Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

Online ISSN
3007-3138

Print ISSN
3007-312X

An Enhanced Machine Learning based Data Privacy and Security Mitigation Technique: An Intelligent Federated Learning (FL) Model for Intrusion Detection and Classification System for Cyber-Physical Systems in Internet of Things (IoTs)

M. Aetsam Javed[1*]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan. Corresponding Author Email: SU92-PHCSW-F24-023@superior.edu.pk
Muhammad Ahmad[2]
National University of Sciences & Technology (NUST)
mailingtoahmad@gmail.com
Junaid Ahmed[3]
Punjab Safe Cities Authority. iub.junaid@gmail.com
Syed Muhammad Rizwan[4]
Punjab Safe Cities Authority, Department of Computer Engineering, University of Engineering and Technology Lahore, Pakistan.
rizwan.naqvi@ieee.org
Anum Tariq[5]
University of Engineering and Technology Lahore.
connectanumtariq@gmail.com
Hamayun Khan[6]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan.
hamayun.khan@superior.edu.pk

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

Abstract

The rapid development of industrial infrastructures with intelligent networking and computing technologies have dramatically increased the attack surface of cyber-physical systems (CPSs). Federated learning is a distributed learning method used to solve data security and privacy using machine learning, aiming to train global models together via multiple clients without sharing data. The rapid evolution of cyber threats poses significant challenges to modern cybersecurity systems and their associated legal frameworks. This paper addresses the problem of increasingly sophisticated breach methods that outpace traditional defense mechanisms. we propose an optimal federated learning Model, to detect and classify cyber threats against CPSs. Specifically for IoTs intrusion detection using federated learning framework. Data security and privacy received a great deal of research attention recently, as privacy protection becoming a key factor in the development of artificial intelligence based IOTs. It noted that security is a crucial issue in the End-to-End data security approach. The application of Machine Learning (ML) techniques to the well-known intrusion detection systems (IDS) is key to cope with increasingly sophisticated cybersecurity attacks through an effective and efficient detection process. This paper provides a comprehensive exploration of Federated Learning and Virtual security techniques emphasizing their importance in modern networking for ensuring secure communication over untrusted networks like the internet. This study delves into various data security protocols such as PPTP, L2TP/IPsec, OpenVPN, IKEv2/IPsec, and WireGuard, evaluating their security mechanisms, strengths, and vulnerabilities. The paper also

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

examines the emerging challenges in Machine Learning based model. In future a Deep learning based Fedrated model can be used in detecting cyber threats to industrial CPSs by optimizing VPN usage to enhanced network security in an increasingly complex digital landscape.

Keywords: Cyber-physical systems (CPSs). Security Protocols, Encryption, OpenVPN, IKEv2/IPsec, WireGuard, Quantum Computing

Introduction

Modern IT infrastructures can cover large geographic areas, and therefore, secure and reliable IT infrastructures are needed, while also guaranteeing low-cost factors, both in terms of space and time. The virtual private network (VPN) is one of the most reliable technology to satisfy this type of need, passing both through the "old" (PSTN) and through the most modern 4G/5G architectures [1]. A Virtual Private Network (VPN) creates a secure connection between a user's device and a remote server, ensuring privacy and data integrity over public networks. This is achieved through tunneling protocols, encryption standards, and robust authentication mechanisms [2, 3]. As cyber threats become increasingly sophisticated, understanding the role of VPNs in mitigating these risks is critical. This paper explores the technological evolution of VPNs, examines their contemporary applications, and identifies potential advancements to address emerging security challenges [4]. The Internet of Things (IoT) has achieved great popularity and acceptance with the rapid growth of high-speed networks and smart devices. In this respect, IoT represents a network, in which "things" or devices are interconnected

Vol. 3 No. 2 (2025)
Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

through a public or a private network [5, 6]. These devices are equipped with tiny sensors and powerful hardware that collect and process data at unprecedented speed Researchers have explored various approaches to address these concerns, including the development of lightweight cryptographic algorithms to secure data transmission and storage in resource-constrained IoT devices. Additionally, efforts have been made to design secure frameworks and authentication protocols to mitigate the risks of IoT-related security breaches. Another key challenge in the IoT domain is the protection of user privacy [7, 8]. As IoT devices collect and transmit vast amounts of personal data, there is a growing concern about the potential misuse of this information, such as unauthorized surveillance, profiling, and targeted advertising [9].

