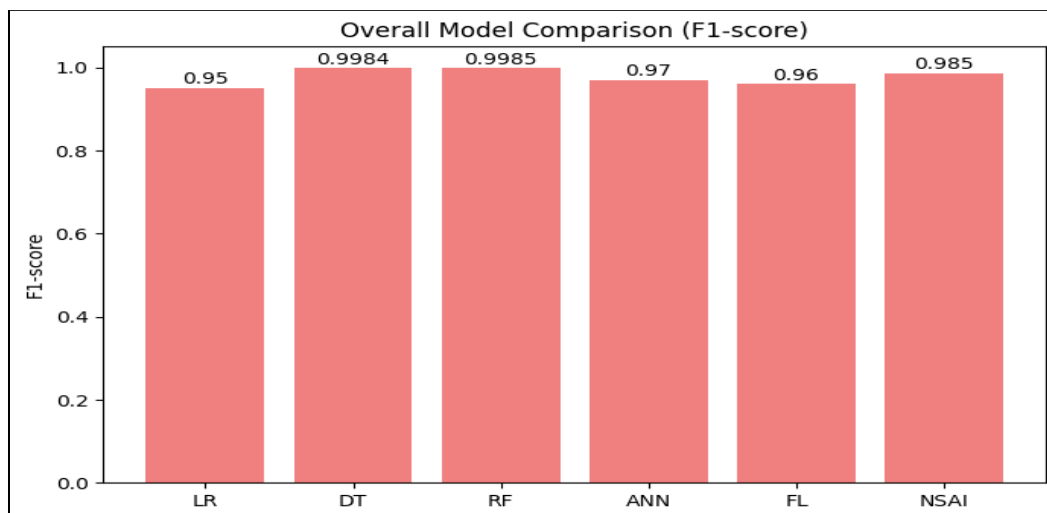


Figure 2. Comparison of all Evaluated Models Performances in Terms of F1-scores on the CICIDS2017 Test Dataset.

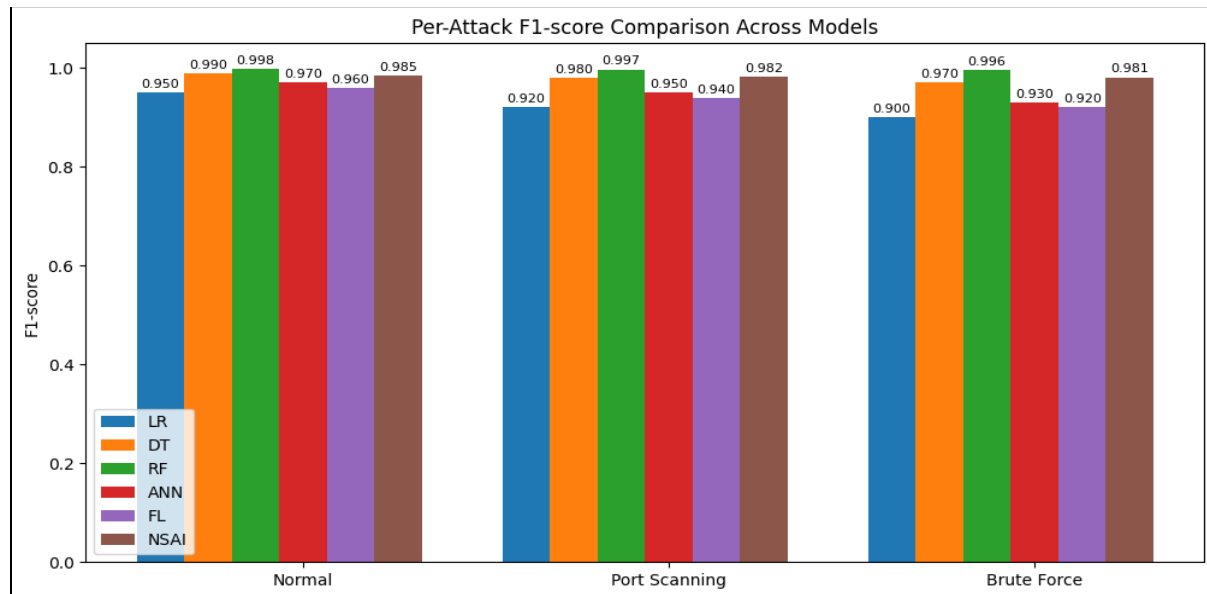


Figure 3. Per-Attack F1-score Comparison Across model.

Further examination of the per-attack metrics will show that the Federated Learning (FL) model can continue being competitive in the minority attack types, including Port Scanning or Brute Force. FL is more sensitive to such attacks than Logistic Regression, with no change in overall performance.

This action indicates how federated learning can pool together various local tendencies, which can lead to increased generalization in privacy preserving-conditions.

Logistic Regression (LR) The overall accuracy of Logistic Regression was about 0.9573 , results in relation to ensemble and deep learning models. Figure 4 shows the accuracy of training and testing of the LR model as a training model, and there is no excessive overfitting in training. Nevertheless, LR proves to be weak in dealing with extremely unbalanced types of attacks. Although the model works well with classes that occur frequently like the normal and DoS traffic, the model also shows a high decrease in its performance with additional minority classes like Web Attacks and Infiltration. This weakness can be seen in the normalized confusion matrix presented in Figure 5 with low recall values of underrepresented attacks. Therefore, LR is not applicable to the complete intrusion detection cases that need the high sensitivity to the rare attacks.

