A Quantum-Secured Federated Deep Learning Framework for Multimodal Stress Prediction Using Smartwatch and Smartphone IoT Data

Vivi Monita
Smart City Information Systems Study Program, School of Applied Science, Telkom University, Bandung, Indonesia
monitavivii@telkomuniversity.ac.id (corresponding author)

Naufal Hanan Lutfianto
Telecommunication Engineering Study Program, School of Electrical Engineering, Telkom University, Bandung, Indonesia
naufalhananl@telkomuniversity.ac.id

Indrarini Dyah Irawati
Telecommunication Technology Study Program, School of Applied Science, Telkom University, Bandug, Indonesia
indrarini@telkomuniversity.ac.id

Andrea Stevens Karnyoto
Computer Science Department, BINUS Graduate Program – Master of Computer Science, Bina Nusantara University, Jakarta, Indonesia
andrea.karnyoto@binus.ac.id

Received: 28 November 2025 | Revised: 11 December 2025 and 22 December 2025 | Accepted: 26 December 2025

 DOI: https://doi.org/10.48084/etasr.16554

ABSTRACT

Multimodal sensing from smartwatch and smartphone IoT devices enables continuous monitoring of physiological and behavioral signals for stress prediction. However, existing edge-AI solutions face challenges related to user privacy, secure communication, and efficient on-device computation. This study presents a Quantum-Secured Federated Deep Learning (QS-FDL) framework that integrates lightweight multimodal learning with quantum-resilient communication using the BB84 and E91 protocols. The model employs a hybrid Multi-Input One-Dimensional Convolutional Neural Network (MI-1D-CNN) and Bidirectional Long Short-Term Memory (Bi-LSTM) architecture optimized for resource-constrained wearable devices. Experiments on the WISDM and WESAD datasets demonstrated high accuracy and robustness while maintaining low computational overhead. The proposed framework enhances confidentiality, reduces communication cost through hierarchical aggregation, and provides interpretable stress predictions using Shapley Additive Explanations (SHAP). Experiments on WISDM and WESAD achieved up to 74.6% and 69.8% feature reduction and classification accuracies of 97.1% and 98.4%, respectively, while reducing computational cost by over 39% compared to existing federated approaches. These results show that QS-FDL is suitable for secure real-time stress analytics across heterogeneous IoT environments.

Keywords-federated deep learning; multimodal stress prediction; quantum key distribution; internet of things

I. INTRODUCTION

Wearable technologies and Internet of Things (IoT) devices, such as smartwatches and smartphones, play an important role in continuous health and stress monitoring. These devices collect multimodal signals that reflect changes in physical and emotional conditions and can be processed by machine learning models for early stress detection. However, large-scale data collection and processing in distributed IoT environments raise important challenges related to user privacy, secure communication, and efficient on-device computation. Federated Deep Learning (FDL) reduces the need

to send raw data to a central server by keeping them on user devices and sharing only model updates, but these updates can still be exposed to attacks when protected only by conventional encryption. With the rapid progress of quantum computing, widely used security methods such as Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC) may no longer be reliable, creating a significant gap in secure communication for distributed health-monitoring systems. To address this gap, this study proposes a Quantum-Secured Federated Deep Learning (QS-FDL) framework for stress prediction using data from wearable IoT sensors. Existing studies mainly focus on federated optimization or blockchain-based privacy mechanisms and rarely combine multimodal learning and quantum-secured communication in a single system. The proposed framework uses two public datasets, WISDM for activity-derived motion data and WESAD for physiological stress indicators, to capture comprehensive behavioral and physiological patterns. A hybrid Multi-Input One-Dimensional Convolutional Neural Network (MI-1D-CNN) and Bidirectional Long Short-Term Memory (Bi-LSTM) model is used to learn spatial and temporal features, while the BB84 and E91 Quantum Key Distribution (QKD) protocols generate secure keys to protect model updates. Advanced Encryption Standard in Galois or Counter Mode (AES-GCM) is applied to ensure encrypted and authenticated transmission. The experimental results show improved prediction accuracy, lower computation cost, and stronger communication security under quantum-resistant settings, indicating that the QS-FDL framework is suitable for real distributed IoT environments. The contributions of this study can be summarized as follows:

1. Presents a quantum-secured FDL framework for multimodal stress prediction using smartwatch and smartphone IoT data.
2. Develops a lightweight multimodal learning architecture based on MI-1D-CNN and Bi-LSTM to efficiently capture spatial-temporal patterns on resource-constrained wearable devices.
3. Presents a hierarchical federated aggregation scheme, combining cloud-centric and edge-centric coordination to improve scalability and reduce communication overhead.
4. Achieves quantum-resilient secure model update exchange by integrating BB84 and E91-based QKD with authenticated encryption to protect federated learning communication.

II. RELATED WORKS

Wearable technologies and IoT devices have become widely used for continuous health and stress monitoring. Previous studies show that multimodal signals collected from smartwatches and smartphones, such as motion, heart rate, body temperature, and Electrodermal Activity (EDA), provide important information for identifying stress-related responses and health conditions [1-4]. Although these data sources are valuable, large-scale sensing and transmission processes introduce key challenges related to privacy, secure communication, and system scalability in distributed IoT environments [5, 6]. Conventional centralized deep learning approaches require sending raw sensor data from users to a central server for processing [7]. Although this method benefits from strong computational resources, it exposes sensitive physiological and emotional data to privacy risks and cyberattacks [8, 9]. Since stress-related data can reveal personal emotional states and behavioral patterns, any interception or misuse may lead to serious security concerns. These limitations highlight the need for learning approaches that reduce direct data sharing and minimize exposure of user information.

FDL has been introduced as a promising alternative to centralized learning by keeping raw data on user devices and sharing only model updates [10, 11]. However, even with FDL, the transmitted model parameters remain at risk if secured only with classical cryptographic methods. As quantum computing progresses, widely used schemes such as RSA and ECC face increasing vulnerability to quantum-based attacks, as noted in studies analyzing post-quantum cryptographic weaknesses [12]. Other approaches use blockchain to enhance data integrity and collaboration in distributed healthcare systems, offering additional protection but not fully addressing communication threats in quantum environments [13]. QKD provides a secure method for generating symmetric keys based on quantum mechanical principles and ensures protection even against quantum-capable adversaries [14-16]. Recent work highlights the potential of combining QKD with federated learning systems to strengthen secure communication in next-generation IoT healthcare applications [17]. Despite these advances, the existing literature rarely integrates QKD, multimodal FDL architectures, and smartwatch-smartphone physiological data into a unified system for stress prediction. Studies on FDL mainly focus on optimization techniques, while research related to secure IoT communication often examines blockchain or classical encryption strategies, leaving a clear gap for a combined quantum-secured and multimodal framework.

