

DISCRIMINATIVE AI DRIVEN QUANTUM SIGNCRYPTION FOR QoS-AWARE RELIABLE AND SCALABLE SOCIAL MEDIA STREAMING DATA TRANSMISSION IN 5G NETWORK

N. Suresh¹ and P. Kanmani²

¹Department of Computer Science, Mahendra Arts and Science College, India

²Department of Computer Science, Thiruvalluvar Government Arts College, India

Abstract

The fifth generation (5G) of mobile networks represents a major advancement over previous wireless technologies to deliver ultra-fast data transmission, low latency, and massive connectivity. 5G technologies provide a highly reliable, scalable, and flexible communication for modern social media applications. 5G allows users to stream high-definition videos, live broadcasts, and interactive content with lesser buffering. Moreover, due to massive connectivity of users and devices interact simultaneously in social media platforms, latency and high reliability also major concern. 5G networks incorporate advanced technologies to ensure high Quality of Service (QoS) for social media streaming. Many researchers carried out their research on secured data transmission in 5G network. But the data confidentiality rate has not been significantly improved, and end-to-end delay has not been reduced. To enhance the QoS-Aware Reliable and Scalable data Transmission in 5G Network, a new method named Discriminative AI Transient Quantum Signcryption Cryptography (DAITQ- SigCrypt) method is introduced. The designed DAITQ-SigCrypt method simultaneously achieves both security and QoS aware data transmission in social media streaming data transmission. The discriminative AI model is a used for analyzing the each device's resources such as bandwidth, signal strength and SINR. Next, identifies resource-efficient devices to achieve the QoS optimized data transmission. During the data transmission, reliability is achieved using Transient Quantum Signcryption Cryptography to deliver data accurately and securely, ensuring that information reaches the authorized receiver without loss, corruption, or unauthorized access. By this way, DAITQ- SigCrypt method achieved Reliable and QoS optimized data transmission. Experimental evaluation of proposed DAITQ- SigCrypt method is carried out with respect to the different performance metrics such as data delivery rate, data loss rate, throughput, latency, jitter, confidentiality rate, integrity rat with respect to number of streaming data samples. Quantitative results reveal that DAITQ- SigCrypt method significantly enhances streaming data communication in 5G networks, achieving higher throughput, data delivery, confidentiality and integrity with lower latency, jitter and packet loss compared to existing methods.

Keywords:

5G Network, Social Media Streaming Data, QoS, Reliability, Discriminative AI, Transient Quantum Signcryption Cryptography

1. INTRODUCTION

5G networks are designed to support highly mobile environments and dynamic network conditions, providing seamless connectivity and robust performance to meet the growing demands of high-speed, low-latency, and densely connected applications. Unlike traditional data transfer, streaming requires a consistent and high-quality connection to avoid buffering, latency, or packet loss, which is critical for ensuring a smooth user experience. In 5G networks, streaming data

transmission refers to the continuous delivery of multimedia content such as video and audio. Several methods have been developed for streaming data transmission but they have faced various challenges.

A QoS-aware Deep Reinforcement Learning-based Link Adaptation (QDRLLA) was developed in [1] for optimizing resource usage and reliable data transmission. However, Latency remains low and achieves high reliability. However, robust hybrid cryptographic schemes were not implemented to strengthen security in terms of data confidentiality and integrity. A robust and adaptive security framework was developed in [2] that hybrids AI-enhanced lightweight encryption to protect user preferences and communication data during resource allocation while ensuring optimal system performance. But the efficient device to device communication in next-gen wireless networks was major issues.

A Secure Blockchain-based Data Transmission Protocol (SBDTP) was developed in [3] for enhancing data integrity with reduced latency. A novel security mitigation model was developed in [4] by integrating artificial neural network (ANN) to improve the 5G network security system. A data security system was designed in [5] for 5G networks that provide the security of the network based on data encryption. A strongly secure identity-based authenticated key agreement method was developed in [6] for 5G environment to improve efficiency and security. An integration of Blockchain and Machine learning model was developed in [7] to enhance the Security of 5G Network. A blockchain-based multi-party distributed certificate management framework was proposed in [8] to address security, authentication, and authorization in 5G networks. Progressive Recurrent Generative Adversarial Network (PRGAN) based routing protocol was designed in [9] to perform seamless and reliable data communication within the 5G network. A new approach that integrates a multi-layer parallel low-density parity-check (MLP-LDPC) algorithm was designed in [10] by using post-quantum cryptography aimed to enable reliable and secure transmission. A Deep Reinforcement Learning was proposed in [11] to achieve reliable data transmission in 5G networks. In order to optimize the network performance, DL techniques was integrated in [12] within 5G framework to strengthen security measures. In order to increase throughput and efficiency, a modified Resource Allocation (RA) scheme was developed in [13] using modified RFA. A novel maximum capacity model (MCM) was introduced in [14] to enhance performance of dynamic resource allocation, robust encryption, QoS within 5G networks. A hybrid particle swarm Cauchy approach and a modified long short-term memory based approach were developed in [15] to ensure that QoS constraints for efficient resource allocation.

1.1 PROPOSAL CONTRIBUTIONS

The limitations of existing methods are overcome by proposing a new approach, the DAITQ-SigCrypt method. Contributions of DAITQ-SigCrypt are summarized as follows:

- Design a DAITQ-SigCrypt method to solve QoS-Aware reliable and scalable social media streaming data transmission in 5G network by integrating the Discriminative AI and Transient Quantum Signcryption Cryptography.
- To achieve QoS-aware data transmission, a novel Discriminative AI model is employed to analyze resources of mobile devices using a Laplace kernel function and dynamically allocate resources. This resource allocation strategy is then used for improving the data delivery ratio and reduced packet loss, latency, and jitter.
- To enhance reliable data transmission, Transient Quantum Signcryption Cryptography is employed, comprising three processes namely key generation with quantum key distribution, signcryption, and unsigncryption. Additionally, a ring signature algorithm is integrated into DAITQ-SigCrypt method to prevent unauthorized access, thereby improving both data confidentiality and integrity.
- Finally, extensive simulations are conducted to evaluate the performance of DAITQ-SigCrypt method and other models.

