THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 5. Issue 1 (2025)
https://doi.org/10.62019/qe5e0s45

An Enhanced Data Privacy and Security Mitigation Technique: A Novel Federated Deep Learning (FDL) Model for Intrusion detection and Classification System For Cyber -Physical Systems in Internet of things (IoTs)

Salheen Bakhet*, Hafiz Tanveer Ahmed, Taliah Tajammal, Muhammad Usman Saleem

Chronicle

Article history
Received: 1st Jan, 2025
Received in the revised format: 12th Jan, 2025
Accepted: 17th Feb, 2025
Available online: 15 March, 2025

Salheen Bakhet and Taliah Tajammal are currently affiliated with Department of Computer Science, University of Engineering and Technology, Lahore, Pakistan.
Email: salheen@ieee.org
Email: taliah@uet.edu.pk

Hafiz Tanveer Ahmed is currently affiliated with Victorian Institute of Technology, Australia.
Email:tanveerahmedapc@hotmail.com

Muhammad Usman Saleem is currently affiliated with the Department of Computer Science, Government College Women University Sialkot, Pakistan.
Email: usman.saleem@gcwus.edu.pk

Rizwan Asghar Qureshi is currently affiliated with the Department of Computer Science, COMSATS University Islamabad, Lahore Campus, Pakistan.
Email: rqureshi@cuilahore.edu.pk

Corresponding Author*

Abstract

The Internet of Things (IoT) has faced difficulties in its adoption because of security and data privacy issues that exist in the modern technological environment. Modern cybersecurity systems face multiple problems due to the fast-paced development of cyber threats. The research examines the issue where modern breach methods surpass traditional defense systems. Through federated learning, multiple clients train global models together by sharing machine learning without having to exchange actual data. The document emphasized that security functions as a vital component throughout End-to-End data security configurations. FL operates as an autonomous framework that provides improved data security through decentralized IDS training mechanisms implemented across separate connected devices. This paper analyzes Federated Learning methods and Virtual security protocols which demonstrate their vital role in modern networking infrastructure for establishing secure data transfer on unsecured internet networks. The paper explores the new difficulties that confront Machine Learning model implementations. These techniques help analyze large datasets from IoT devices that connect to the internet due to their effectiveness in processing internet-based application data. A Federated CNN model will serve as an effective system in the future to detect cyber threat identification.

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

INTRODUCTION

Advancement A virtual private network (VPN) represents a dependable solution to meet such requirements by connecting through both PSTN networks and 4G/5G modern architectures [1]. The Virtual Private Network establishes an encrypted link that extends from user devices to distant servers to protect their data security when using public networks. The combination of tunneling protocols with encryption

standards along with robust authentication systems allows VPN networks to function [2, 3]. Machine Learning has gained broad acceptance because fast networks plus smart devices continue to increase in speed. A network configuration under IoT interconnects various physical and digital objects together through local or international networking elements [4]. The L-smooth condition of f (x) requires that f (x) exhibits L-Lipschitz continuous gradient properties for all x1,x2 ∈ Rd that fulfill ∇f (x1)−∇f (x2) ≤ L x1 −x2. Scientists have investigated multiple security solutions such as developing lightweight cryptographic codes to protect both IoT device transmissions and data storage while maintaining resources available for processing information rapidly. Research teams have worked to create protected authentication protocols alongside safe frameworks as methods to reduce IoT security breach dangers. The protection of user privacy represents a major challenge within the IoT domain according to [5, 6]. FL operates through multiple clients accessing a shared global model found on the cloud server before running data training locally. Clients submit their locally enhanced models to the cloud server during periodic updates.

