Quantum Information and Computation, Vol. 24, No.15&16 (2024) 1261-1282

INTEGRATION OF SECURE QUANTUM COMMUNICATION PROTOCOLS INTO EDGE DEVICE USING QUANTUM-ENHANCED GENERATIVE ADVERSARIAL NETWORKS (QE-GANS)

ABILASH RADHAKRISHNAN*
[1]*Master of Engineering, Maria College of Engineering and Technology*
Attoor, 629177, Tamil Nadu, India,
Email: abilash.res2k21@gmail.com

DANI JERMISHA RAILIS
Master of Engineering, Maria College of Engineering and Technology
Attoor, 629177, Tamil Nadu, India,
Email: danijermisha01@gmail.com

DINESH R S
Master of Business Administration, Department of Operations Management
Vins Christian College of Engineering
Chunkankadai, 629807, Tamil Nadu, India,
Email: dineshradhakrishnan94@gmail.com

DANI JOAN FREADY R
Bachelor of Architecture, Sigma College of Architecture and Planning
Kuzhithurai, 629168, Tamil Nadu, India,
Email: joanfreadyarchitect@gmail.com

SENTHIL KUMAR CHANDRASEKARAN
Independent Researcher, 28/11,
New Agraharam Street, Kosapet, Vellore, 632001, Tamilnadu, India,
Email: csenthil.network@outlook.com

Received May 6, 2024
Revised November 18, 2024

Enhancing data security and privacy in distributed computing environments presents a key challenge in effectively deploying quantum protocols on edge devices with limited resources. The objective of this project is to enhance the security of edge devices by integrating secure quantum communication protocols using Quantum-Enhanced Generative Adversarial Networks (QE-GANs). To provide safe quantum communication integration for QE-GANs on edge devices, researchers can gather the necessary data through the data collection process from edge devices. For data pre-processing in speech recognition applications, Mel-frequency Cepstral Coefficients (MFCCs) are a popular choice. Measurement-Device-Independent Quantum Key Distribution (MDI-QKD) is a cutting-edge method that provides advanced security compared to conventional QKD for secure communication among edge devices. SMLA refers to secure multiparty logic and its utilization, a framework that enables secure communication between multiple parties while ensuring the confidentiality and integrity of the transmitted data. Qubit-masked messages (QMM) and Quantum Coded Modulated Discrete Permutation (QC-MDPC) are two sophisticated quantum communication methods for data encryption. ρ represents the quantum state density matrix; DFR refers to Device-Independent Quantum Secure Randomness Generation Protocol. MATLAB will be utilized to simulate and analyse the performance of QE-GANs) for integrating secure quantum communication protocols into edge devices. The findings show that the peak energy value of 23.7568 represents the dominant frequency component, which plays a key role in significantly influencing the signal. Integrating secure quantum communication protocols with edge devices via QE-GANs could revolutionize data privacy, enhancing real-time encryption, robust authentication, and decentralized trust, paving the way for next-gen secure IoT networks.
.

Keywords: Secure Quantum Communication, Edge Device, Quantum-Enhance, Generative Adversarial Networks (QE-GANs), Quantum Key Distribution (QKD), Quantum Channel Noise Sources.

1. Introduction

The field of quantum communication has witnessed substantial progress over the past decade, offering revolutionary advancements in secure communication protocols based on the principles of quantum mechanics [1-2]. However, integrating quantum communication technologies into practical, resource-constrained environments like edge devices remains a significant challenge. Edge devices, characterized by limited processing power, storage, and communication capabilities, face considerable barriers when implementing quantum protocols that require substantial computational resources and secure data transmission [3-4]. This paper explores the integration of secure quantum communication protocols into edge devices using Quantum-Enhanced Generative Adversarial Networks (QE-GANs), a novel approach combining quantum mechanics with machine learning to enhance the security and efficiency of communication systems [5-6]. The central problem addressed is the difficulty of deploying secure quantum communication protocols on edge devices. Traditional quantum communication methods, such as quantum key distribution (QKD) and quantum secure direct communication (QSDC), are often designed for centralized systems with abundant computational resources and reliable communication channels [7-8]. However, edge devices, which operate in decentralized, resource-constrained environments, require specialized protocols that can balance high security with limited computational capacity [9-10]. This gap in existing literature has hindered the widespread adoption of quantum-secure communication in real-world applications, such as IoT devices, autonomous systems, and edge computing networks [11-12]. The motivation behind this study is driven by the increasing need for secure communication in distributed networks, particularly in applications involving sensitive data transmission, such as healthcare, finance, and national security [13-14]. As edge devices become more pervasive in these industries, the ability to implement quantum-enhanced security directly on these devices becomes crucial. Quantum communication, with its inherent security advantages, offers a promising solution to these challenges. However, without integrating machine learning methods like QE-GANs, the complexity of quantum protocols remains a barrier to practical implementation. By leveraging QE-GANs, this research bridges the gap between quantum communication technologies and

edge computing. This paper demonstrates that QE-GANs can be effectively integrated with quantum communication protocols to enhance their performance on edge devices [15-16]. Outcomes show that QE-GANs can generate high-quality randomness, improve the efficiency of quantum secure communications, and adapt to the dynamic constraints of edge devices. The integration of QE-GANs results in improved data security, scalability, and computational efficiency, making secure quantum communication feasible for practical deployment [17-18]. The primary objectives of the study include designing and implementing a framework that integrates quantum-secure communication protocols into edge devices, developing and optimizing QE-GANs for enhancing quantum security protocols on resource-constrained devices, evaluating the performance of the proposed integration in terms of security, scalability, and computational efficiency, and providing a roadmap for future applications of quantum-enhanced communication in edge and IoT networks [19-20]. By achieving these objectives, the study contributes significantly to the field of quantum communication, making secure quantum protocols accessible and deployable in practical, real-world environments. The following is the order of the remaining sections: Section 2 provided an overview of the literature, Section 3 presented the suggested technique, Section 4 addressed the results, and Section 5 explained the paper's conclusion.

2. Literature Survey

The survey serves as a comprehensive exploration of existing research and developments in edge computing and quantum communication protocols. By synthesizing and analysing relevant literature, this survey aims to identify key challenges, emerging trends, and innovative approaches in integrating secure quantum communication protocols into edge devices. Hasan et al [21] presented the potential of quantum communication technology to revolutionize existing communication systems. The findings indicate that quantum technology can not only enhance performance but also ensure security and reliability in communication systems. Additionally, the research proposes a model for a quantum communication system and discusses the challenges that need to be overcome to fully realize the communication-related potential of quantum technology. Ali et al [22] presented the impact of quantum computing on the future of 6G communication systems, focusing on enhancing security, computing efficiency, and communication reliability. The findings of this study highlight the significant potential of QC as a critical enabler for enhancing security and efficiency in 6G communication systems. Hua et al [23] proposed the hybrid quantum communication scheme using six-qubit entangled states for secure communication in IoT applications. Qiskit Aer simulation investigations demonstrate that the protocols' accuracy is higher than 0.999, indicating the scheme's practicality. Senapati et al [24] suggested the industrial manufacturing sector's potential for quantum communication, specifically in high-security production facilities such as Air and Defense units. The findings suggest that Quantum communication can significantly enhance the security measures in industrial manufacturing, providing a reliable and secure method for data transfer in sensitive industries. Zhou [25] interested in the potential overlap between the upcoming wireless communication and quantum communications systems is growing. The findings demonstrate that quantum communications have the findings demonstrate that quantum communications and open the door to more sophisticated wireless technologies.