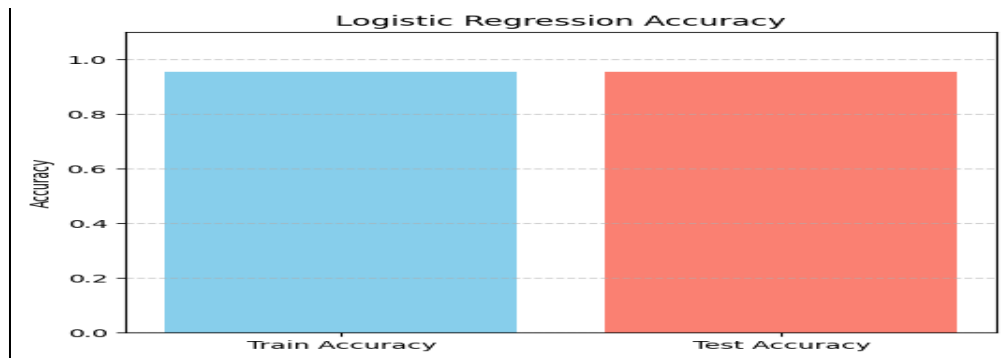


Figure 4. Logistic Regression Train and Test Accuracy.

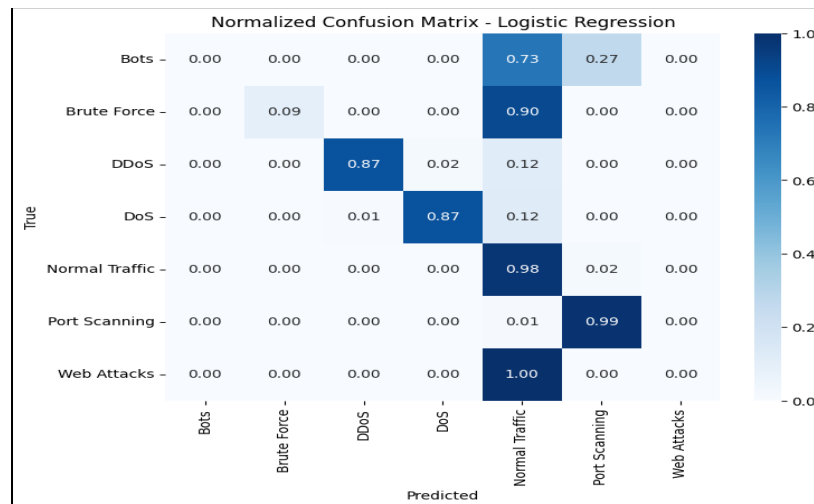


Figure 5. Normalized Confusion Matrix -LR.

4.3 classification performance

DT and RF models showed the best classification performance, and their accruing accuracy was nearly at 0.9984 and 0.9985. Figure 6 shows the training and testing accuracy of both models, which suggests that they have high learning and low overfitting. An additional discussion of the confusion matrices and the per-class performance measures shows that there are significant disparities between the two methods. Although, DT demonstrates rather high misclassification rates within minorities (Web Attacks and Infiltration) RF can decrease these errors since it combines several decision trees. RF has a more stable recall among the types of attacks, as shown in Figure 7, a fact that indicates that it is more robust and shows better generalization than DT.

Both models have a near-perfect accuracy, RF offers a more balanced and accurate detection.

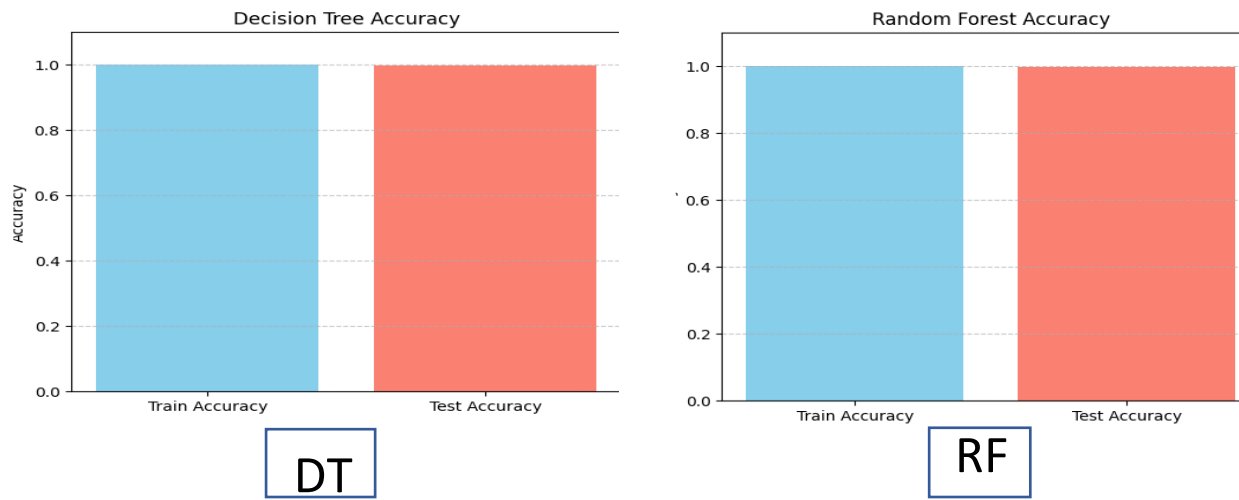


Figure 6. Train and Test Accuracy for DT and RF.

