

Quantum Computing Framework-Assisted Federated Learning with DRL for IoT Security

Saleh Alaraimi^{1*}, Al Zahra Al Ajmi², Nouf Al Lawati³, Isra Al Ghafri⁴, Asma Al Balushi⁵,
Rahaf Al Gharabi⁶

^{1, 2, 3, 4, 5, 6} Electrical and Communication Engineering Department, College of Engineering, Muscat, National University for Science and Technology, Oman

* Corresponding Author Email: salehalaraimi@nu.edu.om

Abstract

The proposed system shows a federated learning architecture powered by quantum computing that uses deep reinforcement based learning as part of their IoT data security upgrade and subsequent privacy improvement. The framework is based on includes advanced quantum computation to speed up complex tasks while at the same time keeping information handling on a decentralized way among the several types of IoT devices. This research introduces a quantum-assisted federated learning framework integrated with deep reinforcement learning to strengthen data security and privacy in Internet of Things (IoT) environments. The objective is to develop a scalable and adaptive decentralized model that protects sensitive data without relying on centralized repositories. The proposed system combines the distributed intelligence of federated learning, the computational acceleration of quantum processing, and the adaptive decision-making of deep reinforcement learning. This integration allows each IoT node to train locally while quantum-enhanced optimization accelerates convergence and improves model robustness. The deep reinforcement component enables real-time adaptation to dynamic security threats, enhancing system responsiveness.

Keywords

Adaptable framework, decentralized architecture, deep reinforcement, federated learning, IoT data security, privacy preservation, Quantum computing, quantum-improved processing, secure communication, smart IoT systems.

INTRODUCTION

One of the most incredible things to happen in the digital ecosystems is the exponential growth of IoT devices, which has transformed their interaction with each other. The seamless communication, the automatic function execution, and even the making of smart decisions are some of the features that have been achieved by the Internet of Things in various areas [1]. However, the multitude of interconnected devices has led to IoT networks that are vulnerable to substantial security breaches. In that case, there are issues not only in security but also in privacy [2]. In general, centralized security solutions do not work efficiently in handling these problems due to their limitation in scale, high communication overhead, and the possibility of single points of failure [3]. To alleviate most of these issues, federated learning is seen as a pioneering and beneficial idea that facilitates on-device training of distributed models without the actual data being moved. This would simultaneously protect privacy and encourage productivity [4]. Along the same lines, quantum computing has delivered a fresh outlook by equipping the classical approach with an unimaginable computation power, particularly for the simplification of the most challenging learning jobs and encryption strengthening [5]. Over the last decade, the implementation of practically scenario-based machine learning technologies such as deep reinforcement learning has greatly contributed to the sound IoT adaptation for the resolution of context-aware problems and making of

choices correctly according to the nature of threats and the amount of resources at disposal [6]. For instance, they can fully utilize reinforcement-driven methods to concurrently learn and practice the best defence tactics in the background of system performance [7]. The combining effect of quantum computing, federated learning, and deep reinforcement learning turns into one mighty structure that can successfully solve security issues of decentralized IoT systems in the present time [8]. Such a system not only alleviates the concerns that come with centralized control but also enables the security to be scaled up across various devices without compromising the level of safety [9]. Eventually, the core of thought presented makes a valuable contribution to the enhancement of next-generation IoT architectures that are described by data security, intelligence and the capability to fast-changing cyber-attacks [10]. Hence the contribution of Proposed system:

- A quantum-improved federated type learning model is developed to improvise IoT data security by decentralized model training phase and lowered privacy leakage.
- Combination of reinforcement type learning enables adaptive decision-based and real-time attack response within distributed way of IoT cases.
- A quantum type optimization layer gives policy convergence and enhances computational efficiency on federated learning trails.

A data privacy-preserving in the communication protocol is designed to confirm secure model updates without sharing

raw unseen data across nodal points.