Nokhwal et al [26] presented the integration of quantum computing elements into Generative Adversarial Networks (GANs) to enhance training processes. Challenges related to quantum-classical amalgamation are addressed, with an emphasis on scalability and

limitations of quantum hardware. Liu et al [27] provided an overview of Generative Adversarial Networks (GANs), concentrating on visual synthesis algorithms and applications, such as neural rendering, processing, image translation, and video synthesis. The article discusses methods for stabilizing GAN training, which makes it possible to produce highly-resolution, lifelike images and videos and makes it easier to create new content creation apps. Tseng et al [28] proposed an approach to train more robust GAN models with limited information that involves employing a regularization strategy that considers the relationship between regularized loss and LeCam-divergence. This method aims to improve the ability to generalize and establish a more consistent learning process in scenarios with limited training data. Zhang et al [29] studied a quantum healthcare model built on intelligent mobile edge computing networks connected to the Internet of Things. Positive test findings were found about reducing reliance on IoT cloud analytics or storage facilities. The framework addresses all of the numerous factors, including design, functional challenges, capability needs, and selection criteria, that affect how feasible it is to integrate an edge-IoT ecosystem. Gorle et al [30] proposed a novel dynamic image watermarking technique with features inspired by quantum computing principles. Furthermore, this approach demonstrates resilience to typical image processing assaults, highlighting its promise for applications involving secure image verification [31-32].

3. Research Proposed Methodology

Imagine ultra-secure communication channels like padlocks but for the tiniest devices at the edge of our networks [33]. This proposal looks at using a special AI called a Quantum-Enhanced Generative Adversarial Network (QE-GAN) to squeeze these complex security protocols onto those devices, even though they have limited resources. Think of the QE-GAN as a smart trainer, helping the devices learn the intricacies of the security system without needing a ton of computing power. This could revolutionize security by bringing unbreakable quantum-level protection to the frontlines of the data flow.

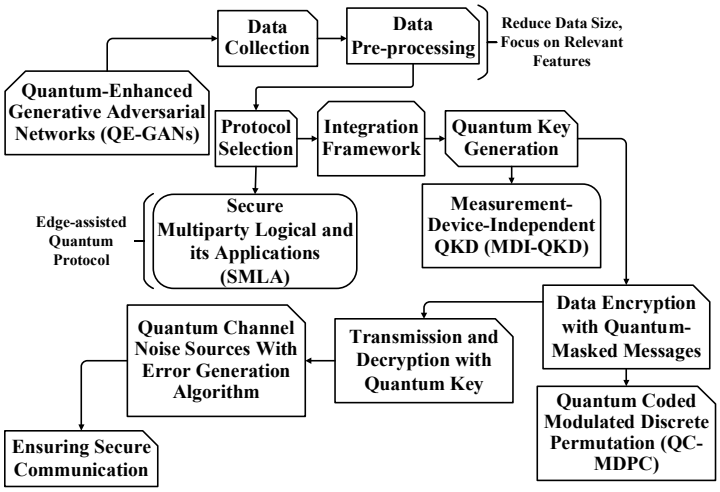

Fig. 1. Block diagram for proposed work

Figure 1 shows the proposed work's block diagram. Through the acquisition of data from edge devices, researchers can obtain the information required to make it easier for QE-GANs on edge devices to integrate secure quantum communication. MFCCs are commonly used for pre-processing speech recognition data and are essential in speech recognition applications. A secure method for communication on edge devices is MDI-QKD. Which provides better security than conventional QKD. Secure multiparty logic and its application (SMLA) refers to a framework that enables secure communication between multiple parties while preserving the confidentiality and integrity of the data being exchanged. Data encryption with Quantum-Masked Messages (QMM) and Quantum Coded Modulated Discrete Permutation (QC-MDPC) are advanced concepts in quantum communication. Noise in quantum channels causes problems for quantum communication, such as detection errors, decoherence, and defective channels. Error generation algorithms aid in the analysis of security, development of mistake correction methods, and understanding of error rates.

3.1 Data Acquisition

Leveraging a combination of direct measurements, protocol analysis, and data collection from edge devices, researchers can acquire the necessary data to facilitate the connection of QE-GANs on edge devices with secure quantum communication. The special characteristics of the quantum channel must be carefully considered, existing communication protocols, and data utilized for QE-GAN training. Moreover, to address challenges related to limited resources, security concerns, and data labelling for an implementation to be effective, the data-collecting procedure is essential [34]. With a robust data acquisition strategy in place, researchers can effectively train QE-GANs to generate realistic and secure outputs tailored to the edge device's application. This integration has great potential to enable intelligent and secure data processing at the network's edge, opening up new opportunities for enhanced communication and information exchange in various industries and applications.

3.2 Pre-processing on the Classical Edge Device

Edge devices, those with limited processing power, are getting a security boost. This approach involves pre-processing data on the device itself before it interacts with complex quantum communication protocols. Quantum-Enhanced Generative Adversarial Networks (QE-GANs) act like AI trainers [35]. They run on the classical (non-quantum) side of the device, getting the information ready for the quantum protocols. This way, even edge devices with less power can leverage the ultra-secure world of quantum communication. It's like having a security prep course for your data before it enters the high-tech vault. Mel-frequency Cepstral Coefficients (MFCCs) are a widely used data pre-processing method in speech recognition applications. Because of their capacity to capture speaker-independent speech aspects while simulating human hearing, MFCCs are especially well-suited for edge devices. MFCCs are effective for devices with limited resources because they minimise data size, concentrate on important aspects, and allow for quicker processing.

3.2.1 Mel Frequency Cepstral Coefficient (MFCC)

Mel-Frequency Cepstral Coefficients (MFCCs) are a popular technique for data pre-processing in speech recognition applications, particularly suitable for edge devices due to their ability to capture speaker-independent features of speech while mimicking human hearing. MFCCs reduce

data size, focus on relevant features, and enable faster processing, making them efficient for resource-constrained devices. This stage involves processing the signal after it has passed through a filter that highlights higher frequencies. In equation (1) Through this process, the (X[n]): Input signal at the (n)-th sample, (Y[n]): Output signal after difference processing at the (n)-th sample, (W[n]): Hamming window applied to the signal, where ($0 \leq n \leq N-1$), (N): Number of samples in each frame, (M): Frame overlap factor, where (M < N).

$$Y[n] = X[n] - X[n-1] \tag{1}$$

Therefore, it is assumed that 95% of each given sample came from a prior sample. Segmenting speech samples that are acquired by analogue to digital conversion (ADC) into brief frames that have a duration of 20–40 milliseconds. N sample frames are created from the voice signal. $M\ (M < N)$ is used to divide adjacent frames apart. The feature extraction processing chain considers the following block and all of the nearest frequency lines are integrated to create a window shape known as a hamming window. As follows is the equation for the Hamming window and the window be described as $W\ (n), 0 \leq n \leq N-1$ where N = the number of samples in every frame, $Y[n]$ = Output signal, $X\ (n)$ = input signal, $W\ (n)$ = Hamming window, then the result of windowing signal is shown below:

$$Y(n) = X(n) \times W(n) \tag{2}$$

$$W(n) = 0.54 - 0.46\cos\left(\frac{2\pi n}{N-1}\right) 0 \leq n \leq N-1 \tag{3}$$

To change the time domain of every N sample frames are entered in the frequency range equation (2) and (3). The convolution of the vocal tract impulse response $H[n]$ and the $U[n]$ Fourier Transform is utilized to translate the glottal pulse in the time domain. The statement supports the equation below:

$$Y(w) = FFT[h(t) * X(t)] = H(w) * X(w) \tag{4}$$

In equation (4) $X\ (w), H\ (w)$ and $Y\ (w)$ are the Fourier Transform of $X\ (t), H\ (t)$ and $Y\ (t)$ respectively. The voice signal deviates from the linear scale and has a relatively broad frequency range in the FFT spectrum. The procedure results in an approximate Mel scale by computing the weighted sum of the spectral components of a collection of triangular filters. Each filter has a triangle magnitude frequency response that, at the centre frequency, is equal to unity and falls linearly to zero frequencies of the two filters next to it. The total of each filter's filtered spectral components is then the filter's output.