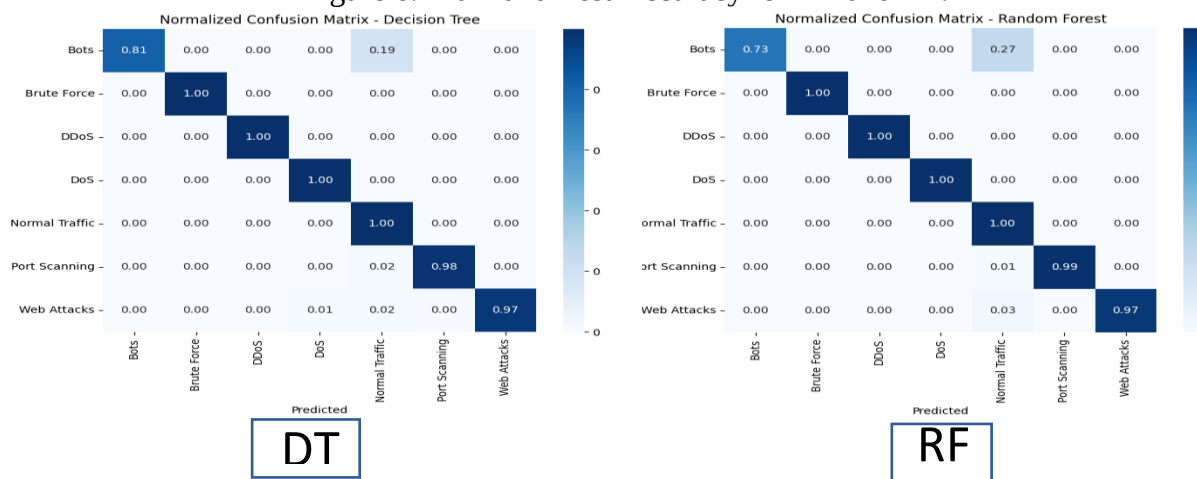


Figure 7. The Normalized Confusion Matrix for DT and RF.

4.4 Accuracy and Confusion Matrix for ANN

ANN had the overall accuracy of about 0.9880. ANN has multiple layers, and thus, it is able to describe intricate nonlinear relationships within network traffic data. The training and validation accuracy and loss curves can be seen in Figure 8 and show stable convergence and minimized over-fitting. The model is effective in identifying the majority classes like the normal and DoS traffic. Like other centralized methods, however, ANN will have lower recall of categories of minority attacks, such as Web Attacks and Infiltration. This is further pointed out in the normalized confusion matrix presented in Figure 9. Despite the high adaptability and robustness of ANN, there is a slight performance of ANN, which is still lower than tree-based models applied to tabular intrusion detection data.

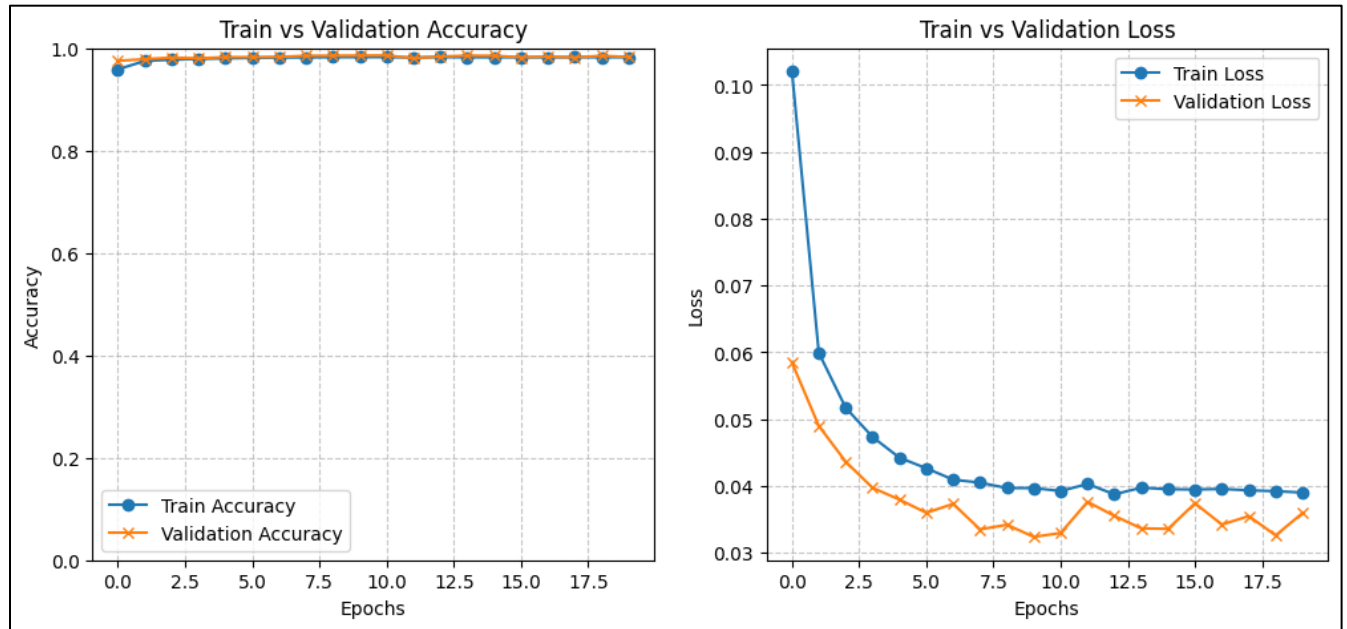


Figure 8. Train Accuracy and Loss for ANN.