2. RELATED WORKS

An open-source framework was introduced in [16] for evaluating QoE within multimedia networks by implementing the machine learning model. A learning-based approach was developed in [17] to facilitate QoS-aware data delivery within the dynamics environment. An enhanced AODV protocol was designed in [18] using reinforcement learning to increase the throughput and minimize the delay. A structured, energy-efficient link sensing and database maintenance approach was proposed in [19] to achieve optimal QoS during device-to-device communication. A robust Multi-Server Authentication framework was proposed in [20] for 5G networks. A Hybrid Enhanced extreme gradient boost model was developed in [21] to improve the performance of QoE within Video Services Over 5G Wireless Networks. QoE-aware mobility management was evaluated in [22] within heterogeneous cellular networks to improve throughput performance and optimize bandwidth allocation. The 5th Generation Interference Management (5G-IM) model was proposed in [23] to reduce interference and improve throughput with lower latency. Artificial Intelligence (AI) and Machine Learning (ML) were developed in [24] to optimize the QoS-aware data transmission. A new user-priority resource allocation (UPRA) algorithm was developed in [25] to optimize the QoS performance. To reduce packet drops and delays, an integrated solution combining user, content, and cache management was proposed in [26]. A novel framework model was developed in [27] for enhancing downlink throughput using ML models within fifth generations cellular network. A novel two-phase approach was proposed in [28] to enable efficient data transmission using machine learning. AI-driven resource allocation strategy was developed in [29] to increase the throughput and minimize the latency. A deep Q-network model

was developed in [30] combined with GAT to execute optimal resource allocation and significantly boosts the QoS performance.

3. PROPOSAL METHODOLOGY

The proposed approach for QoS-aware and secure data transmission in 5G networks is presented, taking into account dynamic network conditions and user mobility patterns. This section outlines the key stages involved in designing and deploying the novel method for Device-to-Device (D2D) communication, which offers significant advantages in terms of spectrum utilization, overall system capacity, high data throughput, and secure information exchange. Several challenges are addressed to ensure reliable and secure D2D integration in 5G networks. To overcome these challenges, a novel model called DAITQ- SigCrypt is introduced, specifically designed to enhance communication efficiency, security, and QoS, while minimizing latency and preventing service disruptions. The proposed DAITQ- SigCrypt method, illustrated in Fig.1 consists of two interconnected stages resource optimization, and secure data transmission. These stages collectively ensure efficient and secure communication by analyzing device resources, ensuring secure connections.

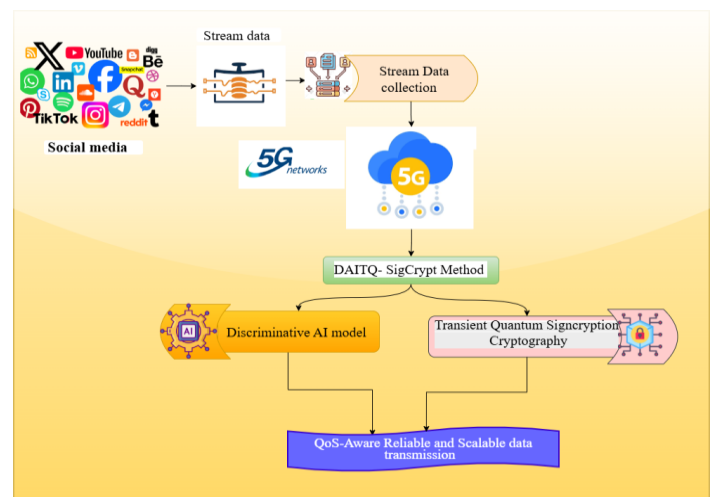


Fig.1. Architecture of proposed DAITQ- SigCrypt method

The Fig.1 presents architecture of proposed DAITQ- SigCrypt method, developed to enable social media streaming data communication within 5G networks. Social-media platforms generate continuous streaming data, which is first collected and transmitted through 5G network infrastructure. This data then enters the DAITQ-SigCrypt method where it undergoes two major processes namely discriminative AI model for identifying resource-efficient devices and data protection through Transient Quantum Signcryption Cryptography, which ensures advanced security. By combining intelligent data processing with strong cryptographic protection, the system enables QoS-aware, reliable, and scalable data transmission, ensuring both performance and security for high-speed social-media data flows.

3.1 NETWORK MODEL

Network model of 5G cellular system consists of mobile devices or nodes $Mn_1, Mn_2, Mn_3, \dots, Mn_n$ to ensure social media

streaming data communication that support the transmission of streaming data $SD_1, SD_2, SD_3, \dots, SD_n$ generated from social media platforms. During this data transmission between the devices through 5G network, QoS-enhancement is achieved through resource allocation ensures that communication requirements such as latency, throughput, reliability, and jitter are continuously achieved and also supports high-volume social-media streams. Simultaneously, security becomes a critical requirement to ensure that sensitive information remains safeguards and ensure high-speed social-media data streams are transmitted with confidentiality, integrity against cyber threats.

3.2 DISCRIMINATIVE AI MODEL BASED QOS AWARE DATA TRANSMISSION

Discriminative AI model-based QoS-aware data transmission refers to an intelligent communication mechanism in which a discriminative AI model analyzes network conditions and data characteristics to optimize QoS across the 5G network. Here the Multilayer perceptron neural learning classifier model is used as a Discriminative AI technique to evaluate parameters such as Received Signal Strength (RSS), Signal-to-Interference-plus-Noise Ratio (SINR), Bandwidth, then predicts the optimal transmission strategy that satisfies the required Quality of Service (QoS). This AI-driven approach enables dynamic resource allocation and improved network efficiency,

A Multilayer perceptron neural learning is types of deep learning that offers several benefits compared to many other deep-learning architectures. Its architecture is simple and efficient, enabling it to handle large amounts of input data without significant performance degradation. This capacity to manage increasing data sizes contributes to the scalability of the model, making it suitable for applications that require flexible learning capabilities.

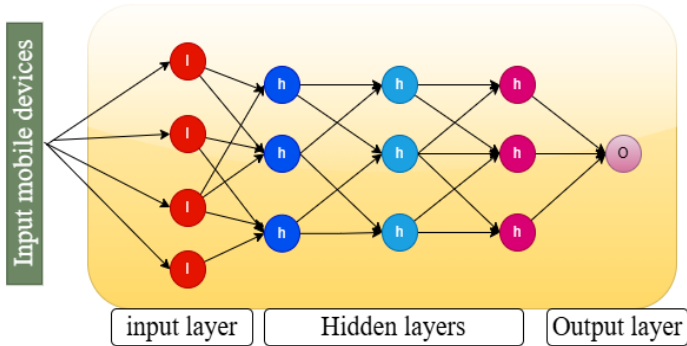


Fig.2. block diagram of the Multilayer perceptron neural learning

The Fig.2 depicts the block diagram of the Multilayer perceptron neural learning designed for accurate detection of resource efficient devices. As shown in Fig.2, the system processes input mobile devices or nodes $Mn_1, Mn_2, Mn_3, \dots, Mn_n$. The huge amount of data and the multitude of connected devices in 5G networks necessitate highly scalable solutions due to changing network conditions without compromising service quality.