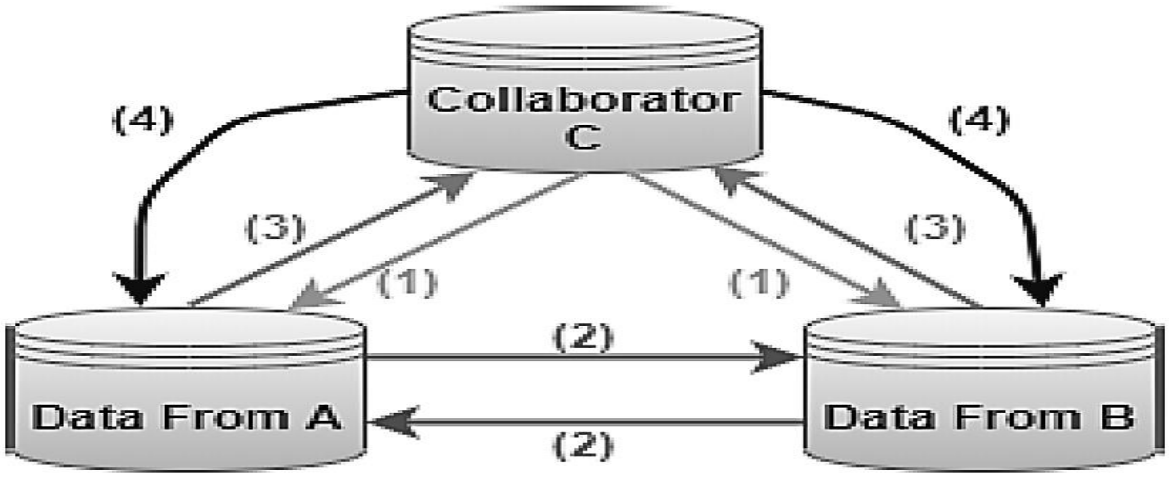

Figure 1.
Vertical FL Model for Data Privacy [7]

The cloud server completes a global average before it combines the improved global model with client systems. Multiple rounds of communication between clients and the cloud server continue until the targeted convergence level becomes satisfactory. The FL security solution combined with Windows systems integration led to widespread acceptance since the solution became easily usable. The cryptographic weaknesses of PPTP showed themselves almost immediately when it became clear that its cryptographic implementation was insufficient [8, 9]. PPTP protocol suffered from critical security weaknesses which made it incapable of delivering necessary protection to protected data. A function f (x) is called μ- strongly convex whenever μ> 0 exists where x1, x belong to Rd, f (x1) > f (x2) + (x1 - x2)T∇f (x2) + μ.

$$w_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_{t+1}^k$$

Eq (1)

$$\mu_i = \frac{1}{n_i}\sum_{j=1}^{n_i} x_j, \quad \sigma_i^2 = \frac{1}{n_i - 1}\sum_{j=1}^{n_i}(x_j - \mu_i)^2$$

Eq (2)

$$\mu_g = \frac{\sum_{i=1}^{k} n_i \mu_i}{\sum_{i=1}^{k} n_i}, \quad \sigma_g^2 = \frac{\sum_{i=1}^{k}(n_i - 1)\sigma_i^2}{\sum_{i=1}^{k} n_i - k}$$

Eq (3)

The data distribution system in FL consists of three main types namely Horizontal Federated Learning (HFL), Vertical Federated Learning (VFL), and Federated Transfer Learning (FTL) [10, 11]. A basic security framework within ML describes its objective to discover minimal-loss models that assess distribution differences using the f-loss parameter. The property of β-Lipschitz continuity exists when β≥ 0 and | f (x1)− f (x2) | ≤ β x1 −x2. The FL system permits various users throughout a network to merge their nearby data collection into an overall global computational model [12-15].