$$F(Mel) = [2595 * log\ 10[1 + f]700] \tag{5}$$

Discrete Cosine Transform (DCT) is utilized to transform the log Mel spectrum within a certain time frame and is calculated by this equation (5). The Mel Frequency Cepstrum Coefficient is the name given to the conversion's outcome. Acoustic vectors are the term assigned to this group of coefficients. In a window spanning time samples t1 through t2, the following equation

represents the energy in a frame for a signal x. (X(t)): Input time-domain signal, (X(w)): Fourier Transform of (X(t)), (H(w)): Fourier Transform of the filter (H(t)), (Y(w)): Fourier Transform of the output signal (Y(t)), (F(Mel)): Mel scale frequency.

$$Energy = \sum X^2[t] \tag{6}$$

In equation (6) Compared to the 39 properties of double delta, which each reflect the change in the related delta features across frames, Equation 8's thirteen delta characteristics each display the change in the energy or cepstral characteristic that is pertinent.

$$d(t) = \frac{c(t-1)-c(t-1)}{2} \tag{7}$$

Implementing MFCCs on classical edge devices may require optimizations such as adjusting the number of coefficients in equation (7), optimizing the filter bank design, and using integer arithmetic. Further exploration can be done through tutorials on MFCCs and research papers focusing on optimizing MFCCs for embedded systems.

3.3 Quantum Key Distribution (QKD) Protocol Execution

Integrating Quantum Key Distribution (QKD) and Quantum-Enhanced Generative Adversarial Networks (QE-GANs) directly on edge devices are positive signs, as they encourage researchers to focus on building a strong foundation for data security. This involves developing practical solutions like post-quantum cryptography and lightweight encryption techniques for resource-constrained devices [36]. It appears that encrypted communication on edge devices will have a bright future, with potential breakthroughs in miniaturized quantum hardware and hybrid quantum-classical approaches.

3.3.1 Measurement-Device-Independent QKD (MDI-QKD)

Measurement-Device-Independent Quantum Key Distribution (MDI-QKD) is an intriguing approach for secure communication on edge devices, offering enhanced security compared to traditional QKD. MDI-QKD eliminates the need to trust measurement devices, making it more suitable for scenarios where device security is challenging. $(Q_{rect}^{n,m})$: (Rectilinear basis QBER, the quantum bit error rate in the rectilinear basis, $(e_{rect}^{n,m})$: Error in the rectilinear basis, related to (Q_{rect}) and the error correction process, (H(x)): Binary Shannon entropy function,

$$R = Q_{rect}^{1,1}\left[1 - H\left(e_{diag}^{1,1}\right)\right] - Q_{rect} f(E_{rect})\, H(E_{rect}), \tag{8}$$

where the equation (8) QBER and gain in the rectilinear basis are denoted by the letters erect and Q_{rect}, respectively (i.e., $Q_{rect} = \sum_{n,m} Q_{rect}^{n,m}$ and $E_{rect} = \sum_{n,m} Q_{rect}^{n,m}, e_{rect}^{n,m} \backslash Q_{rect}$), $f(E_{rect}) > 1$ is a function of inefficiency for the process of error correction, and $H(x) = -x\,log2\,(x) - (1-x)\,log2\,(1-x)$ is the binary Shannon entropy function.

$$Q_{rect}^{1,1} = \mu A \mu B^{e^{-(\mu A+\mu B)}} Y_{rect}^{1,1}, \tag{9}$$

where μA and μB represent, respectively, the typical photon count of the signals in situations when the number of required dummy states is finite in (9). This is similar to standard finite decoy state QKD protocols

$$Q^i = \sum_{n=0}^{\infty} e^{-\mu_i} \frac{\mu_i^n}{n!} Y_n, \tag{10}$$

$$Q^i E^i = \sum_{n=0}^{\infty} e^{-\mu_i} \frac{\mu_i^n}{n!} Y_n e_n, \tag{11}$$

The linear equations (10) and (11) with the index i denoting the different decoy settings can obtain the parameters Y_n and e_n For all n.

$$Q_{rect}^{i,j} = \sum_{n=0}^{\infty} e^{-\mu_i} \frac{\mu_i^n}{n!} Y_{n;rect}^j, \tag{12}$$

$$Y_{n;rect}^j = \sum_{m=0}^{\infty} e^{-\mu_j} \frac{\mu_j^m}{m!} Y_{rect}^{n,m}. \tag{13}$$

For Equations (12) and (13) j fixed, varying in the parameters $Y_{n;rect}^j$. Once the yields $Y_{n;rect}^j$ are obtained for all j, is again equivalent to and the legitimate users can estimate the parameters $Y_{rect}^{n,m}$. MDI-QKD provides benefits such as higher security and flexibility in device choice for edge devices. However, there are still limitations to address, including complexity and distance limitations. As quantum technology advances, MDI-QKD may establish itself as a pillar for communication security in the future IoT landscape.

3.3.2 Edge-assisted Quantum Protocol for SMLA (Secure Multiparty Logical and Its Application)

Secure multiparty logic and its application (SMLA) refers to a framework that enables secure communication between multiple parties while maintaining the integrity and confidentiality of the sent data [37]. This technique can be used to improve dialogue for quantum security protocols by incorporating quantum-enhanced generative adversarial networks (QE-GANs) into edge devices. By using SMLA as a foundation for incorporating QE-GANs into edge devices, organizations can guarantee that confidential information is shielded from unwanted access and manipulation. This method can enable secure and efficient communication between edge devices, providing a foundation for building secure and reliable edge computing systems.

$$U_Y = iY \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \tag{14}$$

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{15}$$

In equations 14 and 15, we can easily deduce that U_Y = I and H2 = I. Both r1½j and s1½j are randomly and privately selected by participant P1.

$$S(i) = \sum_{j=1}^{n} S_{j,i} = \sum_{j=1}^{n} F_j\,(i) mod q. \tag{16}$$

$$S = \sum_{i=1}^{n} S_i = \sum_{i=1}^{n} F_i\,(0) mod q. \tag{17}$$

In contrast, the equations (16) and (17). ES transforms the 8-nary integer S into a 2d-component vector (g1, g2, g2d), wherein the component j th and gj represent the number of participants in the j th group.

In addition, Pauli operator U_Y can also be written as

$$U_Y = |0\rangle\langle 1| - |1\rangle\langle 0| \quad (18)$$

$$U_Y|0\rangle = -|1\rangle, \quad (19)$$

$$U_Y|1\rangle = |0\rangle \quad (20)$$

In equations (18), (19) and (20). The integration of secure quantum communication protocols into edge devices using QE-GANs can help improve the security of data transmission and processing in edge computing environments. QE-GANs are neural networks that are specifically designed to work with quantum data, Therefore, they are ideal for enhancing quantum communication protocols' security.

$$U_Y|+\rangle = |-\rangle, \quad (21)$$

$$U_Y|-\rangle = -|+\rangle. \quad (22)$$

Overall, MDI-QKD holds promise for securing communication in edge-assisted quantum protocols for SMLA. By taking advantage of the special qualities of entanglement and post-processing techniques, it offers a path towards building secure and scalable communication channels for mobile learning applications [38]. The integration of secure quantum communication protocols into edge devices using QE-GANs and SMLA can assist businesses in utilizing the advantages of quantum technology while maintaining high levels of security for their data and communication networks. For equations (21) and (22) When sensitive data is exchanged between devices at the network edge, QKD offers a way to establish a provably secure communication channel. However, unreliable measurement equipment may create security flaws in conventional QKD systems.