The architecture of deep neural consists of three main types of layers namely the input layer, numerous hidden layers, and the output layer. The input layer accepts data from mobile devices

within the 5G network. Between the input (I) and output layer (O) are the hidden layers (h), which contain multiple neurons, or nodes, that process the information using weighted connections and activation functions. The output layer then produces the final predictions based on the patterns and transformations learned by the network. The proposed deep neural network considers the training set $\{Mn_i, Y_k\}$ where Mn_i indicates input mobile devices and Y_k indicates a result. Each neuron in the input layer receives data from the mobile devices and passes it to the hidden layer after incorporating the appropriate weights and biases. In the hidden layer, every neuron computes a weighted sum of the input.

$$X = \sum_{i=1}^n Mn_i * \omega_{ih} + B \quad (1)$$

where, X represents a weighted sum output, Mn_i indicates a mobile devices, ω_{ih} denotes a weight between neuron in input layer and hidden layer, and B denotes a bias. In the hidden layers, resources and connectivity of mobile devices is determined to perform seamless data transmission. Bandwidth is the measure of a network's ability to transmit data within a specific time frame. It is usually quantified in units such as bits per second (bps), kilobits per second (kbps), megabits per second (Mbps), or gigabits per second (Gbps).

$$Bw(Mn_i) = \left[\frac{SD(size)}{T(s)} \right] \quad (2)$$

where, $Bw(Mn_i)$ denotes a bandwidth capacity of a mobile device, SD indicates an amount of data transferred over the network (bits, bytes, kilobytes, etc.), $T(s)$ represents a time period in seconds. Received Signal Strength Indication is a measure of the power level of a radio signal received by a mobile device in a wireless network. It is typically expressed in decibels relative to one milliwatt (dBm), with higher values representing stronger signals and lower values indicating weaker signals. Received signal strength of device is computed using Friis transmission equation.

$$P_{Rx}(M_n) = P_{Tx} G_{Tx} G_{Rx} \left(\frac{\lambda}{4\pi d} \right)^2 \quad (3)$$

From Eq.(3), $P_{Rx}(M_n)$ represents a received signal strength or power, P_{Tx} denotes a transmitted power in dBm, G_{Tx} indicates a gain of the transmitting antenna, G_{Rx} indicates a receiving antenna gain, λ represents a wavelength of the signal (in meters), d represent a distance between the mobile device and base station in meter. The Signal-to-Interference-plus-Noise Ratio is a key parameter for evaluating the quality of a mobile device's connection. It measures the strength of the desired signal relative to the total power of interference from other signals and noise. It is usually expressed in decibels (dB).

$$R_{SIN} = P_{Rx}(M_n) - 10 \log_{10}(I + \mathcal{G}_N) \quad (4)$$

From Eq. (4), R_{SIN} denotes a Signal-to-Interference-plus-Noise Ratio, $P_{Rx}(M_n)$ symbolizes as received signal power of mobile device ' M_n ', ' $\mathcal{G}_N$ ' indicates a noise power, and ' I ' signifies interference power from all nearby base stations. A higher SINR indicates a more robust and stable communication link, which is essential for achieving fast data rates, minimal latency, and dependable connectivity, particularly in 5G networks. Laplace

kernel is a type of radial basis function (RBF) kernel that evaluates similarity between connectivity metrics and their corresponding threshold values.

$$\beta = \exp \left[\sum_{i=1}^n -\frac{|C_M - \delta_R|}{D} \right] \quad (5)$$

From Eq.(5), β symbolizes a Laplace kernel, C_M designates a resource metrics, δ_R designates a threshold for connectivity metrics, D symbolizes deviation. Laplace kernel function generates the output from 0 to 1. The connection quality and resources are assessed according to the output of the kernel, as described below.

$$\beta = \begin{cases} 1, & \text{better resource and connection quality} \\ 0, & \text{poor connection quality} \end{cases} \quad (6)$$

The kernel value β indicates the connection status of a mobile device. An output of 1 signifies a strong connection and efficient resource utilization, while an output of 0 indicates a weak connection and resource inefficient. A robust network connection combined with effective use of mobile device resources improves data transmission and enhances Quality of Service (QoS). When devices manage their bandwidth capabilities efficiently, data flows more reliably and quickly, supporting optimized streaming and reducing latency, and packet loss. This ensures smoother and more consistent data transmission in 5G network. A weak connection combined with inefficient use of mobile device resources negatively impacts data transmission and degrades Quality of Service (QoS). In such situations, data transfer becomes slower, delays increase, and packet loss. In order to solve this problem, a novel proportional fairness dynamic allocation method is employed for assigning bandwidth fairly among mobile devices while considering their instantaneous rates and priorities. Allocated bandwidth is formulated as

$$Bw_i = \frac{T_i}{\sum_i T_i} \quad (7)$$

where, Bw_i is the allocated bandwidth for mobile device i refers to the ratio of speed of data transfer at a specific moment in time of device i and the average is the speed of data transfer of all devices $\sum T_i$. The Proportional Fairness allocation method ensures that mobile device with higher data rates or speed receives a larger share of the available bandwidth. When a mobile device has weak signal strength, it's difficult to maintain a reliable connection with the current base station. To ensure uninterrupted and streaming data transmission, network initiates a handover, switching the device's connection to a nearby base station with a stronger signal. This process helps maintain stable communication, reduces the likelihood of interrupted data streams, and ensures consistent QoS. In this way, DAITQ- SigCrypt method achieved at the output layer of disseminative AI model to ensure the QoS aware data transmission in 5G network.

// Algorithm 1: Discriminative AI model

Input: Number of mobile devices $Mn_1, Mn_2, Mn_3, \dots, Mn_n$
streaming data $SD_1, SD_2, SD_3, \dots, SD_n$.

Output: Achieve QoS aware data transmission

Begin

1: Number of mobile devices $Mn_1, Mn_2, Mn_3, \dots, Mn_n$ given to input layer

2. **For each mobile device** Mn_i **do** --[hidden layer]

3. Compute the weighted sum using Eq.(1)

4. **End for**

5. **For each device do**

6. Compute bandwidth resources using Eq.(2)

7. Compute Received Signal Strength Indication using Eq.(3)

8. Compute Signal-to-Interference-plus-Noise Ratio using Eq.(4)

9. Measure the similarity ' β ' using Eq.(5)

10. if ($\beta=1$) then

11. Devices have better resource and strong connection quality

12. **else**

13. Devices have weak connection quality and resource inefficient

14. **End if**

15. **End for**

16. **For each resource inefficient devices do**

17. Dynamically allocate the resources using Eq.(7)

18. **End for**

19. **For each device with** weak connection quality

20. Initiates handover

21. **Switched** device from current to new base station

22. **End for**

23. Achieved QoS aware data transmission at **output layer**

End

Algorithm 1 given above describes process of discriminative AI model to QoS aware data transmission in 5G network.