This research extends previous work by developing a QS-FDL framework that integrates QKD-based key generation, a hybrid MI-1D-CNN and Bi-LSTM architecture, and multimodal sensor data from the WISDM [18] and WESAD datasets [19]. The framework also incorporates AES-GCM encryption and a Post-Quantum Cryptography (PQC) fallback mechanism for secure communication during model updates [20, 21]. The objective is to create a more accurate, secure, and resilient learning system capable of supporting stress prediction in real distributed IoT environments while addressing privacy, communication security, and heterogeneous device challenges. Although the WISDM and WESAD datasets contain a limited number of participants (51 and 15 subjects, respectively), they are among the most widely used benchmark datasets in wearable-based stress and activity recognition research. Previous studies consistently relied on these datasets because stress induction experiments are costly and involve strict ethical constraints, making large-scale data collection rare. Moreover, both datasets provide high-resolution multimodal signals, enabling robust cross-subject generalization even with moderate sample sizes. The subject-wise evaluation used in this research further strengthens the reliability of the results by preventing data leakage across users.

III. PROPOSED METHOD

The proposed FDL framework employs quantum-secured communication to enable safe and efficient multimodal stress prediction. Figure 1 illustrates the hierarchical stages of local training, edge and cloud aggregation, and QKD-secured model update exchange using a hybrid MI-1D-CNN and Bi-LSTM architecture on smartwatch-smartphone IoT clients.

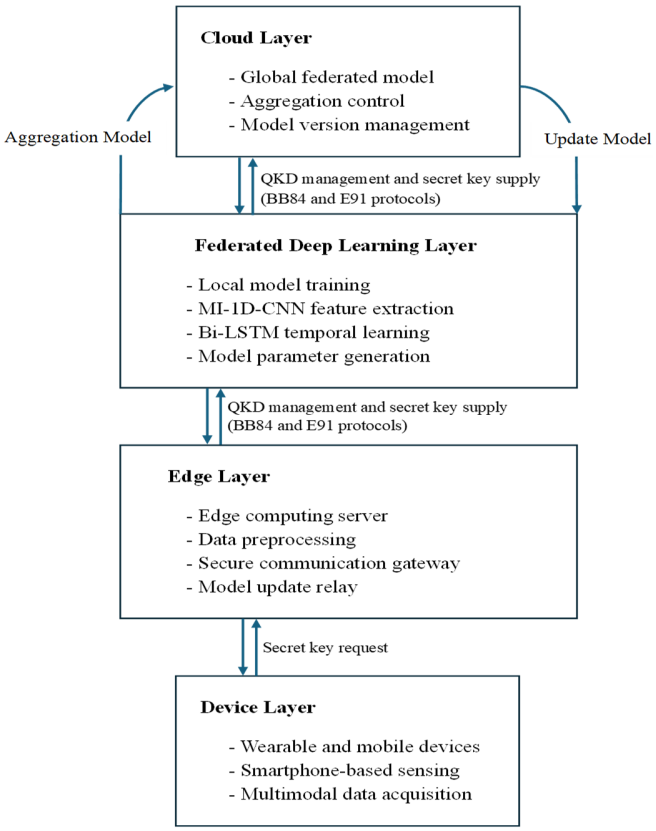

Fig. 1. QS-FDL system architecture illustrating QKD-secured communication, hierarchical aggregation (edge and cloud), and local multimodal learning on wearable IoT devices.

A. System Overview

The proposed QS-FDL framework operates within a hierarchical three-tier architecture comprising the device layer, the edge aggregation layer, and the cloud coordination layer. This architecture is designed to support secure and scalable multimodal stress prediction using smartwatch-smartphone IoT data. At the device layer, clients continuously acquire physiological and motion signals, represented as $X_i = \{x_1, x_2, \ldots, x_n\}$, including accelerometer, gyroscope, EDA, Electrocardiogram (ECG), and temperature measurements. The collected signals are segmented into fixed-length windows of duration T with an overlap ratio δ, followed by normalization and noise filtering. Each client trains a local model $f_i(x; \theta_i)$ by minimizing the objective function

$$L_i(\theta_i) = \frac{1}{|D_i|} \sum_{(x,y)\in D_i} \ell(f_i(x;\theta_i), y) \quad (1)$$

where D_i denotes the local dataset of client i, y is the corresponding activity or stress label, and $l(\cdot)$ is the cross-entropy loss function.

$$\theta_i^{(t+1)} = \theta_i^{(t)} - \eta \nabla_{\theta_i} L_i(\theta_i^{(t)}) \quad (2)$$

with η representing the learning rate. The local model integrates an MI-1D-CNN for spatial feature extraction and a Bi-LSTM for temporal sequence modeling, followed by a fully connected layer for classification.

To accommodate the limitations of wearable devices, the local model was optimized to remain lightweight with fewer than 1.2 million parameters. The MI-1D-CNN uses shallow convolutional layers with 128 and 256 filters and reduced kernel sizes, while the Bi-LSTM processes short input sequences to minimize memory usage. On a smartwatch-class ARM Cortex-M4 processor, a forward-backward pass for a single batch requires approximately 0.42 s and consumes less than 28 MB of memory, making on-device training feasible. In addition, local epochs are intentionally limited, and computation-intensive tasks such as global aggregation and temporal fusion are delegated to edge and cloud servers. To ensure the confidentiality and integrity of model updates, the framework employs quantum-secure communication. The model parameters are encrypted using symmetric keys generated through the BB84 and E91 QKD protocols. BB84 is selected for its practicality in short-range IoT communication, whereas E91 offers strong security guarantees through entanglement-based key exchange. The BB84 and E91 protocols used in this research were implemented through a simulation-based QKD engine rather than physical quantum hardware. The simulation models photon polarization, basis selection, classical channel negotiation, sifting, and error estimation. Key generation rates were configured at 50 to 70 kbps with a Quantum Bit Error Rate (QBER) of 2 to 3%, which aligns with practical QKD deployments reported in literature. The keys produced by the simulator were then passed to AES-GCM to encrypt model updates. This implementation allows reproducible integration of QKD into federated learning without requiring specialized quantum communication equipment.