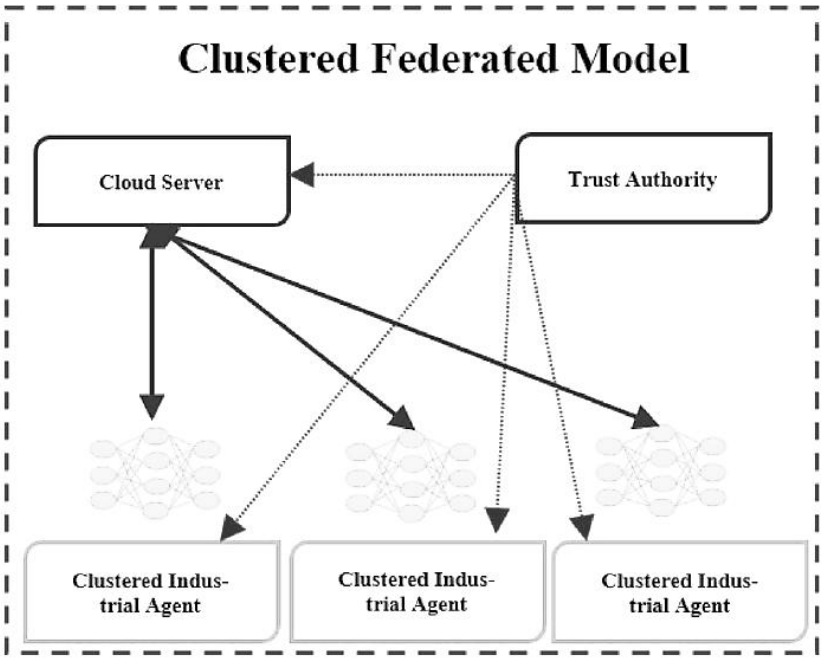

Figure 1: Clustered Federated Model in Emerging CPS for data security [10]

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

Mathews Coefficient Correlation (MCC)

MCC is widely used for accuracy calculation rate in FL while significant advancements have been made in cybersecurity technologies and legal frameworks, [11]. 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 [12].

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

Data Poisoning Attack Methods

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 [13, 14].

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

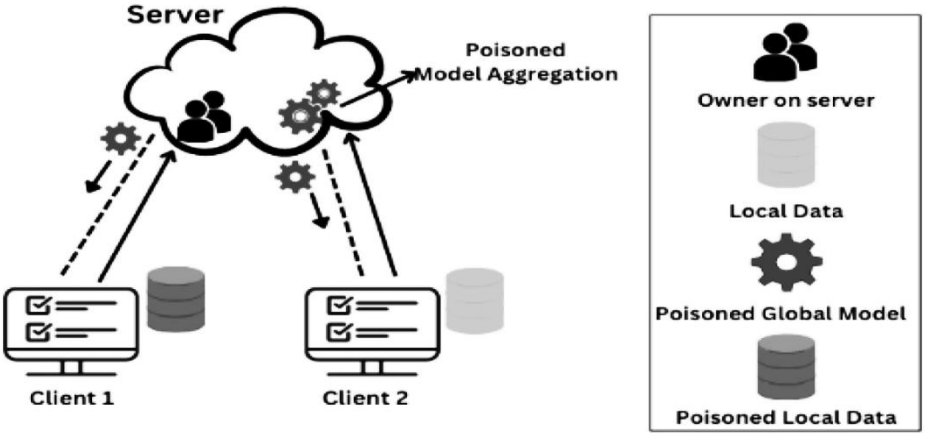

Figure 2: Data Poisoning Security attacks under FL model [15]

In realistic scenarios, the latency of inferring directly from participants is much lower communication 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 . 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 [16, 17]. Transmitting private data through a dedicated private circuit.

PPTP Security Protocol

PPTP was easy to use and integrated well with Microsoft's Windows systems, leading to its widespread adoption. However, it wasn't long before it became clear that PPTP had significant security flaws, particularly with weak encryption. As a result, it couldn't offer the level of protection needed for sensitive data.

