Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 7 (2025)

Reliable Federated Learning (RFL) Assisted Intrusion Detection and Classifications Approach Using (SSL/TlS) For Network Security

[1]Nasir Ayub*, [2]Asad Yaseen, [3]Muhammad Nabeel Amin, [4]Syed Muhammad Rizwan, [5]Irfan Farooq, [6]Muhammad Zunnurain Hussain

Article Details

Keywords: Quantum Computing, Federated Learning, Machine Learning, Learning Process, Machine Learning Models, Internet Of Things, Transfer Learning

Nasir Ayub*
Deputy Head of Engineering Calrom Limited, M1 6EG, United Kingdom.
E-mail: nasir.ayyub@hotmail.com
Asad Yaseen
Senior Solution architect at STC solutions, Saudi Arabia.
E-mail: asad4ntrp2@gmail.com
Muhammad Nabeel Amin
Department of Computer Science, Government College University, Faisalabad.
E-mail: nabeelofficial70@gmail.com
Syed Muhammad Rizwan
Department of Computer Engineering, University of Engineering and Technology Lahore, Pakistan.
E-mail: rizwan.naqvi@ieee.org
Irfan Farooq[5]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan.
F-mail: irfanfarooq9@gmail.com
Muhammad Zunnurain Hussain[6]
Bahria University Lahore Campus.
E-mail: zunnurain.bulc@bahria.edu.pk

ABSTRACT

In the past few decades, machine learning has revolutionized data processing for large-scale applications. Simultaneously, increasing privacy threats in trending applications led to the redesign of classical data training models. In particular, classical machine learning involves centralized data training, where the data is gathered, and the entire training process executes at the central server. Industry 4.0 allows the appearance of Internet of Things-based transactive energy system (IoTES) that involves new services with a number of independent distributed systems. These systems produce bulk data that is heterogeneous and they are prone to cyber-attacks, especially stealthy false data injection attacks (FDIAs). Lossy networks (RPL) security, intrusion detection (ID) is crucial in this area using SSL/TIS, considering that it is highly vulnerable to attacks, especially those executed by an insider. Although a lot of literature suggests the use of ID systems (IDSs) by applying a variety of techniques, there is relatively little literature offering insight into where the IDSs fall within the RPL topology. The gap in this study will be bridged by aggressively comparing three ID architectures in terms of central and distributed location and on several dimensions, including effectiveness, cost, privacy, and security. The results are supported by the overwhelming contribution of attacker position and IDS-to-attacker distance towards the detection. Therefore, in addition to ascertaining the effectiveness of the old ID systems, the research also probes how federated learning (FL) can enhance ID in the RPL networks. The aspect of the decentralized model training approach in FL can overcome the effect of attacker position on the performance of an IDS system by making sure that information that is considered to be pertinent in the context of an attack is gathered at the node along with the IDS system, irrespective of its proximity to the potential attackers. In addition, the approach not only eliminates security issues, but it also reduces communication overhead between the ID nodes. This will mean that FL will lower the rate of large-scale data transfer and thereby eliminate the consequences of packet loss and latency that any lossy network will cause. Also, the gap filled by the research is the impact of local data sharing on FL performance and how it is possible to balance the effectiveness with security. The proposed computing method can be computed in parallel and allows detecting the stealthy FDIA on all the nodes without any failure. The simulation experiments support the suggestion that the scheme under consideration is superior to the state-of-the-art approaches in terms of detection accuracy and the complexity of computation when using a distributed environment and ensuring the data privacy of the messages.

INTRODUCTION

Data does not occupy shared model space or shared feature space in most situations compared to how they are in the horizontal and vertical cases of the FLs. Consequently, this lack of data markers and value-deprived data can be considered the most important challenge in the concerned situation. It is great because transfer learning (TL) enables you to carry information from one domain (the source domain) to another one of learning preferences (the target domain) to enhance your learning results [1, 2]. This way, [2] has proposed FTL as a method to have a high perspective on FL that can be used with shared parties with light intersections. It is the first FL stack, which entails training, evaluation, as well as cross-validation, which is grounded on transfer learning. More so, the neural networks in this frame using the additive homomorphic encryption technology cannot necessarily evade confidentiality leakage alone, though they provide comparable accuracy to the non-confidentiality-saving techniques. However, the issue remains communication proficiency [3, 4]. Consequently, in [5] strive hard to improve FTL. As an alternative to HE, they employed the secret sharing technology in order to save on overheads without a loss in accuracy. It could also be used to block rogue Servers. They assume that the model is semi-honest in the previous work. As an actual example, [6, 7] constructed a FedHealth system, which applies FL in collecting data from numerous organizations and subsequently uses transfer learning to give personalized healthcare services. Some data on the diseases diagnosed and treatment of one infirmary can be transferred to another infirmary in order to support the examination of other diseases with the use of FTL. The FTL research is continuing to be in its initial phases; hence, there is a huge opportunity to make it more versatile with different data structures [8, 9]. FL introduces new avenues for AI research. FL is a revolutionary training strategy for developing tailored models that do not compromise user privacy. The computational resources of client gadgets have become increasingly powerful with the introduction of AI chipsets [10, 11]. Likewise, the training of AI models moves away from the central server and toward the terminal devices. FL is a confidential-protection method that successfully uses terminal instrument processing competencies to train the model, preventing private data from being visible through data transmission. Since there are many mobile devices and devices in various domains, there are plenty of exceptional dataset resources that FL can completely exploit [12. 13].

$$MCC = \frac{TP * TN - FP * FN)}{\sqrt{((TP + FP) * (TP + FN) * (TN + FP) * (TN + FN))}} \quad \text{Eq (1)}$$

$$f = -Ex{\sim}pdata\,[\log pmodel(x)] \quad \text{Eq (2)}$$

$$f(x,y,w) = -\log p(y \mid x;w) \quad \text{Eq (3)}$$

$$minw{\in}Rd\, f(w) = K \sum k{=}1\ nk\ n\ Fk(w) \quad \text{Eq (4)}$$

Table 1: Analysis of Numerous ML algorithms implemented with Federated Learning

Ref	Approaches	Dataset	Assessment Metrics	Limitations
[14, 15]	YOLO, Faster R-CNN	900 images engendered from 26 street cameras and 7 object [42,43]	Interaction Over Union (IOU), Mean Average Precision (mAP)	Limited to just one benchmark on the datasets used in their study
[16, 17]	CNN	MindBigData dataset (Electroencephalography (EEG))	Accuracy	protected multi-party computation and differential confidentiality was not used in this study
[18, 19]	FedMA (Deep CNN and LSTM)	Shakespeare dataset over	Accuracy, Epoch	Lesser deep learning building blocks were used in this study. FedMA fault tolerance and fewer datasets were not considered in this study.
[20, 21]	FedMA (Deep CNN and LSTM)	Shakespeare dataset over	Accuracy, Epoch	Lesser deep learning building blocks were used in this study. FedMA fault tolerance and fewer datasets were not considered in this study.
[22, 23]	FedAVG	MNIST dataset, MIMIC-III dataset	AUROC, F1-score, Precision recall	Real-life medical data with multiple institutions were not considered
[24, 25]	FedBoost, AFLBoost	Synthetic dataset	-	The study proposed performance algorithm was not evaluated
[26, 27]	SVM	MNIST dataset	AoU	Only one ML algorithm was considered in this study. The proposed system has low complexity
[28, 29]	U-net of DCNN	BraTS 2017	Precision	Low datasets were used in this study
[30, 31]	Deep-Q-Reinforcement Learning Ensemble based on Spectral Clustering called DQRE-SCnet	MNIST, Fashion MNIST, and CIFAR-10	Accuracy, AUC, Recall, Kappa, Run time	The study had high computation time and high complexity for any dataset
[32, 33]	CNN	channel data	Accuracy, complexity order	Compression techniques and scheduling time was not considered in the study

We no longer use the amount of information as the subject of our attention, due to the appearance of big data [34]. The problem of data privacy and security has to be dealt with. Data leakage can never be taken lightly and society has been more concerned with the safety of data [35]. People, groups, and society are trying to enhance data protection and privacy safety. The GDPR [36, 37] aims to preserve the privacy and data safety of consumers, like the EU implementation of the Wide-ranging Data Fortification Guidelines on 25 May 2018. This necessitates the operators to declare user agreements correctly and they can not deceive and trick the user into waiving off their privacy rights. Training the model in the absence of authorisation by the handler was also prohibited for the operators. It also allows the deletion of the personal information of the user [38, 39] and the Wide-ranging Values of the Civil Law of the PPC [40, 41] have since 2017 mirrored that network handlers are not permitted to divulge, tamper with, or delete the individual statistics collected by them. Figure 1 shows the generalized Framework for Federated learning. The very small transactions involved in data transfers use a third party to ensure that the contract that is to be entered into gives the dimensions of the amount and type of data to be exchanged, as well as what should be done in terms of fortification of the data. The implementation of these regulations and procedures has created more challenges to the normal data processing mode of AI to a greater extent [42, 43]. The backbone of artificial intelligence is data, and thus, a training model cannot develop without data. Alternatively, data is widely located in the form of data islands. A simple solution to the data islands is the processing of data in a centralized manner. Data processing techniques include centralized data collection, standardized processing, data cleaning and modelling. The majority of the time, the data exudes during the collection and conversion processes [44].