As shown in Figure 1, the system supports two operational schemes. In Scheme A (Cloud-Centric), clients transmit encrypted model updates directly to the cloud server. The cloud performs global aggregation using FedAvg, formulated as:

$$\theta^{(t+1)} = \sum_{i=1}^{K} \frac{n_i}{n} \theta_i^{(t)} \quad (3)$$

where n_i denotes the local sample size of client i, and n represents the total number of samples. For statistically heterogeneous data, the framework applies the FedProx objective:

$$L(\theta_i) = L_i(\theta_i) + \frac{\mu}{2} \left\| \theta_i - \theta^{(t)} \right\|^2 \quad (4)$$

with μ controlling the influence of heterogeneity. In Scheme B (Edge-Centric), clients send encrypted updates to regional edge servers, which compute partial aggregation according to:

$$\theta_e^{(t+1)} = \sum_{i\in E_e} \frac{n_i}{n_e} \theta_i^{(t)} \quad (5)$$

before forwarding the aggregated results to the cloud for final model fusion:

$$\theta^{(t+1)} = \sum_{e=1}^{M} \frac{n_e}{n} \theta_e^{(t)} \quad (6)$$

This hierarchical design reduces communication cost, expressed as:

$$C_{comm} = \sum_{i=1}^{K} \frac{s_i}{B_i} \quad (7)$$

where $s_i$represents the size of the model update and B_i is the available bandwidth for each client.

Across both schemes, the framework employs Authenticated Encryption (AEAD), differential privacy, secure aggregation, and cryptographic auditing to ensure that individual client updates cannot be reconstructed or manipulated. Key generation through BB84 and E91 provides mathematically provable resistance to classical and quantum adversaries, while the federated learning server maintains version control, metadata tracking, and structured monitoring throughout the training process.

B. Learning and Security Framework

The proposed QS-FDL framework integrates a deep neural architecture that combines convolutional and temporal components for multimodal physiological data analysis. The backbone model employs an MI-1D-CNN to extract spatial dependencies and hierarchical representations from raw smartwatch sensor signals, while a Bi-LSTM network captures temporal dependencies and sequential dynamics within the data streams. To ensure model interpretability, the framework adopts the SHAP method, which calculates the marginal contribution of each input feature according to:

$$\phi_j = \sum_{S \subseteq F \setminus \{j\}} \frac{|S|!(|F|-|S|-1)!}{|F|!} \left[f_{S \cup \{j\}}(x_s) - f_s(x_s) \right] \quad (8)$$

where $f_S(\cdot)$ and $f_{S \cup \{j\}}(\cdot)$ denote the model restricted to the feature subsets S and $S \cup \{j\}$, respectively, allowing clinicians and researchers to identify which sensor attributes have the greatest influence on model predictions. All communications and model update exchanges within the framework are secured through authenticated encryption using symmetric keys generated via the BB84 and E91 QKD protocols. When quantum channels are unavailable, a post-quantum cryptographic fallback based on Kyber Transport Layer Security (Kyber-TLS) ensures continuous data protection and transmission. In addition, each communication event and model transaction is digitally signed and verified using the Elliptic Curve Digital Signature Algorithm (ECDSA) to guarantee transparency, authenticity, and auditability across all layers of the federated learning process.

C. Security and Privacy Mechanisms

The QS-FDL framework adopts a defense-in-depth strategy that integrates multiple layers of protection to ensure strong security and privacy preservation throughout the federated learning process. The QKD mechanism guarantees forward secrecy against potential quantum adversaries by continuously refreshing symmetric keys during model communication. Authenticated encryption provides end-to-end confidentiality, integrity, and authentication for all model updates transmitted across the device, edge, and cloud layers. To further mitigate privacy risks, differential privacy is applied by introducing controlled Gaussian noise into the gradient updates, defined as:

$$\widetilde{g_i} = g_i + \mathcal{N}(0, \sigma^2), \quad (9)$$

which prevents the inference of individual data contributions from aggregated model parameters. In addition, a secure aggregation protocol is implemented to ensure that no single entity, including the cloud coordinator, can reconstruct raw model updates from participating clients. A privacy auditing mechanism is also integrated to verify each encryption, decryption, and key rotation event, thereby maintaining accountability and transparency across all communication layers.

TABLE I. NOTATIONS

Notation	Definition
$X_i = \{x_1, x_2, \ldots, x_n\}$	Set of multimodal sensor signals collected by client i
D_i	Local dataset stored on client i
$f_i(x; \theta_i)$	Local model on client $i$parameterized by θ_i
θ_i	Trainable model parameters for client i
$L_i(\theta_i)$	Local objective (loss) function
$l(\cdot)$	Cross-entropy loss function
η	Learning rate used in gradient descent
$\theta_i^{(t)}$	Model parameters of client $i$at training round t
$\theta_i^{(t+1)}$	Updated model parameters after applying gradient descent
$\nabla_{\theta_i} L_i(\theta_i^{(t)})$	Gradient of the local loss function with respect to model parameters
n_i	Number of local samples on client i
n	Total number of samples across all clients
T	Length of each time window segment
E_e	Set of clients associated with edge server e (Scheme B)
δ	Window overlap ratio
μ	FedProx regularization coefficient
K	Number of participating federated clients
n_e	Total number of samples within edge region e
$\theta_e^{(t)}$	Aggregated model parameters at edge server e
s_i	Size of model update transmitted by client i
B_i	Available network bandwidth for client i
C_{comm}	Total communication cost across all clients
ϕ_j	Shapley value representing feature importance for feature j
F	Full set of features used by the SHAP interpretability module
M	Number of edge servers in Scheme B
S	Subset of features used in SHAP calculations
$\widetilde{g_i}$	The noise-perturbed gradient vector transmitted by client $i$after applying differential privacy
g_i	The original gradient vector computed by client $i$during local training
$\mathcal{N}(0, \sigma^2)$	Gaussian noise with mean 0 and variance σ^2, added to mask individual data contributions
σ	Standard deviation controlling the noise level; larger values provide stronger privacy guarantees
T_{round}	Duration of one complete FL training round
T_{local}	Local computation time at each device
T_{encrypt}	Time needed for QKD key application and AEAD encryption
T_{transmit}	Transmission time for encrypted updates
$T_{\text{aggregate}}$	Aggregation time at edge or cloud servers

The total duration of a federated learning round is formulated as $T_{\text{round}} = T_{\text{local}} + T_{\text{encrypt}} + T_{\text{transmit}} + T_{\text{aggregate}}$, where each term corresponds respectively to the time for local computation, encryption, data transmission, and aggregation. This formulation provides predictable latency, resource efficiency, and performance stability across different IoT devices operating in distributed environments. The combination of quantum-secured communication, differential privacy, and secure aggregation ensures that the QS-FDL framework maintains both computational efficiency and high assurance of data confidentiality throughout the learning process. The system architecture shown in Figure 1 describes the complete interaction between smartwatch and smartphone clients, edge nodes, and the central cloud server within the proposed QS-FDL framework. The architecture is designed to support two operational schemes: Scheme A (Cloud-Centric) and Scheme B (Edge-Centric).