Vol. 3 No. 2 (2025)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

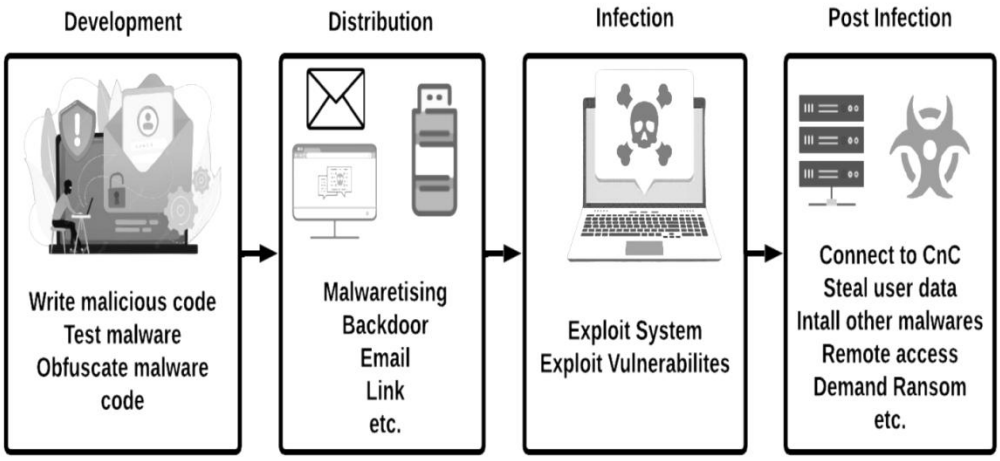

Figure 3: Life Cycle of Malware [18]

The following are common assumptions used in the convergence analysis of Federated Learning optimization algorithms

Machine Learning Based Techniques for Coutner Measure

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 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) [20, 21]. Below, we define general framework from security perspectives: In ML, the goal is to find a model for the training data that minimizes

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

a loss function f that defines how our learned model distribution differs from the empirical distribution.

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

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

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

Lipschitz Objective Function (LOF): $f(x)$ is β-Lipschitz continuous if there exists

$\beta \geq 0$ such that for all $x1,x2 \in Rd$

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

Smooth Objective Function (SOF): $f(x)$ is L-smooth if f (x) has L-Lipschitz con- tinuous gradient, i.e., for all $x1,x2 \in Rd$,

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

Strongly Convex Objective Function (SCOF): $f(x)$ is μ- strongly convex if there exists $\mu \geq 0$ such that for all $x1,x2 \in Rd, f(x1) \geq f^{2}(x2)+(x1 - x2)T \nabla f(x2)+ \mu$

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

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

Bounded Variance (BV): The variance of each stochastic gradient ∇fi(x;ξ) is bounded if there exists $\sigma \in$ R, such that