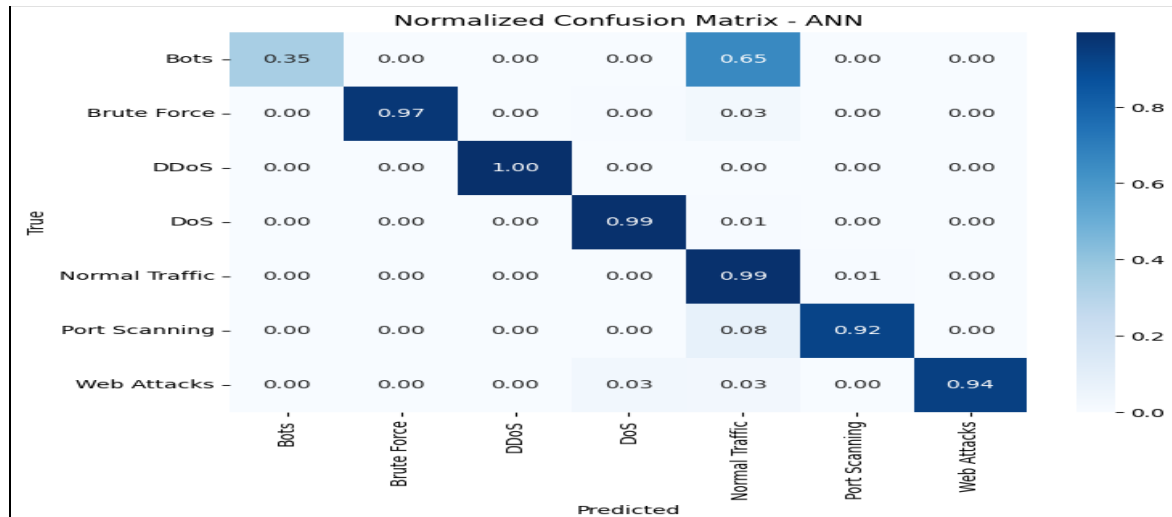


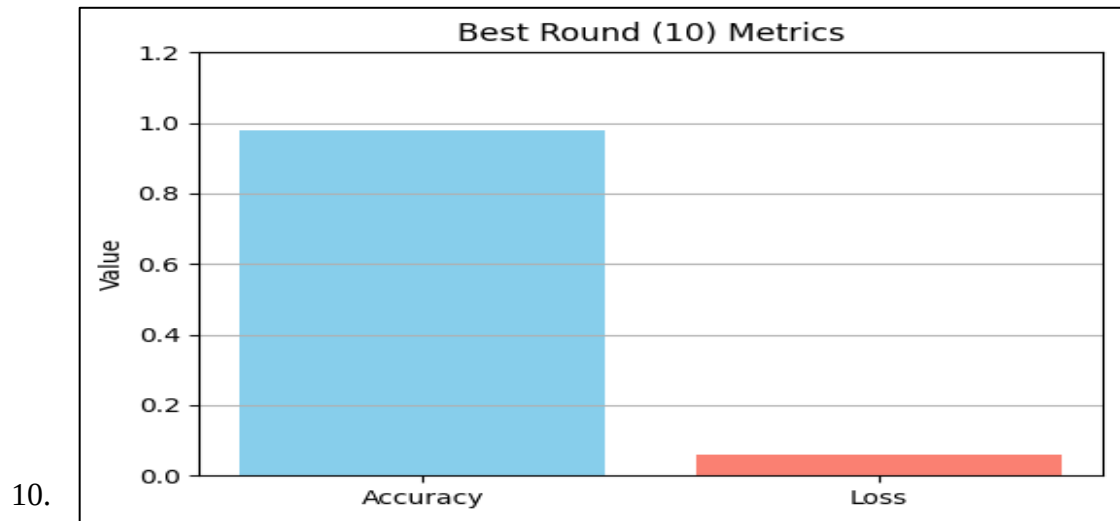
Figure 9. Normalized Confusion Matrix – ANN.

The performance of the ANN plateaued below RF/DT, suggesting that tree-based models may be naturally preferred in tabular network traffic data. However, ANN demonstrated adaptability and durability, demonstrating its value under shifting circumstances.

Performance of Federated Learning

4.5 Accuracy and Loss of The Optimal Federated Learning Iteration.

FL model had an overall accuracy of 0.9838, which is less than centralized Random Forest and DT models. Figure 10 gives the training and testing accuracy and loss curves, which means that it has a stable learning behaviour and can be overfitted. Those factors as the decentralized training process and aggregation of heterogeneous local models can be considered as the reasons why FL performs poorly. The model as shown in Figure 11 has lower recall rates to the underrepresented categories of attacks especially to Web Attacks and Infiltration. Although federated learning is less numerically accurate, it shows the possibility of ensuring privacy of data and still achieving acceptable detection rates, which is why it can be applied in privacy-sensitive collaborative scenarios).



Figure

Accuracy and Loss of the Optimal Federated Learning Iteration.