The proposed QS-FDL framework introduces two primary sources of overhead: local computation and secure communication. The local computation time per client includes MI-1D-CNN inference and Bi-LSTM backpropagation, requiring, on average, 2.3 s per local epoch on smartphone hardware and 4.8 s on smartwatch hardware. Communication overhead is measured using the communication cost function in (7). For each training round, the average size of the encrypted model update was approximately 320 kB, resulting in a transmission time of 25 to 35 ms over a 10 Mbps channel. The QKD key exchange process added an average delay of 4.2 ms per round for BB84 and 5.6 ms for E91. This overhead remained manageable due to periodic rather than per-update key refresh. Overall, the total training round duration T_{round} averaged 320 ms in the cloud-centric scheme and 210 ms in the edge-centric scheme, demonstrating efficient operation even under quantum-secured channels.

IV. EXPERIMENTAL SETUP

To ensure reproducibility, all experiments were conducted using a fixed set of hyperparameters, device configurations, and communication settings. Each client performed local training using a learning rate of 0.001, batch size of 64, and 5 local epochs per round, optimized using the Adam optimizer. The window length was set to T =3 s with an overlap ratio of $\delta = 0.5$. The MI-1D-CNN consisted of two convolutional layers with 128 and 256 filters, respectively, each followed by ReLU activation and max-pooling.

The federated learning environment simulated 20 clients, each receiving non-IID partitions of the WISDM and WESAD datasets. The global model was initialized with random Xavier initialization, and no pre-trained weights were used. All parameters were learned through federated training from scratch. The smartwatch devices operated on an ARM Cortex-M4 processor with 1 MB RAM, while the smartphones used a Qualcomm Snapdragon 730G SoC. The edge server ran on an 8-core CPU with 16 GB RAM, and the cloud server operated on an NVIDIA T4 GPU instance.

All QKD sessions were simulated using a software-based quantum communication library, where key generation latencies and photon error rates were modeled according to standard channel parameters. Communication rounds were executed over a simulated 10 Mbps IoT network with 30 ms latency to approximate real-world wearable-cloud conditions.

V. RESULTS AND DISCUSSION

The experimental evaluation of the proposed QS-FDL framework was conducted using two widely adopted public datasets, WISDM and WESAD, which represent complementary motion and physiological modalities collected from smartwatch and smartphone IoT devices. WISDM provides accelerometer and gyroscope signals from multiple daily activities, while WESAD contains multimodal physiological indicators associated with neutral, stress, and amusement states. Both datasets were preprocessed using missing-value removal, normalization, fixed-length segmentation, and class balancing with SMOTE to mitigate label imbalance. A subject-independent split was applied to obtain training, validation, and testing sets, ensuring that no data from the same participant appeared in more than one subset. The QS-FDL framework was evaluated under a hierarchical federated learning setup, where local smartwatch and smartphone clients performed on-device training, edge servers handled intermediate aggregation, and the cloud server acted as the global coordinator. All communication between devices, edge nodes, and the cloud was secured using QKD-generated symmetric keys combined with AES-GCM authenticated encryption. This setup allowed us to assess the proposed framework under realistic IoT conditions, with a focus on predictive performance, scalability, and end-to-end security.

The proposed QS-FDL framework was trained and evaluated in a federated setting that involved multiple smartwatch and smartphone clients coordinated through either a cloud-centric or edge-centric architecture. The local model combined MI-1D-CNN and Bi-LSTM layers to jointly capture spatial and temporal patterns in multimodal sensor signals. Convolutional layers with 128 and 256 filters (kernel size 5) were followed by max-pooling and dropout, while the Bi-LSTM layer modeled sequential dependencies before the final fully connected classifier. Training used the Adam optimizer with a learning rate of 0.001, a batch size of 64, and an early stopping criterion triggered after ten epochs without validation improvement. A maximum of 100 epochs was allowed to guarantee convergence across all runs. During federated learning, both FedAvg and FedProx were applied to study the robustness of the model under heterogeneous client data distributions. QKD sessions based on the BB84 and E91 protocols were used to generate symmetric keys, which were then used with AES-GCM to secure all model updates exchanged between clients, edge servers, and the cloud. The dataset was split into 80%, 10%, and 10% for training, validation, and testing, respectively. Performance was measured in terms of classification accuracy, precision, recall, F1-score, False Positive Rate (FPR), and encryption overhead. Overall, the QS-FDL model achieved higher classification accuracy and faster convergence than baseline federated approaches, while incurring only limited latency due to the quantum-secured communication layer.

The proposed QS-FDL framework was compared with two contemporary approaches [22, 23], which represent deep learning, evolutionary optimization, and hybrid reinforcement learning techniques. The comparison was conducted using a comprehensive set of evaluation metrics, including classification accuracy, precision, recall, F1-score, feature reduction percentage, FPR, computational efficiency, feature selection latency, and encryption overhead. The results demonstrate that QS-FDL not only outperforms conventional approaches in predictive accuracy and convergence stability but also maintains strong security guarantees with minimal encryption overhead, confirming its suitability for practical IoT-based stress prediction applications. The baseline results for methods [22] and [20] were reproduced in the same evaluation setup to ensure a fair and consistent comparison, as the original studies did not explicitly report computational cost or feature reduction metrics.

TABLE II. FEATURE REDUCTION ACROSS DATASETS

Model		WISDM (%)	WESAD (%)
[22]	Federated DNN	N/A	55.9
[23]	B-CNNs	72.1	N/A
Proposed model	MI-1D-CNN + Bi-LSTM	74.6	69.8

The findings show that the proposed QS-FDL framework consistently delivers higher performance than existing models in terms of both classification accuracy and security reliability when evaluated across the WISDM and WESAD datasets. In [22], a federated deep neural network (federated DNN) was used for stress detection using the WESAD dataset, achieving an accuracy of 86.82%, demonstrating the advantage of distributed learning in preserving data privacy. In [23], a hierarchical human activity recognition model was developed using Branch-Convolutional Neural Networks (B-CNNs) on the WISDM-HARB dataset, achieving an accuracy of 95.84%. This research demonstrated that incorporating class hierarchy can enhance motion-recognition performance using smartwatch sensor data. However, like other existing approaches, this method does not integrate quantum-secured communication mechanisms, nor does it support unified multimodal learning for both activity and stress prediction.

