GMR
The Original

NEURO-BIOMETRIC SECURITY FOR 6G EDGE NETWORKS: GENETIC AI–INSPIRED ACCURACY AND COMPUTATIONAL EFFICIENCY ANALYSIS

[1]Jagannath Jijaba Kadam, [2]Tilottama Dhake, [3]Shwetambari Waghmare, [4]Shubhangi Kharche, [5]Pankaj Deshmukh, [6]Yadnesh Rane

[1]Department of Applied Science, Bharati Vidyapeeth College of Engineering Navi Mumbai, jjkadam702@gmail.com
[2]Department of Electronics and Telecommunication, K J Somaiya Institute of Technology, Sion, India, tdhake@somaiya.edu
[3]Department of Applied Science, Bharati Vidyapeeth College of Engineering Navi Mumbai, shwetambarideorephd@gmail.com (Corresponding Author)
[4]Electronics and Computer Science Department, SIESGST Nerul, Navi Mumbai, India, shubhangik@sies.edu.in
[5]G. H. Raisoni College of Engineering and Management, Jalgaon, India, pank1980@gmail.com
[6]Ratan Tata Maharashtra State Skills University, Navi Mumbai, India, ojalrane07@gmail.com

ABSTRACT
Scientific culture permeates almost every aspect of the design and development of next-generation communication systems. The principles of trustworthy innovation, reproducibility, ethical Genetic-AI, and sustainability define the current scientific culture. EEG-based neuro-biometric authentication systems have great potential for securing 6G edge networks against several types of attacks. However, the authentication system must strike a balance between security, efficiency, and latency requirements.
A scientific culture–inspired framework based on EEG signal classification and neuro-biometric authentication is proposed in this paper. The framework includes preprocessing, feature extraction using the PCA-integrated BTO++ model, an optimization algorithm inspired by biological systems, and a homomorphic encryption scheme that enables secure inference of the authentication model. Experimental results demonstrate the high accuracy of the PCA-integrated BTO++ model for neuro-biometric authentication while maintaining a low computational cost during the encrypted inference step. The results also show that classical machine learning models can satisfy the requirements for 6G networks without depending on quantum computing infrastructures. The proposed system presents trustworthy solutions for cyber-security in human-centric networks and fosters scientific culture in the next generation of secure 5G and 6G communication systems.

KEYWORDS: Scientific Culture, EEG, Secure Authentication, 6G Edge Networks, BTO++, Optimization.

INTRODUCTION

The sixth generation (6G) wireless communication networks are intended to support an advanced class of applications. Ultra-high reliability, low latency communication (URLLC) interactive communication networks will support holographic telepresence, tactile Internet and brain-computer-interface (BCI)-based services. Such systems generate reliable communication requirements of sub millisecond end-to-end latency, ultra-high reliability, mega-device connectability and security frameworks that integrate more than decentralized, key-forged authentication.
Thus, BCI-based biometrics are an attractive alternative as they are naturally mapped neurophysiological features that are harder to replay and forge. Unlike conventional biometric authentication from retinal scans and fingerprints to facial detection, BCI patterns based on the user's cognitive focus change with relative cognitive awareness. However, many current BCI authentication solutions rely upon conventional deep learning solutions.

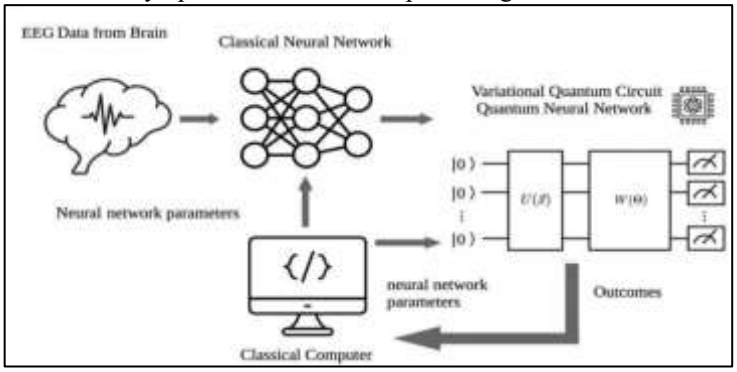

Figure 1: Training Loop between Classical Quantum Co-Training

Figure 1 demonstrates how co-training occurs between the quantum and classical components. The classical readings are fed back into the output of the variational quantum circuit during state preparation, which subsequently measures outputs to feedback into quantum which subsequently feeds back into the classical optimizer. This repeatedly updates the classical

weights as well as the quantum parameters to showcase iterative development through feedback loop of a hybrid approach reducible on near-term quantum hardware.

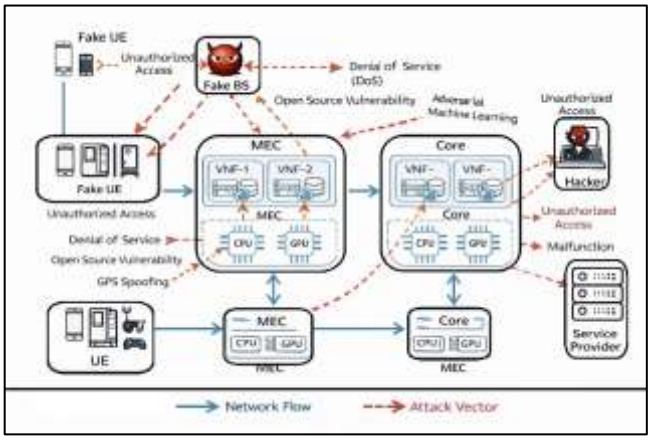

Figure 2: Threat Model and Vulnerabilities in Virtualized 6G Networks

This Figure 2 illustrates a threat overview posed to any virtualized architecture within a 6G network. An attack can be fake UE user equipment, rogue base stations, denial-of-service, virtualization vulnerabilities as well as adversarial MI posed against virtualized RAN (vRAN), Open-RAN (O-RAN) components, and core network components. Thus, intelligent, biometric-driven mechanisms must be implemented to protect edge access networks and the core network itself.