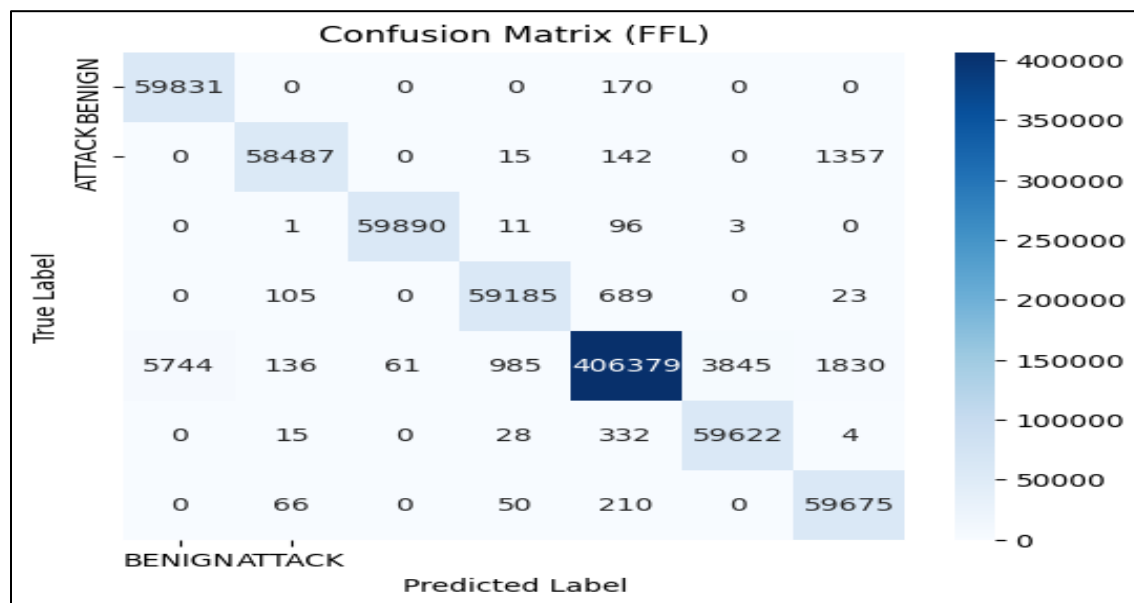


Figure 11. FFL - Confusion Matrix Normalize.

NSAI model has been trained in 20 epochs

with a mean epoch training time of about 129 seconds which makes the total training time about 43 minutes. The test dataset for prediction took around 24.97 seconds. The NSAI model obtained a total accuracy of 98.78 and the value of precision, recall, and F1-score were 98.75, 98.78, and 98.72, respectively. It is important to note that Brute Force class got an F1-score of about 0.95 with high precision and recall values. Normal traffic was reported with almost perfect performance and Port Scanning had rather low recall which means that it was partially misclassified. The study of the per-class F1-score is given in Figure 12, and the trend of the validation accuracy and loss is shown in Figure 13. Those findings suggest that there is addition of symbolic rules which lead to a better interpretability and also helps to identify some rare patterns of attack. In general, NSAI exhibits a competitive performance and equal generalization in various categories of attacks.

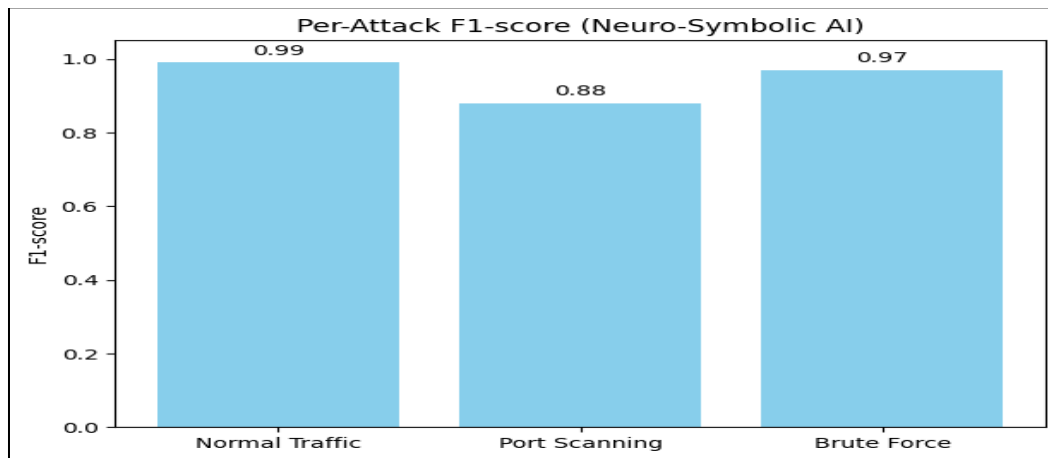


Figure 12. F1-Score Comparison Pre-Class.