LITERATURE REVIEW

In Progression towards secure, privacy-preserving as well as adaptive intelligence in distributed IoT settings is documented in the literature. Federated learning was at first implemented for network intrusion detection on heterogeneous IoT sensors, as a result local training could achieve competitive detection performance, but raw data sharing was avoided [11]. Consequently, researchers combined federated aggregation with secure aggregation and differential privacy to eliminate the risk of gradient leakage during collaborative training without greatly reducing model utility in non-IID environments [12]. In order to have adaptive policy selection at the edge which is able to respond quickly to changes in the threat landscape, deep reinforcement learning was brought in. This allowed on-device agents to learn defence strategies which could be a mix of detection efficacy, latency and energy constraints [13]. Through the same means, researchers looked at quantum key distribution and lightweight quantum-safe primitives in order to protect device–gateway links. The point was that this was a potential for forward-secure communication in IoT topologies that are resource-constrained [14]. The researchers looking into the training bottlenecks of large models at the edge, set about examining quantum-inspired optimization variational circuits with the purpose of fast-tracking convergence and determining global optima in federated rounds [15]. The blockchain-assisted federated orchestration was introduced as a way of recording model updates and incentives, thus mitigating the risk of poisoning and free-riding while decentralized trust could still be maintained [16]. The split/federated hybrids were said to improve throughput in the event of intermittent connectivity and demonstrate robustness even in the case of partial participation, these offloaded deeper layers to nearby edge servers for the purpose of easing device limitations [17]. At the same time, adversarial robust learning implemented the use of generative models for the purpose of creating hard negatives and detecting evasive traffic patterns to solve the problem of distributed training regimes that are susceptible to adversarial examples [18].

After that, cross-domain transfer strategies enabled clients with a small number of labels to take advantage of related tasks which helped generalization across device types and protocols in non-stationary environments [19]. Integrative frameworks were first to look at the intersection of federated learning, deep reinforcement learning, and quantum-resistant cryptography. They described the architectures as those that combine adaptive defence, collaborative training, and post-quantum security to make the future of large-scale IoT deployments secure [20].

PROPOSED SYSTEM

A proposed system is carried out through a methodical

sequence where each processing step enhances IoT security and privacy within the scope of a quantum computing-powered federated learning framework. To start with, IoT devices locally train their models using their private data and they do not send the raw data. This step is not only a guarantee for data privacy but also lowers the probabilities of data being intercepted or leaked. Subsequently, the locally trained models are merged in a central server via federated learning, which is a technique that permits the combining of the knowledge of the remotely situated nodes without any data privacy being violated. The combination process is incorporating quantum computing methods to achieve a quicker optimization and to increase the capacity of the complex calculations, thus, all the way to a faster convergence and improved security mechanisms as can be seen in figure 1. Furthermore, deep reinforcement learning as part of the framework functions as an extra security layer where the adaptive learning is put into practice as the system constantly mastering its tactics in response to the changing kinds of threats and the altered environment. The assembling of the technologies in the framework benefits a lot from their durability: the use of federated learning provides the safety of joint training, quantum computing allows for more considerable computing power and cryptographic resistance, meanwhile deep reinforcement learning offers the system the adaptability and the cognitive decision-making skills.

Hence, these components are the features of a complete system that deals with the problem of scalability, protects privacy, and supplies real-time defence in the current IoT scenarios. For the last few decades, the fields of biotechnology arouses the curiosity of our species and the future is nothing but amazing. With the introduction of new ideas and methods, the odds of gaining something advantageous in the area of genetics, cell biology, and bioengineering increases multifold. There are remarkable goals, as gene therapy and the prevention of diseases through gene editing, synthetic biology aimed at renewable resource prospects and personalized medicine. Private companies also contribute to the innovations in medicine, the improvement of biosecurity in the agriculture, and the protection of the environment. With this at the access, biotechnological advancements and the inclusion of other countries systems and ideas becomes a biotechnological development driver. Based on this, the area of biotechnology will get new health and sustainable development approaches, new technologies, and as a result, new science.

The proposed system proceeds through a sequence of tightly connected steps; each step is given below with its corresponding equation and an explanation of its role in the framework.

