



ASIAN BULLETIN OF BIG DATA MANAGEMENT

<http://abbdm.com/>

ISSN (Print): 2959-0795

ISSN (online): 2959-0809

Critical Evaluation of Data Privacy and Security Threats: An Intelligent Federated Learning-based Intrusion Detection System Poisoning Attack and Defense for Cyber-Physical Systems its Issues and Challenges Related to Privacy and Security in IoT

Rimsha Aziz*, Aneela mehmoood, Asma Tariq, Fawad Nasim, Umar Farooq, Syed Asad Ali Naqvi, Hamayun Khan

Chronicle

Abstract

Article history

Received: Jan 2, 2025

Received in the revised format: Jan 27, 2025

Accepted: Feb 2, 2025

Available online: Feb 10, 2025

Rimsha Aziz, Asma Tariq, Fawad Nasim, Syed Asad Ali Naqvi and Hamayun Khan are currently affiliated with Department of Information Technology, Faculty of Computer Science & IT Superior University Lahore, Pakistan.

Email:

SU92-MSITW-F24007@superior.edu.pk

Email:

SU92-MSITW-F24-006@superior.edu.pk

Email: fawad.nasim@superior.edu.pk

Email: syedasad.alinaqvi@superior.edu.pk

Email: hamayun.khan@superior.edu.pk

Aneela Mehmoood is currently affiliated with the University of Central Punjab, Pakistan.

Email: aneela.mehmoood@ucp.edu.pk

Umar Farooq is currently affiliated with the University of Northumbria.

Email: Umarnorthumbria@gmail.com

Corresponding Author*:

Federated learning is a distributed learning method used to solve data silos and privacy protection in 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. 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. The End-to-End VPN security has an essential role especially in connecting smart objects in the Internet of Things (IoT) environments. 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 Virtual Private Network (VPN) technologies, emphasizing their importance in modern networking for ensuring secure communication over untrusted networks like the internet. VPNs have evolved significantly, addressing the growing need for data protection in both personal and enterprise contexts. 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 examines the emerging challenges facing VPNs, including advanced cyber threats and the impact of evolving technologies such as quantum computing. Furthermore, the study highlights future directions, such as integrating AI for dynamic threat detection and developing quantum-resistant VPN protocols. Through this analysis, the aim is to provide actionable insights into optimizing VPN usage for enhanced network security in an increasingly complex digital landscape.

Keywords: VPN, Security Protocols, Encryption, OpenVPN, IKEv2/IPsec, WireGuard, Quantum Computing

© 2025 EuroAsian Academy of Global Learning and Education Ltd. All rights reserved

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

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) [13]. Below, we define general framework from security perspectives:

Table 1:
Analysis of the Data Poisoning Attack in FL [14]

Attack Type	Attack Methodology	Attack Evaluation Index	DataSet	Training Settings/ (Number-Items)	Result%
Untargeted poisoning	Utilizing the projected stochastic gradient ascent algorithm to maximize the experience loss of the target node	Model error rate	EndAD	6*:no-iid	Base: 6.88 ± 0.52 Result: 28.588 ± 3.74
Untargeted poisoning	Predict changes in the SVM decision function caused by malicious input and use this ability to construct malicious data	Model error rate	MNIST	*,*,*	Base: 2-5 Result: 15-20
Targeted poisoning	Aim for successful poisoning in the final rounds and choose the right tag to flip	Maximum recall loss	CIFAR-10	50*:iid	Base: 0 Result: 2:1.42; 20:25.4
Targeted poisoning	Utilize GAN technology to generate data and implement label flipping	Poisoning task accuracy rate	MNIST	10*:no-iid	Base: 0 Result: 20:60±; 40:80±; 60:85±

These gaps underscore the need for a more integrated approach that addresses technological, legal, and ethical dimensions. 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 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 [15, 16]. 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 [17].