3.3 TRANSIENT QUANTUM SIGNCRYPTION CRYPTOGRAPHY BASED RELIABLE DATA TRANSMISSION

During the transmission of data, DAITQ-SigCrypt method simultaneously performs the reliable data transmission to protect the data from unauthorized access. In order to achieve this contribution, Transient Quantum Signcrypton Cryptographic method is employed in DAITQ- SigCrypt method to achieve data confidentiality and integrity in 5G network data transmission. It is a public key cryptographic method that combines digital signing and encryption into a single, efficient operation thus reducing computational cost and communication overhead. This method provides better confidentiality, integrity, authentication, since it utilizes public key cryptography.

The Transient Quantum Signcrypton Cryptographic method includes four major processes namely key generation quantum key distribution, signcrypton and unsigncrypton. The process begins with key generation, where pair of transient cryptographic keys required for secure communication is created. These keys are then exchanged between the communicating parties using quantum key distribution (QKD), which utilizes the quantum properties. Once the keys are securely shared, the signcrypton phase is carried out, combining both digital signature generation and encryption in a single step. This ensures that the transmitted message remains confidential and authentic. Finally, the receiving party performs unsigncrypton, which decrypts the message and verifies the sender's identity using the cryptographic signatures. These four stages of Cryptographic model enable a reliable communication process in 5G network.

3.3.1 Transient Key Generation and Distribution:

The reliable data transmission begins the key generation process for creating cryptographic keys used to secure communication between mobile devices. In secure systems, this involves producing a pair of keys typically a public key for encryption and a private key for decryption. Advanced techniques, such as post-quantum algorithms, ensure that the keys are resistant to attacks even from powerful quantum computers. Key generation forms the foundation of secure data exchange, authentication, and confidentiality in modern communication systems. The proposed model utilizes the OU Cryptosystem for generating the Transient Key pair for each mobile device in social network. Transient keys are temporary by automatically expire after a defined duration ends. Each time the communication between the device and the base station ended, a new set of keys is created, ensuring that every session uses a fresh key pair. This approach prevents attackers from exploiting old keys and strengthens data confidentiality. The generation of these transient keys is performed using the OU Cryptosystem, which provides strong security and helps to protect sensitive information during transmission.

During the key pair generation, the two large prime numbers a and b are considered.

$$G = a^2b \quad (8)$$

$$H = R^G \bmod G \quad (9)$$

From Eq.(9), R denotes a random integer number. Using the calculated values, the system generates each device public and private keys as described below.

$$K_{BT} = (G, R, H) \quad (10)$$

$$K_{PT} = (a, b) \quad (11)$$

where, K_{BT} denotes a public transient key, K_{PT} denotes a private transient key for particular user. In this manner, a transient key pair is created for every device involved in the data-transmission process. After generating the keys, the base station securely delivers the transient key pairs to the respective devices using a quantum-based mechanism. This approach ensures that the key exchange remains confidential and protects the integrity of communications between the devices. During the key distribution, first convert input keys into the binary string.

$$B = \text{Bin}(K_{BT}, K_{PT}) \quad (12)$$

where, B denotes a binary representation of the keys K_{BT} and K_{PT} , B_{in} denotes a binary operator. Next, the input bit strings are converted into quantum bits (qubits) by applying the principle of superposition. A quantum bit, or qubit, is generally described as a linear combination of its two basis states, $|0\rangle$ and $|1\rangle$ as follows,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (13)$$

where, $|\psi\rangle$ indicates a superposition of the qubit includes two states of $|0\rangle$ and $|1\rangle$ respectively, α and β indicates probability amplitudes both are complex numbers. Generated quantum transient keys are then distributed to mobile device for reliable streaming data communication.

3.3.2 Signcryption:

Signcryption is a cryptographic technique that simultaneously performs both encryption and digital signature generation in a single operation. Block diagram of signcryption is below.

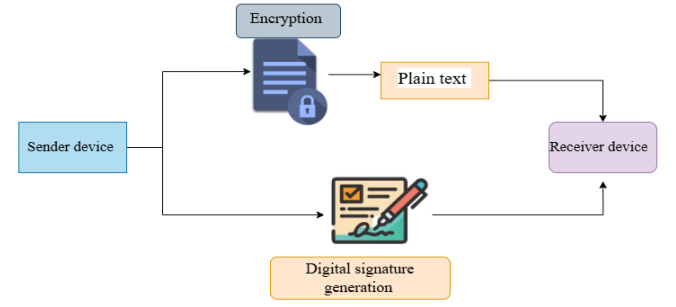


Fig.3. Block diagram of the signcryption

The Fig.3 shows block diagram of signcryption process to improve security of social media streaming data transmission in the 5G network. Let us consider social media streaming data $SD_1, SD_2, SD_3, \dots, SD_n$. First, input data is encrypted using receiver public key to get a cipher text as follows,

$$C = R^{SD} H^r \bmod G \quad (14)$$

where, C indicates a ciphertext of the streaming data ' SD ', R , r indicates a random integer number, H and G are public key of the receivers. In this way, cipher texts of the data are generated. Sequentially, the ring signature is generated through the sender's private key. The signature is generated as follows,

$$T = H(b_m, N) \quad (15)$$

$$N = S(K_{PT}, r) \quad (16)$$

$$Z = (K_{PT}, r, T) \quad (17)$$

$$\text{Sig} = (Z, T) \quad (18)$$

where, h denotes a hash generated by message digest, b_m input message bit, K_{PT} denotes a private key of the sender, r represents a unique random value for each signature, T denote a challenge value, Sig denotes a full signature generated by the particular streaming data. Finally, encrypted cipher text ' C ' and full signature ' Sig ' is sent to the receiver. Whenever, user wants to access the data from the server, they needs to verify signature and perform the decryption

3.3.3 Unsigncryption:

Unsigncryption is a significant process in secure communication systems. It allows a receiver to simultaneously achieve two processes namely retrieving the original message (decryption) and confirming the sender's identity through the signature verification. By combining these operations into a single step, unsigncryption reduces computational overhead, minimizes transmission costs, and enhances overall efficiency.