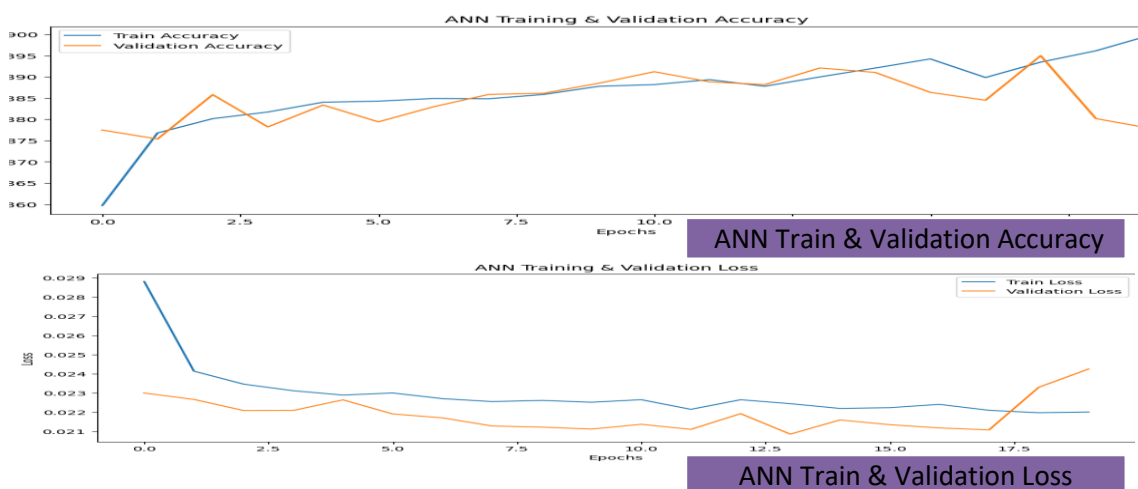


Figure 13. The ANN Train Accuracy and Loss.

4.6 Confusion Matrices Analysis

The normalized confusion matrix for all six evaluated models is presented in Figure 14 and shows how the classifiers performed on different attack types.

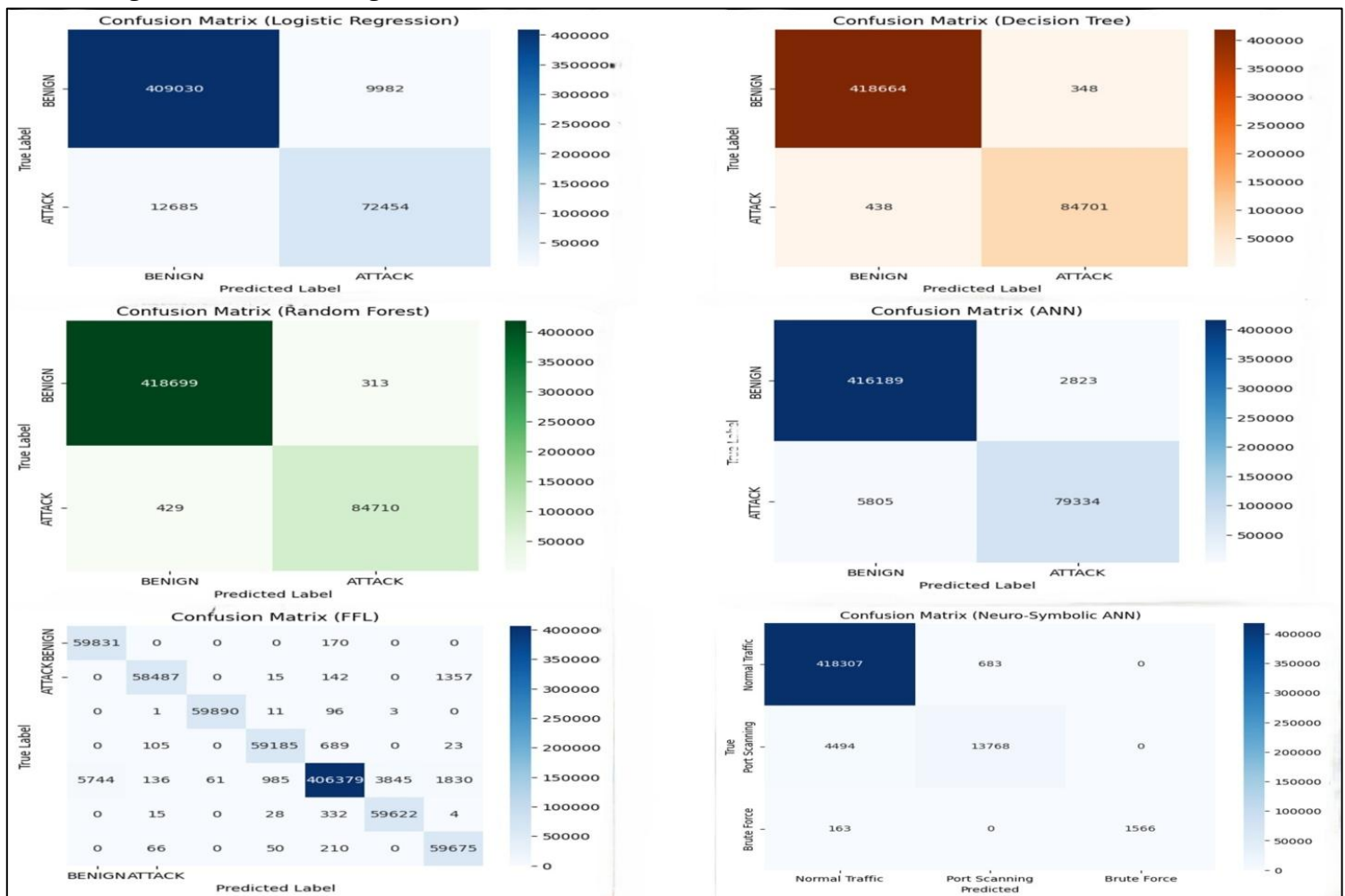
LR: The classifier showed acceptable classification results yet failed to correctly classify many attacks and had relatively low recall scores.

DT and RF: Both classifiers showed good classification results; however, RF appeared more robust and made less mistakes than DT.

ANN and FL: Both models demonstrated strong performance and consistently lower false positive and negative rates compared to baseline models. At the same time, recall decreased for some rare attacks.

NSAI : The model showed excellent results on both precision and recall metrics; the use of symbolic knowledge increased explainability and attack detection efficiency for particular attacks. All in all, the confusion matrix reveals key advantages and weaknesses of all evaluated models and their behaviour on different attacks when attack distribution becomes unbalanced.