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

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

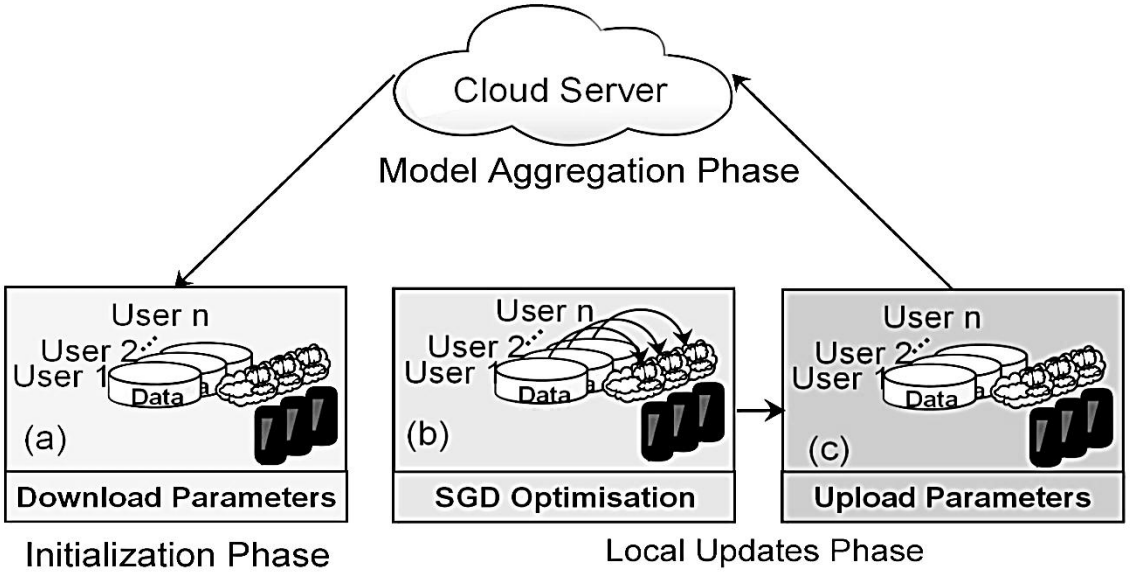

Figure 4: Generalize Framework for Federated Learning

where *fi*(*t*) dẹnotes the local objective function of the i-th client, x is the current model parameter and ξ is the data sampled in the current round of local trainin In 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 proper- ties of gradients. These gaps underscore the need for a more integrated approach that addresses technological, legal, and ethical dimensions.The Proposed Technique works on the basis of below Algorithm:

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

Algorithm 1: Framework for Federated Learning

Step 1. Initialize the training models $\{k_1, k_2, ...k_m\}$, learning rate 'η', regularization 'λ', model parameters ΘA, ΘB, datasets $\{L_1, L_2, ...L_m\}$, space feature M_a and M_b;

Step 2. Minimize *k(i)* parameter '*w*' is

$$Min_w^k(i) = \sum_{j=1}^{M} k_i(w \mid L_i)$$

Step 3. The objective of the training is

$$Min \sum_i [\| \theta_A M_i^A + \theta_B M_i^B] - [N_i \| + \frac{\lambda}{2}(\|\theta_A\|^2 + \|\theta_B\|^2)]$$

Step 4. The encrypted loss is

$$L = \left[\left[\sum_i ((U_i^A + U_i^B - N_i))^2 + \frac{\lambda}{2}(\theta_A^2 + \theta_B^2) \right]\right]$$

Step 5. The gradients are

$$\left[\left[\frac{\delta L}{\delta \theta_A} \right]\right] = \sum_i d_i M_i^A + \lambda \theta_A \text{ , and}$$

$$\left[\left[\frac{\delta L}{\delta \theta_B} \right]\right] = \sum_i d_i M_i^B + \lambda \theta_B$$

Step 6. The models are retrained

Step 7. Encrypts the data randomly

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

$$\sum_{i=\{1.,.,.n\}/k}^{n} \frac{c_i}{\tau_i} + \frac{c_k + \alpha_k}{\tau_k} \quad \text{Eq (9)}$$

While another task t_2 with intrusions arrive with the earliest deadline before the end of the execution task t_1 then the length of the idle interval due to network delay and threat is denoted as λ_j and max time duration for the idle period is represented as α_j during longer data attack that can be measured using Eq. (10).

$$\sum_{i=\{1.,.,.n\}/(k,j)}^{n} \frac{c_i}{\tau_i} + \frac{c_k + \alpha_k}{\tau_k} + \frac{c_j + \alpha_j}{\tau_j} = 1 \quad \text{Eq (10)}$$

$$\sum_{i=\{1.,.,.n\}/(k,j)}^{n} \frac{c_0}{\tau_0} + \frac{c_0 + \alpha_0}{\tau_0} + \frac{c_0 + \alpha_0}{\tau_0} \quad \text{Eq (11)}$$

$$\sum_{i=\{1.,.,.n\}/(k,j)}^{n} \frac{c_1}{\tau_1} + \frac{c_1 + \alpha_1}{\tau_1} + \frac{c_1 + \alpha_1}{\tau_1} \quad \text{Eq (12)}$$

$$\sum_{i=\{1.,.,.n\}/(k,j)}^{n} \frac{c_3}{\tau_3} + \frac{c_3 + \alpha_3}{\tau_3} + \frac{c_3 + \alpha_3}{\tau_3} \quad \text{Eq (13)}$$

$$\sum_{i=\{1.,.,.n\}/(k,j)}^{n} \frac{c_n}{\tau_n} + \frac{c_n + \alpha_n}{\tau_n} + \frac{c_n + \alpha_n}{\tau_n} \quad \text{Eq (14)}$$

This paper aims to provide a comprehensive analysis of the challenges in cybersecurity and legal responses, highlighting existing gaps and proposing potential solutions. By reviewing recent literature and examining emerging trends, this study seeks to outline the critical issues and offer actionable recommendations. The findings