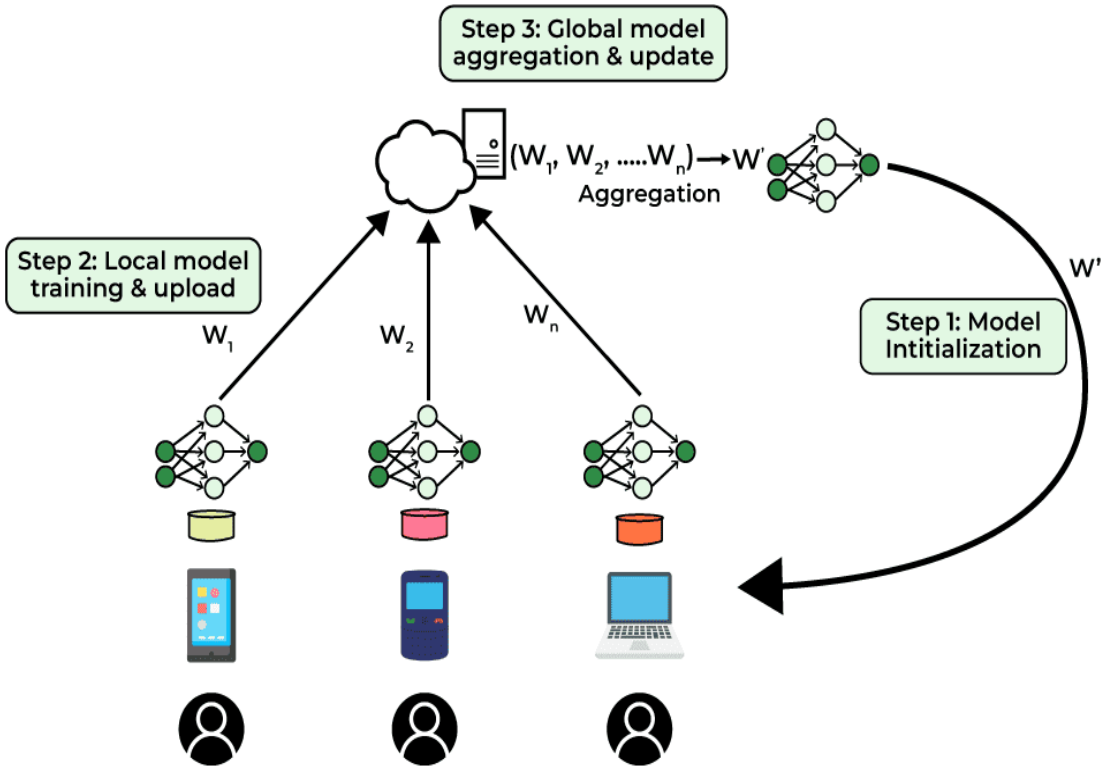

Figure 1: Generalized Framework for Federated learning [45]

1.1 Applicable ML methods for FL

MCC is widely used for accuracy calculation rate in FL, while significant advancements have been made in cybersecurity technologies and legal frameworks [46]. Additionally, the legal frameworks intended to protect consumer data often lag behind technological advancements, creating regulatory gaps that attackers exploit. Ethical concerns, particularly regarding the misuse of surveillance technologies, further highlight the limitations of current approaches [47].

1.2 Linear methods

There are three types of linear models: linear regression, ridge regression, and lasso regression. Suggested using a federated environment to train a linear model, which addresses the security concern of entity analysis and accomplishes the equivalent accuracy as the non-private alternative. Created the highest performing ridge regression system using homomorphic encoding [48]. The linear method is straightforward to apply in comparison to other models, and it is a good model for adopting FL [49].

1.3 Tree models

Single or multiple decision trees (DT), for instance, gradient boosting decision trees and random forests (RF), may be trained via federated learning. The Gradient Boosting Decision Tree (GBDT) method has attracted a lot of consideration lately, owing to its excellent performance in a variety of classification and regression applications. For the first time, [50] used the GBDT confidentiality fortification system in regression and binary classification tasks. To avoid the leak of user data privacy, the system securely combines regression trees learned by multiple data owners into a group [51]. Presented the SecureBoost framework, which allows users to create an FL system by training the gradient lifting DT model for horizontal and vertical partition data [52, 53].

1.4 Neural network (NN) models

The NN model is a prominent ML method right now, and it seeks to train neural networks to do complicated tasks. Deep neural network research is becoming further prevalent in the federal context. Drones may help with a wide range of tasks, including trajectory planning, target identification, and target localization. The UAV (Unmanned Aerial Vehicle) group typically trains the model through DL to provide more efficient services, but owing to the absence of an unceasing linking between the UAV group and the ground base station, the federal training technique cannot produce the UAV's real-time performance [54, 55] were the foremost to apply a distributed FL approach to a UAV group, improve federated learning convergence speed, and perform joint power allocation and scheduling. The principal UAV recaps the local flight method taught by the other UAVs to develop the comprehensive flight method, which is then delivered to the other UAVs over the intra-group network. [56] used TensorFlow to create a scalable FL system for mobile devices that can train a large quantity of distributed data models. To accomplish priority applications incorporating data, set up a federated DL system built on data division [57, 58]. In addition to corporate data applications, traffic flow data in government affairs big data regularly includes a significant amount of user confidentiality. Recommend a clustering FedGRU technique that incorporates the ideal comprehensive method and captures the Spatio-temporal correlation of traffic flow data more precisely by combining GRU (Gated Recurrent Unit) NN for traffic flow forecasting with FL. Experiments on actual data sets reveal that it outperforms non-federated learning approaches significantly [59, 60].

2. Related Work

Data poisoning attacks can be divided into methods such as label flipping, target optimization, gradient optimization, and clean labeling based on technical implementation methods. Data poisoning by directly modifying the label information of the training data of the target category, while the characteristics of the data remain unchanged. Attackers can poison data by modifying data and data labels. Train a softmax

classifier across ten honest clients, each holding a single-digit partition of the original ten-digit MNIST dataset. Attackers achieve data poisoning attack goals by manipulating data labels, such as deliberately labeling the number [61, 62]. Figure 2 elaborates on the Data Poisoning Security attacks under the FL model.

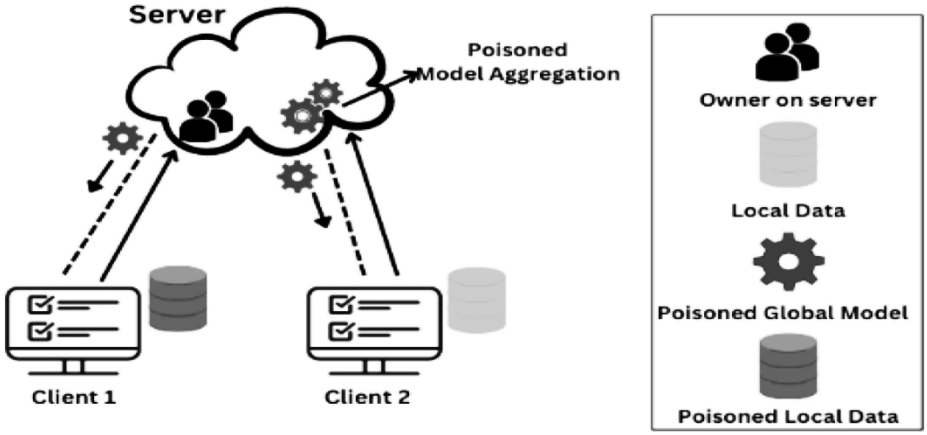

Figure 2: Data Poisoning Security attacks under the FL model [63]

Table 2 represents the analysis of Numerous ML algorithms implemented with Federated Learning. In realistic scenarios, the latency of inferring directly from participants is much lower than predicting in the cloud and then transferring to participants. The implementation of FL in mobile edge networks accelerates content delivery and improves mobile service quality by reducing unnecessary system communication load [64]. The model inference is completed locally without a cloud round-trip that avoids propagation delay caused by transferring data, and thus, latency-sensitive applications can benefit from such a solution [65, 66]. The following are common assumptions used in the convergence analysis of Federated Learning optimization algorithms. Figure 3 below shows the Attack mitigation using the FL model.