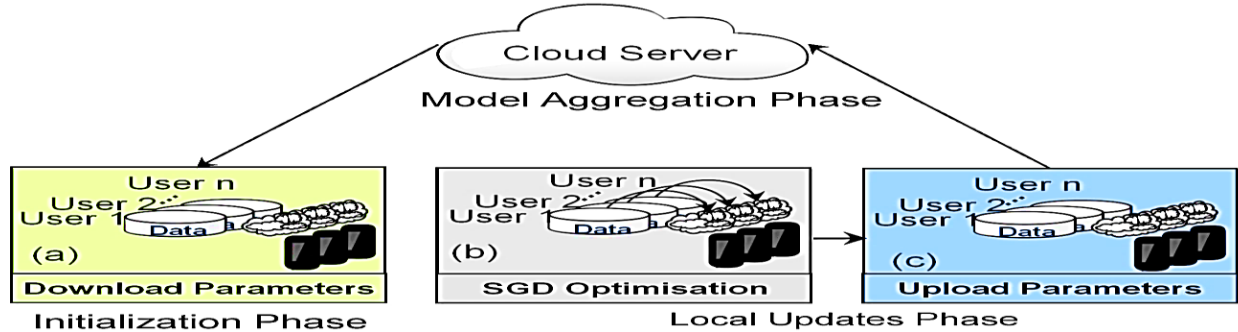


Figure 2: Generalize Framework for Federated learning Framework [18]

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.

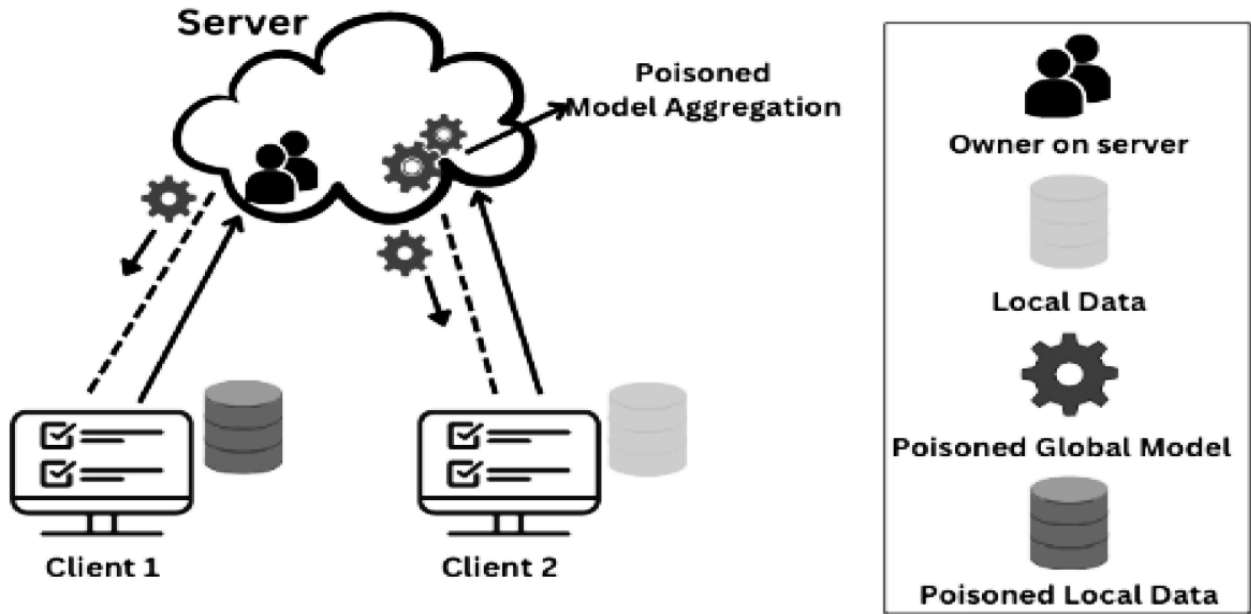


Figure 3: Data Poisoning Security attacks under FL model [19]

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 [20]. Transmitting private data through a dedicated private circuit.