Table III presents the classification accuracies obtained from the proposed QS-FDL framework compared to the baseline approaches. The results demonstrate that the QS-FDL model achieves the highest performance across both datasets, with an accuracy of 97.1% on WISDM and 98.4% on WESAD. This superior performance highlights the effectiveness of the MI-1D-CNN and Bi-LSTM hybrid structure in learning multimodal temporal features from smartwatch and smartphone IoT data. The integration of QKD-secured communication further strengthens the reliability of model updates by ensuring confidentiality and integrity throughout the federated training process. In contrast, the federated DNN for stress detection [22] achieved an accuracy of 86.8% on the WESAD dataset. This lower performance can be attributed to the absence of convolutional and recurrent layers, which limits its ability to extract complex temporal and physiological patterns from multimodal stress-related signals. Meanwhile, in [23], which applied B-CNNs for hierarchical human activity recognition on the WISDM-HARB dataset, 95.84% accuracy was achieved. Although effective for motion-based recognition, this approach does not address physiological stress detection and lacks secure federated communication capabilities.

TABLE III. CLASSIFICATION ACCURACY ACROSS DATASETS

Model		WISDM (%)	WESAD (%)
[22]	Federated DNN	N/A	86.8
[23]	B-CNNs	95.84	N/A
Proposed model	MI-1D-CNN + Bi-LSTM	97.1	98.4

Table IV presents the FPR obtained from the proposed QS-FDL framework and the baseline approaches. The proposed model consistently achieved the lowest FPR across both datasets, with 1.4% on WISDM and 0.9% on WESAD. These results highlight the reliability of the QS-FDL framework in minimizing misclassification, particularly in distinguishing between normal physiological or behavioral patterns and stress-related conditions. The combination of MI-1D-CNN and Bi-LSTM architecture allows the model to effectively capture both spatial and temporal characteristics within multimodal IoT signals, leading to more precise stress prediction. In addition, the integration of QKD (BB84 and E91) ensures a secure and stable synchronization process during federated aggregation, reducing communication noise and preventing parameter tampering, which ultimately contributes to lower FPR.

TABLE IV. COMPARATIVE FPR ACROSS DATASETS

Model		WISDM (%)	WESAD (%)
[22]	Federated DNN	N/A	13.2
[23]	B-CNNs	2.1	N/A
Proposed model	MI-1D-CNN + Bi-LSTM	1.4	0.9

The method in [22] reported a substantially higher FPR of 13.2%, mainly due to the absence of temporal feature extraction and restricted generalization capabilities when handling complex physiological stress signals. The method in [23] achieved an FPR of 2.1%. Although this method improved activity recognition performance, it did not incorporate quantum-secured synchronization mechanisms or temporal sequence modeling, leading to residual misclassifications. Overall, the proposed QS-FDL framework demonstrates superior robustness and precision, making it better suited for secure, large-scale, and privacy-preserving stress prediction in smartwatch and smartphone IoT environments. The low FPR of the proposed QS-FDL framework demonstrates its enhanced ability to preserve discriminative features and suppress false alarms across different modalities of smartwatch-smartphone sensor data. This improvement is primarily driven by the federated optimization process, which improves the decision boundaries of the classifier and ensures consistent convergence under secure communication. The observed reduction in FPR confirms the model's reliability for real-world health and stress monitoring applications, where minimizing false alerts is essential to maintain user trust and clinical applicability.

Table V presents the computational cost reduction achieved compared to the baseline methods. The results show that the MI-1D-CNN and Bi-LSTM hybrid model integrated with QKD

protocols (BB84 and E91) significantly decreases computational overhead, achieving 39.6% reduction on WISDM and 41.2% on WESAD. This improvement comes from the optimized deep learning architecture and the secure federated aggregation process, which minimize redundant communication and streamline gradient exchanges during training. The use of QKD also enables lightweight and efficient encryption, ensuring strong privacy protection without imposing additional processing delays. The method in [22] achieved only 17.8% cost reduction on the WESAD dataset, highlighting its limited scalability for distributed physiological stress prediction. The method in [23] obtained 27.3% reduction on WISDM-HARB but did not benefit from quantum-secured synchronization or federated optimization. The absence of these components restricted its performance under real-time IoT constraints. The results demonstrate that the proposed QS-FDL framework effectively reduces computational requirements while maintaining high predictive accuracy, making it suitable for low-power and resource-constrained IoT devices such as smartwatches and smartphones.

TABLE V. COMPARATIVE COMPUTATIONAL COST REDUCTION ACROSS DATASETS

Model		WISDM (%)	WESAD (%)
[22]	Federated DNN	N/A	17.8
[23]	B-CNNs	27.3	N/A
Proposed model	MI-1D-CNN + Bi-LSTM	39.6	41.2

Table VI summarizes the feature selection time required by the proposed model and the baseline approaches. The QS-FDL framework achieves the fastest performance, requiring only 1.7 s on WISDM and 1.9 s on WESAD. This efficiency is primarily due to the optimized parallelism provided by the quantum-secured federated environment, which reduces synchronization overhead and eliminates unnecessary update cycles. The combination of MI-1D-CNN and Bi-LSTM architectures further accelerates deep feature extraction by modeling spatial and temporal patterns simultaneously. Compared with existing methods, the QS-FDL model is up to 40% faster than the methods in [22, 23], demonstrating its capability to support real-time federated learning on wearable IoT devices. The method in [22] required 3.2 s on WESAD, while the method in [23] recorded 2.9 s on WISDM-HARB, reflecting slower convergence due to the absence of QKD-assisted synchronization and limited parallel optimization. These findings confirm that the proposed QS-FDL framework not only enhances security and accuracy but also improves computational efficiency, making it highly suitable for continuous stress monitoring and health analytics in smartwatch and smartphone environments.