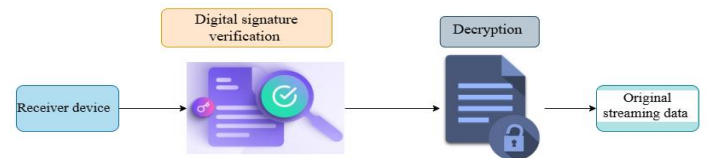


Fig.4. block diagram of the unsigncryption

The Fig.4 illustrates block diagram of unsigncryption process used to retrieve original streaming data. When a receiver access to data, they first performs signature verification to confirm integrity and authenticity of the transmitted information. Verification of this signature is carried out using ring signature algorithm. Steps involved in verification process are as follows:

$$N' = V(K_{BT}, Z, T) \quad (19)$$

$$W = \begin{cases} 0, & T \neq H(b_m, N') \\ 1, & T = H(b_m, N') \end{cases} \quad (20)$$

where, W denotes the signature verification results, V denotes verification, K_{BT} denotes public key of the participant who is verifying the signature, N' denotes a Reconstruct the N value that should match the sender's computed if the signature is valid, Z denotes a received signature component, T represents the challenge value. If the challenge value ' T ' does not match the hash value $H(b_m, N')$, then the signature is invalid, and the function ' W ' return 0. This indicates that the verification attempt has failed, meaning the signature is invalid. If the challenge value ' T ' matches the hash value $H(b_m, N')$, then the signature is valid, and the function ' W ' return 1. This result confirms that the message was legitimately signed by mobile device and has been authorized. If the user is authorized, decryption process is performed as given below,

$$x = \frac{(C^{a-1} \bmod a^2) - 1}{a} \quad (21)$$

$$y = \frac{(R^{a-1} \bmod a^2) - 1}{a} \quad (22)$$

where, C denotes a ciphertext of data, a private key of receiver. Then the new value is calculated as given below,

$$y' = y^{-1} \bmod a \quad (23)$$

Finally, the plain text (SD) is observed as given below,

$$SD = xy' \bmod a \quad (24)$$

As a result, the original plaintext is successfully recovered at the recipient's end, preventing unauthorized access and enhancing the overall security of the streaming data transmission in 5G network.

// Algorithm 2: Transient Quantum signcryption Cryptography based reliable data transmission

Input: Number of mobile devices $Mn_1, Mn_2, Mn_3, \dots, Mn_n$
streaming social data $SD_1, SD_2, SD_3, \dots, SD_n$.

Output: increase the reliable data transmission

Begin

Key generation and distribution

1: For each mobile device Mn_i do

2: Generates private ' K_{BT} ' and public key ' K_{BT} ' using Eq.(10)
Eq.(11)

3. Distributes keys based on Quantum mechanism using Eq.(13)

4. End for

// Signcryption

5. For each streaming data ' SD_j '

6. Convert original into plan text using Eq.(14)

7. Generate the digital signature ' Sig ' using Eq.(18)

8. Send ciphertext ' C ' and digital signature ' Sig ' to receiver

9. End for

// Unsigncryption

10. Verify the signature using Eq.(20)

11. if ($W=0$) then

12. The signature is invalid, and the device is considered unauthorized

13. Decryption is denied

14. else if ($W=1$) then

15. The signature is valid and the device is considered authorized

16. Decryption is allowed

17. End if

18. For each authorized device

19. Decrypt the ciphertext with receiver private key using (24)

20. Obtain original data

21. End for

End

Algorithm 2 introduces a Transient Quantum Signcryption Cryptography framework to ensure reliable transmission of streaming social data across mobile devices in 5G network.

4. SIMULATION SETUP

In this section, simulations are conducted and implemented in the NS3 network simulator for the proposed DAITQ- SigCrypt method and QDRLLA [1] and Robust and adaptive security framework [2]. To make a resalable comparison between the existing and proposed methods, the environmental setup for conducting the simulations are performed by deploying 500 mobile nodes distributed randomly in the squared area of A^2 (1100 m * 1100 m). In order to conduct the simulation, a random waypoint mobility model is used. The Ad hoc on-demand distance vector routing protocol (AODV) is used for QoS aware reliable data communication in 5G network. The simulation time is set as 100 seconds and the sensor nodes' speed is varied from 0-20m/s. In order to conduct the simulation, web-page-phishing-detection-dataset <https://www.kaggle.com/datasets/shashwatwork/web-page-phishing-detection-dataset> is used for QoS aware reliable data communication in 5G network. Dataset includes 1143 URLs and 89 features which include various social media stream data taken from Youtube, facebook, twitter and instagram. The various parameters are listed in table 1.

Table.1. Simulation Parameters

Simulation parameter	Value
Simulator	NS3
Network are	1100m * 1100m
Number of sensor nodes	500
Data packets	1000, 2000, 3000, 4000, 5000, 6000, 7000, 8000, 9000, 10000
Protocol	AODV
Simulation time	100sec
Mobility model	Random Way Point model
Nodes speed	0-20m/s
Communication range of mobile device or node	30m
Number of runs	10

4.1 SIMULATION RESULTS

This section offers a comprehensive description of the various stages of the proposed DAITQ- SigCrypt method.

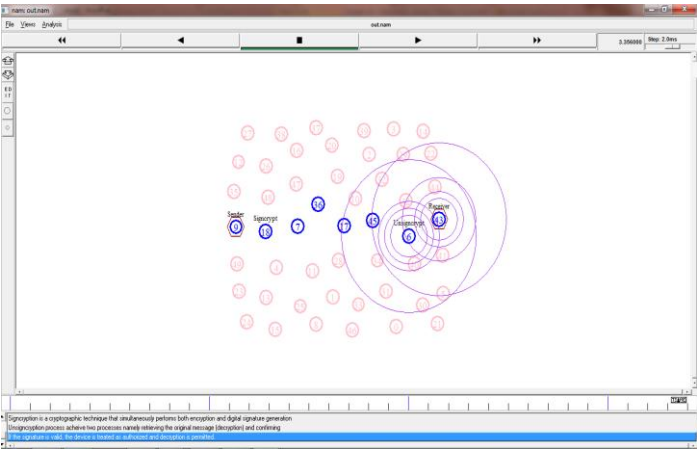


Fig.5. Data encryption and transmission

The Fig.5 illustrates process of data encryption and transmission within a secure communication system. Initially, original data or message is encrypted using receiver’s public key, converting it into ciphertext to protect it from unauthorized access during transmission. This encrypted data is then sent through the network to intended receiver. Upon receiving the ciphertext, receiver performs digital signature verification and utilizes their private key to decrypt the data. This encryption and decryption process ensures confidentiality, and integrity.