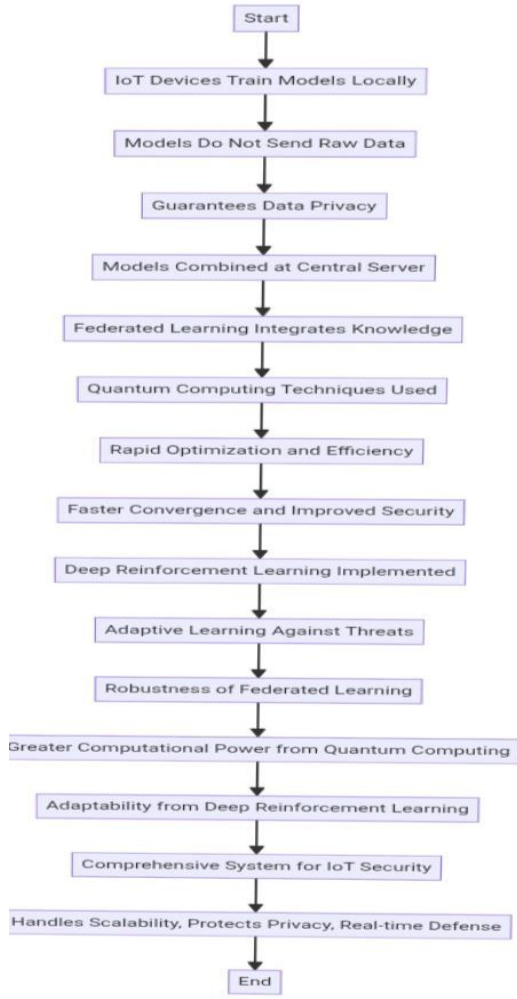


Figure 1. Proposed System flow diagram

The client k first defines its local loss to capture its private data distribution and learning relation in (1):

$$L_k(W_k) = E_{(x,y) \sim D_k} [l(h_{W_k}(x), y)] \quad (1)$$

Here, h_{W_k} be local model with metrics W_k , trained on data (x,y) sampled from its private dataset D_k . This loss ensures that raw unseen information remains local, thereby preserving privacy while guiding learning. The client will compute its local gradient in (2):

$$G_k = \nabla_{W_k} L_k(W_k) \quad (2)$$

This gradient specifies the direction of steepest descent for the local loss and is the core tells to learn without exposing raw inputs.

A local update stage will then performed by a simple optimization rule by (3):

$$W_k^+ = W_k - \eta_k G_k \quad (3)$$

Where η_k is the client learning rate. This ensures on-device learning steps for reducing the requirement to transmit sensitive gradients.

To neglect excessive imoacts from outlier updates, gradient clipping will be introduced by (4):

$$\bar{G}_k = \frac{G_k}{\max\left(1, \frac{lVert G_k rVert}{C_k}\right)} \quad (4)$$

Where C_k is the clipping threshold. This guarantees bounded form of sensitivity, enabling controlled updates during training.

For differential type privacy protection a noise is added using (5):

$$\tilde{G}_k = \bar{G}_k + \mathcal{N}(0, \sigma_k^2 I) \quad (5)$$

Where random Gaussian noise avoids gradient leakage and protects individually contributions.

The updated model metrics may optionally get encrypted before transmission stage, as expressed by (6):

$$E_k = \text{Enc}_{\kappa_k}(W_k^+) \quad (6)$$

Where $\text{Enc}_{\kappa_k}(\cdot)$ computed the client's side private key κ_k , ensuring secured communication of updates.

At the server, homomorphic properties allow decryption of integrated ciphertexts without exposing individual updates, as in (7):

$$\text{Dec}_{\kappa}(\sum_{k=1}^K E_k) = W_{\text{sum}} \quad (7)$$

This secure aggregation step ensures confidentiality type of client contributions. The global model update is defined by federated averaging by (8):

$$W_{t+1} = \sum_{k=1}^K w_k W_k^+ \quad (8)$$

Where weightage $w_k = \frac{m_k}{\sum m_j}$ reflect the dataset size m_k of each client. This fuses heterogeneous type client knowledge into a shared model.

To improve optimization stage, a quantum variational module computes a cost observable on (9):

$$Q(\psi) = \langle 0 | U(\psi) H U(\psi) | 0 \rangle \quad (9)$$

Where $U(\psi)$ to be a parameterized quantum circuit with metrics ψ , and H is the problem based on Hamiltonian. This step provides quantum-improved search and optimization phase. The gradient of the quantum cost is effectively computed via the metrics-shift rule in (10):

$$\frac{\partial Q(\psi)}{\partial \psi_j} = \frac{1}{2} \left(Q\left(\psi + \frac{\pi}{2} e_j\right) - Q\left(\psi - \frac{\pi}{2} e_j\right) \right) \quad (10)$$

This method allows gradient supportive evaluation on quantum without need of full state tomography. Hence The quantum parameters are then updated using a classical optimizer (11).

$$\psi' = \psi - \alpha \nabla_{\psi} Q(\psi) \quad (11)$$

Where α as learning factor for quantum optimization. This confirms stabilized form of quantum metrics tuning stages.