3.4 Data Encryption with Quantum-Masked Messages

The expedition for securing data on classical edge devices is advancing with promising developments. Even so, direct quantum communication integration with Quantum-Enhanced Generative Adversarial Networks (QE-GANs) is not yet feasible, Quantum computing is a rapidly developing field. Quantum-masked messages (QMM) provide a look into the potential applications of quantum physics to data security [39]. In the meantime, advancements in post-quantum cryptography provide robust encryption methods for today's classical devices, ensuring data security on edge devices. The narrative of data security on edge devices continues to unfold with exciting developments in quantum-inspired security. A cryptographic method called Quantum Coded Modulated Discrete Permutation (QC-MDPC) combines discrete permutation and quantum coding to improve security. QC-MDPC combines the two techniques to encrypt data with a very resilient method against attackers.

3.4.1 Quantum Coded Modulated Discrete Permutation (QC-MDPC)

Quantum Coded Modulated Discrete Permutation (QC-MDPC) is a cryptographic technique that combines quantum coding with discrete permutation to enhance security. Utilizing a blend of the two methods, Data is encrypted in this manner, and QC-MDPC becomes highly resilient to

attacks. This method involves encoding the data using quantum coding and then applying discrete permutation to shuffle the encoded data in a specific pattern. This creates a complex and dynamic encryption scheme that is difficult for hackers to break. An innovative method for safeguarding private data in networks and communication systems is QC-MDPC in equation (23).

$$C : GF_2^k \mapsto GF_2^n \tag{23}$$

which univocally associates each possible binary k-tuple (or information vector) to a binary n-tuple (or code vector, or code word). If $C\ (n, k)$ is a vector subspace and a linear block code Γ is required to have k linearly independent codewords $\{g_0 \dots g_{k-1}\}$ that form a basis of Γ. This time, each codeword $C = [c_0, c_1, \dots, c_{n-1}]$ can be articulated as a consolidation of the foundational vectors in (24):

$$c = u_0 g_0 + u_1 g_1 + \cdots + u_{k-1} - 1 g_{k-1} \tag{24}$$

where the coefficients are taken from the information vector $u = [u_0, u_1, \dots, u_{k-1}]$. Equation (25) can be written in matrix format, as follows:

$$c = u.G \tag{25}$$

The matrix G is named a generator matrix for the code, having size $k \times n$: A special case of systematic is when each code word is obtained by appending r redundancy bits to the k information bits. Specifically, the general codeword $c \in \Gamma$ assumes the following form.

$$c = [u_0, u_1, \dots, u_{k-1} | t_0, t_1, \dots, t_{r-1}] \tag{26}$$

where each redundant (or "parity") bit t_1 can be articulated using the informational scraps via a related "parity-check equation". A systematic block code can be defined through a generator matrix G in the following form in (26):

$$G = [I|P] \tag{27}$$

where I represents the $k \times k$ identity matrix while P is a matrix of size $k \times r$ representing the set of parity-check equations (27).

$$G = [I|(B^{-1}A)^T] \tag{28}$$

where I represents the $k \times k$ identity matrix. A particular case is when $B = B^{-1} = I$, the $r \times r$ identity matrix. This implies that G assumes the form (2.5), with $P = A^T$, therefore in this instance, a proper parity-check matrix is produced in equation (28)

$$H = [P^T|I] \tag{29}$$

Because of these alternatives, the number of iterations used is often much smaller than the maximum number (29). Hence, to define a complexity measure, We can make use of I_{max} or to the typical quantity of iterations I_{avg}. By considering the quantity of information bits as well, the decoding complexity can be determined using the two definitions that follow at the bit level (BC) in (30):

$$BC_1 = \frac{I_{max} \cdot E}{k} \tag{30}$$

$$BC_2 = \frac{I_{avg} \cdot E}{k} \tag{31}$$

In equation (31) Data encryption with Quantum-Masked Messages (QMM) and Quantum Coded Modulated Discrete Permutation (QC-MDPC) are enhanced concepts in quantum communication and coding that are currently in the early stages of development and difficult to implement with current technology. It is crucial to focus on practical security measures for outdated edge devices. This may involve utilizing post-quantum cryptography, adopting lightweight encryption techniques, and integrating homomorphic encryption to strengthen data security. While large-scale adoption of QMM and QC-MDPC might be far off, advancements in quantum technology and hybrid quantum-classical approaches should be monitored for future possibilities. In the meantime, Present-day edge device data security requires a laser-like focus on workable solutions.

3.5 Transmission and Decryption with Quantum Key and Noise Removal

The ultra-secure communication of the future on-edge devices with QKD, noise removal, and Quantum-Enhanced Generative Adversarial Networks (QE-GANs) faces some challenges due to current technology limitations. Concepts like QKD and QE-GANs are complex and require significant resources, making them difficult to integrate with resource-constrained edge devices. Noise removal in quantum communication channels is also a hurdle, as implementing QE-GANs for this purpose is far off [40]. Research in quantum communication is progressing, and miniaturization and simplification of the technology are ongoing. With advancements in QKD and the near future, more secure communication will be a possible acknowledgement of noise-resistant coding schemes.

3.5.1 Quantum Channel Noise Sources with Error Generation Algorithm

Quantum communication faces challenges due to noise in quantum channels, including decoherence, channel imperfections, and detection errors. Error generation algorithms help understand error rates, develop error correction techniques, and analyse security. QKD is a secure communication system based on quantum concepts. Noise removal techniques like error correction codes help mitigate the impact of noise. A proper subset of the EB channels is provided by the completely depolarizing maps, which transform any input state ρ of S into an assigned fixed point $\rho 0 \in \mathfrak{S}(HS)$, i.e.

$$\Phi_{DEP}^{\rho o}[\rho] = \rho o Tr[\rho] \tag{32}$$

For equation (32), each completely depolarizing channel $\Phi_{DEP}^{\rho o}$ define $\mu(\Phi;\ \rho 0)$ to be the minimum value of the mixing probability parameter $\mu \in [0,1]$ that transforms the convex convolution $(1-\mu)\Phi + \mu\Phi_{DEP}^{\rho o}$ into an element of EB, i.e.

$$\mu(\Phi;\rho o) \coloneqq \min_{\mu\in[0,1]}\{(1-\mu)\Phi + \mu\Phi_{DEP}^{\rho o} \in EB\} \tag{33}$$

Computing $\mu(\Phi;\ \rho 0)$ corresponds to determining the minimum μ for which the state in (33)

$$\Gamma_{\rho o,\mu}^{\Phi} = (1-\mu)(\Phi \otimes \mathrm{I})[\psi +] + \mu\rho o \otimes \frac{\mathbb{1}}{d} \tag{34}$$

To get a functional of Φ alone we need hence to optimize the possible choices of the fixed point $\rho 0$. This brings us to define the function in (34) and (35)

$$\mu_c(\Phi) \coloneqq \min_{\rho o} \mu(\Phi;\rho o) \tag{35}$$

Equations (36), (37) and (38) in below. Given Φ and Ψ CPT transformations we have

$$\mu_c(\Phi \circ \Psi) \leq \mu_c(\Psi) \tag{36}$$
$$\mu_c(\Phi \circ \Psi) \leq \mu_c(\Phi) \tag{37}$$

Accordingly, the following inequality holds,

$$2 = n_c(\Phi) < n_c(\mathcal{V} \circ \Phi) \tag{38}$$

which explicitly disproves the monotonicity of n_c under concatenation.