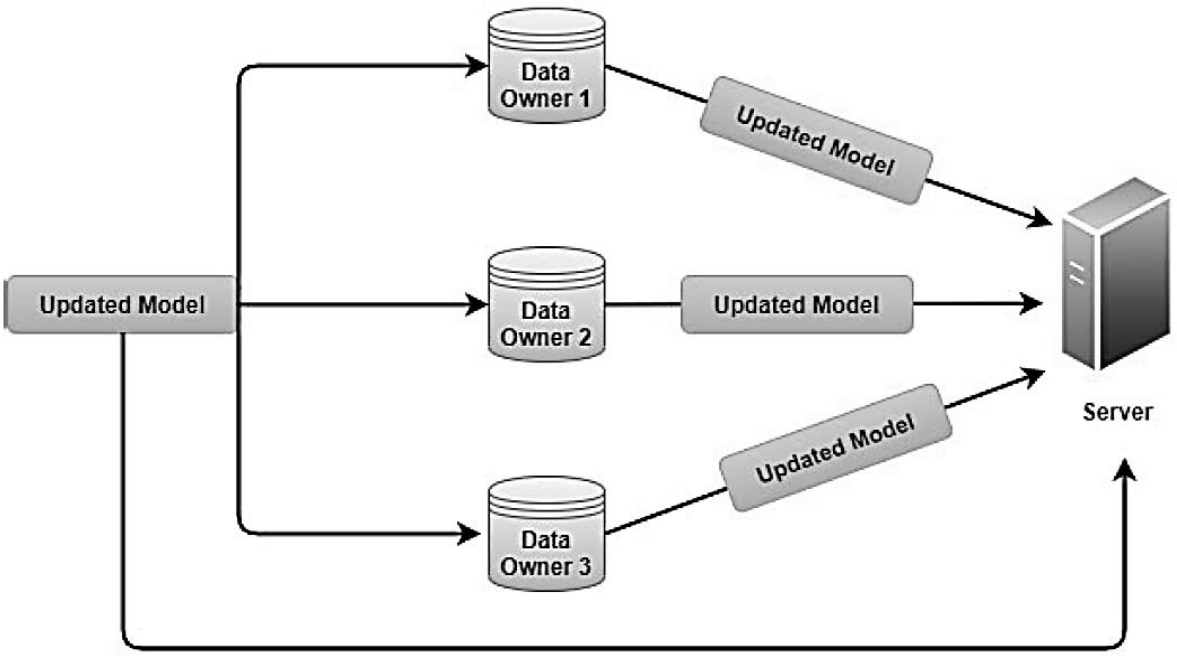

Figure 2.
General Architecture for Federated learning [16]

Related Architectures and Platforms of Federated Learning

The research papers combines extensive analysis of FL with finding discussions and ends by demonstrating practical solutions and new investigation paths. Modern cyber threats surpass traditional defensive measures which make the identification of threat intelligence a fundamental issue because organizations must handle enormous data

volumes before they can stop attacks. Security trends in the emerging field demonstrate that the field depends increasingly on multinational community partnerships while requiring data exchange across all domains [17-21]. All countries must establish standardized procedures for cybersecurity since they become necessary to combat international cyber threats. Blockchain technology along with decentralized systems has begun to offer effective solutions that resolve specific cybersecurity hurdles. Blockchain brings better data integrity and less risky breaches to security systems yet attackers discover ways to compromise blockchain vulnerabilities. The system evaluates the likelihood of query classification based on examining various data attributes to determine belongingness between normal and malicious classes [22,23].

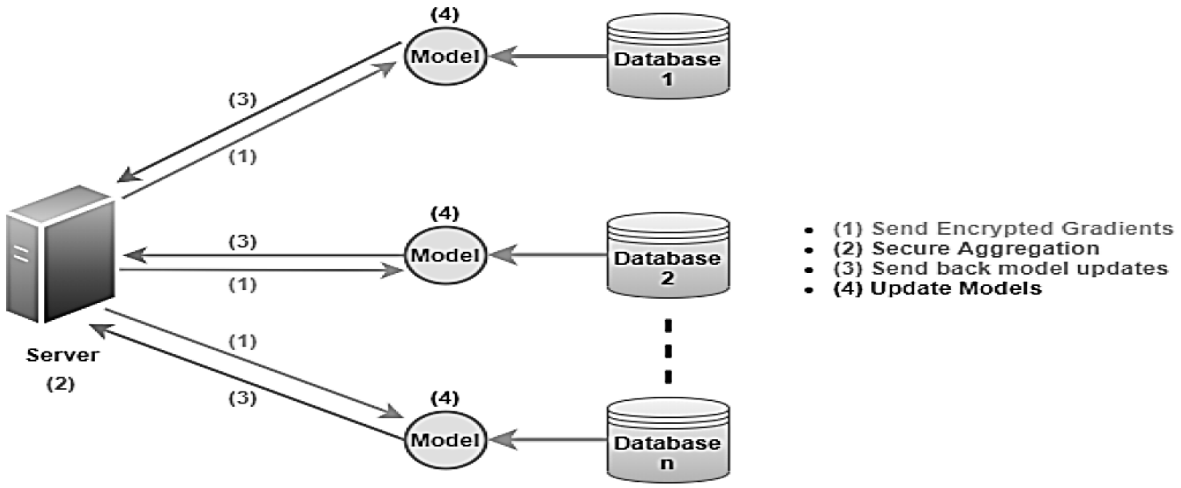

Figure 3.
Architecture for Federated Learning (Horizontal FL) [24]

Federated Deep Learning (FDL)