5. PERFORMANCE COMPARISON ANALYSIS

To assess the effectiveness of the proposed DAITQ- SigCrypt method, as well as the existing methods QDRLLA [1] and Robust and adaptive security framework [2] with respect to various evaluation metrics such as data delivery rate, data loss rate, throughput, latency, jitter, confidentiality rate, integrity rate. These metrics are described as given below.

5.1 Impact of Data delivery rate:

Data delivery rate represents the ratio of social data successfully received to the total number of social data sent across a 5G network within a given period. A higher delivery rate signifies that the network transmits data efficiently with minimal loss, providing reliable and stable communication.

$$DD_{rate}=(SD_{SR}/SD_{SN})*100 \tag{25}$$

where, DD_{rate} denotes a data delivery rate, SD_{SN} indicates a social data packets sent from sender, SD_{SR} data packets successfully received. Data delivery rate are measured in terms of percentage (%).

Table.2. Comparison of Data delivery rate vs. stream data samples

Stream Data Samples	Data delivery rate (%)		
	Proposed DAITQ- SigCrypt method	Existing QDRLLA [1]	Existing Robust and adaptive security framework [2]
1000	98.1	94.5	93.6
2000	98.05	94.22	93.22
3000	98.36	94.23	93.14

4000	98.02	93.74	92.85
5000	98.23	94.22	92.63
6000	98.33	93.89	92.45
7000	98.15	93.74	92.63
8000	98.32	94.08	92.44
9000	98.4	94.32	93.24
10000	98.24	94.41	93.00

The Table.2 illustrates the performance relationship between data delivery ratio and number of stream data samples. Overall, analysis indicates that DAITQ- SigCrypt method improves data packet delivery by 4% over [1] and 6% over [2], ensuring more reliable transmission between sender and receiver.

5.1 IMPACT OF DATA LOSS RATE:

Data loss rate represents the ratio of social data lost to the total number of social data sent across a 5G network within a given period. A lesser loss rate signifies that the network transmits data efficiently, providing stable communication.

$$DLR = \frac{SD_L}{SD_{SN}} * 100 \tag{26}$$

where, DLR denotes a data loss rate, SD_L indicates a social data lost, SD_{SN} denotes a number of social stream data. Data loss rate are measured in terms of percentage (%).

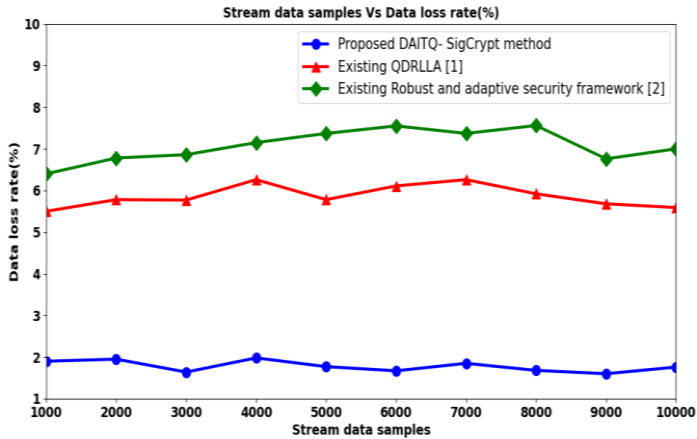


Fig.6. Graphical illustration of Data loss rate

The Fig.6 illustrates performance analysis of Data loss rate versus number of stream data samples. Average of ten comparative experiments shows DAITQ- SigCrypt method achieved improvement in loss rate, reduced by 70% and 75% over the existing approaches.

5.2 IMPACT OF THROUGHPUT

Throughput represents the amount of data successfully delivered across a network in a specified period. It is usually measured in megabits per second (Mbps), depending on the network size. Higher throughput indicates that more data is being delivered efficiently within the given time frame.

$$Throughput=[(SDD(Mb))/(time(s))] \tag{27}$$

where, SDD (Mb) denotes a successful delivery of data packets in Mb per one seconds (Mbps).

Table.3. Comparison of Throughput versus data sample size

Stream data samples size (MB)	Throughput (Mbps)		
	Proposed DAITQ-SigCrypt method	Existing QDRLLA [1]	Existing Robust and adaptive security framework [2]
100	58	41	38
200	112	88	67
300	168	125	92
400	236	198	156
500	288	233	188
600	322	285	236
700	414	325	274
800	475	426	316
900	522	455	349
1000	576	488	419

The Table.3 presents the relationship between throughput and data size, ranging from 100 MB to 1000 MB. Overall, the model outperformed existing methods by 23%, and 53%.

5.2 Impact of latency

It refers to the average time taken for a social media data transmitted from the sender to the receiver. The average of latency is measured as follows,

$$Lat = \sum_{i=1}^n SD_i \times Time(SDD) \quad (28)$$

where, Lat indicates an latency, SD symbolizes the social media stream data samples, $Time(SDD)$ denotes an actual time consumption of social media stream data delivering. It is measured in terms of milliseconds (ms).

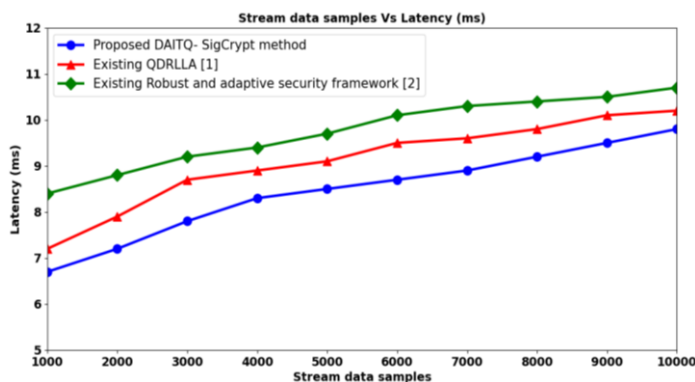


Fig.7. Graphical illustration of latency

The Fig.7 given above demonstrates graphical analysis of latency using three method. Various data samples counts were tested and results illustrate that latency is minimized using DAITQ- SigCrypt by approximately 7% and 13%, when compared to [1] - [3].

5.3 IMPACT OF JITTER

Jitter refers to the absolute difference in the time delay between data packets arriving at their receiver over a network. It

usually expressed in milliseconds (ms). Low jitter indicates that data are arriving at regular intervals in video streaming.

$$JT = |de(i) - de(i-1)| \quad (29)$$

where, JT indicates a jitter, SD symbolizes the social media stream data samples, $de(i)$ denotes a delay of i^{th} data, $de(i-1)$ denotes a delay of $(i-1)^{\text{th}}$ data. It is measured in terms of milliseconds (ms).