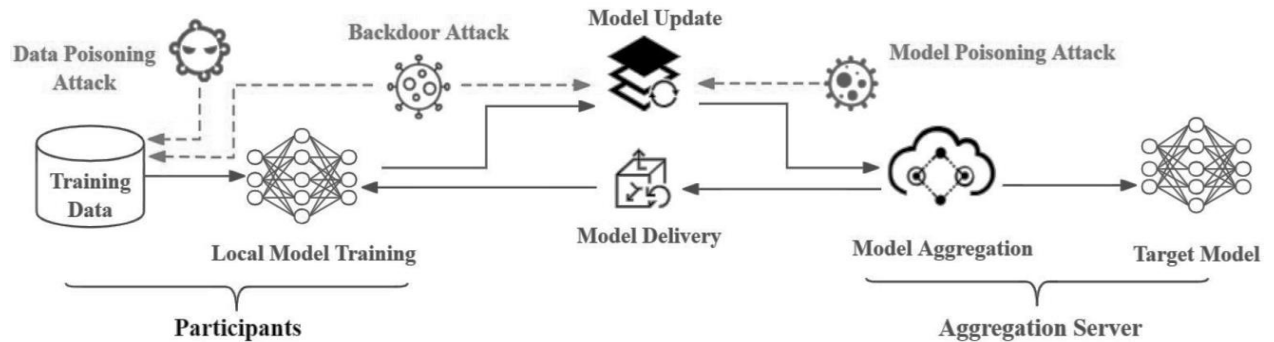


Figure 4:
Security attacks under training phase of FL model [21]

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 [22, 23]. 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 [24, 25].



Figure 5:
Numerous Factor and Data security Requirements [26]

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 PTP had significant security flaws, particularly with weak encryption. As a result, it couldn't offer the level of protection needed for sensitive data.