Figure 14. The Five Algorithms' Confusion Matrix.



5. Discussion

A comparative analysis of the chosen models is performed by considering the detection accuracy, speed and privacy aspects. This research identifies the differences between the approaches of centralized learning, Federated Learning and Neuro-Symbolic AI in the field of intrusion detection systems. Figure 14 shows the normalized confusion matrices of all six models that were analyzed. The logistic regression algorithm provides acceptable accuracy but displays higher levels of errors in cases of minority attacks. On the other hand, decision trees and random forests produce satisfactory results, with the latter method being superior to the former one in almost all cases. The artificial neural network and federated learning techniques provide similar results, coupled with high levels of false positives and false negatives, particularly in cases of minority attacks. On the contrary, the NSAI method produces relatively stable levels of precision and recall and improves the detection of complex patterns. However, the distribution of the clients' data in the Federated Learning setting was nearly equal (near-IID). This helped achieve stable convergence and reduced degradation in performance that is usually seen in the case of non-IID setups. However, this equality can result in a positive evaluation of the performance of Federated Learning compared to the practical world.

6. Limitations and Future Work

The research has a number of limitations. Firstly, the experimental assessment was conducted only with the aid of CICIDS2017; therefore, the model's results may differ according to other networks with different attacks' distributions. Secondly, the efficiency of Federated Learning may depend on clients' data disparity and imbalance that affect the quality of the globally generated model. NSAI and FL also require increased computational costs compared to traditional machine learning algorithms that might impede the efficient application of the solution.

In future research, a combination of tree models with neural networks' interpretative capabilities will be considered to increase the interpretability of the solution. Further research will involve assessing the algorithm's performance using various larger and more diversified multi-organizational datasets. Furthermore, explainable AI can be used to achieve better results.

7. Conclusion

A critical analysis of various machine learning, deep learning, federated learning, and neuro-symbolic intrusion detection models. The outcomes of the experiment show that tree-based models especially the Random Forest and Decision Tree have the best overall accuracy (around 0.9985), and thus are applicable to high speed and resource conscious detection systems.

In general, the results suggest that the intrusion detection system is capable of balancing its accuracy, computational efficiency, interpretability, and privacy preservation. According to the outcomes of the experiment, NSAI can be applied in the situation when it is necessary to confirm complex attacks reliably, tree-based models are applicable to a real-time and resource-constrained setting, and federated learning is more suitable in a collaborative environment with privacy preservation. Future work is focuses on testing these models on bigger and more heterogeneous datasets, increasing model interpretability by using explainable AI and exploring

more advanced federated learning and clustering approaches to enhance better cybersecurity applications.

Acknowledgements

I thank everyone who supported me in presenting this research.

Declaration of Competing Interest

The authors declare no conflicts of interest. The authors acknowledge that there was no financial support for the research presented in their research paper.

REFERENCE:

- 1- Adjewa, F., Esseghir, M. and Merghem-Boulahia, L. (2024) 'Efficient Federated Intrusion Detection in 5G Ecosystem Using Optimized BERT-Based Model', *International Conference on Wireless and Mobile Computing, Networking and Communications*, pp. 62–67. <https://doi.org/10.1109/WiMob61911.2024.10770340>.
- 2- Agheeb Al-Hamdawae, Z. M. (2025) 'Optimizing Feature Selection for IoT Intrusion Detection Using RFE and PSO', *Misan Journal of Engineering Sciences*, 4(1), pp. 236–248. <https://doi.org/10.61263/mjes.v4i1.158>.
<https://uomisan.edu.iq/eng/mjes/index.php/eng/article/view/158/106>
- 3- Al-Hammash, M. S. H., & Maarouf, H. 'Enhancement methods of intrusion detection systems using artificial intelligence methods (TLBO) Algorithm', *Misan Journal of Academic Studies*, 23(49), pp. 105–112. <https://doi.org/10.54633/2333-023-049-010>
- 4- Davide Ariu, G. et al. (2011) 'HMMPayl: An intrusion detection system based on Hidden Markov Models', *Computers & Security*, 112(6), pp. 18–30. <https://doi.org/10.1016/j.cose.2010.12.004>
- 5- Chavan, P. V. and Alone, N. V. (2025) 'Optimizing Intrusion Detection with Random Forest: A High-Accuracy Approach Using CIC-IDS 2017', *International Journal of Computer Applications*, 187(3), pp. 17–22. <https://doi.org/10.5120/ijca2025924816>
- 6- Chen, J. et al. (2024) 'When Federated Learning Meets Privacy-Preserving Computation', *ACM Computing Surveys*, 56(12). <https://doi.org/10.1145/3679013>
- 7- Colelough, B. C. and Regli, W. (2024) 'Neuro-Symbolic AI in 2024 : A Systematic Review', 3403, pp. 0–1. <https://doi.org/10.48550/arXiv.2501.05435>
- 8- Daly, K. et al. (2024) 'Federated Learning in Practice: Reflections and Projections', *Proceedings - 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications, TPS-ISA 2024*, pp. 148–156 /TPS-ISA62245.2024.00026. <https://doi.org/10.1109/TPS-ISA62245.2024.00026>.
- 9- Devlin, N., Parkin, D. and Janssen, B. *Methods for Analysing and Reporting EQ-5D Data*. <https://doi.org/10.1007/978-3-030-47622-9>.
- 10- Gupta, N., Jindal, V. and Bedi, P. (2022) 'CSE-IDS: Using cost-sensitive deep learning and ensemble algorithms to handle class imbalance in network-based intrusion detection systems', *Computers & Security*, 112, p. 102499/j.cose.2021.102499. <https://doi.org/10.1016/j.cose.2021.102499>.
- 11- Hasan, M., Al-Maliki, A. and Jasim, N. (2022) 'Review of SQL injection attacks: Detection, to enhance the security of the website from client-side attacks', *Int. J. Nonlinear Anal. Appl*, 13, pp. 2008–6822. <https://doi.org/10.22075/ijnaa.2022.6152> /ijnaa.2022.6152.
- 12- Hitzler, P. et al. (2022) 'Neuro-symbolic approaches in artificial intelligence', *National Science Review*, 9(6), pp. 2–4. <https://doi.org/10.1093/nsr/nwac035>.
- 13- Jimenez-Gutierrez, D. M. et al. (2025) 'On the Security and Privacy of Federated Learning: A Survey with Attacks, Defenses, Frameworks, Applications, and Future Directions'. <https://doi.org/10.48550/arXiv.2508.13730>
- 14- Li, L. et al. (2020) 'A review of applications in federated learning', *Computers & Industrial*