Table.4. Comparison of jitter versus Stream data samples

Stream data samples	Jitter (ms)		
	Proposed DAITQ-SigCrypt method	Existing QDRLLA [1]	Existing Robust and adaptive security framework [2]
1000	3.5	4.2	4.5
2000	3.8	4.6	4.9
3000	3.9	4.8	5.3
4000	4.2	5.1	5.7
5000	4.6	5.4	5.9
6000	4.7	5.6	6.1
7000	4.9	5.8	6.4
8000	5.1	6.1	6.7
9000	5.3	6.2	6.8
10000	5.5	6.4	7.1

The Table.4 presents the jitter performance of three methods namely the proposed DAITQ- SigCrypt method, QDRLLA [1] and Robust and adaptive security framework [2]. Overall, the comparative analysis demonstrates that DAITQ- SigCrypt method achieves an approximate jitter reduction of 16% and 23% relative to the existing approaches.

5.4 IMPACT OF CONFIDENTIALITY RATE

Confidentiality rate refers to the number of social media Stream data samples accessed by an authorized receiver and denied access for unauthorized devices in 5G network. The confidentiality rate is calculated as follows,

$$CFR = \sum_{i=1}^n \left(\frac{SDAAD}{SD_i} \right) \times 100 \quad (30)$$

where, CFR represent the confidentiality rate, SD denotes the number of Stream data samples, $SDAAD$ denotes a Stream data sample accessed by authorized device. It is measured in the unit of percentage (%).

The Fig.8 presents the confidentiality rate achieved by the three methods as the number of data samples increases from 1000 to 10000. Overall, the DAITQ- SigCrypt method improves confidentiality by approximately 4% over [1] and 5% over [2].

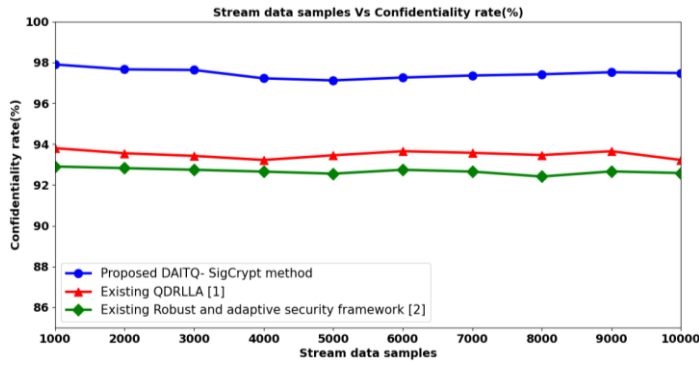


Fig.8. Graphical illustration of Confidentiality rate

5.5 IMPACT OF DATA INTEGRITY RATE

Integrity rate refers to the Stream data samples that remain unaltered or unmodified by any unauthorized or illegitimate mobile devices. Integrity rate is calculated as follows,

$$IRR = \sum_{i=1}^n \left[\frac{SDU}{SD_i} \right] \times 100 \quad (31)$$

where, IRR represent the Integrity rate, SD denotes the number of Stream data samples, SDU denotes a stream data sample unmodified by any unauthorized or illegitimate mobile devices. It is measured in the unit of percentage (%).

Table.5. Comparison of Integrity rate vs. Stream data samples

Stream data samples	Integrity rate (%)		
	Proposed DAITQ- SigCrypt method	Existing QDRLLA [1]	Existing Robust and adaptive security framework [2]
1000	97.5	93.2	92.2
2000	97.2	93.11	92.11
3000	97.15	93.06	91.89
4000	96.88	92.89	91.65
5000	96.56	92.74	91.74
6000	96.88	92.66	91.66
7000	96.45	92.87	91.87
8000	96.77	92.63	91.69
9000	96.89	92.55	91.88
10000	96.33	92.44	91.46

The Table.5 presents the integrity rate achieved by the three methods as the number of data samples increases from 1000 to 10000. Across ten comparative trials, the DAITQ- SigCrypt method demonstrated an average improvement of 4% over [1] and 5% over [2].

6. CONCLUSION

The rapid expansion of modern wireless applications has created an urgent need for communication networks that provide high QoS and reliable data transmission. However, achieving

consistent QoS and maintaining reliable data delivery remains a complex challenge due to dynamic network conditions. In order to address these challenges, a novel DAITQ- SigCrypt method is developed. The proposed DAITQ-SigCrypt method effectively integrates QoS optimization with strong security to support reliable social media streaming. By utilizing discriminative AI, the system identifies resource-efficient devices and ensures optimal data transmission performance. This process effectively enhances QoS performance metrics, including delivery ratio, loss rate, throughput, latency, and jitter. At the same time, the incorporation of Transient Quantum Signcryption Cryptography guarantees secure and accurate data delivery with high confidentiality and integrity. Experimental assessment was conducted to evaluate the performance of the DAITQ-SigCrypt method, comparing it with conventional methods using various metrics namely data delivery rate, data loss rate, throughput, latency, jitter, confidentiality rate, integrity rate. The results reveal that the proposed DAITQ-SigCrypt method technique significantly outperforms traditional methods, demonstrating notable improvements in data delivery rate, throughput, data confidentiality, and integrity. Furthermore, the DAITQ-SigCrypt method reduces loss rate, latency as well as jitter time compared to conventional approaches.

REFERENCES

- [1] Ali Parsa, Neda Moghim and Sachin Shetty, "QoS-Aware Link Adaptation for Beyond 5G Networks: A Deep Reinforcement Learning Approach", *IEEE Open Journal of the Communications Society*, Vol. 6, pp. 6368-6382, 2025.
- [2] Musaad Alruwaili, Junghwan Kim and Jared Oluoch, "Enhancing Security and Privacy in 5G Device-to-Device Communication: A Secure Gale-Shapley Algorithm Approach", *IEEE Access*, Vol. 13, pp. 30623-30635, 2025.
- [3] Mohanad Sameer Jabar, "Blockchain-Enabled Secure Data Communication Protocols for 5G Networks", *Engineering, Technology and Applied Science Research*, Vol. 15, No. 1, pp. 20151-20161, 2025.
- [4] Rafiq Ahmad Khan, Habib Ullah Khan, Hathal Salamah Alwageed, Hussein Al Hashimi and Ismail Keshta, "5G Networks Security Mitigation Model: An ANN-ISM Hybrid Approach", *IEEE Open Journal of the Communications Society*, Vol. 6, pp. 881-925, 2025.
- [5] Haider Salim Alrikabi, A. Ibtisam Aljazaery and Abdul Hadi Mohammed Alaidi, "Using a Chaotic Digital System to Generate Random Numbers for Secure Communication on 5G Networks", *Engineering, Technology and Applied Science Research*, Vol. 14, No. 2, pp. 13598-13603, 2024.
- [6] Huanhuan Lian, Burong Kang and Libao Yang, "Strongly Secure Identity-based Authenticated Key Agreement Protocol with Identity Concealment for Secure Communication in 5G Network", *IEEE Access*, Vol. 12, pp. 98611-98622, 2024.
- [7] Anichur Rahman, Md Saikat Islam Khan, Antonio Montieri, Md Jahidul Islam, Md Razaul Karim, Mahedi Hasan, Dipanjali Kundu, Mostofa Kamal Nasir and Antonio Pescape, "BlockSD-5GNet: Enhancing Security of 5G Network through Blockchain-SDN with ML-based Bandwidth Prediction", *Transaction on Emerging*