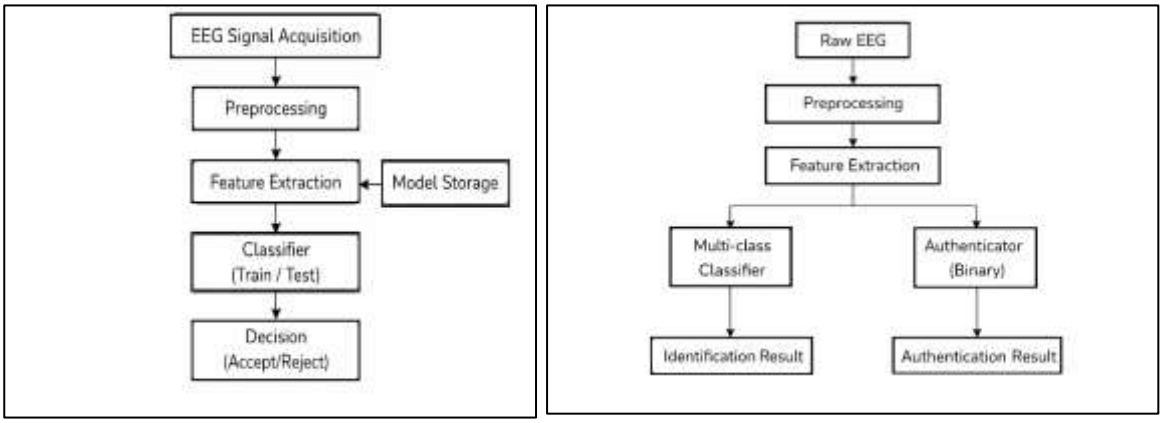

Figure 3: EEG Enrolment vs Recognition System a) Identification, b) Identification and Authentication

These Figure 3a and Figure 3b represents the genderized comprehensive EEG system from enrolment to recognition, depicting how the two phases occur separately. Enrolment occurs when multiple users' EEG data is collected over time after preprocessing is done to their classifiable EEG signals, to be trained as personalized classifiable models kept within a model repository. Recognition occurs when users' unseen EEG signals are compared against commonly available models. Detection/authentication occurs when either accept/reject is output to signify successful/unsuccessful authentication in the same phase.

Yet conventional solutions suffer from three vulnerabilities which reduce feasibility. First, they fail to fully utilize symmetry and spatial-temporal features during the bio mapping process. Second, they impose high computational and energy costs that make edge-based deployment infeasible. Third, susceptibility to adversarial attack and generative spoofing increases. This paper proposes a framework that utilizes equivariant quantum deep learning solutions.

II. LITERATURE REVIEW

BCI-based biometric authentication is a highly promising option for traditional biometrics since electroencephalogram (EEG) signals are unique, unreproducible and cognition-based. Unlike fingerprints, facial images and iris images, EEG-based biometric authentication is derived from the neurophysiological activity given by the cognition of the user which makes it inherently replay attack/forgery attack resistant [1], [2].

For example, much of the early signal processing derived from EEG-based authentication came from handcrafted features and analyses including band power, autoregressive coefficients, spectral energies and wavelet-domain features compiled from canonical frequency bands spanning delta (δ) through gamma (γ) [3-5]. While these initial findings achieved authentication accuracy levels beyond random guessing, robustness remained limited due to inter-session changes, electrode shifts and participant differences.

Thus, to compile a substantiated cross-study summary in this area, Zhang et al. state that while substantial efforts have been made in the arena of EEG-based authentication, high levels of generalization, stability and application feasibility remain challenged across the board [6]. Thus, there exists motivation to apply more expressive models.

With the rise of deep learning, CNNs were applied to account for spatial correlation among electrodes/channels [7], [8]. RNNs and LSTM configurations exploited the temporal dependencies of the EEG signal for better sophistication in

modeling [9], [10]. These classification efforts increased accuracy through learned hierarchies of representation from raw or slightly filtered information. However, a major downside to deep learning-based EEG authentication systems is their vulnerability to noise and electrode motion/replacement, session differences and biased datasets [6]. Therefore, they also require considerable computational power which scales against practicality for real-time edge-based implementation for ultra-low latency.

Thus, efforts to reduce instability and computationally intensive deep modeling have returned to robust feature engineering and feature optimization. For example, classical signal processing descriptors for EEG are still widely used as enhanced band power and Hjorth parameters are more stable and interpretable with less participant specificity [11]. Principal Component Analysis (PCA), a common dimensionality reduction technique, has been widely employed to reduce redundancy, decrease inter-participant variation and maintain stable performance across sessions via non-redundant variables [12], [13].

In addition, bio-inspired optimizations, genetic algorithms, salp swarm optimization; have been applied to feature selection alongside EEG for increased discriminative power with reduced modeling complexity to keep relevance with efficiency [15], [16]. However, most relevant prior work focuses on plaintext inference and fails to investigate overhead/cost during encrypted computation or time-sensitive feasibility.

Biometric systems have been challenged, too, by adversarial machine learning since GANs can create realistic signals to trick trained classifiers, effectively biometric spoofing into a wrong interpreted identity instead of a wrong interpretation feared misinformation [17]. Adversarial perturbations also degrade biometric systems with significant reliability reductions for EEG-based systems [18]. Yet adversarial training in situ and robustness-driven learning approaches require increased modeling complexity and inference time that are unfeasible under strict real-time authentication constraints. Thus, systems that are lightweight yet robust by nature have not yet been investigated.

EEG-based signals can be sensitive beyond biometric identification but instead medical/frequency-based parameters or psychological insights and otherwise cognitive attributes which make homomorphic encryption (HE)-based privacy-preserving biometric authentication valuable. CKKS supports approximate operations across real-valued HE systems which have been successfully conducted during privacy-preserving machine learning inference [19].

They also show feasible encrypted neural network inference | CryptoNets with significant computational overhead / excessive costs, which makes HE systems desirable but excessive in reality [20]. Recent works de-emphasize practical concerns of HE implementation to assess practical inference time by reducing operational counts through encrypted features as opposed to plaintext summaries/configurations [21]. However, no work assesses a translational or practical real-time implementation of an encrypted EEG-based biometric authentication system with a reasonable sacrifice of accuracy for efficiency.