Table 2: Analysis of Numerous ML algorithms implemented with Federated Learning.

Ref	Approaches	Dataset	Assessment Metrics	Limitations
[67, 68]	CNN	local Datasets	RMSE, NMSE	Compression-centered approaches for both training data and the approach constraints to additionally decrease the communication overhead was not considered
[69, 70]	Local policy, global policy, learning idea	TCP CUBIC streams	Loss comparison, throughput,	Time complexity was not considered in this study
[71, 72]	Federated Averaging (Federated CIFG)	7.5 billion sentences	Recall	The time complexity and accuracy were not considered
[73, 74]	CNN	Fashion MNIST	Accuracy, weight values, time	The system was not robust enough to prevention from attackers

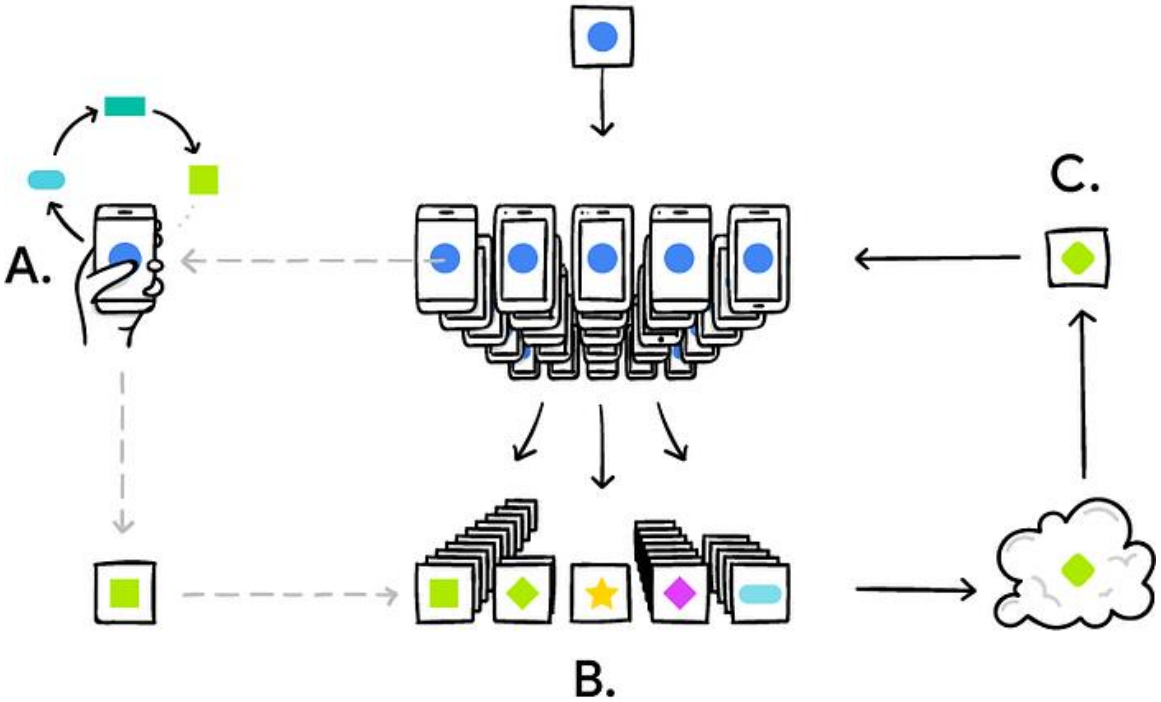

Figure 3: Attack mitigation using FL model [75]

3. Machine Learning Based Techniques for Countermeasure

3.1 Federated Learning

The general framework of FL consists of multiple clients and a cloud server, where each client downloads a shared global model from the cloud server for the local training of data. Afterward, all of the clients periodically forward their locally trained models to the cloud server. The cloud server performs a global average and aggregates the improved global model to the clients. This communication between the clients and the cloud server (usually known as a communication round) is continuously repeated until the desired convergence level is achieved. The data distribution among clients in FL further classifies it into three categories; Horizontal Federated Learning (HFL), Vertical Federated Learning (VFL), and Federated Transfer Learning (FTL). Below, we define a general framework from security perspectives: In ML, the goal is to find a model for the training data that minimizes a loss function f that defines how our learned model distribution differs from the empirical distribution.

Lipschitz Objective Function (LOF): $f(x)$ is β-Lipschitz continuous if there exists $\beta \geq 0$ such that for all $x1, x2 \in R^d$

$$|f(x1) - f(x2)| \leq \beta \|x1 - x2\|. \quad \text{Eq (5)}$$

Smooth Objective Function (SOF): $f(x)$ is L-smooth if f (x) has L-Lipchitz continuous gradient, i.e., for all $x1, x2, R^d$,

$$\|\nabla f(x1) - \nabla f(x2)\| \leq L \|x1 - x2\| \quad \text{Eq (6)}$$

Strongly Convex Objective Function (SCOF): $f(x)$ is μ- strongly convex if there exists $\mu \geq 0$ such that for all x1,x2, $Rd, f(x1) \geq f(x2)+(x1-x2)T\nabla f(x2)+\mu$

$$f(x1) \geq f(x2)+(x1-x2)T\nabla f(x2 \quad \text{Eq (7)}$$

Coercive Function (CF): $f(x)$ is coercive if $\lim \| x \| \to \infty f(x) \to \infty$.

Figure 4 represents the predictive Framework based on Federated learning. Bounded Variance (BV): The variance of each stochastic gradient $\nabla fi(x;\xi)$ is bounded if there exists $\sigma \in R$, such that.

$$E\| \nabla fi(x;\xi)- \nabla fi(x)\| 2 \leq 2, \quad \text{Eq (8)}$$

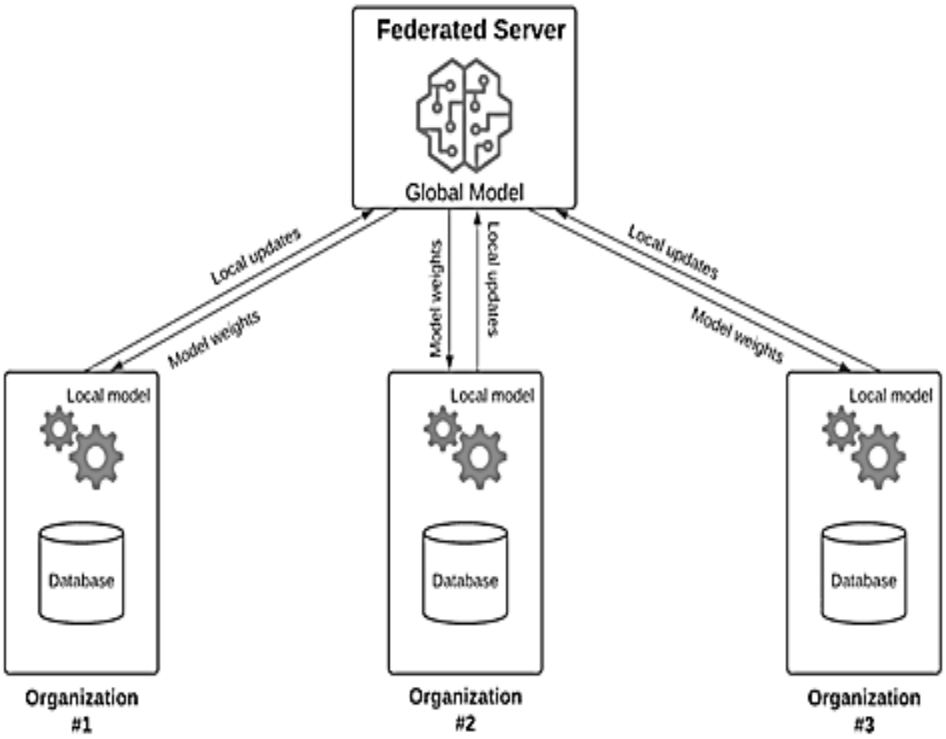

Figure 4: Predictive Framework based on Federated learning

where $fi(t)$ denotes thè local objective function of the i-th client, x is the current model parameter and is the data sampled in the current round of local training. In the above assumptions, LOF, SOF, and LH describe the smoothness of the objective function. SCOF and COF characterize the convexity of objective functions. CF ensures that the objective function has a global minimum. BG, BV, and BGD capture the properties of gradients. These gaps underscore the need for a more integrated approach that addresses technological, legal, and ethical dimensions. The Proposed Technique works based on below Algorithm:

Naive Bayes is a fast machine learning model that is based on Bayes' theorem. This predicts the probability of a query belonging to a certain class, like malicious or normal, by looking at the various features of the data. It works well when features are independent of each other.

$$P(c|x) = \frac{P(X|C).P(C)}{P(X)} \quad \text{Eq (9)}$$

P (C|X): The probability that which query belongs to the class C malicious.