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

emphasize the importance of global collaboration, adaptive legal frameworks, and ethical considerations in creating a more secure digital environment. The structure of the paper includes an extended literature review, a discussion of key findings, and a conclusion outlining practical implications and future research directions. The increasing sophistication of cyber threats has rendered traditional defense mechanisms inadequate. identify a critical issue in leveraging threat intelligence, noting that organizations struggle to process and act on the vast amounts of data required to prevent attacks. Emerging trends in cybersecurity highlight the growing importance of global collaboration and information sharing. Argue that a standardized international approach to cybersecurity is essential for addressing cross-border threats. Additionally, advancements in blockchain technology and decentralized systems offer promising solutions to some of the challenges in cybersecurity. Note that blockchain can enhance data integrity and reduce the risk of breaches, though attackers are already finding ways to exploit vulnerabilities in these systems. VPNs are indispensable tools in today's digital ecosystem, serving as safeguards for personal privacy, enterprise data security, and secure communication in remote work settings. They ensure confidentiality, integrity, and authentication, enabling secure transmission of sensitive information. Moreover, VPNs are instrumental in circumventing geo-restrictions and ensuring internet freedom, particularly in regions with stringent censorship laws [23, 24].

$$P(c|x) = \frac{P(X|C).P(C)}{P(X)} \qquad \text{Eq (15)}$$

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

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

P (X|C): This is the likelihood 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.

WireGuard was designed to be simpler, faster, and more secure than older protocols. Unlike its predecessors, WireGuard features a minimalistic codebase, making it easier to implement and audit for security flaws. WireGuard quickly gained attention due to its excellent performance and simplicity, making it a popular choice for both developers and users. It became a strong contender against established VPN protocols like OpenVPN and IKEv2, offering both speed and high-level encryption. Naive Bayes is the fast machine learning model which is based on Bayes' theorem. Which predicts the probability of a query belonging to a certain class like malicious or normal, by looking at the various features of data. It works well when features are independent of each other. 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 the overfitting.

$$Gini\ (t) = 1 - \sum_{i-1}^{k} p_i^2 \qquad \text{Eq (16)}$$

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*.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

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:

$$f(x) = w^T x + \quad b \qquad \text{Eq (17)}$$

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. The feature important 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.

$$\mathbf{f(x) = max(0, x)\ \ (ReLU)} \qquad \text{Eq (18)}$$

Evalaution of Cyber-Physical Systems in Internet of Things

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 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 in order to obtain a new global model

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[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 this below figure represents the two modes Network Security Protocols (a) Transport mode .

Vol. 3 No. 2 (2025)
Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

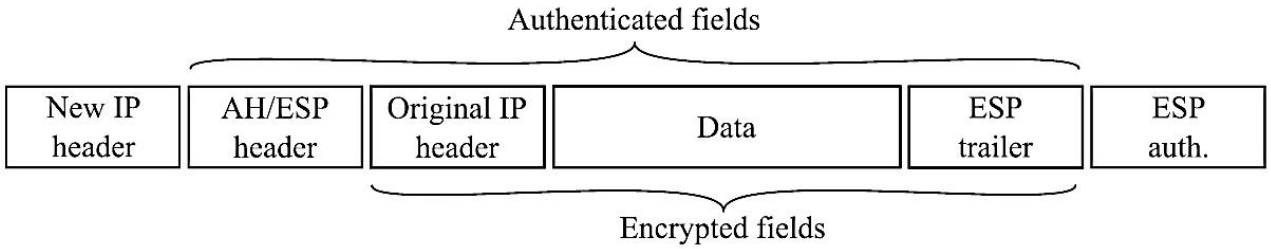

Figure 5: Network Security Protocols (a) Transport mode [28]

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:

$$\boldsymbol{Accuracy} = \frac{\boldsymbol{TP+TN}}{\boldsymbol{TP+TN+FP+FN}} \qquad \textit{Eq (19)}$$

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

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

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

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

The precision calculates how many predicted positive instances were positive.

$$\boldsymbol{Precision} = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FP}} \qquad \textit{Eq (20)}$$

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

$$\boldsymbol{Recall} = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FN}} \qquad \text{Eq (21)}$$

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

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

$$F1 - Score = 2 . \frac{Precision . Recall}{Precision + Recall}$$ Eq (22)

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.