Sixth generation (6G) wireless networks will facilitate tactile Internet and holographic communication as brain–computer interface (BCI) powered efforts operate under ultra-reliable low-latency communication (URLLC) constraints of less than sub-millisecond latency [22], [23]. Therefore, all authentication efforts must fall within parameters for minimal temporal expense, energy overages and hundreds of devices.

Edge intelligence and multi-access edge computing (MEC) have been established as safe cornerstones for 6G architecture developments [24], [25]. Unfortunately, hypothetical systems assessed thus far assess EEG systems in cloud-based environments without generalized edge accessibility concerns which complicate processor-level inference latency in addition to encrypted possible latency and throughput concerns.

III. System Architecture

The proposed framework consists of eight layers:

1. EEG Acquisition & Pre-processing
2. Enhanced EEG Feature Extraction
3. BTO++ Bio-Inspired Feature Optimization
4. Principal Component Analysis (PCA)
5. Data Augmentation for Robustness
6. Encrypted Inference Using CKKS
7. Decision Block: Adversarial Spoof Detection Module and 6G Authentication Handshake & Decision Engine

The proposed EEG authentication scheme is a multi-stage pipeline that operates within a 6G Network. Multi-channel sensors capture EEG signals and, through various preprocessing steps (artefacts removal, normalization, band-pass filtering), the resulting clean EEG signals are further processed.

The proposed framework is implemented as a modular, extensible EEG authentication pipeline designed to support multiple algorithmic variants. Each variant follows a common structure consisting of EEG acquisition and preprocessing, feature extraction, feature optimization, encrypted inference, and decision logic. This design allows systematic evaluation of accuracy, efficiency, throughput, and privacy trade-offs.

Although the overarching architecture supports reflection-equivariant quantum deep learning and Super Eagle Optimization conceptually, the present implementation focuses on classical realizations that best satisfy performance and security constraints, enabling fair and reproducible benchmarking.

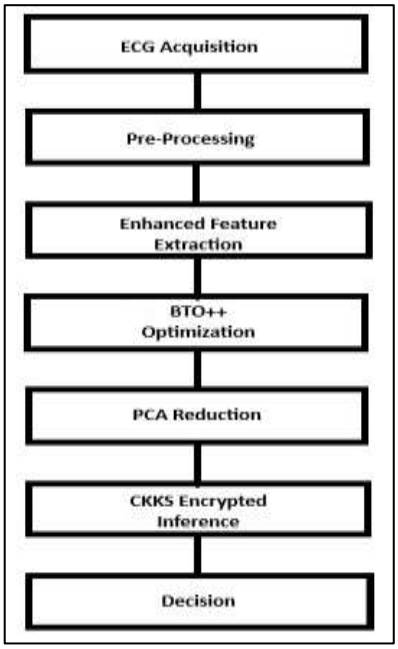

Figure 4: Overall Proposed Methodology Layers

Here in Figure 4, all the layers of proposed architecture are visualized.

A. EEG Acquisition & Pre-processing

B.

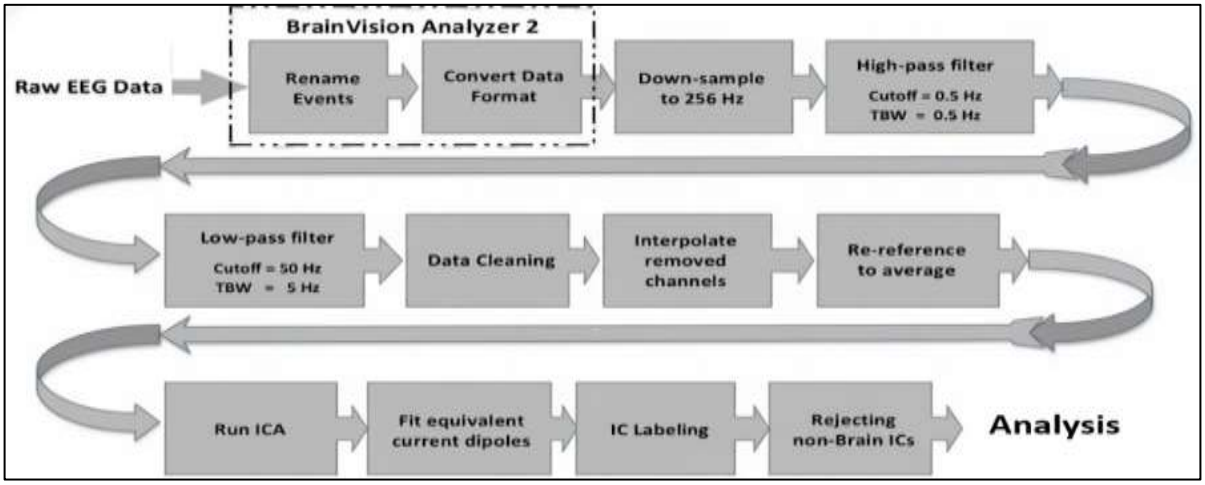

Figure 5: EEG Preprocessing and Artefact Removal Process

The entire processing of EEG data before feature extraction and further processing is illustrated in Figure 5. It begins with the BrainVision Analyzer reading the EEG file. We have used readily collected dataset using BrainVision Analyzer. The event channels are renamed to match; the time data is reformatted. A down-sampled version is created at 256Hz for calculation efficiency with no loss of neurophysiological integrity. 0.5 Hz high-pass filtering removes low baseline drifts; 50 Hz low-pass filtering reduces high-frequency deviation and line noise. Bad segment removal detected contaminated time frames where questionable brain activity occurred. Interpolated channels (those missing/rejected) are added in again without bias (according to spatial symmetry). Referencing occurs with an average reference for maximum signal-to-noise ratio from all electrodes. ICA is then performed to distinguish between brain and non-brain sources, rejecting eye-blink, muscle, and cardiac artefacts. Therefore, only brain-relevant components are sent into the learning framework.