P (X|C): This is the likelihood that the data of X is given to class C.

P (C): This prior probability of the class C is a common class.

P (X): This is the total probability of the data X.

This model is used for baseline because it works fast and is easy to implement. It works well with simple and structured data. A decision tree is a model that splits data based on maximum information gain. Pruning techniques were applied to reduce over-fitting.

Algorithm 1: Framework for Federated Learning

Algorithm 1 `FederatedAveraging`. The K clients are indexed by k; B is the local minibatch size, E is the number of local epochs, and η is the learning rate.

Server executes:
initialize w_0
for each round $t = 1, 2, \dots$ **do**
$m \leftarrow \max(C \cdot K, 1)$
$S_t \leftarrow$ (random set of m clients)
for each client $k \in S_t$ **in parallel do**
$w_{t+1}^k \leftarrow \text{ClientUpdate}(k, w_t)$
$w_{t+1} \leftarrow \sum_{k=1}^{K} \frac{n_k}{n} w_{t+1}^k$

ClientUpdate(k, w): *// Run on client k*
$\mathcal{B} \leftarrow$ (split $\mathcal{P}_k$ into batches of size B)
for each local epoch i from 1 to E **do**
for batch $b \in \mathcal{B}$ **do**
$w \leftarrow w - \eta \nabla \ell(w; b)$
return w to server

$$Gini\ (t) = 1 - \sum_{i-1}^{k} p_i^2 \quad \text{Eq (10)}$$

t. This is a specific node in the decision tree.

k. The classes of malicious queries in the SQL injection detection.

p_i. The proportion of the elements belonging to class I in the node T.

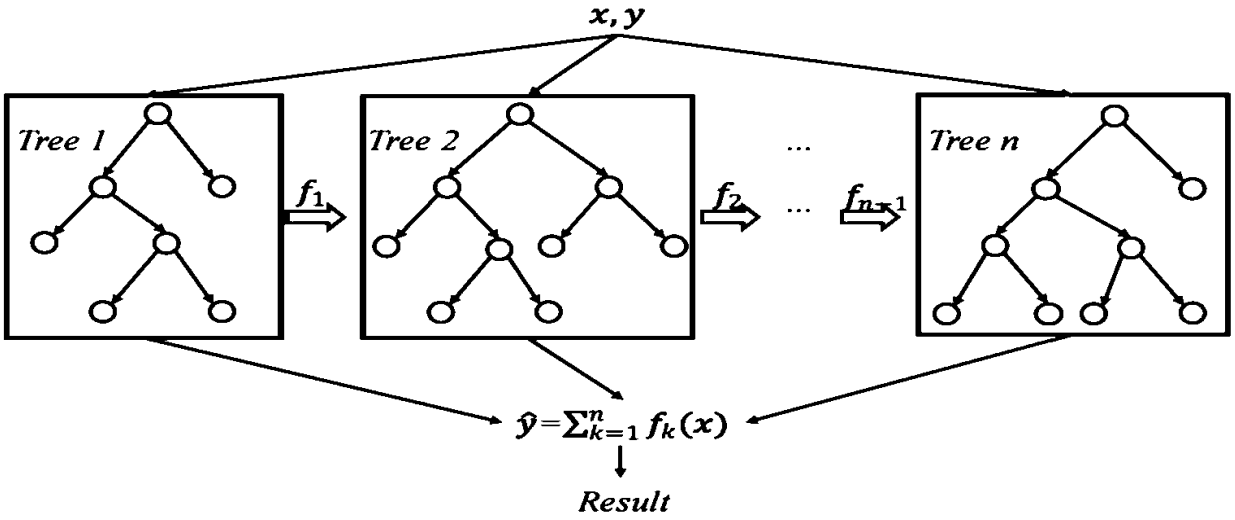

Figure 5. Machine Learning Architecture for FL

Algorithm 2: Federated Learning Algorithm for FedAvg

Algorithm 2. FedAvg

Server Procedure:

for global round $t = 0, 1, 2, ..., T-1$ do

$S \leftarrow$ sample clients at random

for $i \in S$ do

$\theta_i^{t+} \leftarrow$ Client Procedure (θ_i^t)

end for

$$\theta^{t+} \leftarrow \sum_{i=1}^{S} \frac{|D_i|}{|D_S|} \theta_i^{t+}$$

end for

Client Procedure:

$\theta_i^t = \theta^t$

for local epoch $e = 1, 2, ..., K$ do

Updates θ_i^t for e epoch of SGD on F_i with step-size μ to obtain θ_i^{t+}

end for

Return: the updated model θ_i^{t+}

We optimized the support vector machine (SVM) with a Radial Basis function kernel for non-linear classification. Hyperparameters C regularization parameter and γ kernel coefficient, were fine-tuned using the grid search strategy to achieve the optimal performance. The SVM decision function:

$$f(x) = w^T x + \quad b \qquad \text{Eq (11)}$$

W is the weight of the vector. *X* represents the feature of a vector as an input sample. *b* is the bias term. An ensemble model combining 1,000 decision trees with each tree trained on the bootstrapped samples. An important feature analysis was conducted to optimize the feature selection. A deep neural network with hidden layers, each containing 256 neurons. The dropout and batch normalization were used to prevent overfitting and accelerate convergence.

$$f(x) = \max(0, x) \ \text{(ReLU)} \qquad \text{Eq (12)}$$

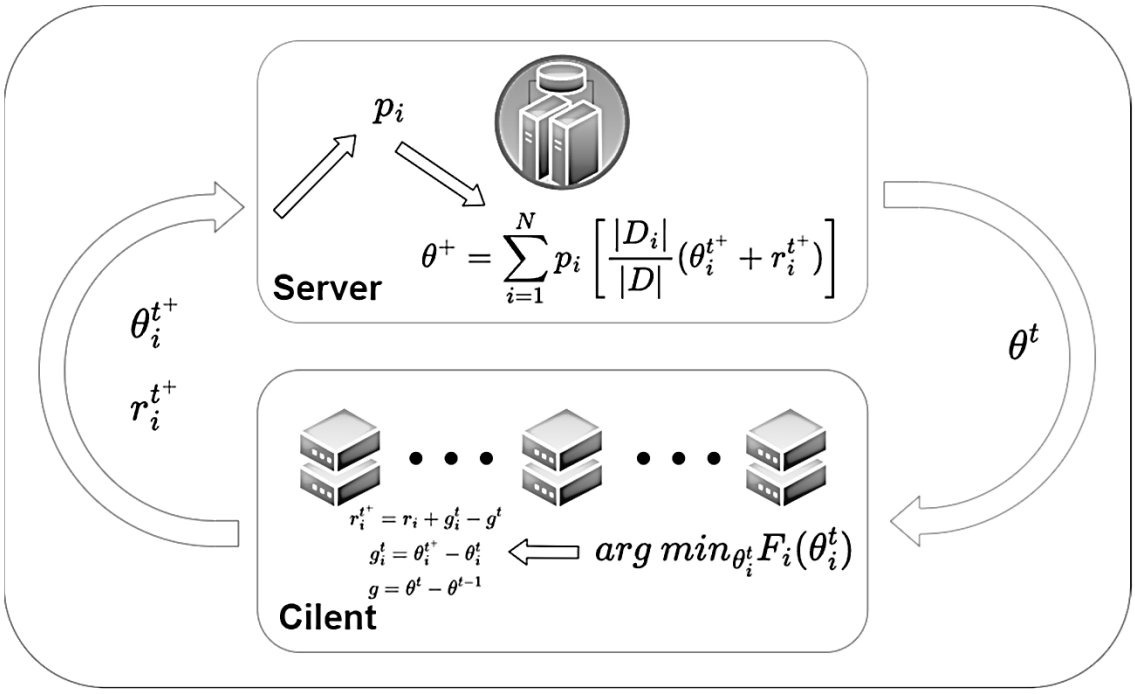

Figure 6. The training process of the FedUB algorithm.