FDL represents a decentralized deep learning training model that collects model updates from separate devices sharing their datasets without revealing actual raw information for preserving independence and delivering superior model results. The method brings successful results in cases where features function autonomously from one another. Customers who hold numerous options in the current market seek personalized interactions. The business position of FL makes it ready to meet market demand. The baseline model uses this method due to its speed along with its simple implementation procedure. The system performs effectively when dealing with basic and organized information [25- 27]. Decision trees use data splitting to attain maximum information gain from the data. The pruning techniques worked to minimize the occurrences of overfitting. t. The decision tree and k include a precise node which serves as the selection criteria. 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. The support vector machine (SVM) received optimization with the Radial Basis function kernel to perform non-linear classifications. The optimal performance of the system was reached through the grid search strategy which adjusted both the C regularization parameter and γ kernel coefficient [28, 29].

$$f(x) = w^T a + \quad b \qquad \text{Eq (4)}$$

The weight term is W while X stands for features which are input examples and b serves as the bias term. This model groups 1,000 decision trees that execute training procedures on random sets of data. The team completed an feature important analysis that served to enhance the process of feature selection. The model possesses hidden layers with 256 neurons per layer. Albuquerque used the dropout along with batch normalization to overcome overfitting issues and boost convergence speed [30, 31].

$$f(x) = w^n a + \quad b \qquad \text{Eq (5)}$$

$$P(c|x) = \frac{P(X|C).P(C)}{P(X)} \qquad \text{Eq (6)}$$

The weight term is W while X stands for features which are input examples and b serves as the bias term. This model groups 1,000 decision trees that execute training procedures on random sets of data. The team completed an feature important analysis that served to enhance the process of feature selection. The model possesses hidden layers with 256 neurons per layer. Albuquerque used the dropout along with batch normalization to overcome overfitting issues and boost convergence speed [32, 33]. The SVM classifier uses the ANN-generated output for ultimate prediction refinement. The process of hyperparameter optimization ran on both components of the system although the cryptography technology used for encryption combined with secure multi-party computation methods matches common approaches adopted for privacy-preserving decentralized learning. Every client applies encryption to their update files before the cloud server upload after which the server decrypts received updates to acquire a new global model [34, 35].

Inference attacks become possible since each client needs to make their gradient information accessible during the sharing process. The term P (C | X) represents the likelihood of an X query incident belonging to the class C malicious while P(X | C) shows the probability of X data happening under class C. Moreover, CP(C) represents the previous probability of class C infections alongside P(X) indicating total X data probability. VPNs provide businesses with an essential security tool to grant remote employees secure access to their networks. The internet connection created by VPNs provides secure access to essential company resources even when workers operate remotely. The secure network access provided by Virtual Private Networks protects work-related databases and applications both from home and other offices when employees use public Wi-Fi networks [36, 37].

METHOD & EVALUATION

This equation represents the local objective function fi(t) for the i-th client as well as the current model parameter x that operates on data point ξ during the current local training round. The assumptions state that LOF, SOF, and LH define objective function smoothness while SCOF and COF determine convexity properties and the function becomes coercive when f (x1) ≥ f (x2)+(x1 −x2)T∇f (x2) is true. The objective function position relationship between convexity is defined by SCOF and COF while a coercive objective holds f (x1) ≥ f (x2)+(x1 −x2)T∇f (x2) and lim x $\rightarrow\infty$ f (x) $\rightarrow \infty$. The Capability of Committal ensures that the objective function reaches its absolute minimum point. The properties of gradients are detected through the combination of BG and BV with

BGD. The current gaps demonstrate the necessity of implementing an integrated solution that addresses technological regulations along with ethical considerations.