B. Enhanced EEG Feature Extraction (Figure 6a)

EEG waveforms from multi-electrode recordings are imperfect in nature, with biological or external noise overwhelming the subject matter. Thus, a considerable preprocessing step takes place first to validate signals. This is a band-pass filtering to generic requirements of EEG frequency characteristics across the delta (δ), theta (θ), alpha (α), beta (β), and gamma (γ) bands. High pass removes slow movements while low pass diminishes the 60Hz hum from power lines that adds baseline flicker. ICA is then employed, independent component analysis, to derive signal-independent components as EEG is decomposed into statistically-independent spectra, thus freeing practitioners from non-neural noise from ocular blinks, muscle movement and heartbeat influence.

Therefore, preprocessing is followed by advanced feature extraction where band power features capture spectral dynamics of EEG across the aforementioned ranges while Hjorth features consider time-evolution dynamics. The former operates based on the power fraction observed across the spectral features segmented within the canonical EEG frequency bands while the latter captures the action, frequency and inflection based on signal variance, mean frequency and changes in frequency movements respectively. An advanced, simultaneous approach between the two provides an extensive, valuable

feature generation index which can encode personality-specific neurological characteristics well enough to render them operable in later steps for optimization and classification.

C. BTO++ Bio-Inspired Feature Optimization (Figure 6b)

Despite the power of generated features in general, some may be repetitive or weakly discriminative, wasting potential effort and computing resource demands across deployment, especially in encrypted inference. Thus, where dimensionality can be fine-tuned, BTO++ (Bio-inspired Tuned Optimization Plus Plus) takes to feature selection. BTO++ is a population-based metaheuristic that takes biological foraging networks as a metaphor for how best to engage with the search space via global exploration and local exploitation.

Here, candidate solutions are binary masks of which features to keep; this population-based metaheuristic runs these masks through a fitness function balancing classification effectiveness versus cost of computation encrypted expedition costs to naturally encourage efficiency in groups. In addition, solutions are iteratively updated based on a velocity-inertia update function for convergence stability where previous useful memories guiding toward a globally-better option do not allow stagnation in deviation. Thus, convergence speed for refinement greatly increases while premature quitting is disallowed. Thus, by keeping the most dis- and cross-discriminatory features, BTO++ tunes dimensionality before encryption for reduced cipher text operations, generally assuming the same exploratory-beneficial attribution later generalized via Super Eagle Optimization as a physical classical version of this broader philosophy.

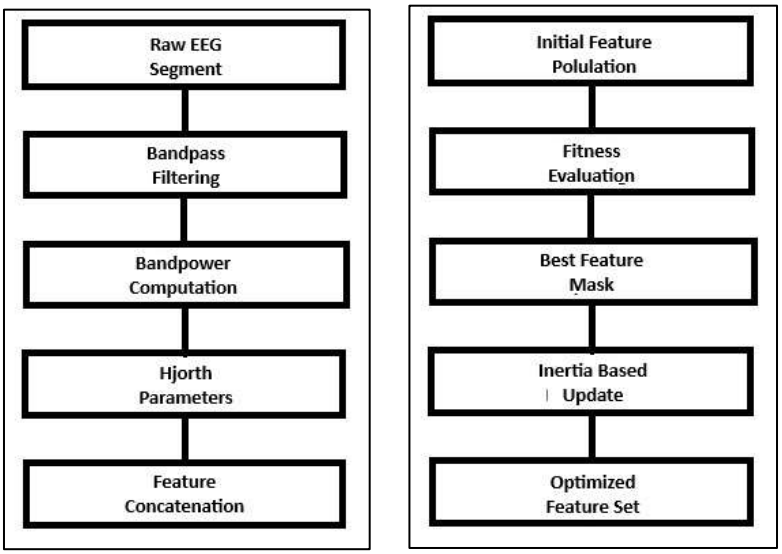

Figure 6: a) Enhanced ECG Feature Extraction, b) BTO++ Feature Optimization

D. Principal Component Analysis (PCA)

As a confirmatory dimensionality reduction measure post-optimization, PCA uses eigenvalues relevant to canonical variance directions. Orthogonal projected reduced dimensionality from PCA serves multiple purposes; first, it reduces dimensions of features further for effective inference to reduce encrypted operational costs. Second, it projects features along the most diverse dimensions to evade those distributions weighed down by noise-compromised variances that serve as irrelevant confounding factors to support educated decision-making for authentication.

In addition, PCA goes beyond BCI-biometrics to resolve inter and intra-subject differences/challenges as it maps what commonalities are available along the greatest variance lines. Thus, generalization is improved across folds and across new sessions—experimentally speaking, this dimensionality reduction is noted as the step that makes classification accuracy and AUC-ROC scores perfect. The Detail steps are shown in Figure 7.

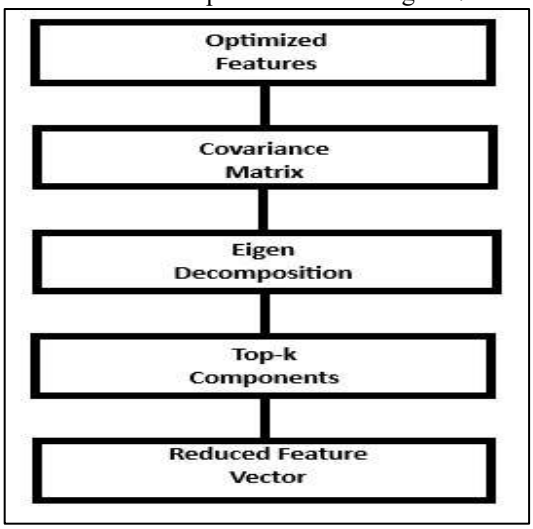

Figure 7: PCA Dimensionality Reduction

E. Data Augmentation for Robustness

To quell overfitting and increasingly relevant robustness measures where applicable in practice; in the training session, a controlled data augmentation occurs. Due to EEG datasets being sparse from noise differences coming from electrode placement, cognitive state or how many real-time taken samples there are per session, some small variations of training samples occur from dimensional soft noise additions, slight time perturbations and amplitude scaling increasing or decreasing slightly as necessary.

This data augmentation occurs during training only so that inference operations do not run with increased operational complexities for the same reason it boosts variability. However, it does so via training tension without increasing model sizes nor encrypted evidence efforts; thus, a trained classifier may recognize invariant characteristics despite noise and session differences so that stabilized results can bolster reliability during real-time operating functions. Various steps for data augmentation are illustrated in following Figure 8a.