The stacked ensemble combines ANN's nonlinear learning capacity and SVM's decision boundaries. The ANN outputs are fed into the SVM classifier to refine the prediction. Hyperparameter tuning was performed for both components. While the cryptography techniques, such as homomorphic encryption and secure multi-party computation (SMC), are widely used in the existing literature of privacy-preserving FL algorithms. In particular, each client encrypts the update before uploading it to the cloud server, where the cloud server decrypts these updates to obtain a new global model [25]. However, these techniques are vulnerable to inference attacks because each client has to share the gradients accessible to the adversaries. Applying cryptography techniques to the FL systems can also result in major computation overhead, due to the extra operations of encryption and decryption. By examining the memory for suspicious processes and DLLs used also the APIs used for call making, the examiner can find important artifacts related to any

malware. The main techniques used for the analysis of memory are memory injections and uncovering the persistence mechanism of any malware. As remote work becomes more common, VPNs are a lifeline for businesses, allowing employees to securely access company networks from anywhere. VPNs create a safe connection over the internet, ensuring that remote workers can access crucial resources without compromising security. Whether employees are working from home or different locations, VPNs ensure they can access company databases and applications securely, even on public Wi-Fi networks [26, 27]. Modern attackers employ sophisticated techniques, such as advanced persistent threats and zero-day vulnerabilities, to compromise VPN connections. Future quantum computers could render current encryption algorithms obsolete, necessitating the development of quantum-resistant protocols. Balancing robust encryption with minimal latency remains a challenge, particularly for high-traffic environments. Considering the figure below represents the two modes of Network Security Protocols, (a) Transport mode.

4. Evaluation Metrics:

The accuracy measures the proportion of the correctly classified instances, both true positives and true negatives, out of all instances. The accuracy is defined as:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad \text{Eq (13)}$$

TP: True positives where malicious queries are correctly classified as malicious.

TN: True Negative, which benign queries are correctly classified as benign.

FP: False positive, which benign queries incorrectly classified as malicious.

FN: False Negatives which malicious queries are incorrectly classified as benign.

The precision calculates how many predicted positive instances were positive.

$$Precision = \frac{TP}{TP+FP} \quad \text{Eq (14)}$$

Recall measures the model's ability to identify the actual positive instances.

$$Recall = \frac{TP}{TP+FN} \quad \text{Eq (15)}$$

The F1 Score is the harmonic mean of the Precision and Recall, Which provides a single metric to balance both.

$$F1 - Score = 2 . \frac{Precision .Recall}{Precision+Recall} \quad \text{Eq (16)}$$

The duration is required for the model to learn from the training dataset while The time taken to make the predictions on the testing dataset, is critical for real-time applications.

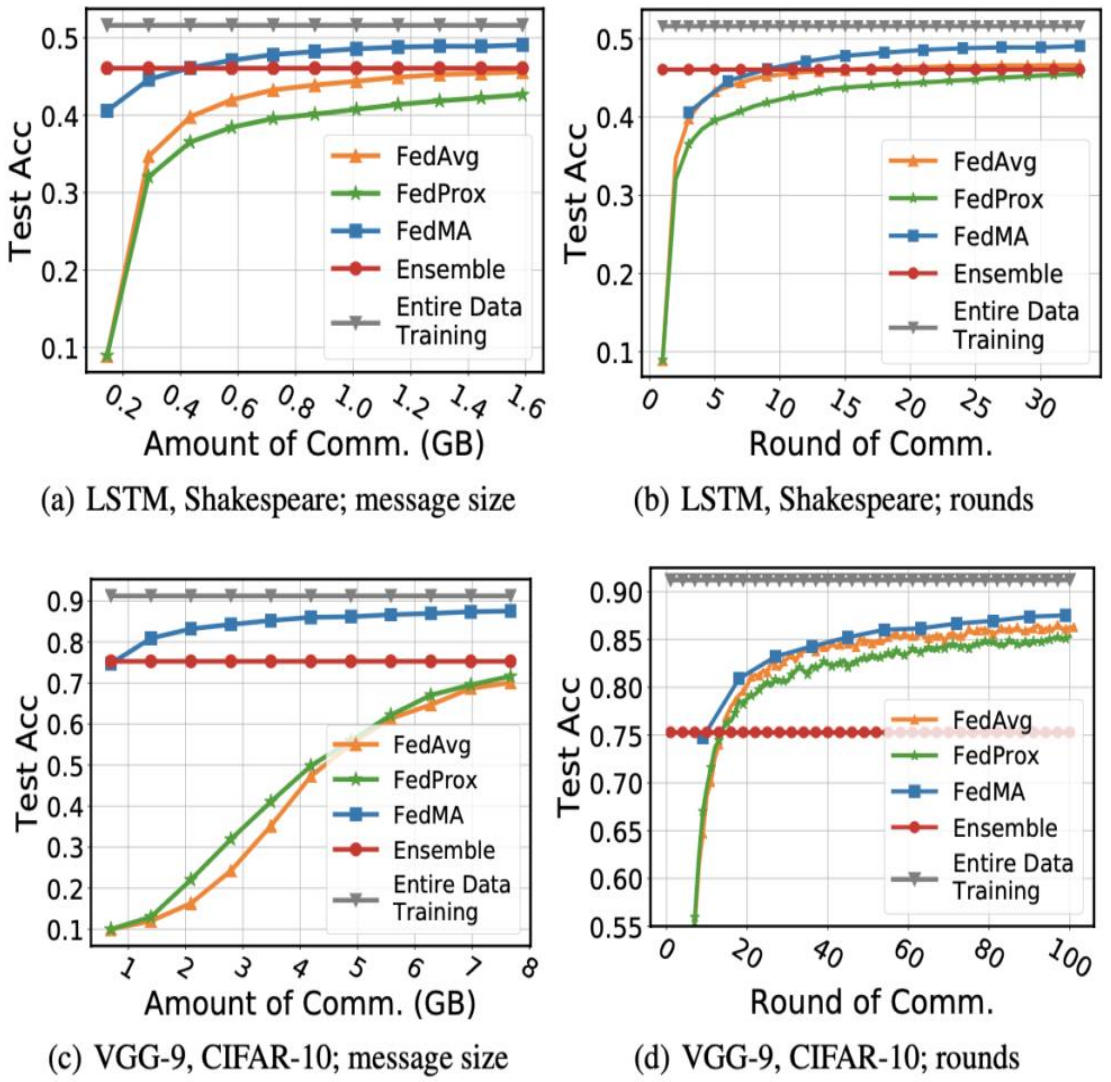

Figure 6: Convergence rates of various methods in two federated learning scenarios: training VGG-9 on CIFAR-10 with J = 16 clients and training LSTM with J = 66 clients.

Leveraging artificial intelligence for real-time threat detection and adaptive security configurations. Post-Quantum Encryption: Developing SSL/TIS protocols that resist quantum-based attacks. Edge Computing and IoT: Enhancing SSL/TIS compatibility with resource-constrained devices in edge networks. This study synthesizes insights from recent international research and practical case studies. Performance and security evaluations of SSL/TIS protocols were conducted using real-world scenarios, network analysis tools, and surveys with cybersecurity professionals. Authentication makes sure that only authorized users can connect to a SSL/TIS. Some SSL/TIS protocols offer stronger authentication methods to prevent unauthorized access and attacks like man-in-the-middle (MITM). Open SSL/TIS and IKEv2/IPsec, for instance, provide multi-factor authentication, requiring users to verify their identity through something like a password or certificate—adding an extra layer of security.

Table 3 Results of Intrusion Detection based on Federated Learning Model 1st Round

Classifier	Set	FedAvg	FedProx	Scaffold	FedDyn	FedDC	FedAvg	FedProx	Scaffold	FedDyn	FedDC	FedUB
	$K = 3$	23.48	52.34	90.58	59.89	23.48	52.34	91.34	90.62	63.23	62.19	59.89
CNN	$K = 9$	17.45	54.32	90.73	54.32	17.45	54.31	91.30	90.18	56.71	57.34	54.32
	$K = 15$	16.74	53.37	90.18	57.92	16.74	54.32	90.77	89.65	59.89	57.78	57.92
	$K = 3$	24.64	55.79	91.87	60.21	24.64	53.37	92.49	92.08	54.32	61.28	60.21
RNN	$K = 9$	19.42	54.72	91.53	53.68	19.42	55.79	92.41	92.01	57.92	56.84	53.68
	$K = 15$	17.16	54.32	91.07	57.97	17.16	54.72	92.19	91.98	**60.21**	58.92	57.97