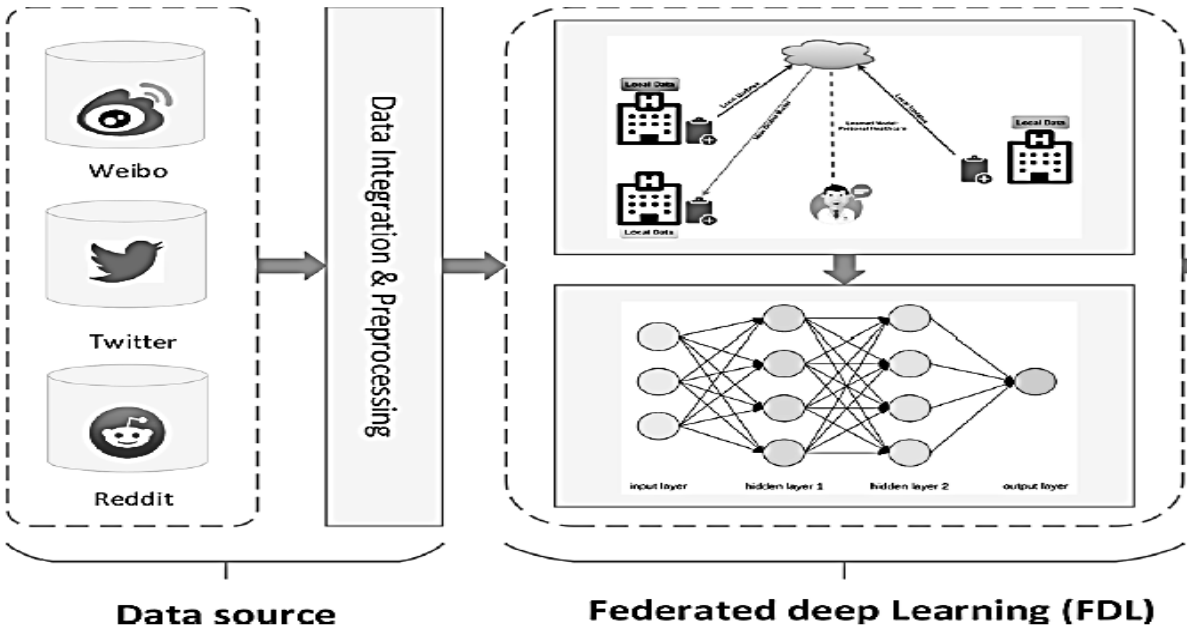

Figure 2.
Architecture for Federated Deep Learning Model

$$\sum_{i=\{1,.,.,n\}/k}^{n} \frac{c_i}{\tau_i} + \frac{c_k + \alpha_k}{\tau_k} \qquad \textbf{Eq (7)}$$

While another task $\mathbf{t_2}$ with intrusions arrive with the earliest deadline before the end of the execution task $\mathbf{t_1}$then the length of the idle interval due to network delay and threat is denoted as $\boldsymbol{\lambda_j}$ and max time duration for the idle period is represented as $\boldsymbol{\alpha_j}$ during longer data attacks that can be measured using Eq. (10).

$$\sum_{i=\{1,.,.,n\}/(k,j)}^{n} \frac{c_i}{\tau_i} + \frac{c_k + \alpha_k}{\tau_k} + \frac{c_j + \alpha_j}{\tau_j} = 1 \qquad \textbf{Eq (8)}$$

$$\sum_{i=\{1,.,.,n\}/(k,j)}^{n} \frac{c_0}{\tau_0} + \frac{c_0 + \alpha_0}{\tau_0} + \frac{c_0 + \alpha_0}{\tau_0} \qquad \textbf{Eq (9)}$$

$$\sum_{i=\{1,.,.,n\}/(k,j)}^{n} \frac{c_1}{\tau_1} + \frac{c_1 + \alpha_1}{\tau_1} + \frac{c_1 + \alpha_1}{\tau_1} \qquad \textbf{Eq (10)}$$

$$\sum_{i=\{1,.,.,n\}/(k,j)}^{n} \frac{c_3}{\tau_3} + \frac{c_3 + \alpha_3}{\tau_3} + \frac{c_3 + \alpha_3}{\tau_3} \qquad \textbf{Eq (11)}$$

$$\sum_{i=\{1,.,.,n\}/(k,j)}^{n} \frac{c_n}{\tau_n} + \frac{c_n + \alpha_n}{\tau_n} + \frac{c_n + \alpha_n}{\tau_n} \qquad \textbf{Eq (12)}$$

Table 1.
Comparative Analysis of Intrusion Detection based on Federated Learning Model at K=3

		1st Round						10th Round					
Classifier	**Client**	**IID**			**Non-IID**			**IID**			**Non-IID**		
		B	**W**	**G**	**B**	**W**	**G**	**B**	**W**	**G**	**B**	**W**	**G**
RNN	*K* = 3	59.89	23.48	62.19	59.89	59.89	62.19	91.34	90.62	63.23	62.19	59.89	59.89
DT	*K* = 3	54.32	17.45	57.34	54.32	54.32	57.34	91.30	90.18	56.71	57.34	54.32	54.32
NBB	*K* = 3	57.92	16.74	57.78	57.92	57.92	57.78	90.77	89.65	59.89	57.78	57.92	57.92
RF	*K* = 3	60.21	24.64	61.28	60.21	60.21	61.28	92.49	92.08	54.32	61.28	60.21	60.21
SVM	*K* = 3	53.68	19.42	55.79	92.41	92.01	55.79	92.41	92.01	57.92	56.84	53.68	53.68
CNN	*K* = 3	57.97	17.16	54.72	92.19	91.98	54.72	92.19	91.98	60.21	58.92	57.97	57.97