Table 1 presents the Error Generation Algorithm is an iterative procedure used to optimize a codebook for clustering or quantization by minimizing the error between training vectors and codebook entries. The algorithm begins by initializing a training sequence (T), a codebook (C) containing the mean of all training vectors, and an error vector (E). Two empty clusters, Cluster 1 and Cluster 2, are also initialized. In the first step, the algorithm computes the initial code vector (C) as the mean of all training vectors. Next, it computes the error vector (E) by identifying the closest codebook entry to each training vector and assigning an error based on a ratio condition if the ratio C_i / C_j <= 10, the error is the ratio; otherwise, it is set to 10. The error vector is then used to form two new vectors, v_1 and v_2 by adding and subtracting \(E \) from the code vector. The Euclidean distances between the training vectors and v_1, v_2 are then computed, and each training vector is assigned to the closest cluster. The codebook is updated based on the newly formed clusters, and the error vector is recomputed. This process repeats iteratively until convergence. The final output consists of the optimized clusters, Cluster1 and Cluster2. Through this iterative refinement,

the algorithm adjusts the codebook and minimizes error, improving clustering accuracy [41-45].

Table 1. Error generation algorithm

Algorithm 1: Error Generation Algorithm
Initialize parameters:
T = {X_1, X_2, .. X_N} (training sequence)
K = length of the source vector
C = initial codebook (containing the mean of all training vectors)
E = error vector
Cluster1 = {}
Cluster2 = {}
Compute initial code vector C
Calculate the mean of all training vectors to get the initial code vector C
Compute error vector E:
Find j such that C_j is the minimum value in code vector C
Assign E:
If C_i / C_j <= 10, assign E_i = C_i / C_j
Else, assign E_i = 10
Form vectors v_1 and v_2:
Add error vector E to code vector C to get v_1
Subtract error vector E from code vector C to get v_2
Calculate Euclidean distances between training vectors and v_1, v_2:
For each training vector X_i:
Calculate d_1 = $\| v_1 - X_i \|^2$
Calculate d_2 = $\|v_2 - X_i\|^2$
If $d_1 < d_2$, *put* X_i *in Cluster1; else put* X_i *in Cluster2*
Repeat steps 3 to 5 until convergence:
Update codebook C based on Cluster1 and Cluster2
Recompute error vector E
Form new v_1 *and* v_2
Recalculate Euclidean distances and update clusters
Output
Final clusters Cluster1 and Cluster2.

4. Experimentation and Result Discussion

This study delves into the practical implementation of our proposed methodology. This section aims to evaluate the performance, security, and efficiency of the integrated architecture through testing and outcome analysis. Various metrics and benchmarks are employed to assess the efficiency of using QE-GANs in unification with quantum communication methods in improving edge device communication security and dependability. Performance metrics for QE-GANs integration include security efficiency, computational efficiency, scalability, and quantum error correction. System configuration involves quantum communication layers, edge devices with quantum encryption, and hybrid classical-quantum GAN architectures. Furthermore, Python simulations in Jupiter will be used to confirm the efficacy of our approach in practical applications, providing valuable insights into its practical applicability and potential limitations.

Table 2. System configuration for simulation

Python Jupiter	Version 3.8.0
Operation System	Ubuntu
Memory Capacity	4GB DDR3
Processor	Intel Core i5 @ 3.5GHz

Table 2 outlines the system configuration utilized for the simulation in this study. The simulations were conducted using Python Jupiter version 3.8.0 on an Ubuntu operating system. The system had a memory capacity of 4GB DDR3 and was powered by an Intel Core i5 processor clocked at 3.5GHz. This configuration ensured sufficient computational resources to execute the simulations effectively and accurately capture the intended phenomena under investigation.

4.1 Pre-processed on the Classical Edge Device

The method's initial phase is to extract characteristics from the input data that are Mel-Frequency Cepstral Coefficients (MFCC). In this vital pre-processing step, the unprocessed audio signals are converted into a representation that captures the frequency content and temporal dynamics of the audio. By extracting MFCC features, the classical edge device prepares the data for subsequent analysis and classification tasks, establishing the basis for precise and effective processing [46- 49].

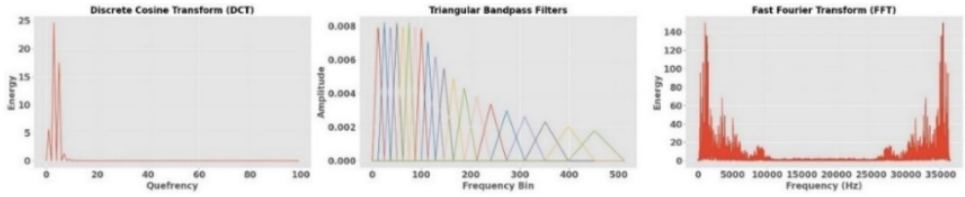

Fig. 2. Analysis of frequency domain in various techniques

Figure 2 displays the frequency versus energy Discrete Cosine Transform (DCT), showcasing the distribution of energy across different frequency components. The highest recorded energy value reaches 23.7568, indicating the dominant frequency component contributing significantly to the signal. Following closely is the second-highest energy value at 17.6997, representing another notable frequency component. Conversely, the lowest energy value is observed at 6.5790, signifying a frequency component with minimal contribution to the overall signal energy. This visualization offers insights into the frequency-domain representation of the signal, highlighting the relative importance of different frequency components based on their energy levels. Another displays the triangular band pass filter's response, depicting frequency bin versus amplitude. The highest recorded amplitude within the specified frequency range is noted at 0.0077, indicating the peak intensity of the filtered signal. The Fast Fourier Transform (FFT) plot illustrates frequency (Hz) versus energy, showcasing the distribution of energy across different frequency components. The highest recorded energy value exceeds 140, indicating significant signal power at a specific frequency or frequency [50-51].

4.2 Quantum Key Distribution (QKD) Protocol Execution

The Quantum Key Distribution (QKD) Protocol is being carried out. This critical phase involves the implementation and deployment of QKD protocols to establish secure cryptographic keys between communicating parties. Through the application of quantum concepts, including quantum entanglement and uncertainty, QKD protocols ensure the generation of secure keys immune to eavesdropping attempts, thus laying the foundation for secure communication channels in quantum networks.

Figure 3 represents the relationship between key rate and distance (Km), with different legends denoted as (-5,0,25, 0.5), (-5,0.0,1.0), (-8, 0,.25, 0.5) PLOB, and (-8,0.0,1.0). Each legend corresponds to a specific parameter setting or condition, influencing the key rate at various distances. For instance, the legend (-5, 0, 25, 0.5) may represent different signal-to-noise ratios or modulation schemes, while (-8, 0, .25, 0.5) PLOB could indicate variations in the polarization state of light. By examining the key rate across different distances and under different conditions, this visualization aids in assessing the performance and feasibility of quantum networks over various transmission distances. The relationship between key rate and distance (Km), with various legends denoting different scenarios or conditions. The corresponding values for each legend are as follows: "zero" has a key rate value of -1.5499, "total" corresponds to a key rate of -1.630, "one" is associated with a key rate of -1.2495, and "PLOB" exhibits the highest key rate value at 0.6554.

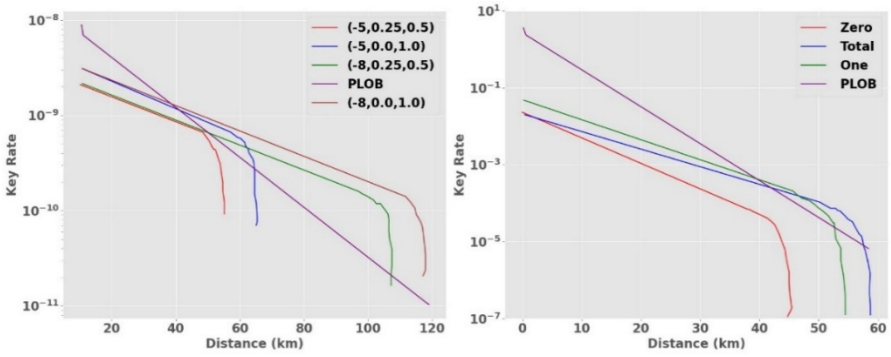

Fig. 3. Key rate Vs distance analysis for quantum communication systems

4.3 Data Encryption with Quantum-Masked Messages

The process of encrypting data using quantum-masking techniques. In this step, quantum masking is employed as a sophisticated encryption method to secure sensitive information. Quantum-masked communications are created from information by applying the ideas of quantum mechanics, ensuring unparalleled security and resilience against conventional decryption methods. This step is essential in guaranteeing the confidentiality and integrity of data in modern cryptographic systems.