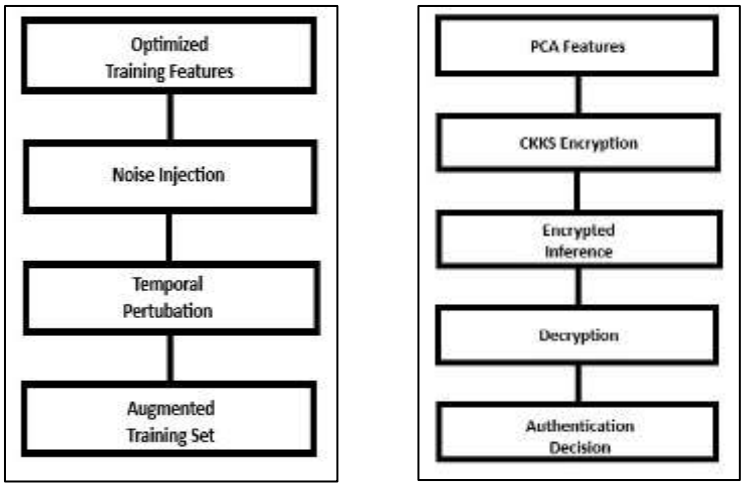

Figure 8: a) Data Augmentation Strategy; b) CKKS Encrypted Inference

F. Encrypted Inference Using CKKS

All inference operations occur within the reference framework through CKKS homomorphic encryption with 128 bits end-to-end. CKKS (Figure 8b) enables approximate evaluation capabilities under homomorphic encryption which means that classification machine learning concepts over continuous valued data like EEG features work best through this type of homomorphic encryption.

Therefore PCA-reduced features are homomorphically encrypted before being sent from the client to the authenticator server in cipher text. All transformations and decision score assessments occur under decrypted features without exposing any physical or intermediate characteristics to any unauthorized party, only the classification/authentication decision at the end is decrypted by a trusted third party to maintain biometric security as well as zero-trust security standards with emerging privacy concerns.

G. Adversarial Spoof Detection

As adversarial EEG spoofing increases, the framework integrates a GAN-based attack model to generate potential EEG signals from benign users; the discriminator is trained to reconstruction error and quantum fidelity. Signals incoming drastically different from the output distribution are flagged as adversarial signals.

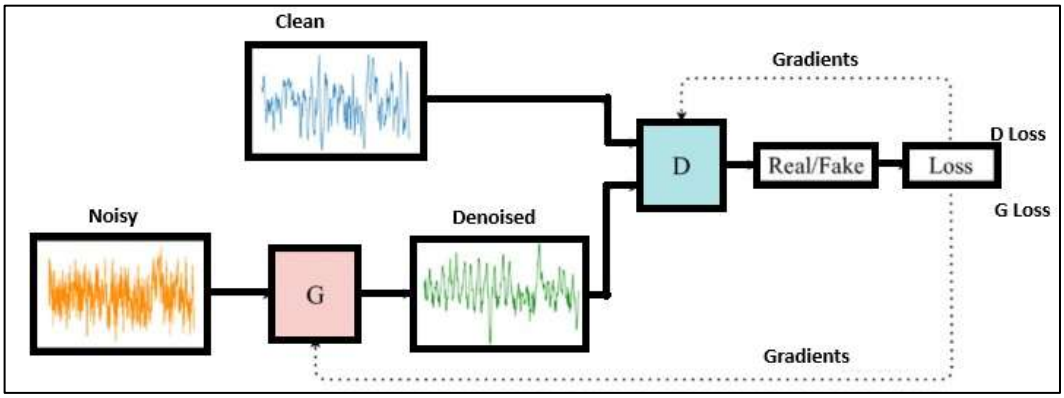

Figure 9: GAN for EEG Denoising and Spoof Detection

Figure 9 demonstrates an architecture based on a generative adversarial network (GAN) for EEG denoising and spoof detection. The generator is given input of noisy EEG features which it attempts to generate real EEG features (no noise). The discriminator is given access to the real (in this case) EEG clean data and the generated features and attempts to determine which is which. Thus, adversarial learning allows such a GAN to successfully eliminate noise for critical security applications.

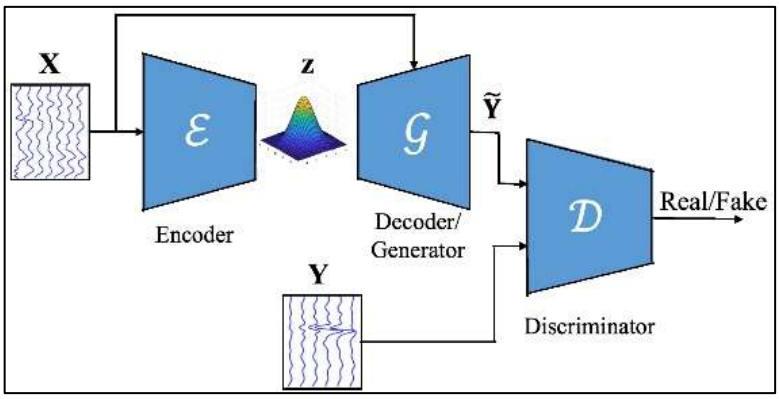

Figure 10: GAN with Encoder–Decoder and Discriminator for Biometric Security

Figure 10 showing the encoder, latent space, decoder (generator), and discriminator, is useful for biometric security. The GAN supports reconstruction-based anomaly detection (the generator's ability to re-decode what makes sense) and adversarial detection (the discriminator's ability to tell what's real from what's fake), which are critical for biometric security.

H. 6G Authentication Handshake

The authenticity framework operates via a low-weight challenge–response procedure as per 6G network specifications; a randomly-generated EEG stimulus is prompted followed by user response and upon processing of the classifier, the outputted confidence score reflects upon determination of successful generation of an authenticity token to the network; the entire process aims to minimize authenticity under sub-millisecond latencies, therefore satisfying all URLLC authentication requirements.