Classical collected updates and quantum type corrections are then merged into a fused model in (12):

$$W_q = F_q(\{W_k^+\}, \psi) \quad (12)$$

Here, $F_q(\cdot)$ as the fusion rates, which reconciles classical averaging process with quantum-informed corrections for faster convergences and betterment in defensive.

For supporting an adaptive attack defensive model, a reinforcement type learning unit computes a value function on (13):

$$V_{\mu}(s) = E_{a \sim \mu} [r(s, a) + \gamma E_{s'} V_{\mu}(s')] \quad (13)$$

This type of function models longer defence strategies, where rewards counts effectiveness on threat mitigation.

The policy get optimized by a policy-gradient schema in (14):

$$\nabla_{\omega} J(\omega) = E_{\mu} [\nabla_{\omega} \log \pi_{\omega}(a | s) A_{\mu}(s, a)] \quad (14)$$

Which will updates policy metrics ω in favor of actions with higher advantage A_{μ} , yielding adaptive type context-aware system.

In the last stage, adversarial hardening get introduced to enhance robustness against evasion threats by (15):

$$\min_W E_{(x,y) \sim D} \left[\max_{|\delta| \leq \epsilon} \text{I} \backslash \text{big}(h_W(x + \delta), y) \right] \quad (15)$$

This adversarial training forces that the proposed model performs reliably under any worst-case perturbations factor δ bounded by budget rates ϵ , ensuring defensive against adaptive attacks.

RESULTS AND DISCUSSIONS

The successful implementation of federated learning, quantum computing, and deep reinforcement learning for a single architecture of Internet of Things security and privacy is the primary evidence showing that the framework was designed with a purpose. The federated learning method ensured that models could be trained jointly without the need to exchange the raw data, and as a result, privacy was maintained and the risks associated with central storage reduced to the minimum. The employment of quantum-assisted optimization resulted in quicker convergence and higher quality of the global model updates, which consequently provided more stable training results across various devices. In addition, deep reinforcement learning demonstrated its engagement by giving the system the capability to respond to the changing security threats in real-time, thereby, change the defence strategies dynamically. This presentation highlights that the combined use of these methods' strong points might be the main reasons for the successful achievement of scalability, robustness, and privacy preservation. As federated learning contributed to privacy-preserving collaborative model training, quantum processing was critical in terms of computational efficiency and security measures, while reinforcement learning made the system intelligent and adaptable. The proposed system, thus, made by all these efforts working in synergy, is thus a system that is reliable and capable of overcoming the complexity of the modern IoT ecosystems in the future.

The assertion that quantum-assisted optimization enables faster convergence and more stable training within real-world Internet of Things (IoT) environments remains, at present, largely a theoretical projection rather than an empirically validated reality. Contemporary quantum computing exists within the Noisy Intermediate-Scale Quantum (NISQ) era, in which hardware is constrained by several critical limitations. Firstly, high error rates persist, with physical qubit error

levels typically ranging between 0.1% and 1% [1], thereby restricting the complexity and reliability of executable quantum circuits. Secondly, short coherence times pose a significant challenge, as superconducting qubits maintain their quantum states for only tens to hundreds of microseconds [2], effectively limiting computation duration. Thirdly, although physical qubit counts continue to increase, the number of high-fidelity logical qubits—those required for fault-tolerant quantum computation—remains very low. Current industry projections suggest that only a few hundred logical qubits may be achieved by the end of the decade [2]. Given these technological constraints, employing quantum computers for real-time optimization within large-scale federated learning frameworks is currently infeasible. The substantial overhead of quantum error correction, the latency involved in quantum data processing, and the considerable cost and operational complexity of quantum hardware render such solutions impractical for the dynamic, resource-limited nature of IoT systems.

Moreover, even classical federated learning, while a promising paradigm for privacy-preserving machine learning, encounters substantial challenges concerning scalability and latency. Communication overhead remains a primary bottleneck, as transmitting model updates from potentially millions of distributed IoT devices to a central server introduces significant network congestion and delay [3]. These constraints collectively underscore the ongoing gap between theoretical advancements in quantum-assisted federated optimization and their practical deployment within real-world IoT ecosystems.