- Engineering, 149, p. 106854. <https://doi.org/10.1016/j.cie.2020.106854> ./J.CIE.2020.106854.
- 15- Liu, B. *et al.* (2024) 'Recent advances on federated learning: A systematic survey', *Neurocomputing*, 597(June), p. 128019. <https://doi.org/10.1016/j.neucom.2024.128019> /j.neucom.2024.128019.
- 16- Marra, G. (2024) 'From Statistical Relational to Neuro-Symbolic Artificial Intelligence', *Proceedings of the AAAI Conference on Artificial Intelligence*, 38(20), p. 22678. <https://doi.org/10.1609/aaai.v38i20.30294> ./aaai.v38i20.30294.
- 17- Mathur, A., Gupta, A. and Das, S. K. (2025) 'When Federated Learning Meets Quantum Computing: Survey and Research Opportunities', pp. 1–25. <https://doi.org/10.1109/COMST.2025.3634143>
- 18- Moussaoui, J. and Kmiti, M. (2025) 'A Systematic Review on Hybrid AI Models Integrating Machine Learning and Federated Learning'. <https://doi.org/10.3390/jcp5030041>
- 19- Oyeboode, O. (2025) 'Decentralized neuro-symbolic cognitive architectures : Integrating federated reasoning , governance , and causal inference for trustworthy , resilient Artificial Intelligence'. <https://doi.org/10.30574/gjeta.2025.24.3.0266>
- 20 - Piplai, A. *et al.* (2023) 'Knowledge-enhanced Neuro-Symbolic AI for Cybersecurity and Privacy', pp. 1–4. <https://doi.org/10.48550/arXiv.2308.02031>
- 21- Renkhoff, J. *et al.* (2024) 'A Survey on Verification and Validation, Testing and Evaluations of Neurosymbolic Artificial Intelligence', *IEEE Transactions on Artificial Intelligence*, 5(8), pp. 3765–3779. <https://doi.org/10.1109/TAI.2024.3351798> ./TAI.2024.3351798.
- 22- Zhang, H., Ye, J., Huang, W., Liu, X., & Gu, J. (2025). *Survey of federated learning in intrusion detection*. *Journal of Parallel and Distributed Computing*, 195, 104976. <https://doi.org/10.1016/j.jpdc.2024.104976>
- 23- Belenguer, A., Pascual, J. A., & Navaridas, J. (2025). *A review of federated learning applications in intrusion detection systems*. *Computer Networks*, 258, 111023. <https://doi.org/10.1016/j.comnet.2024.111023>
- 24 Abdelaziz, M. T., Radwan, A., Mamdouh, H., Saad, A. S., Abuzaid, A. S., Abdelhakeem, A. A., Zakzouk, S., Moussa, K., & Darweesh, M. S. (2025). *Enhancing network threat detection with random forest-based NIDS and permutation feature importance*. *Journal of Network and Systems Management*, 33(2). <https://doi.org/10.1007/s10922-024-09874-0>
- 25- Tran, H. T. T., Sander, J., Cohen, A., Jalaian, B., & Bastian, N. D. (2025). *Neurosymbolic AI transfer learning improves network intrusion detection*. <https://doi.org/10.48550/arXiv.2509.10850>
- 26- Tran, H. T. T., Sander, J., Cohen, A., Jalaian, B., & Bastian, N. D. (2025). *Neurosymbolic artificial intelligence for robust network intrusion detection: From scratch to transfer learning*. arXiv preprint arXiv:2506.04454. <https://doi.org/10.48550/arXiv.2506.04454>
- 27- Wan, Z., Liu, C. K., Yang, H., Li, C., You, H., Fu, Y., Wan, C., Krishna, T., Lin, Y., & Raychowdhury, A. (2024). *Towards cognitive AI systems: A survey and prospective on neuro-symbolic AI*. arXiv preprint arXiv:2401.01040. <https://doi.org/10.48550/arXiv.2401.01040>
- 28- Younus, Y. M., Ibraheem, A. S., Tuama, M. H., & Mashloosh, W. M. (2025). *Improved machine learning techniques for precise DoS attack forecasting in cloud security*. *Misan Journal of Academic Studies*, 23(52), 120–129. <https://doi.org/10.54633/2333-023-052-011>