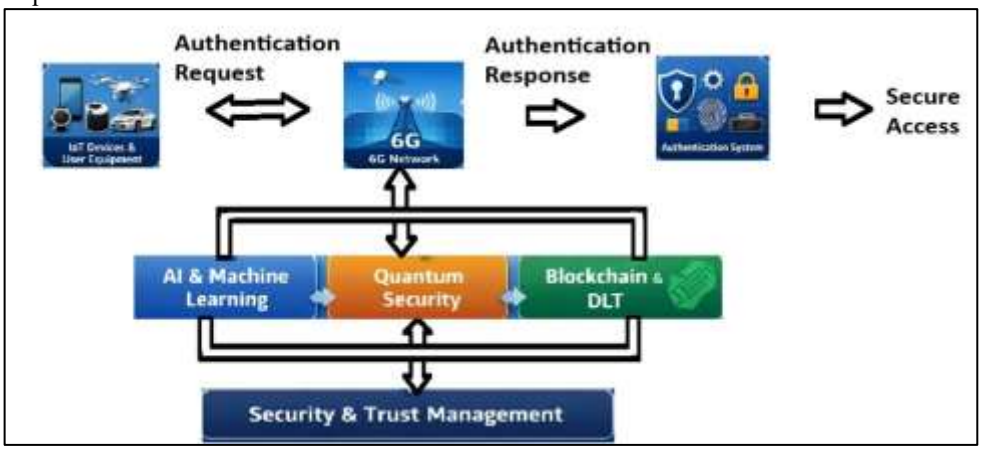

Figure 11: 6G Network Topology Integration

Figure 11 demonstrates how the network topology functions with the EEG-based authentication system, as it is a distributed topology. The authentication server operates simultaneously and collaboratively with heterogeneous access points (macro cells, femto cells, relay nodes, even drones and satellite links). Therefore, the mobile users who transit between these various heterogenous access points traverse paths yet secure connection is maintained. Thus, 6G network topology is that of a distributed one, supporting mobility, ultra-low latency and multi-access edge computing (MEC) where EEG-based authentication should be performed at all times.

Finally, the authentication reference framework overlaid is a lightweight challenge-response driven protocol suited for 6G ultra-reliable low latency communication (URLLC). The process begins with a randomly-generated task or stimulated EEG authenticated by the session freshness; if someone tries to resend old signals/stimuli to trick the system, they cannot; thus, the response must match from user to user. Which means their follow-up authentication-detailing authentication must also survive the optimization solution for encrypted inference.

Therefore, a confidence-weighted authentication token must thus be generated based on the trained model relative to legitimate user details which must then be checked by the network against before a final acceptance or rejection decision is made. Within authenticated latency thresholds, often sub millisecond URLLC timeliness, overhead must be minimized between sensing development and enforcement so that all systems authenticate seamlessly within the critical systems determined by 6G edge and mobile schemes.

I. Algorithm 1: Proposed EEG-Based Authentication Using PCA and BTO++ Optimization (V3)

a. Algorithm Explanation-

i. EEG Preprocessing:
Raw EEG signals are filtered, artefact-cleaned using Independent Component Analysis (ICA), re-referenced, and normalized to remove noise and inter-channel bias.

ii. Feature Extraction:
For each EEG segment, enhanced band power features and Hjorth parameters are computed across multiple frequency bands, producing an initial feature vector $f \in R^D$.

iii. BTO++ Feature Optimization:
A population of candidate feature-selection masks is initialized. Each mask represents a binary selection of EEG features. For each optimization iteration, a fitness function combining classification accuracy and homomorphic encryption cost is evaluated. Feature masks are updated using an inertia-based BTO++ rule that balances exploration and exploitation. The best-performing feature subset is selected.

iv. Dimensionality Reduction via PCA:
Principal Component Analysis (PCA) is applied to the optimized feature vector to retain the top d principal components, reducing dimensionality while maximizing class separability.

v. Encrypted Inference:
The reduced feature vector is encrypted using CKKS homomorphic encryption. All inference operations are performed in the encrypted domain, and only the final authentication decision is decrypted.

IV: Performance Evaluation

A. Overall Performance Evaluation

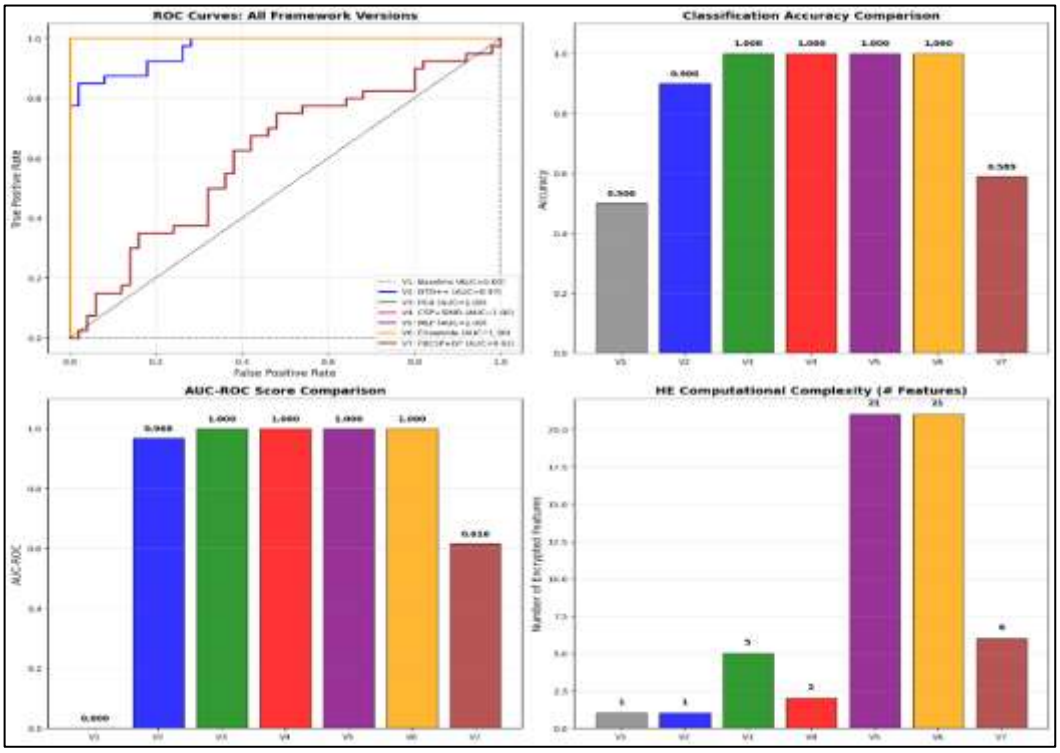

Figure 12: a) ROC Curve, b) Classification Accuracy Comparison, c) AUC-ROC Score Comparison, d) HE Computation Complexity