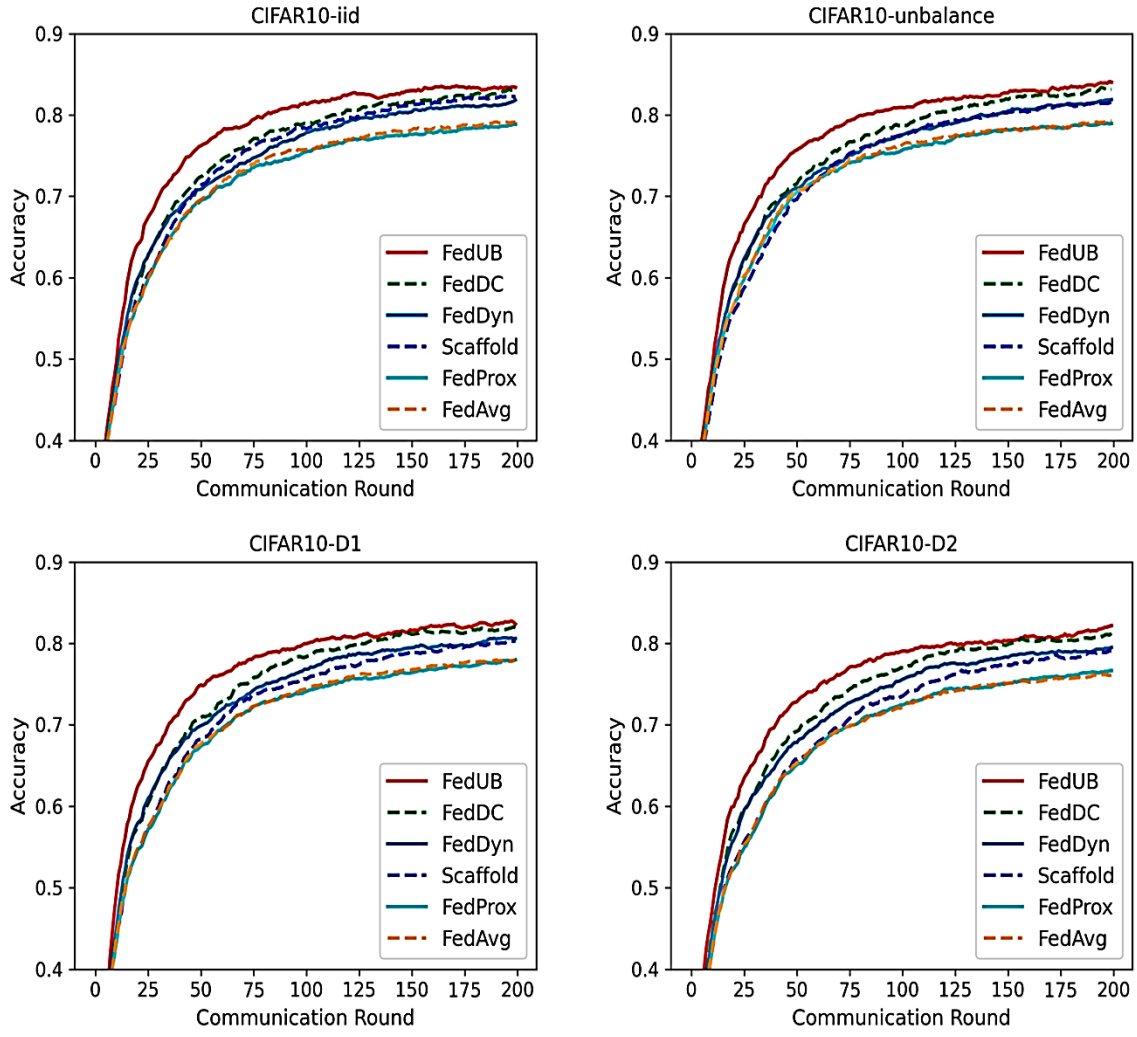

Figure 7: CNN The accuracy curves of various federated learning algorithms under four settings on CIFAR10.

The simulated the number of communication rounds required for FedUB and FedBR to achieve the specified accuracy on the CIFAR10 and CIFAR100 datasets, with a Dirichlet coefficient of 0.1.

Specifically, the target accuracy was set to 0.4 for CIFAR10 and 0.3 for CIFAR100. Additionally, we compared the final accuracy achieved by FedUB and FedBR after 200 communication rounds on the CIFAR10 dataset and 400 communication rounds on the CIFAR100 dataset. The experimental results indicate that FedUB converges faster than FedBR in the early stages but has a lower final accuracy than FedBR.

Table 4: Performance results of different federated learning algorithms on multiple data sets.

DataSet	FedAvg	FedProx	Scaffold	FedDyn	FedDC	FedUB	Ref
CIFAR10-iid	0.7911	0.7887	0.8224	0.8183	0.8322	0.8338	[76]
CIFAR10-D1	0.7794	0.7797	0.8033	0.806	0.8192	0.8236	[77]
CIFAR10-D2	0.761	0.7665	0.7905	0.7949	0.8148	0.8217	[78]
CIFAR10-unbalance	0.7928	0.7895	0.8154	0.8188	0.8317	0.8403	[79]
CIFAR100-iid	0.3935	0.3921	0.4925	0.5075	0.5468	0.5426	[80]
CIFAR100-D1	0.4058	0.4068	0.49	0.5033	0.5311	0.5271	[81]
CIFAR100_D2	0.3982	0.4039	0.49	0.4992	0.5277	0.5171	[82]
CIFAR100-unbalance	0.4029	0.4043	0.498	0.5074	0.5315	0.534	[83]
MNIST-iid	0.9806	0.9814	0.9845	0.9838	0.9836	0.984	[84]
MNIST-D1	0.979	0.9789	0.984	0.9819	0.9838	0.9843	[85]
MNIST-D2	0.9781	0.9775	0.9837	0.9828	0.9835	0.9841	[86]
MNIST-unbalance	0.9807	0.9802	0.9833	0.9835	0.9843	0.9838	[87]
EMNIST-iid	0.945	0.9457	0.9538	0.948	0.9555	0.9558	[88]
EMNIST-D1	0.9418	0.9427	0.9537	0.9473	0.9541	0.9544	[89]
Proposed	0.9807	0.9802	0.9833	0.9835	0.9843	0.9838	

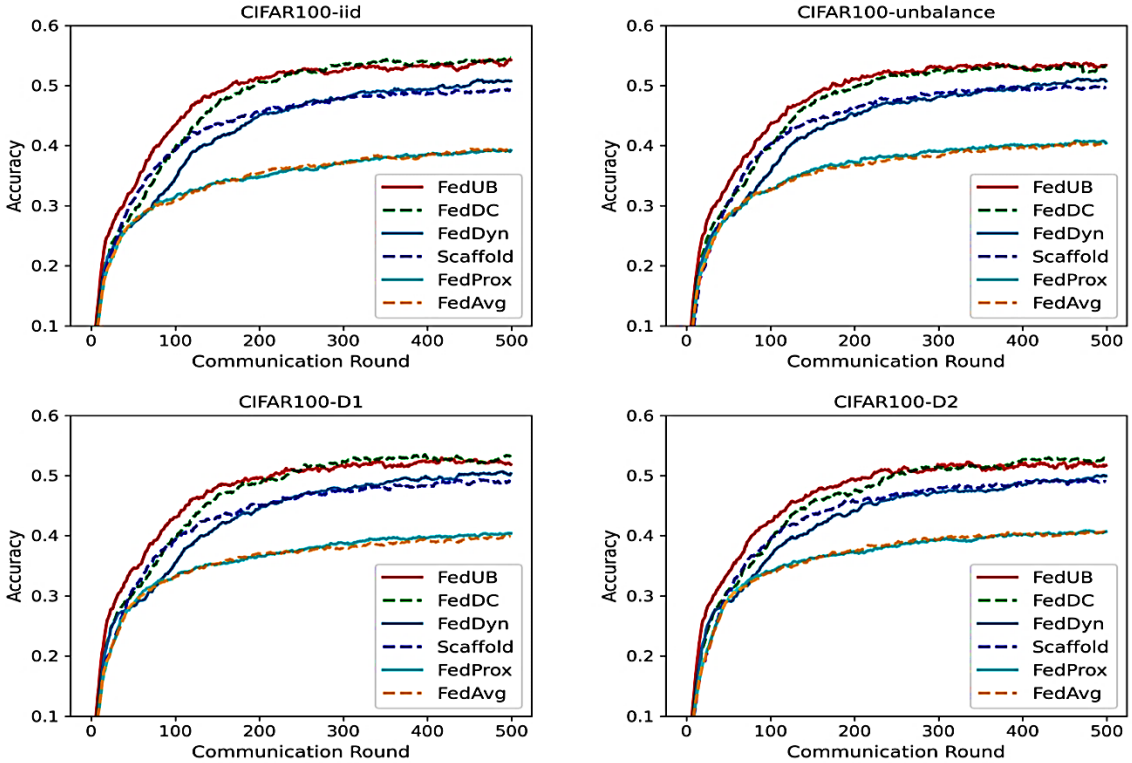

Figure 8: The accuracy curves of various federated learning algorithms under four different settings on CIFAR100.