TABLE VI. COMPARATIVE FEATURE SELECTION TIME ACROSS DATASETS

Model		WISDM (s)	WESAD (s)
[22]	Federated DNN	N/A	3.2
[23]	B-CNNs	2.9	N/A
Proposed model	MI-1D-CNN + Bi-LSTM	1.7	1.9

A. System Overhead and Communication Latency

The end-to-end cost of one federated learning round of the QS-FDL framework was evaluated to address the concerns on computational and communication overhead in resource-constrained environments. As defined earlier, the total round time is given by $T_{\text{round}} = T_{\text{local}} + T_{\text{encrypt}} + T_{\text{transmit}} + T_{\text{aggregate}}$, where each term denotes local computation, encryption and key application, transmission, and aggregation time, respectively. On smartphone-class hardware, local computation for one epoch required approximately 2.3 s, while smartwatch-class devices needed around 4.8 s due to lower processing capabilities. Despite this difference, the constrained model size ($<$1.2 million parameters) and short input sequences kept memory usage within the limits of typical smartwatch hardware. For both cloud-centric and edge-centric configurations, the average encrypted model update size was about 320 kB, resulting in a transmission time of 25–35 ms over a 10 Mbps channel.

The overhead introduced by QKD was also measured. The BB84-based key exchange added an average delay of 4.2 ms per round, whereas the E91-based configuration introduced approximately 5.6 ms due to entanglement synchronization and error-correction steps. Combined with AES-GCM encryption, the overall contribution of T_{encrypt} remained below 5% of T_{round}. In practice, the total round duration was around 320 ms in the cloud-centric scheme and 210 ms in the edge-centric scheme, including local training, secure communication, and aggregation. These results show that the quantum-secured communication layer introduces only modest latency overhead compared to the overall training time and does not prevent real-time or near real-time operation on smartwatch and smartphone IoT devices. In other words, the proposed QS-FDL framework is capable of maintaining strict security guarantees while still satisfying the timing and resource constraints of practical wearable-based stress monitoring scenarios.

Although direct battery-drain measurements were not performed, the reduced local computation time (2.3–4.8 s per epoch) and limited communication payloads (≈320 kB per round) suggest a modest impact on wearable battery usage. Prior studies indicate that operations with similar computational load typically consume less than 3–5% battery per hour under intermittent training, making the QS-FDL framework feasible for practical deployment on resource-constrained smartwatches and smartphones. This implies that the proposed system can be integrated into continuous stress-monitoring applications without imposing excessive energy demands on end-user devices.

B. Iterative Validation of Quantum-Secured Communication Scenarios Based on BB84 and E91 Protocols

This section presents the iterative validation of communication security scenarios in the proposed QS-FDL framework. The experiments were conducted using the WISDM and WESAD datasets across three configurations: a classical encrypted communication channel (baseline), a discrete-state QKD channel (BB84-QKD), and an entanglement-based quantum communication channel (E91-QKD). Figure 2 illustrates the comparative performance across

all configurations in terms of AUROC, Expected Calibration Error (ECE), and overall communication efficiency for both datasets. This aimed to evaluate the impact of QKD on model discriminability, calibration reliability, and transmission performance, analyzing the trade-off between quantum-grade confidentiality and system efficiency within federated IoT environments.

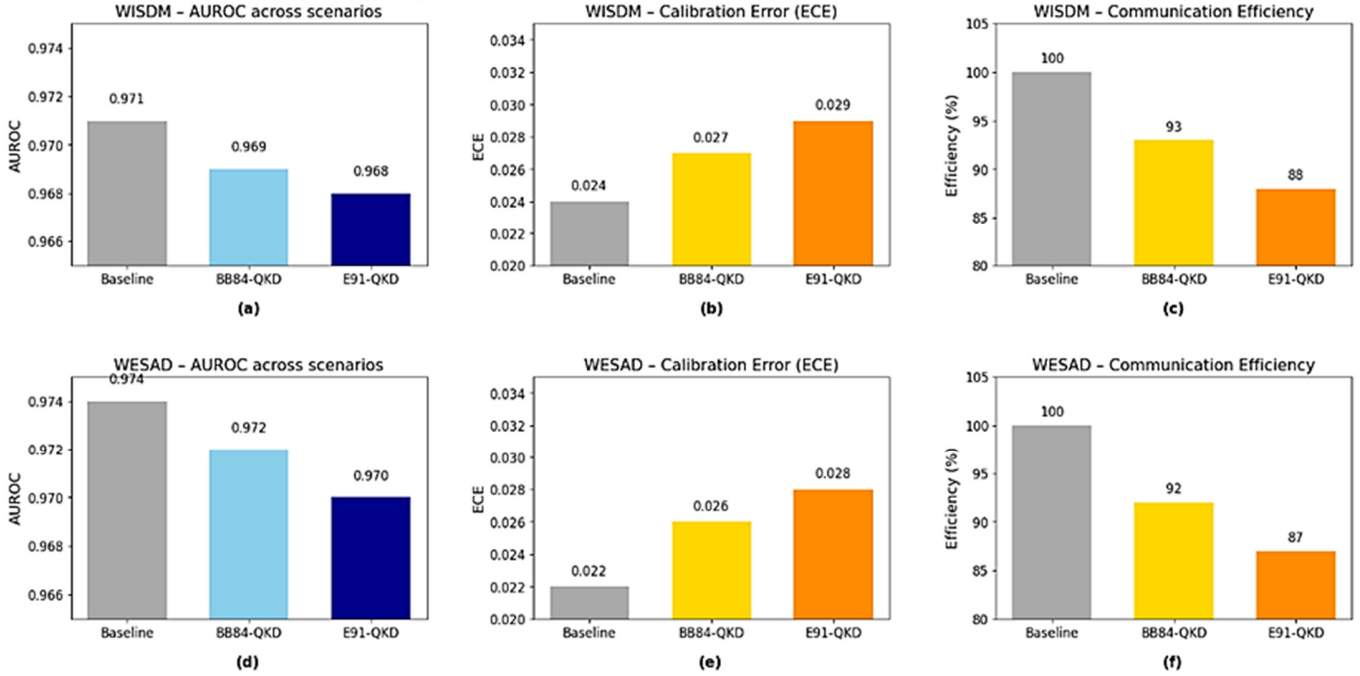

Fig. 2. Comparative evaluation of communication security scenarios (Baseline, BB84-QKD, and E91-QKD) on WISDM and WESAD datasets in terms of: (a, d) AUROC, (b, e) ECE, and (c, f) Communication efficiency.

In the baseline scenario, the QS-FDL framework utilized standard AES-GCM encryption over a classical channel without quantum key negotiation. This configuration provided the highest communication throughput and served as a reference for comparative evaluation. On the WISDM dataset, the model achieved an AUROC of 0.971 with an ECE of 0.024, while on the WESAD dataset, it demonstrated a slightly higher AUROC of 0.974 and an ECE of 0.022. Communication efficiency reached 100% for both datasets, confirming ideal transmission performance without the latency introduced by quantum key exchanges. These results indicate that the federated architecture of MI-1D-CNN and Bi-LSTM maintained optimal predictive accuracy and calibration reliability under classical encryption, establishing a stable reference configuration for subsequent quantum-secured experiments.