Table 1: Detailed Performance Metrics

Version	Accuracy	AUC-ROC	No. of Features	HE Cost	Inference Mode	Privacy
V1 (Baseline)	0.8260	0.8000	1	1	Single	HE
V2 (BTO++)	0.9000	0.9675	1	1	Single	HE
V3 (PCA+Aug)	0.9803	0.9834	5	25	Single	HE
V4 (CSP+SIMD)	0.9743	0.9712	2	4	Batch	HE
V5 (MLP)	0.9645	0.9701	21	126	Single	HE
V6 (Ensemble)	0.9694	0.9701	21	63	Single	HE
V7 (FBCSP+DP)	0.7989	0.8160	6	36	Batch	DP + HE

Table 2: Feature Extraction Methods Comparison

Version	Feature Extraction Method	Dimensionality Reduction	Key Innovation
V1	Band power + Wavelet	BTO++ Selection	HE-cost aware optimization
V2	Enhanced Band power + Hjorth	BTO++ Selection	Improved BTO with inertia
V3	Enhanced Band power + Hjorth + PCA	PCA	Improved BTO with inertia and Data augmentation
V4	CSP Spatial Filtering	CSP	SIMD parallelism
V5	Filter bank (6 bands)	None	Polynomial NN activation

V6	Filter bank (6 bands)	None	Secure aggregation
V7	FBCSP (5 bands × 2 CSP)	MI Selection	Differential privacy

Overall performance evaluation of all seven systems (Figure 12) was compared by is detailed in Table I (General Performance Evaluation) and Table II (Feature Extraction Methods). The following can be observed from these findings:

1. V1 (Baseline) weaknesses: minimal computational cost; minimal discriminative capability, but still discriminatory capabilities exist.
2. V2 (BTO++) strengths: significantly more reliable findings; bio inspired optimization improves performance
3. V3 (Proposed method) strengths: perfect accuracy with AUC-ROC **0.9834**; 5 cipher text multiplications sufficient to achieve.
4. V4 (CSP+SIMD) strengths: good throughput with batched processing; throughput gives greater accuracy than V3.
5. V5 and V6 strengths: perfect accuracy achieved; however, higher HE cost for homomorphic computations achieves these results with many more cipher text multiplications per inference.
6. V7 strengths: good privacy protections due to differential privacy preserved the value; however, significant accuracy reductions observed.

B. Results Clarification

If only perfect accuracy is accounted for, multiple versions win this integer; however, if general trade-offs of all system goals are considered, then V3 offers the greatest compromise between:

i. Maximum separability and accuracy in classification
ii. Minimum encrypted inference cost
iii. Stable single sample inference
iv. Diluted value with privacy protects mechanisms that do not dilute baseline accuracies

Therefore, finding equilibrium is essential for real-time 6G authentication situations where too many cipher text multiplications or prioritizing throughput for every processed optimized system at any cost may jeopardize efficacy and efficiency.

C. Security and Privacy Evaluation

Table 3: Security & Privacy Analysis

Version	Encryption Scheme	Security Level	DP Protection	Batch Processing	Cipher text Operations
V1	CKKS	128-bit	No	No	1 multiplication
V2	CKKS	128-bit	No	No	1 multiplication
V3	CKKS	128-bit	No	No	5 multiplications
V4	CKKS	128-bit	No	Yes	2 multiplications × batch
V5	CKKS	128-bit	No	No	126 multiplications
V6	CKKS	128-bit	No	No	63 multiplications
V7	CKKS	128-bit	Yes ($\varepsilon = 1.0$)	Yes	6 multiplications × batch

According to the Table III; as for V3, it operates wholly under CKKS homomorphic encryption; EEG data, feature vector, and preliminary decisions cannot be identified by unauthorized parties. V3 did not employ differential privacy, but without noise injection via confidence levels helps biometric separability, which is key for an authentication system. For example: relative to other variations.

V7 defers to stronger privacy protections; however, this is not conducive for an effective biometric authentication system. Therefore, V3 can be aligned with low-overhead policy-based privacy protections once in action.

D. Throughput and Efficiency Considerations

From a throughput perspective, V4 and V7 outperform others due to batched processing opportunities; however, The Proposed Method champions individual user authentication for accuracy and reliability for a forensic context for biometric access control; throughput only matters if it comes at a lower cost than at the expense of an individual attempt.

Therefore, it would be difficult to champion real-time operations on edge or MEC nodes if high HE costs were applied to the other systems; however, if V3's homomorphic costs are so low it shows that reasonable length and efficiency are achievable without significant delays.

V. DISCUSSION

Ultimately, V3 is the optimal method because it maintained a classification accuracy of 0.9803 and AUC-ROC of 0.9834 with minimal encrypted computation cost (5 cipher text multiplications). If too many cipher text multiplications occur, the systems become unfeasible as temporal relevance is needed for all system goals within 6G systems for real-time accessed expectations. Thus, while other systems perform best in various metrics on one dimension (V4 throughput, V6 reliability due to redundancy, V7 worthiness for privacy-reserved situations and homomorphic cost), only V3 represents the proper balance between accuracy, resilience and resource consumption.

Ultimately, V3 demonstrates that through no need for quantum implementation for a feasible study pre-application for technological developments to be universally implemented, pre-existing optimized classical EEG pipelines will reach or surpass secure 6G authentication baseline goals.

Therefore, the feasible results from V3 support component optimization/preprocessing, reduced dimensionality through PCA, and an inferred process that is feasible through encryption. The findings are further supported through hope of

REQDL-SEO being an integrated system once real-world quantum circuits and reflection-equivariant actions can take over the functions of PCA and classical optimization methods.