$$\ln fl_{it}^{+} = \sum_{j=0}^{t} \Delta \ln w^{T} x + \quad b_{it}^{+} = \sum_{j=0}^{t} \max(\Delta w^{T}{}_{ij,0}) + \in_{it} \qquad \textbf{Eq (13)}$$

Table 2.
Comparative Analysis of Intrusion Detection based on Federated Learning Model at K=6

		1st Round						20th Round					
Classifier	**Clients**	**IID**			**Non-IID**			**IID**			**Non-IID**		
		B	**W**	**G**	**B**	**W**	**G**	**B**	**W**	**G**	**B**	**W**	**G**
RNN	*K* = 6	23.48	52.34	59.89	23.48	62.19	59.89	59.89	62.19	91.34	62.19	23.48	59.89
DT	*K* = 6	17.45	54.32	54.32	17.45	57.34	54.32	54.32	57.34	91.30	57.34	17.45	54.32
NBB	*K* = 6	57.78	57.92	57.92	16.74	57.78	57.92	57.92	57.78	90.77	57.78	23.1	57.92
RF	*K* = 6	61.28	60.21	60.21	24.64	61.28	60.21	60.21	61.28	92.49	61.28	17.45	60.21
SVM	*K* = 6	56.84	53.68	53.68	19.42	55.79	92.41	92.01	55.79	92.41	56.84	53.68	53.68
CNN	*K* = 6	17.16	54.32	91.07	57.97	17.16	54.72	92.19	91.98	**60.21**	58.92	57.97	57.97

The following are the explanatory variable's positive and negative shocks when they change during intrusion detection at K=6.

$$\ln fl_{it}^{+} = \sum_{j=1}^{t} \Delta \ln w^{T} x + \quad b_{it}^{+} = \sum_{j=1}^{t} \max(\Delta w^{T}{}_{ij,1}) + \in_{it} \qquad \textbf{Eq (14)}$$

Table 3.
Comparative Analysis of Intrusion Detection based on Federated Learning Model at K=12

		1st Round						30th Round					
Classifier	**Clients**	**IID**			**Non-IID**			**IID**			**Non-IID**		
		B	**W**	**G**	**B**	**W**	**G**	**B**	**W**	**G**	**B**	**W**	**G**
RNN	*K* = 12	59.89	52.34	91.07	57.97	55.79	61.28	55.79	91.07	57.97	54.32	54.31	91.30
DT	*K* = 12	54.32	54.32	57.34	52.34	62.19	52.34	62.19	90.18	56.71	57.92	54.32	90.77
NBB	*K* = 12	57.92	53.37	57.78	54.32	57.34	54.32	57.34	62.19	59.89	60.21	53.37	92.49
RF	*K* = 12	59.89	55.79	61.28	53.37	57.78	53.37	57.78	57.34	54.32	53.68	55.79	92.41
SVM	*K* = 12	54.32	54.72	56.84	53.68	53.37	57.78	53.37	61.28	53.37	61.28	54.31	91.30
CNN	*K* = 12	17.16	54.32	91.07	57.97	55.79	61.28	55.79	62.19	59.89	62.2	57.97	51.5

The following are the explanatory variable's positive and negative shocks when they change during intrusion detection at K=12.

$$\ln fl_{it}^{+} = \sum_{j=2}^{t} \Delta \ln w^{T} x + \quad b_{it}^{+} = \sum_{j=2}^{t} \max(\Delta w^{T}{}_{ij,2}) + \in_{it} \qquad \textbf{Eq (15)}$$

Table 4.
Comparative Analysis of Intrusion Detection based on Federated Learning Model at K=15