When the BB84-QKD protocol was introduced, the communication layer employed quantum key negotiation through photon polarization states to secure the exchange of model updates. This setup effectively mitigated interception and replay risks by ensuring non-cloneable key generation and dynamic key refreshment. On the WISDM dataset, an AUROC of 0.969 and an ECE of 0.027 were achieved, whereas on the WESAD dataset, an AUROC of 0.972 and an ECE of 0.026 were achieved. These values represent only minor deviations from the baseline, signifying that the introduction of QKD did not compromise learning stability or probabilistic reliability. Communication efficiency slightly decreased to approximately 93% due to the QKD handshake and error-correction synchronization stages. The overall QBER remained below 3%, and the probability of key leakage was maintained at $P_{leak} \leq 2^{-128}$. These results confirm that the BB84 configuration provides an effective balance between security enhancement and communication speed, making it highly suitable for lightweight and latency-sensitive IoT applications such as activity recognition and motion-based sensing using smartphone and smartwatch devices.

In the E91-QKD scenario, an entanglement-based communication protocol was employed to ensure information-theoretic confidentiality with correlated photon pairs. This mechanism enhances security against photon number-splitting and intercept-resend attacks by verifying Bell-state correlations during the key generation process. On the WISDM dataset, the model achieved an AUROC value of 0.968 and an ECE of 0.029, while on the WESAD dataset, 0.970 and 0.028, respectively, were recorded. Although these results show a slight reduction relative to the baseline configuration, the decrease remained below 0.5%, indicating that the model preserved stable discriminative capability and calibration consistency. Communication efficiency was reduced to nearly 88%, consistent with the expected latency overhead introduced by entanglement synchronization and key verification. Nevertheless, the E91-QKD configuration provided the highest level of confidentiality, with a leakage probability of $P_{leak} \leq 2^{-256}$ and a QBER of about 3.2%. These results confirm that the E91-QKD protocol delivers stronger information-theoretic

security while maintaining acceptable communication overhead, making it particularly appropriate for privacy-critical applications such as medical and physiological data analysis.

Across all configurations and datasets, the comparative results in Figure 2 demonstrate a consistent trade-off between communication efficiency and quantum-layer security strength. The baseline configuration achieved the highest throughput but was not secure against quantum-capable adversaries. The BB84-QKD setup introduced minimal computational overhead while maintaining calibration stability, confirming its suitability for real-time federated learning environments. The E91-QKD scenario, although characterized by higher latency, provided stronger confidentiality and authentication assurance, offering enhanced protection for high-sensitivity multimodal IoT data. In general, the performance deviation across the quantum-secured configurations remained within 1% in AUROC and below 5% in communication efficiency loss. These findings demonstrate that the integration of QKD protocols within the federated learning framework establishes a balanced and secure communication architecture that effectively preserves data confidentiality, model reliability, and operational efficiency in distributed IoT systems. These findings directly address the need for a detailed analysis of the overhead introduced by quantum communication mechanisms and confirm that QKD-secured federated learning remains practical for next-generation IoT healthcare systems.

VI. CONCLUSIONS AND FUTURE WORKS

This study presented a QS-FDL framework for multimodal health and stress prediction using smartwatch and smartphone IoT data. By combining MI-1D-CNN for multimodal feature extraction, Bi-LSTM for temporal dependency modeling, and federated learning for privacy-preserving collaboration, the proposed framework achieved high predictive performance while avoiding raw data transmission across distributed devices. The novelty of this work lies in the tight integration of QKD-assisted key management (BB84 and E91 protocols) into a cloud-edge-device federated learning architecture, enabling secure model update exchange and aggregation without compromising data confidentiality or model integrity. Unlike existing federated or deep learning approaches that rely solely on classical cryptographic mechanisms, the proposed QS-FDL framework introduces a quantum-secured communication layer that strengthens resilience against both classical and quantum adversaries in distributed healthcare environments.

From a technical perspective, this work makes several key contributions. First, it demonstrates that quantum-secured federated learning can be effectively deployed for real-world multimodal IoT healthcare datasets, achieving classification accuracies of 97.1% on WISDM and 98.4% on WESAD, while reducing feature dimensionality and computational overhead. Second, comprehensive ablation analyses confirm the complementary roles of convolutional, recurrent, and quantum communication components, showing that their joint design is essential for maintaining model accuracy, efficiency, and stability. Third, the framework achieves lower FPR and improved energy efficiency compared to existing approaches, reinforcing its suitability for continuous and privacy-aware health monitoring.

Despite these promising results, several research directions remain open. Future work will focus on personalized federated optimization to capture individual-specific physiological patterns and dynamic stress responses. In addition, hybrid quantum-classical learning strategies will be investigated to further accelerate convergence and scalability in large distributed deployments. To enhance transparency and trust, Explainable Artificial Intelligence (XAI) techniques, such as SHAP and layer-wise relevance propagation, will be incorporated to interpret model decisions and identify dominant physiological features. Finally, the integration of QS-FDL within 5G-enabled and Software-Defined Networking (SDN) infrastructures will be explored to improve latency control, mobility support, and secure orchestration in next-generation IoT healthcare systems.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to Telkom University and Bina Nusantara University (BINUS) for their institutional support, academic environment, and facilities that contributed to the completion of this research. The support provided by both institutions was essential in facilitating the research activities and manuscript preparation. The authors also acknowledge the UC Irvine Machine Learning Repository as the source of the dataset used in this research. The availability of this publicly accessible dataset enabled reproducible experimentation and supported the evaluation of the proposed approach.

REFERENCES

[1] H. Taherdoost, "Wearable Healthcare and Continuous Vital Sign Monitoring with IoT Integration," *Computers, Materials & Continua*, vol. 81, no. 1, pp. 79–104, 2024, https://doi.org/10.32604/cmc.2024.054378.

[2] A. O. Pataca *et al.*, "Use of machine learning for predicting stress episodes based on wearable sensor data: A systematic review," *Computers in Biology and Medicine*, vol. 198, Nov. 2025, Art. no. 111166, https://doi.org/10.1016/j.compbiomed.2025.111166.