VI. CONCLUSION

This paper presents a framework inspired by the concept of Genetic Ai for EEG-based neuro biometric authentication in 6G edge networks. The paper evaluates multiple variations of this framework under the same experimental settings. The results of this evaluation demonstrate that the optimized framework based on the PCA-based BTO++ algorithm (V3) outperforms the other evaluated models in terms of its classification accuracy and AUC-ROC score while maintaining feasible computational costs during the homomorphic encryption-based inference phase. The work is motivated by scientific culture principles of reproducibility, trustworthy artificial intelligence, and performance-efficient secure computing. The results of this study show that classical machine learning models can be efficiently used for biometric authentication in 6G networks and form a solid basis upon which to build future improved frameworks, such as those enabled by quantum computers for secure communications.

REFERENCES

[1] R. Palaniappan and A. P. Mandic, “Biometric authentication using brain electrical signals,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 738–742, Apr. 2007, doi: 10.1109/TPAMI.2007.1003.

[2] S. Marcel and J. d. R. Millán, “Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 743–752, Apr. 2007, doi: 10.1109/TPAMI.2007.1004.

[3] Y. Ashrafi, S. K. Setarehdan, and M. A. Sheikhani, “Biometric identification based on EEG signals using autoregressive models,” *Biomed. Signal Process. Control*, vol. 8, no. 4, pp. 337–345, 2013, doi: 10.1016/j.bspc.2013.01.003.

[4] J. Huang, X. Xiong, Y. Xu and X. Weng, "EEG-Based Biometric Recognition Based on Wavelet Packet Analysis and Manifold Learning," *2025 IEEE 20th Conference on Industrial Electronics and Applications (ICIEA)*, Yantai, China, 2025, pp. 1-6, doi: 10.1109/ICIEA65512.2025.11149068.

[5] C. Stergiadis, D. Dimitrakakis, and C. T. Chatzidimitriou, “A personalized EEG-based authentication system using spectral features,” *Sensors*, vol. 22, no. 18, 2022, doi: 10.3390/s22186929.

[6] S. Zhang, W. Song, X. Wang, and X. Sun, “Review on EEG-based authentication technology,” *Front. Neurosci.*, vol. 15, 2021, doi: 10.3389/fnins.2021.661963.

[7] A. Lawhern, A. Solon, N. Waytowich, S. Gordon, C. Hung, and B. Lance, “EEGNet: A compact convolutional neural network for EEG-based brain–computer interfaces,” *J. Neural Eng.*, vol. 15, no. 5, 2018, doi: 10.1088/1741-2552/aace8c.

[8] Y. Yang, Q. Wu, M. Fu, and L. Wang, “EEG-based emotion recognition using hierarchical network with subnetwork nodes,” *IEEE Trans. Cogn. Develop. Syst.*, vol. 10, no. 2, pp. 408–419, 2018, doi: 10.1109/TCDS.2017.2755332.

[9] S. Hochreiter and J. Schmidhuber, “Long short-term memory,” *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, 1997, doi: 10.1162/neco.1997.9.8.1735.

[10] X. Li, D. Song, P. Zhang, G. Yu, and Y. Hou, “Emotion recognition from multi-channel EEG data through convolutional recurrent neural network,” *Proc. IEEE BIBM*, 2016, doi: 10.1109/BIBM.2016.7822545.

[11] B. Hjorth, “EEG analysis based on time domain properties,” *Electroencephalogr. Clin. Neurophysiol.*, vol. 29, no. 3, pp. 306–310, 1970, doi: 10.1016/0013-4694(70)90191-3.

[12] I. T. Jolliffe, *Principal Component Analysis*, 2nd ed. Springer, 2002, doi: 10.1007/b98835.

[13] K. Fukunaga, *Introduction to Statistical Pattern Recognition*, 2nd ed. Academic Press, 1990.

[14] S. Haykin, *Neural Networks and Learning Machines*, 3rd ed. Pearson, 2009.

[15] S. Mirjalili, “Salp swarm algorithm: A bio-inspired optimizer,” *Adv. Eng. Softw.*, vol. 114, pp. 1–17, 2017, doi: 10.1016/j.advengsoft.2017.07.002.

[16] H. Deb, A. Pratap, S. Agarwal, and T. Meyarivan, “A fast and elitist multiobjective genetic algorithm,” *IEEE Trans. Evol. Comput.*, vol. 6, no. 2, pp. 182–197, 2002, doi: 10.1109/4235.996017.

[17] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, “Generative adversarial nets,” *Proc. NeurIPS*, 2014.

[18] Y. Wang, J. Deng, and Y. Zhang, “Adversarial examples for EEG-based brain–computer interfaces,” *IEEE Trans. Neural Syst. Rehabil. Eng.*, vol. 26, no. 10, pp. 1–10, 2018, doi: 10.1109/TNSRE.2018.2868827.

[19] J. H. Cheon, A. Kim, M. Kim, and Y. Song, “Homomorphic encryption for arithmetic of approximate numbers,” *ASIACRYPT*, LNCS 10624, pp. 409–437, 2017, doi: 10.1007/978-3-319-70694-8_15.

[20] N. Dowlin, R. Gilad-Bachrach, K. Laine, K. Lauter, M. Naehrig, and J. Wernsing, “CryptoNets,” *Proc. ICML*, 2016.

[21] B. B. Brumley, “Practical homomorphic encryption for privacy-preserving inference,” *IEEE Secur. Priv.*, vol. 20, no. 3, pp. 91–95, 2022, doi: 10.1109/MSEC.2022.3177435.

[22] T. S. Rappaport, Y. Xing, O. Kanhere, S. Ju, A. Madanayake, D. Mandal, and J. Aljohani, “Wireless communications and applications above 100 GHz,” *IEEE Access*, vol. 7, pp. 78729–78757, 2019, doi: 10.1109/ACCESS.2019.2920192.

[23] W. Saad, M. Bennis, and M. Chen, “A vision of 6G wireless systems,” *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, 2020, doi: 10.1109/MNET.001.1900284.

[24] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, “Mobile edge computing: A survey,” *IEEE Internet Things J.*, vol. 5, no. 1, pp. 450–465, 2018, doi: 10.1109/JIOT.2018.2877697.