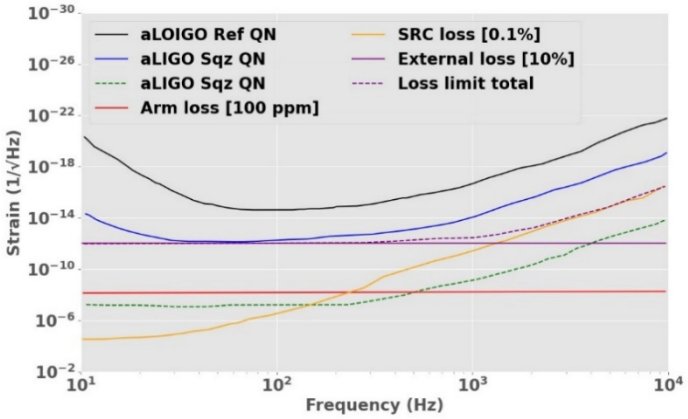

Fig. 4. Frequency-strain relationship in strain-sensitive system components

Figure 4 illustrates the relationship between frequency (Hz) and strain (1/√ (Hz)) for various components or phenomena within the system. The data points represent different sources of strain or strain-related quantities, such as aLOIGO reference quantum noise (QN), aLOIGO squeezed quantum noise, arm loss, SRC loss, external loss, and the total cost limit. Each data point corresponds to a specific frequency and its corresponding strain value. For instance, the aLOIGO reference quantum noise exhibits a strain value of 10-20.3736 at the given frequency, while the arm loss contributes a strain of 10-8.1614. This visualization aids in understanding the distribution and impact of strain across different frequency ranges, providing insights into the performance and limitations of the system components in terms of strain sensitivity.

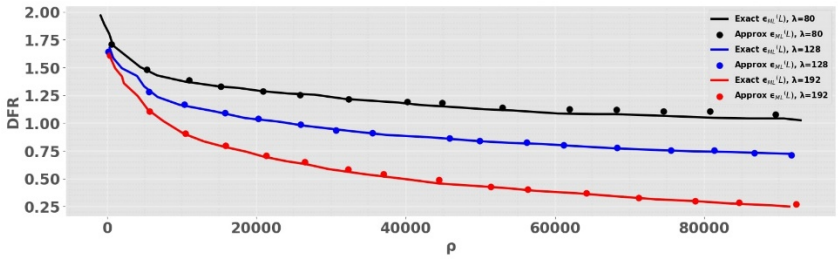

Fig. 5. Relationship between ρ and DRF

Figure 5 illustrates the relationship between ρ (a parameter representing a certain characteristic) and DFR for the highest recorded value, which stands at 1.9218. This value signifies the peak point or maximum intensity of the relationship between ρ and DFR. By investigating this highest value, the figure provides valuable insight into the optimal conditions or critical points within the examined parameter space, aiding in the identification of significant trends or phenomena.

4.4 Transmission and Decryption with Quantum Key and Noise Removal

The transmission and decryption utilise the generated quantum key while addressing potential errors through error generation algorithms and mitigating the effects of quantum channel noise sources. This step involves the crucial task of securely transmitting encrypted data over quantum channels and then decrypting it using the quantum key. Assuring the transmission's dependability and accuracy, error generation algorithms are utilized to identify and rectify any potential faults that may emerge along the transmission procedure. Moreover, quantum channel noise sources, such as photon loss, de-coherence, and other environmental factors, are considered and succeeded in boosting the communication system's resilience and effectiveness.

Figure 6 shows the generation and error algorithm for two different legends. Each legend represents a distinct algorithm or method employed for error correction or mitigation during data generation processes. Through an analysis of these algorithms' performance across various generations, the figure provides insights into their effectiveness in reducing errors and improving data quality over successive iterations. This comparison aids in identifying the most suitable algorithm for achieving reliable and accurate data generation in the given context.

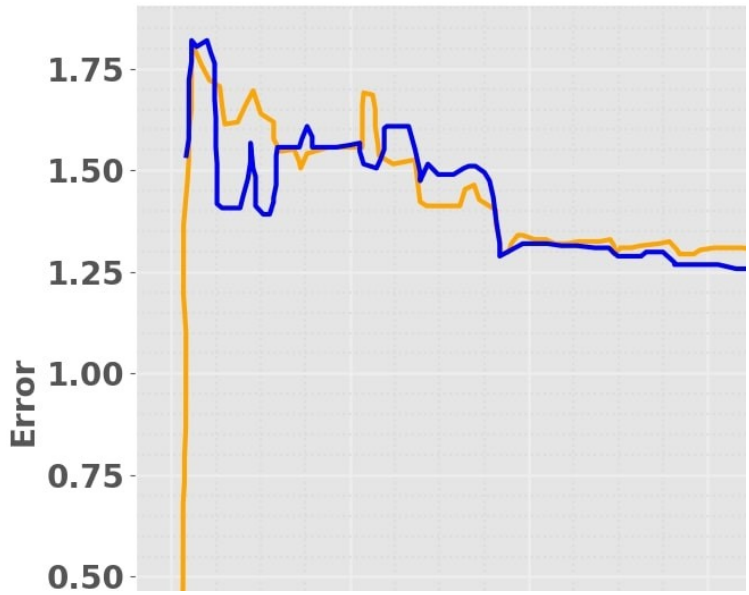

Fig. 6. Generation Vs error values

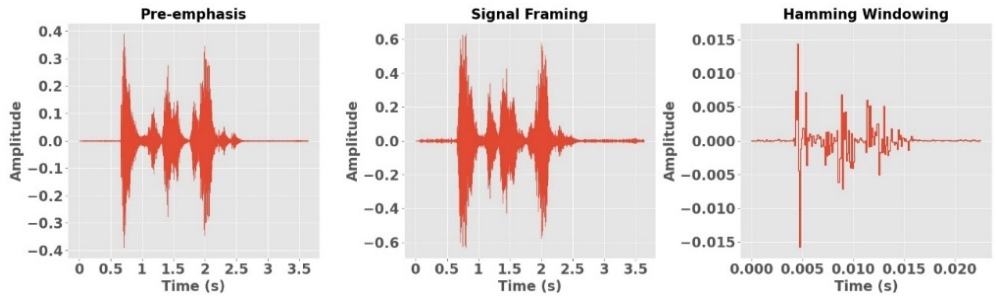

Fig. 7. Analysis of pre-emphasis, signal framing and hamming windowing

Figure 7 illustrates the pre-emphasis for time (s) versus amplitude, showcasing the amplitude levels ranging from the highest point of 0.3602 to the lowest level of -0.10513. This graphical depiction highlights the range of signal amplitudes over time and provides crucial information about the dynamic amplitude alterations done during pre-emphasis. Signal framing over time (s) versus amplitude, with the highest level reaching 0.5379 and the lowest level descending to -0.2875. This illustration offers a visual portrayal of the amplitude variation of the signal over time, highlighting its dynamic nature and amplitude range. Analysing signal framing enables researchers to understand signal characteristics, such as peak levels and fluctuations, crucial for signal processing and analysis tasks in various domains, including telecommunications, audio processing, and biomedical signal analysis. The Hamming windowing time (s) is shown in the figure that is plotted against the corresponding amplitude levels. The highest recorded amplitude reaches 0.01237, representing the peak signal intensity, while the lowest level is noted at -0.10513, indicating the trough or minimum amplitude value. This visualization provides valuable insight into the temporal characteristics of the signal under Hamming windowing, showcasing both its peak and nadir amplitudes over time.