5. Conclusion and Recommendations

In this article, one will find out more about federated learning technology, attack types, data poisoning methods, and others. Four significant issues in federated learning were revealed, such as the poor robustness of the situation prediction, the need for high computing resources, the weak communication efficiency, and the vulnerability of the system architecture. The problem of response strategies to each type of problem was introduced. The dynamic cybersecurity environment poses major challenges, which should be solved with the help of a multifaceted approach. Although technological improvements and legal systems have made significant progress, there are still gaps. These are manifested by the malfunctions between technological possibilities and the efforts of regulation and even the dilemmas of the ethics issue of the presence of surveillance technologies. To begin with, we chose some of the most popular encryption protocols and wrote down their packet structure and regular activity within a network. Secondly, our attention was on the information that is offered by the encryption protocols themselves. SSL/TIS protocols are very important for protection in modern networks, and the choice of any one will depend on its environment. In choosing SSL/TIS solution, organizations have to consider issues such as security requirements, performance requirements, network size and workforce requirements. With the ever-changing nature of technology, research and development is crucial to stay abreast of the emerging challenges such as the introduction of quantum computing and the complexity of network infrastructures, among others.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

REFERENCES

[1] Luo, J.; Wu, S. Adapt to adaptation: Learning personalization for cross-silo federated learning. In Proceedings of the IJCAI: Proceedings of the Conference, Vienna, Austria, 23–29 July 2022; Morgan Kaufmann: Amsterdam, The Netherlands; p. 2166.

[2] Zhang, J.; Hua, Y.; Wang, H.; Song, T.; Xue, Z.; Ma, R.; Guan, H. Fedala: Adaptive local aggregation for personalized federated learning. In Proceedings of the AAAI Conference on Artificial Intelligence, Washington, DC, USA, 7–14 February 2023; pp. 11237–11244.

[3] Luo, J.; Wu, S. Adapt to adaptation: Learning personalization for cross-silo federated learning. In Proceedings of the IJCAI: Proceedings of the Conference, Vienna, Austria, 23–29 July 2022; Morgan Kaufmann: Amsterdam, The Netherlands; p. 2166.

[4] Li, H.; Luo, L.; Wang, H. Federated learning on non-independent and identically distributed data. In Proceedings of the Third International Conference on Machine Learning and Computer Application (ICMLCA 2022), Shenyang, China, 16–18 December 2023; SPIE: Bellingham, WA, USA; pp. 154–162.

[5] Qu, L.; Zhou, Y.; Liang, P.P.; Xia, Y.; Wang, F.; Adeli, E.; Fei-Fei, L.; Rubin, D. Rethinking architecture design for tackling data heterogeneity in federated learning. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, New Orleans, LA, USA, 18–24 June 2022; pp. 10061–10071.

[6] Gao, L.; Fu, H.; Li, L.; Chen, Y.; Xu, M.; Xu, C.-Z. Feddc: Federated learning with non-iid data via local

drift decoupling and correction. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, New Orleans, LA, USA, 18–24 June 2022; pp. 10112–10121.

[7] M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

[8] Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

[9] U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

[10] Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

[11] Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023

[12] Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.

[13] Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

[14] Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018

[15] Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (Al) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power loT Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.

[16] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

[17] Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

[18] H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

[19] Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.

[20] S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

[21] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

[22] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[23] Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

[24] Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

[25] Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

[26] Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

[27] Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

[28] Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

[29] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3),

420-454.

[30] Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

[31] Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

[32] Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

[33] Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

[34] Fatima, M., Ali, A., Ahmad, M., Nisa, F. U., Khan, H., & Raheem, M. A. U. Enhancing The Resilience Of Iot Networks: Strategies And Measures For Mitigating Ddos Attacks. Cont.& Math. Sci., Vol.-19, No.-10, 129-152, October 2024 https://jmcms.s3.amazonaws.com/wp-content/uploads/2024/10/10072102/jmcms-2410025-ENHANCING-THE-RESILIENCE-OF-IOT-NETWORKS-MF-HK.pdf

[35] Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.

[36] Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

[37] Mustafa, M., Ali, M., Javed, M. A., Khan, H., Iqbal, M. W., & Ruk, S. A. (2024). Berries of Low-Cost Smart Irrigation Systems for Water Management an IoT Approach. Bulletin of Business and Economics (BBE), 13(3), 508-514.

[38] Hassan, A., Khan, H., Ali, A., Sajid, A., Husain, M., Ali, M., ... & Fakhar, H. (2024). An Enhanced Lung Cancer Identification and Classification Based on Advanced Deep Learning and Convolutional Neural Network. Bulletin of Business and Economics (BBE), 13(2), 136-141.

[39] Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product

and Process Modeling, 19(4), 473-515.

[40] Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, "An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

[41] Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

[42] Zaheer, M., Azeem, M. H., Afzal, Z., & Karim, H. (2024). Critical Evaluation of Data Privacy and Security Threats in Federated Learning: Issues and Challenges Related to Privacy and Security in IoT. Spectrum of Engineering Sciences, 2(5), 458-479.

[43] Ali, I., Saleem, M. U., Khan, A. A., Naz, A., Nawaz, M., & Khan, H. (2025). An Enhanced Artificial Intelligence Generated Virtual Influencer Framework: Examining the Effects of Emotional Display on User Engagement based on Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 184-209.

[44] Ayub, N., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). Forecasting Multi-Level Deep Learning Autoencoder Architecture (MDLAA) for Parametric Prediction based on Convolutional Neural Networks. Engineering, Technology & Applied Science Research, 15(2), 21279-21283.

[45] Mumtaz, J., Rehman, A. U., Khan, H., Din, I. U., & Tariq, I. Security and Performance Comparison of Window and Linux: A Systematic Literature Review. Securing the Digital Realm, 272-280.

[46] Khan, H., Ali, A., & Alshmrany, S. (2023). Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs. Computers, Materials & Continua, 75(1).

[47] Ali, R., Khan, H., Arif, M. W., Tariq, M. I., Din, I. U., Afzal, A., & Khan, M. A. Authentication of User Data for Enhancing Privacy in Cloud Computing Using Security Algorithms. In Securing the Digital Realm (pp. 187-200). CRC Press.

[48] Noor, H., Khan, H., Din, I. U., Tarq, M. I., Amin, M. N., & Fatima, M. (2025). 12 Virtual Memory Management. Securing the Digital Realm: Advances in Hardware and Software Security, Communication, and Forensics, 126.

[49] Ayub, N., Iqbal, M. W., Saleem, M. U., Amin, M. N., Imran, O., & Khan, H. (2025). Efficient ML Technique for Brain Tumor Segmentation, and Detection, based on MRI Scans Using Convolutional Neural Networks (CNNs). Spectrum of Engineering Sciences, 3(3), 186-213.

[50] Yousaf, M., Khalid, F., Saleem, M. U., Din, M. U., Shahid, A. K., & Khan, H. (2025). A Deep Learning-Based Enhanced Sentiment Classification and Consistency Analysis of Queries and Results in Search Using Oracle Hybrid Feature Extraction. Spectrum of Engineering Sciences, 3(3), 99-121.

[51] Khan, H., Usman, R., Ahmed, B., Hashimi, U., Najam, Z., & Ahmad, S. (2019). Thermal-aware real-

time task schedulabilty test for energy and power system optimization using homogeneous cache hierarchy of multi-core systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

[52] Mumtaz, J., Rehman, A. U., Khan, H., Din, I. U., & Tariq, I. Security and Performance Comparison of Window and Linux: A Systematic Literature Review. Securing the Digital Realm, 272-280.

[53] Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

[54] Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

[55] Asghar, M. A., Aslam, A., Bakhet, S., Saleem, M. U., Ahmad, M., Gohar, A., & Khan, H. (2025). An Efficient Integration of Artificial Intelligence-based Mobile Robots in Critical Frames for the Internet of Medical Things (IoMTs) Using (ADP2S) and Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 160-183.

[56] Jabeen, T., Mehmood, Y., Khan, H., Nasim, M. F., & Naqvi, S. A. A. (2025). Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), 143-161.

[57] Khan, A. K., Bakhet, S., Javed, A., Rizwan, S. M., & Khan, H. (2025). Framework for Predicting Customer Sentiment Aware Queries and Results in Search Using Oracle and Machine Learning. Spectrum of Engineering Sciences, 3(2), 588-617.