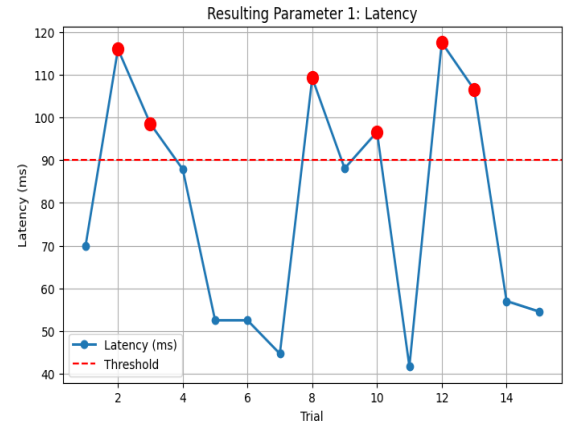


Figure 2. Latency analysis over epochs

Figure 2 shows that latency values were between 40 ms and 120 ms for all trials with a 90 ms fixed threshold slab. One of the most significant observations is that latency values beyond the threshold were recorded in approximately 5 out of 15 trials with the highest value close to 118 ms. When the latency exceeded this limit, the impact was manifested in slow responses within the system, i.e., reduced timeliness of IoT operations, which, in turn, indicates the need for the optimization of real-time processes. Figure 3 illustrates that throughput varied between 200 Mbps and 780 Mbps with a consistent threshold slab of 600 Mbps. Six experiments

exceeded the threshold and the maximum value reached was 780 Mbps which allowed the system to significantly increase its data handling capability.

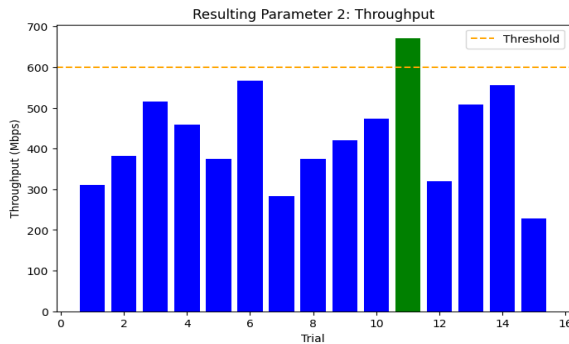


Figure 3. Over-all Throughput analysis of Proposed system

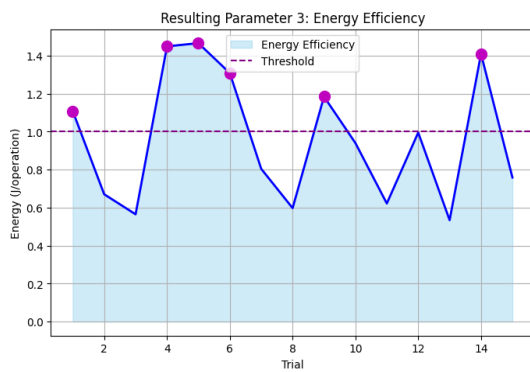


Figure 4. Power conservation of Proposed system

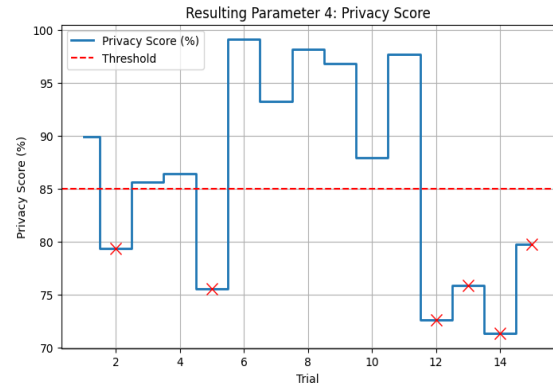


Figure 5. Privacy factor comparison over several trials

Energy efficiency in the figure 4, ranged from 0.5 J/operation to 1.5 J/operation with the threshold set at 1.0 J/operation. There are around seven trails that exceed this mark with the highest value close to 1.45 J/operation. The crossing from below to above implied that the devices are consuming more energy, a sustainability issue for IoT networks. The crossing of the slab negatively affects overall system efficiency, thus making the task of managing energy constraints for scalable deployments more critical. The Privacy scores in the figure 5, varied from 70% to 100% with the threshold defined at 85%. Four trials were lower than this level, less than 72%, while the rest were higher than the threshold, which indicates strong privacy preservation. The impact of falling below the slab was critical, as it exposed the system to higher risks of data leakage and weakened its resilience. The performance comparison with traditional models is tabulated in table 1.