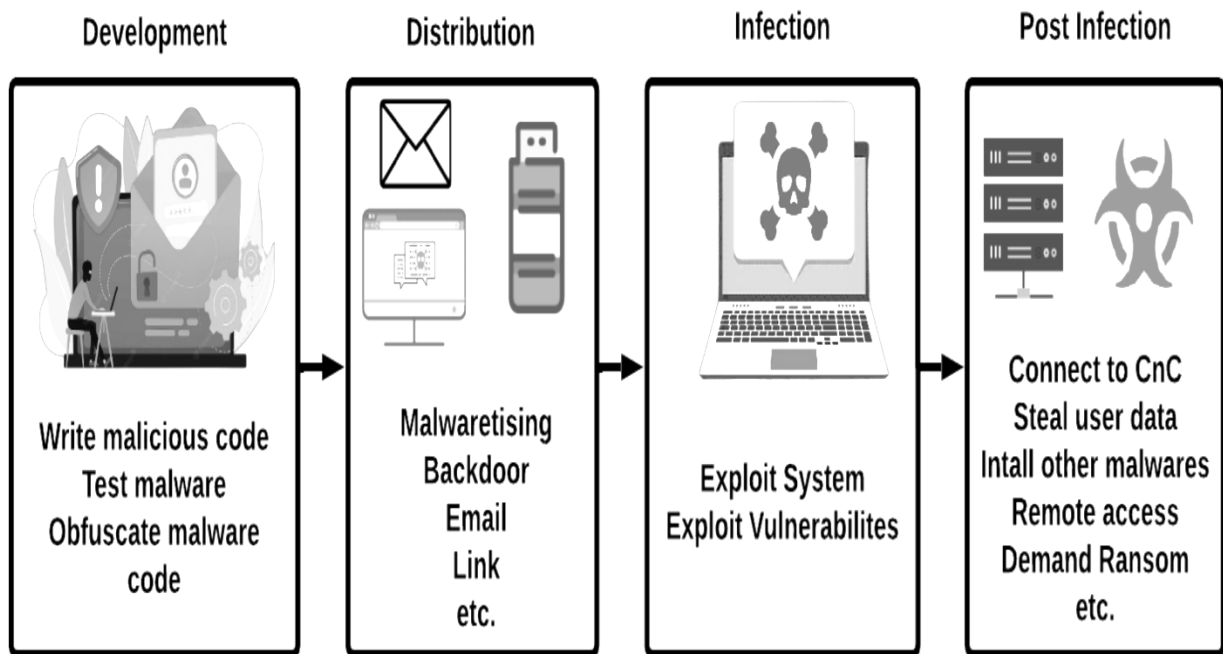


Figure 6:
Life cycle of Malware [27]

Machine Learning Based Techniques for Couter Measure

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.

$$P(c|x) = \frac{P(x|c).P(c)}{P(x)} \quad \text{Eq (1)}$$

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.

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.

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

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 l in the node 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:

$$f(x) = w^T x + b \quad \text{Eq (3)}$$

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.

$$f(x) = \max(0, x) \text{ (ReLU)} \quad \text{Eq (4)}$$

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 [28]. 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.

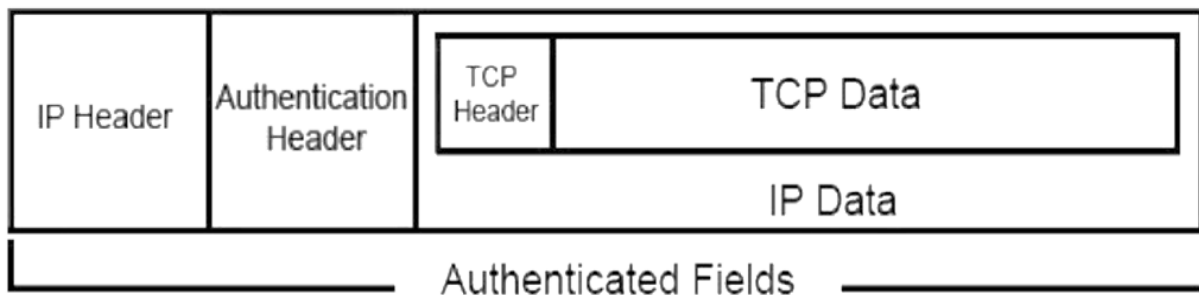


Figure 7:
VPN based IPsec [29]

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 [32, 33]. 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 [30, 31].

Security Challenges & Evaluation Metrics

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 .