		1st Round						40th Round					
Classifier	**Clients**	**IID**			**Non-IID**			**IID**			**Non-IID**		
		B	**W**	**G**	**B**	**W**	**G**	**B**	**W**	**G**	**B**	**W**	**G**
RNN	*K* = 15	54.32	17.45	90.58	59.89	23.48	52.34	91.34	90.58	59.89	23.48	52.34	91.34
DT	*K* = 15	57.92	16.74	90.73	54.32	17.45	54.31	23.48	90.73	54.32	17.45	54.31	23.48
NBB	*K* = 15	60.21	24.64	90.18	57.92	16.74	54.32	17.45	54.32	24.64	55.79	91.87	24.64
RF	*K* = 15	24.64	55.79	91.87	60.21	24.64	53.37	55.79	91.87	60.21	24.64	91.53	19.42
SVM	*K* = 15	19.42	54.72	91.53	53.68	19.42	55.79	55.79	91.87	57.92	16.74	90.73	60.21
CNN	*K* = 15	17.16	54.32	91.07	57.97	17.16	54.72	92.19	91.98	54.32	17.45	90.58	59.89

$$\ln fl_{it}^{+} = \sum_{j=n}^{t} \Delta \ln w^{T} x + \quad b_{it}^{+} = \sum_{j=n}^{t} \max(\Delta w^{T}{}_{ij,n}) + \in_{it} \qquad \text{Eq (16)}$$

The model requires training duration to learn from its training dataset yet real-time applications depend heavily on the testing dataset prediction speed. The improvement of VPN capabilities for restricted edge network devices needs attention. Current international research investigations with practical case examples provide the foundation for this study. Testing of VPN protocols involved using practical security and performance benchmarks together with network analysis instruments combined with professional cybersecurity specialist surveys. The basis of VPN authentication ensures that only permitted users get access to the network. The stronger authentication methods of certain VPN protocols make it possible to stop malicious intruders and protect against man-in-the-middle (MITM) attacks. Two examples of secure VPN protocols are OpenVPN and IKEv2/IPsec which combine the Multi-Factor Authentication system by requiring users to use both passwords and certificates for access verification.

CONCLUSION AND RECOMMENDATIONS

The article provides detailed insights into federated learning technology and its attack types and data poisoning methods. The four main challenges in federated learning involved system architectural brittleness alongside inefficient communication links and excessive resource utilization and deficient situation prediction reliability. Each problem received specific response measures. The security environment evolves with significant obstacles that need comprehensive solutions for effective outcomes. Our analysis began by choosing popular encryption protocols to present their network communication structure together with their protocol standards. The analysis centered on encryption protocol-provided information. Modern networks require VPN protocols for security however selecting the appropriate method depends on individual environment requirements and conditions. Organizations need to make VPN solution decisions based on the combination of security needs with performance requirements and both network and staff scale.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the supervisors and their different affiliations.
Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.

Availability of data and material: In the approach, the data sources for the variables are stated.

Authors' contributions: Each author participated equally to the creation of this work.

Conflicts of Interests: The authors declare no conflict of interest.

Consent to Participate: Yes

Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

P. P. Liang, T. Liu, L. Ziyin, N. B. Allen, R. P. Auerbach, D. Brent, R. Salakhutdinov, nd L.-P. Morency, ``Think locally, act globally: Federated learning with local and global representations,'' 2020, arXiv:2001.01523. [Online]. Available: http://arxiv.org/abs/2001.01523

H. H. Zhuo, W. Feng, Y. Lin, Q. Xu, and Q. Yang, ``Federated deep reinforcement learning,'' Feb. 2020, arXiv:1901.08277. [Online]. Available:
https://arxiv.org/abs/1901.08277

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.

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.

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

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.

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.

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.

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

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

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.

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.

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

Abdullah, M., Khan, H., Shafqat, A., Daniyal, M., Bilal, M., & Anas, M. (2024). Internet of Things (IoT's) in Agriculture: Unexplored Opportunities in Cross–Platform. Spectrum of engineering sciences, 2(4), 57-84.

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

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

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

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

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

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

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.

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

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

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

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. 201

Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024

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

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

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

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

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.

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

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

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.

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.

H. Yu, Z. Liu, Y. Liu, T. Chen, M. Cong, X. Weng, D. Niyato, and Q. Yang, ``A fairness-aware incentive scheme for federated learning,'' in Proc. AAAI/ACM Conf. AI, Ethics, Soc., Feb. 2020, pp. 393_399.

S. Truex, N. Baracaldo, A. Anwar, T. Steinke, H. Ludwig, R. Zhang, and Y. Zhou, ``A hybrid approach to privacy-preserving federated learning,'' in Proc. 12th ACM Workshop Artif. Intell. Secur. (AISec), 2019, pp. 1_11.