[58] Abdullah, M. M., Khan, H., Farhan, M., & Khadim, F. (2024). An Advance Machine Learning (ML) Approaches for Anomaly Detection based on Network Traffic. Spectrum of engineering sciences, 2(3), 502-527.

[59] Hashmi, U., & ZeeshanNajam, S. A. (2023). Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

[60] P. Mathur, Overview of machine learning in healthcare, in: Machine Learning Applications using Python, A Press, Berkeley, CA, 2019, pp. 1–11.

[61] P. Guleria, M. Sood, Intelligent learning analytics in healthcare sector using machine learning, in: Machine Learning with Health Care Perspective, Springer, Cham, 2020, pp. 39–55.

[62] V.V. Kumar, Healthcare Analytics Made Simple: Techniques in Healthcare Computing using Machine Learning and Python, Packt Publishing Ltd., 2018, Available at: https://books.google.com/books?hl=en&lr=&id=nwZnDwAAQBAJ&

[63] Sultan, H., Rahman, S. U., Munir, F., Ali, A., Younas, S., & Khan, H. (2025). Institutional dynamics,

innovation, and environmental outcomes: a panel NARDL analysis of BRICS nations. Environment, Development and Sustainability, 1-43.

[64] Hussain, M., Ahmed, H. A., Babar, M. Z., Ali, A., Shahzad, H. M., Rehman, S. U., ... & Alshahrani, A. M. (2025). An Enhanced Convolutional Neural Network (CNN) based P-EDR Mechanism for Diagnosis of Diabetic Retinopathy (DR) using Machine Learning. Engineering, Technology and Applied Science Research, 15(1), 19062-19067.

[65] Ramzan, M. S., Nasim, F., Ahmed, H. N., Farooq, U., Nawaz, M. S., Bukhari, S. K. H., & Khan, H. (2025). An Innovative Machine Learning based end-to-end Data Security Framework in Emerging Cloud Computing Databases and Integrated Paradigms: Analysis on Taxonomy, challenges, and Opportunities. Spectrum of engineering sciences, 3(2), 90-125.

[66] Hussain, S., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). An Enhanced Random Forest (ERF)-based Machine Learning Framework for Resampling, Prediction, and Classification of Mobile Applications using Textual Features. Engineering, Technology & Applied Science Research, 15(1), 19776-19781.

[67] Ahmad, I., Nasim, F., Khawaja, M. F., Naqvi, S. A. A., & Khan, H. (2025). Enhancing IoT Security and Services based on Generative Artificial Intelligence Techniques: A Systematic Analysis based on Emerging Threats, Challenges and future Directions. Spectrum of engineering sciences, 3(2), 1-25.

[68] Khan, H., Imtiaz, M. A., Siddique, H., Rana, M. T. A., Ali, A., Baig, M. Z., ... & Alsaawy, Y. (2025). An Enhanced Task Migration Technique Based on Convolutional Neural Network in Machine Learning Framework.

[69] Fawy, K. F., Rodriguez-Ortiz, G., Ali, A., Jadeja, Y., Khan, H., Pathak, P. K., ... & Rahman, J. U. (2025). Catalytic exploration metallic and nonmetallic nano-catalysts, properties, role in photoelectrochemistry for sustainable applications. Reviews in Inorganic Chemistry, (0).

[70] Liaqat, M. S., Sharif, N., Ali, A., Khan, H., Ahmed, H. N., & Khan, H. (2024). An Optimal Analysis of Cloud-based Secure Web Applications: A Systematic Exploration based on Emerging Threats, Pitfalls and Countermeasures. Spectrum of engineering sciences, 2(5), 427-457.

[71] Khawar, M. W., Salman, W., Shaheen, S., Shakil, A., Iftikhar, F., & Faisal, K. M. I. (2024). Investigating the most effective AI/ML-based strategies for predictive network maintenance to minimize downtime and enhance service reliability. Spectrum of Engineering Sciences, 2(4), 115-132.

[72] Ahmad, J., Salman, W., Amin, M., Ali, Z., & Shokat, S. (2024). A Survey on Enhanced Approaches for Cyber Security Challenges Based on Deep Fake Technology in Computing Networks. Spectrum of Engineering Sciences, 2(4), 133-149.

[73] Ayub, N., Ejaz, A., Hassan, B., Hussain, M. Z., Nadeem, M., Sabir, L., & Fatima, S. (2025). An Efficient Machine Learning And Deep Learning Based Deep Packet Security Framework For Detection Of Computing Network Faults In The Iots. Spectrum of Engineering Sciences, 3(5), 659-674.

[74] Ayub, N., Habib, Z., Bakhet, S., Riaz, S., Rizwan, S. M., Abid, M., ... & Khan, H. (2025). An Optimal Ai & Deep Learning Mechanism For Mitigating Hacking Threat Identification Using Secure Network Infrastructure Based On Linux And Software-Defined Network (Sdn). Spectrum of Engineering Sciences, 3(5), 675-687.

[75] Zebrack, J. S. et al. Usefulness of high-sensitivity C-Reactive protein in predicting long-term risk of death or acute myocardial infarction in patients with unstable or stable angina pectoris or acute myocardial infarction. Am. J. Cardiol. 89, 145–149 (2002).

[76] Aslam, I., Tariq, W., Nasim, F., Khan, H., Khawaja, M. F., Ahmad, A., & Nawaz, M. S. (2025). A Robust Hybrid Machine Learning based Implications and Preventions of Social Media Blackmailing and Cyber bullying: A Systematic Approach.

[77] Ayub, N., Anwer, M. A., Iqbal, A., Rizwan, S. M., Shahbaz, A., Abid, M. H., & Rafi, S. (2025). Enhanced ML Framework based on Artificial Neural Network for countermeasures of Data Protection and Network Vulnerabilities Detection in Industrial Internet of Things. Annual Methodological Archive Research Review, 3(5), 410-431.

[78] Gordon, T. & Kannel, W. B. Multiple risk functions for predicting coronary heart disease: The concept, accuracy, and application.Am. Heart J. 103, 1031–1039 (1982).

[79] Ayub, N., Imtiaz, M. A., Ali, E., Alqahtani, A. M., Ali, A., Ashurov, M., ... & Law, F. L. (2025). A Decision Framework for Intra Task Fixed Priority INTEL PXA270 Distributed Architecture for Soft RT-Applications Based on Deep Learning. Engineering, Technology & Applied Science Research, 15(3), 23553-23558.

[80] Ayub, N., Waheed, A., Ahmad, S., Akbar, M. H. A., Fuzail, M. Z., & Hashmi, A. H. (2025). Strengthening Network Security: An Efficient DL Enabled Data Protection and Privacy Framework for Threat Mitigation and Vulnerabilities Detection in IoT Network. Annual Methodological Archive Research Review, 3(6), 1-25.

[81] Wilson, P. W. F. et al. Prediction of coronary heart disease using risk factor categories. Circulation 97, 1837–1847 (1998).

[82] Gordon, T. Diabetes, blood lipids, and the role of obesity in coronary heart disease risk for women. Ann. Intern. Med. 87, 393 (1977).

[83] Ayub, N., Waheed, A., Ahmad, S., Akbar, M. H. A., Fuzail, M. Z., & Hashmi, A. H. (2025). Strengthening Network Security: An Efficient DL Enabled Data Protection and Privacy Framework for Threat Mitigation and Vulnerabilities Detection in IoT Network. Annual Methodological Archive Research Review, 3(6), 1-25.

[84] Rumelhart, D.E.; Hinton, G.E.; Williams, R.J. Learning representations by back-propagating errors. Nature 1986, 323, 533–536.

[85] Criado, M.F.; Casado, F.E.; Iglesias, R.; Regueiro, C.V.; Barro, S. Non-iid data and continual learning

processes in federated learning: A long road ahead. Inf. Fusion 2022, 88, 263–280.

[86] Xu, J.; Tong, X.; Huang, S.-L. Personalized federated learning with feature alignment and classifier collaboration. arXiv 2023, arXiv:2306.11867.

[87] Mothukuri, V.; Parizi, R.M.; Pouriyeh, S.; Huang, Y.; Dehghantanha, A.; Srivastava, G. A survey on security and privacy of federated learning. Future Gener. Comput. Syst. 2021, 115, 619–640.

[88] Rahman, A.; Hasan, K.; Kundu, D.; Islam, M.J.; Debnath, T.; Band, S.S.; Kumar, N. On the ICN-IoT with federated learning integration of communication: Concepts, security-privacy issues, applications, and future perspectives. Future Gener. Comput. Syst. 2023, 138, 61–88.