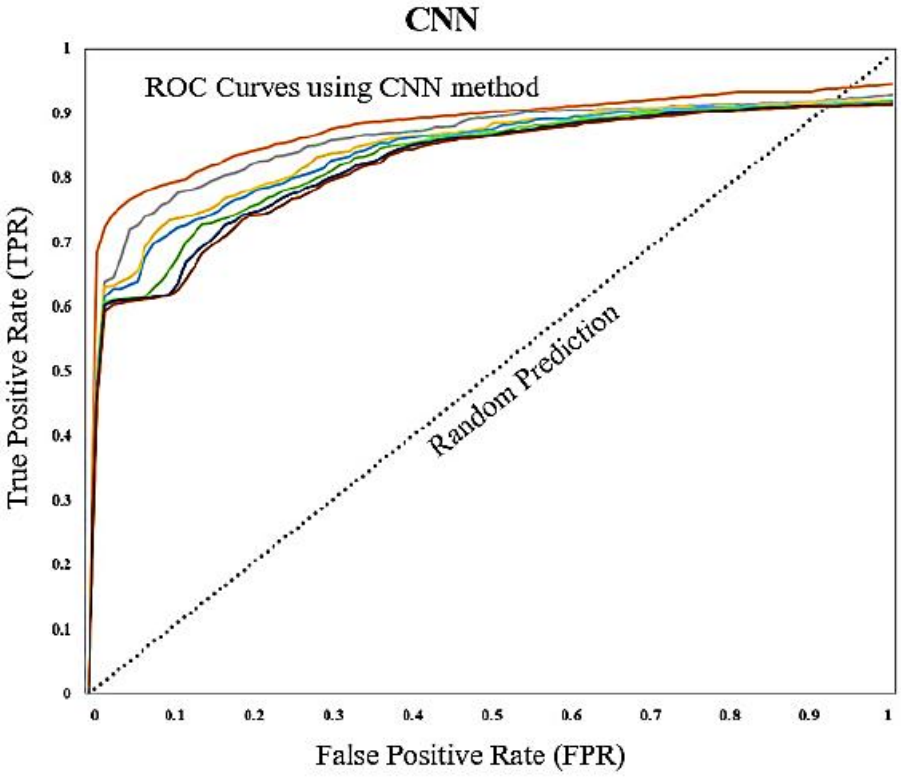

Figure 6: CNN ROC curves with K=3, K=9, K=15

Table 1: Security Countermeasures Effectiveness

Countermeasure	Description	Effectiveness Rating
Machine Learning-Based Detection	Using machine learning algorithms to detect anomalous behaviors indicating attacks.	85%
Blockchain-Based	Decentralized, tamper-proof	75%

Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

Authentication	authentication to secure sessions and credentials.	
Web Application Firewalls (WAFs)	Filtering and monitoring HTTP requests to detect and block malicious activity.	80%
Secure Coding Practices	Implementing code practices like input sanitization and parameterized queries.	90%
Multi-Factor Authentication (MFA)	Enhancing user authentication by requiring multiple verification factors.	95%