5. Research Conclusion

Secure quantum communication protocols integrated into edge devices using the utilization of Quantum-Enhanced Generative Adversarial Networks (QE-GANs) show great potential in improving Quantum communication's security and efficiency in edge computing environments. The proposed methodology demonstrates how QE-GANs can enhance Quantum communication protocols' security and optimize quantum keys to suit the limited resources of edge devices. This research highlights the importance of utilizing QE-GANs to address the challenges posed by real-time processing and resource constraints in edge computing, enabling the application of secure quantum communication solutions at the network's edge. Future research avenues may explore the scalability and adaptability of QE-GANs in various edge computing scenarios, as well as investigate other potential applications of quantum-enhanced generative adversarial networks beyond secure communication protocols. The development of QE-GAN models using MATLAB might offer insightful information on the performance and quantum communication protocols optimized for edge devices, clearing the path for useful applications in actual settings. The findings show that the highest recorded energy value reaches 23.7568, indicating the dominant frequency component contributing significantly to the signal. Through continued

advancements in quantum-enhanced technologies and edge computing frameworks, we anticipate significant strides in enhancing the effectiveness and safety of edge device communication networks. The future scope of integrating secure quantum communication protocols into edge devices via QE-GANs includes advancing privacy-preserving IoT, real-time secure data transfer, adaptive encryption, and decentralized security in quantum-enhanced networks.

References

1. ER. Chan, CZ. Lin, MA. Chan, K. Nagano, B. Pan De, S. Mello et al (2021), *Efficient geometry-aware 3D generative adversarial networks* [Internet]. arXiv [cs.CV]. Available from: http://arxiv.org/abs/2112.07945

2. Y-L. Wu, H-H. Shuai, Z-R. Tam, H-Y. Chiu (2021), *Gradient normalization for Generative Adversarial Networks* [Internet]. arXiv [cs.LG]. Available from: http://arxiv.org/abs/2109.02235

3. H-L. Huang, Y. Du, M. Gong, Y. Zhao, Y. Wu, C. Wang et al (2021), *Experimental quantum generative adversarial networks for image generation*, Phys Rev Appl [Internet], Vol. 16, No. 2. Available from: http://dx.doi.org/10.1103/physrevapplied.16.024051

4. A. Sajeeda, B.M.M. Hossain (2022), *Exploring generative adversarial networks and adversarial training*, International Journal of Cognitive Computing in Engineering [Internet], Vol. 3, pp. 78–89. Available from: http://dx.doi.org/10.1016/j.ijcce.2022.03.002

5. J. Kong, J. Kim, J. Bae (2020), *HiFi-GAN: Generative adversarial networks for efficient and high fidelity speech synthesis* [Internet]. arXiv [cs.SD]. Available from: http://arxiv.org/abs/2010.05646.

6. SR. Hasan, MZ. Chowdhury, M. Saiam, Y.M. Jang (2023), *Quantum Communication Systems: Vision, Protocols, Applications, and Challenges*, IEEE Access [Internet], Vol. 11, pp. 15855–77. Available from: http://dx.doi.org/10.1109/access.2023.3244395

7. A. Lizardo, R. Barbosa, S. Neves, J. Correia, F. Araujo (2021), *End-to-end secure group communication for the Internet of Things*, J Inf Secur Appl [Internet], Vol. 58, No. 102772, pp. 102772. Available from: http://dx.doi.org/10.1016/j.jisa.2021.102772

8. L. Ma, L. Ding (2022), *Hybrid quantum edge computing network*, In: Deacon KS, Meyers RE, editors, Quantum Communications and Quantum Imaging XX. SPIE.

9. H. Abulkasim, B. Goncalves, A. Mashatan, S. Ghose (2022), *Authenticated secure quantum-based communication scheme in internet-of-drone's deployment*, IEEE Access [Internet], Vol. 10, pp. 94963–72. Available from: http://dx.doi.org/10.1109/access.2022.3204793

10. T.H. Szymanski (2022) *The cyber security via determinism paradigm for a quantum-safe zero trust deterministic internet of things (IoT),* IEEE Access, Vol. 10, pp. 45893–930.

11. M. Nakkar, R. Altawy, A. Youssef (2020) *Lightweight broadcast authentication protocol for edge-based applications*, IEEE Internet Things J [Internet], Vol. 7, No. 12, pp. 11766–77. Available from: http://dx.doi.org/10.1109/jiot.2020.3002221

12. A. Stavdas, E. Kosmatos, C. Maple, E. Hugues-Salas, G. Epiphaniou, D.S. Fowler et al (2024), *Quantum Key Distribution for V2I communications with software-defined networking*, IET Quantum Communication [Internet], Vol. 5, No. 1, pp. 38–45. Available from: http://dx.doi.org/10.1049/qtc2.12070

13. G. Zhang, I.W. Primaatmaja, J.Y. Haw, X. Gong, C. Wang, C.C.W. Lim (2021), *Securing practical quantum communication systems with optical power limiters*, PRX quantum [Internet], Vol. 2, No. 3. Available from: http://dx.doi.org/10.1103/prxquantum.2.030304 14. N. Corrias, I. Vagniluca, S. Francesconi, C. De Lazzari, N. Biagi, M. Menchetti et al (2024), *Implementation of Italian industry 4.0 quantum testbed in Turin*, IET Quantum Communication [Internet], Vol. 5, No. 1, pp. 46–51. Available from: http://dx.doi.org/10.1049/qtc2.12074

15. P. Wright, C. White, RC. Parker, J-S. Pegon, M. Menchetti, J. Pearse et al (2021), *5G network slicing with QKD and quantum-safe security*, J Opt Commun Netw [Internet], Vol. 13, No. 3, p. 33. Available from: http://dx.doi.org/10.1364/jocn.413918

16. J. Senor, J. Portilla, G. Mujica (2022), *Analysis of the NTRU post-quantum cryptographic scheme in constrained IoT edge devices*, IEEE Internet Things J [Internet], Vol. 9, No. 19, pp. 18778–90. Available from: http://dx.doi.org/10.1109/jiot.2022.3162254

17. *A privacy-preserving authentication protocol using quantum computing for V2I authentication in vehicular ad hoc networks*, Security and Communication Networks (2022).

18. D. Dhinakaran (2024), *Quantum-based privacy-preserving techniques for secure and trustworthy internet of medical things an extensive analysis*, Quantum Inf Comput, Vol. 24, pp. 227–0266.

19. S. Suhail, R. Hussain, A. Khan, C.S. Hong (2021), *On the role of hash-based signatures in quantum-safe internet of things: Current solutions and future directions*, IEEE Internet Things J [Internet], Vol. 8, No. 1, pp. 1–17. Available from: http://dx.doi.org/10.1109/jiot.2020.3013019

20. Q. Zhu, X. Yu, Y. Zhao, A. Nag, J. Zhang (2021), *Resource allocation in quantum-key-distribution-secured datacenter networks with cloud-edge collaboration*, In: Asia Communications and Photonics Conference 2021. Washington, D.C.: Optica Publishing Group.

21. SR. Hasan, MZ. Chowdhury, M. Saiam and Y.M. Jang (2023), *Quantum communication systems: vision, protocols, applications, and challenges*, IEEE Access.

22. M.Z. Ali A. Abohmra M. Usman A. Zahid H. Heidari M.A. Imran et al (2023), *Quantum for 6G communication: A perspective*, IET Quantum Communication [Internet], Vol. 4, No. 3, pp. 112–24. Available from: http://dx.doi.org/10.1049/qtc2.12060

23. X. Hua, D. Li, Y. Fu, Y. Zhu, Y. Jiang, J. Zhou, X. Yang and Y. Tan (2023), *Hierarchical controlled hybrid quantum communication based on six-qubit entangled states in IoT*, Sensors, Vol. 23, No. 22, p. 9111.