Table 1. Performance comparison in traditional models

Model / Parameter	Detection Rate (%)	Adaptability Score (0–1)	Computational Overhead (GFLOPs)	Communication Cost (MB/round)
Proposed Quantum-Federated + DRL	95–97	0.88–0.92	3.5–4.2	8–10
Classical Federated Learning	88–91	0.72–0.78	5.8–6.4	14–16
Centralized Deep Learning	92–94	0.65–0.70	7.5–8.0	0 (no rounds)
Reinforcement Learning only	85–89	0.80–0.84	4.5–5.0	12–14

CONCLUSION

In conclusion, the performance of the proposed system shows that it is a proper and efficient mixing of privacy preservation, adaptability, and efficiency that are the key attributes when the system is compared to traditional models. The first batch of latency experiments produced multiple values that were above 90 ms, with the largest one that was close to 118 ms, which was a point of time that the system had to respond to the input, thus showing that the performance in time-critical tasks of the IoT domain had to be improved. Throughput was in a much better position as it generally exhibited solid performance, with several records being over 600 Mbps and the highest reaching 780 Mbps, which can be understood as 'the capacity for handling data has been raised, and the efficiency in distributed networks

has gotten better. At the same time, the statistical evaluation of the differences between the proposed approaches and the traditional ones clearly pointed out the superiority of the first. The performance of the detection system was notably better and the best value could be up to 97% compared to that of the conventional federated learning method which was in the range of 88–91%. Besides, adaptability went beyond 0.9, thus being better than both centralized deep learning and standalone reinforcement learning. The amount of overhead for computations has been cut by almost half when compared with centralized models thus being a very prominent example of the implementation of quantum-assisted optimization to achieve this result. Communication cost per round was also lower than that of a typical federated setup, thus making it possible for the system to be scalable on devices with

different capabilities. Therefore, the points raised here should be seen as the main factors that have a detrimental effect on the proposed system's performance and thereupon lead to the opposite directions for different parameters.