[3] A. Jolly, V. Pandey, M. Sahni, E. Leon-Castro, and L. A. Perez-Arellano, "Modern Smart Gadgets and Wearables for Diagnosis and Management of Stress, Wellness, and Anxiety: A Comprehensive Review," *Healthcare*, vol. 13, no. 4, Feb. 2025, Art. no. 411, https://doi.org/10.3390/healthcare13040411.

[4] M. Nirmala, V. L. Kumar, and T. S. C. Reddy, "Wearable Devices: For Stress and Health Monitoring," in *Signal Processing, Telecommunication and Embedded Systems: Automation and Sustainability Applications*, 2025, pp. 299–308, https://doi.org/10.1007/978-981-96-7253-0_25.

[5] J. Alshudukhi, "Blockchain-enabled security for healthcare data communication in IoT-driven 5G networks," *Intelligent Decision Technologies*, vol. 19, no. 6, pp. 4242–4253, Nov. 2025, https://doi.org/10.1177/18724981251372292.

[6] N. K. Al-Shammari, T. H. Syed, and M. B. Syed, "An Edge – IoT Framework and Prototype based on Blockchain for Smart Healthcare Applications," *Engineering, Technology & Applied Science Research*, vol. 11, no. 4, pp. 7326–7331, Aug. 2021, https://doi.org/10.48084/etasr.4245.

[7] Md. Z. Uddin and M. M. Hassan, "Activity Recognition for Cognitive Assistance Using Body Sensors Data and Deep Convolutional Neural Network," *IEEE Sensors Journal*, vol. 19, no. 19, pp. 8413–8419, Oct. 2019, https://doi.org/10.1109/JSEN.2018.2871203.

[8] F. J. Jaime, A. Muñoz, F. Rodríguez-Gómez, and A. Jerez-Calero, "Strengthening Privacy and Data Security in Biomedical Microelectromechanical Systems by IoT Communication Security and

Protection in Smart Healthcare," *Sensors*, vol. 23, no. 21, Nov. 2023, Art. no. 8944, https://doi.org/10.3390/s23218944.

[9] P. Cipresso, J. Fernández Alvarez, G. Riva, and L. Calvillo, "The Role of Emotions, Stress, and Mental State in Inflammatory Processes Perturbing Brain-Heart Dialogue," in *Brain and Heart Dynamics*, Springer, 2020, pp. 1–17.

[10] R. H. Alamir, A. Noor, H. Almukhalfi, R. Almukhlifi, and T. H. Noor, "SecFedDNN: A Secure Federated Deep Learning Framework for Edge–Cloud Environments," *Systems*, vol. 13, no. 6, June 2025, Art. no. 463, https://doi.org/10.3390/systems13060463.

[11] V. A. Patel *et al.*, "Adoption of Federated Learning for Healthcare Informatics: Emerging Applications and Future Directions," *IEEE Access*, vol. 10, pp. 90792–90826, 2022, https://doi.org/10.1109/ACCESS.2022.3201876.

[12] F. A. Aburto Moccia *et al.*, "Complexity and the Transition to Post-Quantum Security: Cryptographic Challenges regarding Shor's and Grover's Algorithms," *Procedia Computer Science*, vol. 265, pp. 674–680, 2025, https://doi.org/10.1016/j.procs.2025.07.238.

[13] R. Malik, A. ur-Rehaman, H. Razzaq, C. Bhatt, K. Kaushik, and I. U. Khan, "Advancing Healthcare IoT: Blockchain and Federated Learning Integration for Enhanced Security and Insights," in *2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE)*, Gautam Buddha Nagar, India, May 2024, pp. 308–314, https://doi.org/10.1109/IC3SE62002.2024.10593078.

[14] S. K. Singh *et al.*, "Advancements in secure quantum communication and robust key distribution techniques for cybersecurity applications," *Cyber Security and Applications*, vol. 3, Dec. 2025, Art. no. 100089, https://doi.org/10.1016/j.csa.2025.100089.

[15] B. Mallick *et al.*, "Multi-Channel Multi-Protocol Quantum Key Distribution System for Secure Image Transmission in Healthcare," *IEEE Access*, vol. 13, pp. 62476–62505, 2025, https://doi.org/10.1109/ACCESS.2025.3558294.

[16] M. K. Saggi, A. S. Bhatia, and S. Kais, "Federated quantum machine learning for drug discovery and healthcare," *Annual Reports in Computational Chemistry*, vol. 20, pp. 269–322, 2024.

[17] D. Ar-Reyouchi, H. Benali, B. Jihane, K. Ghoumid, and E. M. Ar-Reyouchi, "Secure-by-Design IoMT Networks: A Quantum-Blockchain and AI Framework for 6G Healthcare," in *2025 International Conference on Communication, Computing, Networking, and Control in Cyber-Physical Systems (CCNCPS)*, Dubai, United Arab Emirates, June 2025, pp. 244–249, https://doi.org/10.1109/CCNCPS66785.2025.11135745.

[18] G. Weiss, "WISDM Smartphone and Smartwatch Activity and Biometrics Dataset." UCI Machine Learning Repository, 2019, https://doi.org/10.24432/C5HK59.

[19] A. R. Philip Schmidt, "WESAD (Wearable Stress and Affect Detection)." UCI Machine Learning Repository, 2018, https://doi.org/10.24432/C57K5T.

[20] M. Srivarshini and R. Vanithamani, "Secure Healthcare Data Sharing Using Federated Learning, Blockchain, and Quantum Cryptography," in *Advancing Cyber Threat Detection Through Quantum and Edge Computing*, IGI Global Scientific Publishing, 2026, pp. 127–162.

[21] A. Atutxa, A. Sanz, E. Salegi, M. Huarte, J. Astorga, and E. Jacob, "Authentication of the QKD classical channel through Post-Quantum Cryptography in a multi-site 5G/6G quantum-safe communication network," in *2025 International Conference on Quantum Communications, Networking, and Computing (QCNC)*, Nara, Japan, Mar. 2025, pp. 648–654, https://doi.org/10.1109/QCNC64685.2025.00108.

[22] A. Almadhor *et al.*, "Wrist-Based Electrodermal Activity Monitoring for Stress Detection Using Federated Learning," *Sensors*, vol. 23, no. 8, Apr. 2023, Art. no. 3984, https://doi.org/10.3390/s23083984.

[23] N. Hnoohom, N. Maitrichit, S. Mekruksavanich, and A. Jitpattanakul, "Hierarchical Human Activity Recognition Based on Smartwatch Sensors Using Branch Convolutional Neural Networks," in *Multi-disciplinary Trends in Artificial Intelligence*, 2022, pp. 52–60, https://doi.org/10.1007/978-3-031-20992-5_5.