24. B. Senapati, B.S. Rawal (2023), *Quantum communication with RLP quantum resistant cryptography in industrial manufacturing*, Cyber Security and Applications [Internet], Vol. 100019, p. 100019. Available from: http://dx.doi.org/10.1016/j.csa.2023.100019

25. X. Zhou, A. Shen, S. Hu, W. Ni, X. Wang, E. Hossain et al (2023), *Towards quantum-native communication systems: New developments, trends, and challenges* [Internet]. arXiv [quant-ph]. Available from: http://arxiv.org/abs/2311.05239

26. S. Nokhwal, S. Nokhwal, S. Pahune, A. Chaudhary (2024), *Quantum generative adversarial networks: Bridging classical and quantum realms*, In: 2024 8th International Conference on Intelligent Systems, Metaheuristics & Swarm Intelligence (ISMSI). New York, NY, USA: ACM.

27. M-Y. Liu, X. Huang, J. Yu, T-C. Wang, A. Mallya (2021), *Generative adversarial networks for image and video synthesis: Algorithms and applications*, Proc IEEE Inst Electr Electron Eng [Internet], Vol. 109, No. 5, pp. 839–62. Available from: http://dx.doi.org/10.1109/jproc.2021.3049196

28. H-Y. Tseng, L. Jiang, C. Liu, M-H. Yang, W. Yang (2021), *Regularizing generative adversarial networks under limited data*, In: 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). IEEE.

29. J. Zhang (2024), *Quantum healthcare analysis based on smart IoT and mobile edge computing: way into network study*, Opt Quantum Electron [Internet], Vol. 56, No. 4. Available from: http://dx.doi.org/10.1007/s11082-024-06285-y

30. R. Gorle and A. Guttavelli (2024), A *novel dynamic image watermarking technique with features inspired by quantum computing principles*, AIP Advances, Vol. 14, No. 4.

31. D. Dhinakaran, D. Selvaraj, N. Dharini, S.E. Raja and C. Priya (2024), *Towards a novel privacy-preserving distributed multiparty data outsourcing scheme for cloud computing with quantum key distribution*. arXiv preprint arXiv:2407.18923.

32. G. Kornaros, G. Berki and M. Grammatikakis (2023. June), *Quantum-Secure Communication for Trusted Edge Computing with IoT Devices*, In IFIP International Conference on ICT Systems Security and Privacy Protection, pp. 163-176. Cham: Springer Nature Switzerland.

33. C. Cicconetti, D. Sabella, P. Noviello and G.D. Paduanelli (2024), *Quantum-safe Edge Applications: How to Secure Computation in Distributed Computing Systems*. arXiv preprint arXiv:2405.17008.

34. S.R. Hasan, M.Z. Chowdhury, M. Saiam and Y.M. Jang (2023), *Quantum communication systems: vision, protocols, applications, and challenges*, IEEE Access, Vol. 11, pp. 15855-15877.

35. S. Dhar, A. Khare, A.D. Dwivedi and R. Singh (2024), *Securing IoT devices: A novel approach using blockchain and quantum cryptography*, Internet of Things, Vol. 25, p. 101019.

36. S. Biswas, R.S. Goswami, K.H. Kumar Reddy, S.N. Mohanty and M.A. Ahmed (2024), *Advancing quantum communication security: Metamaterial based quantum key distribution with enhanced protocols*, IET Quantum Communication.

37. Y.K. Wong, Y. Zhou, Z.Y. Li, Y.S. Liang and X. Zhou (2024 May), *Software Security and Quantum Communication: A Long-distance Free-space Implementation Plan of QSDC Without Quantum Memory*, In Proceedings of the 2024 6th International Conference on Software Engineering and Development, pp. 1-13.

38. X. Zhou, A. Shen, S. Hu, W. Ni, X. Wang, E. Hossain and L. Hanzo (2023), *Towards Quantum-Native Communication Systems: New Developments, Trends, and Challenges*. arXiv preprint arXiv:2311.05239.

39. M. Xu, D. Niyato, J. Kang, Z. Xiong, Y. Cao, Y. Gao, C. Ren and H. Yu (2024), *Generative AI-enabled Quantum Computing Networks and Intelligent Resource Allocation*. arXiv preprint arXiv:2401.07120.

40. A. Sharma (2024), *The Development of an Automated Approach for Designing Quantum Algorithms Using Circuits Generated by Generative Adversarial Networks (Gans),* Journal of Artificial Intelligence General science (JAIGS), Vol. 4, No. 1, pp. 1-140, ISSN: 3006-4023.

41. Lokesh S. Khedekar (2023), *Strength of Data Matrix Image over Analysis and Design of Exam Processing System*, IEEE 8th International Conference for Convergence in Technology (I2CT)

42. P. K. Veni and A. Gupta (2023), *Acne Assessment and Grading: Challenges and Opportunity*, 2023 2nd International Conference on Computational Systems and Communication (ICCSC), Thiruvananthapuram, India, pp. 1–5, doi: 10.1109/ICCSC56913.2023.10143016.

43. C. Radhiya Devi, S. K. Jayanthi (2023), *DCNMAF: Dilated Convolution Neural Network Model with Mixed Activation Functions for Image De-Noising*, International Journal of Intelligent Systems and Applications in Engineering, Vol. 11, No. 4, pp. 552–557.

44. Attili Venkata Ramana and Dr.E. Kesavulu Reddy (2015), *OCCSR: Document Classification By Order Of Context*, Concept and Semantic Relations Indian Journal of Science and Technology, Vol 8, No. 30, DOI:10.17485/ijst/2015/v8i30/75398, November 2015

45. Amirthayogam Gnanasekaran, Anbu Ananth Chinnasamy, Elango Parasuraman (2022), *Analyzing the QoS prediction for web service recommendation using time series forecasting with deep learning techniques*. Concurrency Computat Pract Exper., pp. e7356. doi: 10.1002/cpe.7356

46. R.S. Shankar, V.M. Gupta, K.V. Murthy, C.S. Rao (2019 May 1), *Breast Cancer Data Classification Using Machine Learning Mechanisms*, Indian Journal of Public Health Research & Development, Vol. 10, No. 5.

47. S. Priyadarshini, T.N. Sawant, G. Bhimrao Yadav et al. (2024), *Enhancing security and scalability*

by AI/ML workload optimization in the cloud. Cluster Computing https://doi.org/10.1007/s10586-024-04641-x

48. Jayesh Sarwade, Sagar Shetty, Aman Bhavsar, Mahesh Mergu, Ajay Talekar (March 2019), *Line Following Robot Using Image Processing*, Conference: 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC).

49. S. V. Balshetwar and R. M. Tugnayat (2017), *Framing and sentiment: Cumulative effect*, 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, India, pp. 2873-2877, doi: 10.1109/ICECDS.2017.8389980

50. P. L. M. Anushka Deepak Kadage, Banoth Meghya Nayak,Vishal Sharad Hingmire, *AI-Enhanced Digital Forensics: Automated Techniques for Efficient Investigation and Evidence Collection, Journal of Electrical Systems, Vol. 20, No. 1*

51. Nilima Prakash Patil1 & R. J. Ramteke (2023), *A novel optimized deep learning framework to spot keywords and query matching process in Devanagari scripts,* Multimedia Tools and Applications, https://doi.org/10.1007/s11042-023-14912-1

52. K.N. Asha and R. Rajkumar (August 23, 2024), *Cross domain and adversarial learning based deep learning approach for web recommendation,* International Journal of Critical Infrastructures, Vol. 20, No. 4, pp 341-355. https://doi.org/10.1504/IJCIS.2024.140556