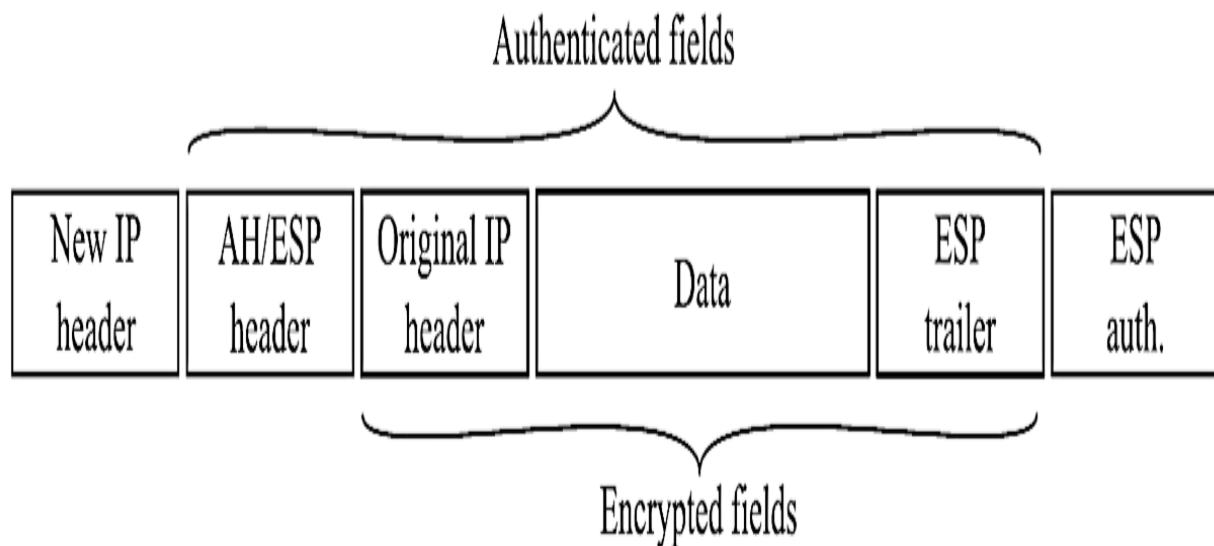


Figure 8: Network Security Protocols (a) Transport mode [32]

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:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad Eq (5)$$

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.

$$Precision = \frac{TP}{TP+FP} \quad Eq (6)$$

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

$$Recall = \frac{TP}{TP+FN} \quad \text{Eq (7)}$$

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

$$F1 - Score = 2 \cdot \frac{Precision \cdot Recall}{Precision+Recall} \quad \text{Eq (8)}$$

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.

Table 4:
Security Countermeasures Effectiveness [33]

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

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 [34]

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.

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

- Tahir, R. A study on malware and malware detection techniques. *Int. J. Educ. Manag. Eng.*, vol. 8, no. 20, 2018.
- Aliyyah Rosyidah1, Jumadi Mabe Parenreng, "Network Security Analysis Based on Internet Protocol Security Using Virtual Private Network (VPN)" July, 06 2023
- 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.
- 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.
- 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.
- Reddy, B. I., & Srikanth, V. (2019). Review on wireless security protocols (WEP, WPA, WPA2 & WPA3). *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 5(4), 28-35.
- Halbouni, A., Ong, L. Y., & Leow, M. C. (2023). *Wireless Security Protocols WPA3: A Systematic Literature Review*. IEEE Access.
- 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.
- 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.
- 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.
- 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
- 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 *Salvia Sclarea*, their characterization, antibacterial activity, and catalytic reduction ability. *Zeitschrift für Physikalische Chemie*, 238(5), 931-947.
- 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
- 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
- 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
- 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.
- 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
- 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
- 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 Schedulability 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.
- 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
- 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
- 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 sciences*, 2(3), 528-586.
- 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.
- Zscaler. (2024). VPN Risk Report: Over Half of Organizations Experienced VPN-related Cyberattacks. Retrieved from <https://www.zscaler.com/press/vpn-risk-report-finds-more-half-organizations-experienced-vpn-related-cyberattack-last-year>
- MDPI. (2024). Zero Trust VPN: A Systematic Literature Review. *Information*, 15(11), 734. Retrieved from <https://www.mdpi.com/2078-2489/15/11/734>

Critical Evaluation of Data Privacy and Security Threats

Rimsha, A., et al. (2025)

- DiVA Portal. (2024). VPN Performance and Configuration Challenges. Retrieved from <https://www.diva-portal.org/smash/get/diva2%3A1778036/FULLTEXT03.pdf>
- ArXiv. (2024). WireGuard and IoT Security: Evaluations and Perspectives. Retrieved from <https://arxiv.org/abs/2402.02093>
- ArXiv. (2024). DoS Vulnerabilities in VPNs: Analysis and Countermeasures. Retrieved from <https://arxiv.org/abs/2110.00407>
- ArXiv. (2024). Security Analysis of Proprietary VPN Clients. Retrieved from <https://arxiv.org/abs/2202.05573>



2025 by the authors; EuroAsian Academy of Global Learning and Education Ltd. Pakistan. This is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (<http://creativecommons.org/licenses/by/4.0/>).