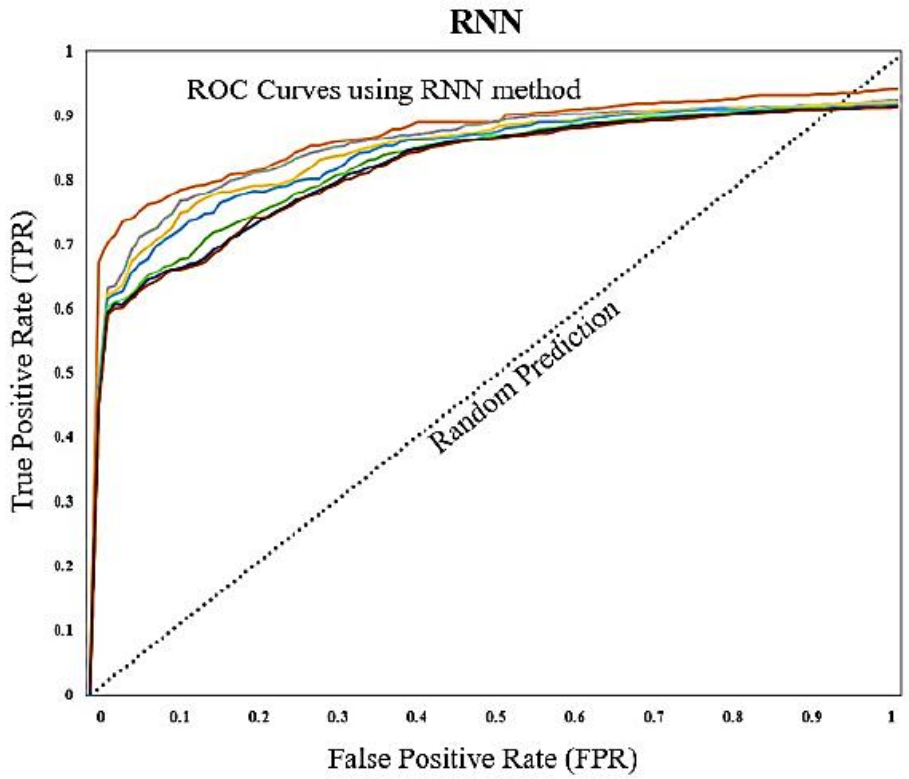

Figure 6: RNN ROC curves with K=3, K=9, K=15

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

AI Integration: Leveraging artificial intelligence for real-time threat detection and adaptive security configurations. Post-Quantum Encryption: Developing VPN protocols that resist quantum-based attacks. Edge Computing and IoT: Enhancing VPN 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 VPN 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 VPN. Some VPN protocols offer stronger authentication methods to prevent unauthorized access and attacks like man-in-the-middle (MITM). OpenVPN 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 2: Results of Intrusion Detection based on Federated Learning Model

		1st Round						50th Round					
Classifier	**Clients**	**IID**			**Non-IID**			**IID**			**Non-IID**		
		B	**W**	**G**	**B**	**W**	**G**	**B**	**W**	**G**	**B**	**W**	**G**
	K = 323.48	52.34	90.58	59.89	23.48	52.34	91.34	90.62	63.23	62.19	59.89	59.89	
CNN	*K* = 917.45	54.32	90.73	54.32	17.45	54.31	91.30	90.18	56.71	57.34	54.32	54.32	
	K = 1516.74	53.37	90.18	57.92	16.74	54.32	90.77	89.65	59.89	57.78	57.92	57.92	
	K = 324.64	55.79	91.87	60.21	24.64	53.37	92.49	92.08	54.32	61.28	60.21	60.21	
RNN	*K* = 919.42	54.72	91.53	53.68	19.42	55.79	92.41	92.01	57.92	56.84	53.68	53.68	

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

K =	1517.16	54.32	91.07	57.97	17.16	54.72	92.19	91.98	**60.21**	58.92	57.97	57.97

Conclusion and Recommendations

This article elaborates on the concepts of federated learning technology, attack types, data poisoning methods, etc. Four major problems in federated learning were identified: fragile system architecture, low communication efficiency, large consumption of computing resources, and poor situation prediction robustness. Response strategies for each type of problem were introduced.The evolving cybersecurity landscape presents significant challenges that require a multifaceted approach to address effectively. While technological advancements and legal frameworks have made important strides, critical gaps remain. These gaps are evident in the disconnect between technological capabilities and regulatory measures, as well as the ethical concerns surrounding surveillance technologies.

First, we selected a number of the most widely used encryption protocols and described their packet structure and standard behavior in a network. Second, we focused on information that is provided by encryption protocols themselves. VPN protocols are crucial for securing modern networks, but choosing the right one depends on the specific needs and conditions of each environment. Organizations must weigh factors like security requirements, performance needs, network size, and workforce demands when selecting a VPN solution. As technology continues to evolve, ongoing research and development will be necessary to keep up with emerging challenges, including the rise of quantum computing and the increasing complexity of network infrastructures.

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

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] Tahir, R. A study on malware and malware detection techniques. Int. J. Educ. Manag. Eng. , vol. 8, no. 20, 2018.

[2] Aliyyah Rosyidah1 , Jumadi Mabe Parenreng, "Network Security Analysis Based on Internet Protocol Security Using Virtual Private Network (VPN)" July, 06 2023

[3] Leukfeldt, E.R.; Kleemans, E.R.; Stol, W.P. Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. Br. J. Criminol. 2017, 57, 704–722.