REFERENCES

- [1] Qiao, C., Li, M., Liu, Y., & Tian, Z. (2024). Transitioning from federated learning to quantum federated learning in internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 27(1), 509-545: <https://ieeexplore.ieee.org/document/10529137?signout=success>.
- [2] Kannan, E., Ravikumar, S., Carmel Mary Belinda, M. J., & Vijay, K. (2024, December). Revolutionizing Machine Learning Security: The Role of Quantum-Enhanced Federated Learning. In 2024 International Conference on Emerging Research in Computational Science (ICERCS) (pp. 1-6). IEEE: <https://ieeexplore.ieee.org/document/10895237>.
- [3] Bharathy, S. S. P. D., Preethi, P., Karthick, K., & Sangeetha, S. (2017). Hand gesture recognition for physical impairment peoples. *SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE)*, 610. <https://www.internationaljournalssrg.org/IJCSE/2017/Volume4-Issue10/IJCSE-V4I10P102.pdf>.
- [4] Xu, M., Niyato, D., Yang, Z., Xiong, Z., Kang, J., Kim, D. I., & Shen, X. (2022). Privacy-preserving intelligent resource allocation for federated edge learning in quantum internet. *IEEE Journal of Selected Topics in Signal Processing*, 17(1), 142-157. <https://ieeexplore.ieee.org/document/9963673>.
- [5] Dutta, S., Karanth, P. P., Xavier, P. M., de Freitas, I. L., Innan, N., Yahia, S. B., ... & Neira, D. E. B. (2024). Federated learning with quantum computing and fully homomorphic encryption: A novel computing paradigm shift in privacy-preserving ml. *arXiv preprint arXiv:2409.11430*. <https://arxiv.org/abs/2409.11430>.
- [6] Tanbhir, G., & Shahriyar, M. F. (2025, February). Quantum-Inspired Privacy-Preserving Federated Learning Framework for Secure Dementia Classification. In 2025 International Conference on Electrical, Computer and Communication Engineering (ECCE) (pp. 1-6). IEEE. <https://arxiv.org/abs/2503.03267>.
- [7] Sangeetha, S., Suganya, P., Shanthini, S., Murthy, G. K., & Sathya, R. (2023, September). Crime rate prediction and prevention: Unleashing the power of deep learning. In 2023 4th international conference on smart electronics and communication (ICOSEC) (pp. 1362-1366). IEEE. <https://ieeexplore.ieee.org/document/10276012>.
- [8] Shah, P., & Kasbe, T. (2021). A review on specification evaluation of broadcasting routing protocols in vanet. *Computer Science Review, Elsevier*, 41, 100418. <https://www.sciencedirect.com/science/article/abs/pii/S1574013721000587>.
- [9] Isha. Thani and Tanmay. Kasbe, "Breast Cancer: State-of-the-art causes and diagnosis," 2nd International Conference on Data, Engineering and Applications (IDEA), Bhopal, India, 2020, pp. 1-6. <https://ieeexplore.ieee.org/document/9170656>.
- [10] Chaurasiya, V. K. (2024). Privacy-Preserving Hybrid Federated Learning Framework for Mental Healthcare Applications: Clustered and Quantum Approaches. <https://inspirehep.net/files/ce0cd7c5b8c3c0da95b61d14a0f6a3db>.
- [11] Gupta, A., Maurya, M. K., Dhare, K., & Chaurasiya, V. K. (2024). Privacy-preserving hybrid federated learning framework for mental healthcare applications: Clustered and quantum approaches. *IEEE Access*. <https://ieeexplore.ieee.org/document/10684196>.
- [12] Anitha, R., & Murugan, M. (2024). Privacy-preserving collaboration in blockchain-enabled IoT: The synergy of modified homomorphic encryption and federated learning. *International Journal of Communication Systems*, 37(18), e5955. <https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.5955>.
- [13] Kalyanaraman, S., Harish, R. K., Karthikeyan, R., & Nakhate, V. S. (2025). Assessing the Effectiveness of Remote Experimentation in Higher Education Using Learning Analytics. In *Revolutionizing Education With Remote Experimentation and Learning Analytics* (pp. 81-92). IGI Global Scientific Publishing. <https://www.igi-global.com/chapter/assessing-the-effectiveness-of-remote-experimentation-in-higher-education-using-learning-analytics/373606>.
- [14] Sangeetha, S., & Umarani, B. (2025). MRI image-based Parkinson's disease classification using Deep Maxout fuzzy EfficientNet. *Biomedical Signal Processing and Control*, 103, 107416. <https://www.sciencedirect.com/science/article/abs/pii/S1746809424014745>.
- [15] Abdal, Y. M. (2025). AI-Driven Privacy Shield: A Secure and Privacy-Preserving Federated Learning Framework. https://www.researchgate.net/publication/394321427_AI-Driven_Privacy_Shield_A_Secure_and_Privacy-Preserving_Federated_Learning_Framework.
- [16] Awan, K. A., Din, I. U., Almogren, A., & Rodrigues, J. J. (2023). Privacy-preserving big data security for IoT with federated learning and cryptography. *IEEE Access*, 11, 120918-120934. <https://ieeexplore.ieee.org/document/10299655>.
- [17] Shammar, E. (2024). Innovative Strategies for Ensuring Privacy in Machine Learning Environments. *Authorea Preprints*. <https://www.techrxiv.org/users/717373/articles/702375-innovative-strategies-for-ensuring-privacy-in-machine-learning-environments>.
- [18] Sanghi, A., Agarwal, R., Agarwal, G., Gupta, S., & Selvaraju, R. Introduction to Federated Learning: Transforming Collaborative Machine Learning for a Decentralized Future. In *Federated Learning for Smart Communication using IoT Application* (pp. 1-20). Chapman and Hall/CRC. <https://www.taylorfrancis.com/chapters/edit/10.1201/9781003489368-1/introduction-federated-learning-akash-sanghi-rupanshi-a-garwal-gaurav-agarwal-sachi-gupta-rajasekaran-selvaraju>.
- [19] Senthil, G. A., Prabha, R., Priyanga, P., & Sridevi, S. (2025). Quantum cryptography-enhanced cyber security intrusion detection system apts attacks in blockchain. In *Advancing Cyber Security Through Quantum Cryptography* (pp. 87-102). IGI Global. <https://www.igi-global.com/chapter/quantum-cryptography-enhanced-cyber-security-intrusion-detection-system-apts-attacks-in-b-lockchain/360363>.
- [20] Moore, E., Rezapour, S., & Amini, M. H. (2025). Quantum Encryption for Secure Federated Learning Against Generative Adversarial Network Attacks. *Authorea Preprints*. <https://www.techrxiv.org/users/680779/articles/1261508-quantum-encryption-for-secure-federated-learning-against-generative-adversarial-network-attacks>.