[4] Alenezi, M.N.; Alabdulrazzaq, H.; Alshaher, A.A.; Alkharang, M.M. Evolution of malware threats and techniques: A review. Int. J. Commun. Netw. Inf. Secur. 2020, 12, 326–337.

[5] Ghafir, I., Hammoudeh, M., Prenosil, V., Han, L., Hegarty, R., Rabie, K., & Aparicio-Navarro, F. J. (2018). Detection of advanced persistent threat using machine-learning correlation analysis. Future Generation Computer Systems, 89, 349-359.

[6] Joloudari, J. H., Haderbadi, M., Mashmool, A., GhasemiGol, M., Band, S. S., & Mosavi, A. (2020). Early detection of the advanced persistent threat attack using performance analysis of deep learning. IEEE Access, 8, 186125-186137.

[7] Reddy, B. I., & Srikanth, V. (2019). Review on wireless security protocols (WEP, WPA, WPA2 & WPA3). International Journal of

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Scientific Research in Computer Science, Engineering and Information Technology, 5(4), 28-35.

[8] Halbouni, A., Ong, L. Y., & Leow, M. C. (2023). Wireless Security Protocols WPA3: A Systematic Literature Review. IEEE Access.

[9] Ambavkar, P. S., Patil, P. U., Meshram, B. B., & Swamy, P. K. (2012). Wpa exploitation in the world of wireless network. Int J Adv Res Comput Eng Technol, 1(4), 609-618.

[10] Cahyadi, D., Astuti, I. F., & Nazaruddin, N. (2023, February). Comparison of throughput and CPU usage between WPA3 and WPA2 security methods on wireless networks 802.11 n. In AIP Conference Proceedings (Vol. 2482, No. 1). AIP Publishing.

[11] Baray, E., & Ojha, N. K. (2021, April). WLAN security protocols and WPA3 security approach measurement through aircrack-ng technique. In 2021 5th International conference on computing methodologies and communication (ICCMC) (pp. 23-30). IEEE.

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

[13] 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

[14] 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

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

[15] 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.

[16] 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

[17] 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

[18] 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.

[19] Hooper, M., Tian, Y., Zhou, R., Cao, B., Lauf, A. P., Watkins, L., ... & Alexis, W. (2016, November). Securing commercial WiFi-based UAVs from common security attacks. In MILCOM 2016-2016 IEEE Military Communications Conference (pp. 1213-1218). IEEE.

[20] Zscaler. (2024). VPN Risk Report: Over Half of Organizations Experienced VPN-related Cyberattacks. Retrieved from

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

https://www.zscaler.com/press/vpn-risk-report-finds-more-half-organizations-experienced-vpn-related-cyberattack-last-year

[21] MDPI. (2024). Zero Trust VPN: A Systematic Literature Review. Information, 15(11), 734. Retrieved from https://www.mdpi.com/2078-2489/15/11/734

[22] DiVA Portal. (2024). VPN Performance and Configuration Challenges. Retrieved from https://www.diva-portal.org/smash/get/diva2%3A1778036/FULLTEXT03.pdf

[23] ArXiv. (2024). WireGuard and IoT Security: Evaluations and Perspectives. Retrieved from https://arxiv.org/abs/2402.02093

[24] ArXiv. (2024). DoS Vulnerabilities in VPNs: Analysis and Countermeasures. Retrieved from https://arxiv.org/abs/2110.00407

[25] J. Haris, M. Shafique, J. Henkel and S. Parameswaran, "System-level application-aware dynamic power management in adaptive pipelined MPSoCs for multimedia," IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Washington, D.C, Country, pp. 616-623, 2011.

[26] K. George and D. Pnevmatikatos, "Dynamic power and thermal management of noc-based heterogeneous mpsocs," ACM Transactions on Reconfigurable Technology and Systems (TRETS), vol. 7, no. 1, pp. 1-26, 2014

[27] ArXiv. (2024). Security Analysis of Proprietary VPN Clients. Retrieved from https://arxiv.org/abs/2202.05573

[28] K. Huang, K. Wang, D. Zheng, X. Jiang, X. Zhang, R. Yan et al., "Expected energy optimization for real-time multiprocessor socs running periodic tasks with uncertain execution time, " IEEE

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

Transactions on Sustainable Computing, vol. 6, no. 3, pp. 398-411, 2018.