- Telecommunications Technology*, Vol. 35, No. 4, pp.1-33, 2024.
- [8] Shalitha Wijethilaka, Awaneesh Kumar Yadav, An Braeken and Madhusanka Liyanage, "Blockchain-based Secure Authentication and Authorization Framework for Robust 5G Network Slicing", *IEEE Transactions on Network and Service Management*, Vol. 21, No. 4, pp. 3988-4005, 2024.
 - [9] Samuthira Pandi, Mariya Princy Antony Saviour, B. Devisri, N. Vinoth Kumar, N. Arockia Rosy, M.D. Boomija and A. Anandh, "Revolutionizing 5G Wireless Sensor Networks: Unleashing Efficiency with Progressive Recurrent Generative Adversarial Networks Powered Routing Protocol for Seamless Data Transmission", *Results in Engineering*, Vol. 28, pp. 1-13, 2025.
 - [10] Linh Nguyen, Quoc Bao Phan and Tuy Tan Nguyen, "Highly Reliable and Secure System with Multi-Layer Parallel LDPC and Kyber for 5G Communications", *IEEE Access*, Vol. 12, pp. 157260-157271, 2024.
 - [11] Prakhar Consula, Ishan Budhirajab and Deepak Garg, "Deep Reinforcement Learning based Reliable Data Transmission Scheme for Internet of Underwater Things in 5G and Beyond Networks", *Procedia Computer Science*, Vol. 235, pp. 1752-1760, 2024.
 - [12] Mohammed Salah Abood, Hua Wang, S. Bal Virdee, Dongxuan He and Maha Fathy, "Improved 5G Network Slicing for Enhanced QoS Against Attack in SDN Environment using Deep Learning", *IET Communication*, Vol. 18, No. 13, pp. 759-777, 2024.
 - [13] Ramkumar Jayarama, Baskar Manickam, Suresh Annamalai, Manoj Kumar, Ashutosh Mishra and Rakesh Shrestha, "Effective Resource Allocation Technique to Improve QoS in 5G Wireless Network", *Electronics*, Vol. 12, No. 2, pp. 1-16, 2023.
 - [14] M. Abdullah Alashjaee, Sumit Kushwaha, Hayam Alamro, Asma Abbas Hassan, Fuhid Alanazi and Abdullah Mohamed, "Optimizing 5G Network Performance with Dynamic Resource Allocation, Robust Encryption and Quality of SERVICE (QoS) Enhancement", *PeerJ Computer Science*, Vol. 4, pp. 1-19, 2023.
 - [15] Shaik Ahmed Pasha and Noor Mohammed Vali Mohamad, "A Modified LSTM with QoS Aware Hybrid AVO Algorithm to Enhance Resource Allocation in D2D Communication", *EURASIP Journal on Wireless Communications and Networking*, Vol. 2024, pp. 1-28, 2024.
 - [16] Parsa Hassani Shariat Panahi, Amir Hossein Jalilvand and Abolfazl Diyanat, "An Efficient Network-based QoE Assessment Framework for Multimedia Networks using a Machine Learning Approach", *IEEE Open Journal of the Communications Society*, Vol. 6, pp. 1653-1669, 2024.
 - [17] Erfan Farhangi Maleki, Weibin Ma, Lena Mashayekhy and J. Humberto La Roche, "QoS-Aware Content Delivery in 5G-Enabled Edge Computing: Learning-based Approaches", *IEEE Transactions on Mobile Computing*, Vol. 23, No. 10, pp. 9324-9336, 2024.
 - [18] Le Huu Binh and T. Thuy-Van Duong, "An Improved Method of AODV Routing Protocol using Reinforcement Learning for Ensuring QoS in 5G-based Mobile Ad-Hoc Networks", *ICT Express*, Vol. 10, No. 1, pp. 97-103, 2024.
 - [19] Sanusi Mohammad Bunu, Omar Younis Alani and Mohammad Sarace, "An Improved Routing Protocol for Optimum Quality of Service in Device-to-Device and Energy Efficiency in 5G/B5G", *Future Internet*, Vol. 16, No. 9, pp. 1-31, 2024.
 - [20] Azeem Irshad and Mohammed Alreshoodi, "SEMS-5G: A Secure and Efficient Multi-Server Authentication Scheme for 5G Networks", *IEEE Access*, Vol. 12, pp. 49062-49077, 2024.
 - [21] K.B. Ajeypasaath and Vetrivelan Pandu, "Hybrid EXGBStackQoE Classifier and Stackelberg Game-Theoretic Approaches for Enhanced QoE in Video Services Over 5G Wireless Networks", *IEEE Access*, Vol. 13, pp. 70269-70281, 2021.
 - [22] Inam Ullah, Hesham El Sayed, Sumbal Malik and Manzoor Ahmed Khan, "Performance Evaluation of Quality of Experience Aware Mobility Management in Heterogeneous Cellular Networks", *IEEE Access*, Vol. 12, pp. 97994-98003, 2024.
 - [23] Muhammad Ayaz, Altaf Hussain, Tariq Hussain and Iqtidar Ali, "Optimization of Quality of Service in 5G Cellular Network by Focusing on Interference Management", *Wireless Personal Communications*, Vol. 135, pp. 2229-2254, 2024.
 - [24] Aqsa Sayed, "Intelligent Optimization of LTE and 5G Networks using AI and Machine Learning", *International Journal of Artificial Intelligence, Data Science and Machine Learning*, Vol. 6, No. 3, pp. 24-31, 2023.
 - [25] Raymond Chia, Wai Leong Pang, Swee King Phang, Hui Hwang Goh and Kah Yoong Chan, "Machine Learning-Driven Analysis of User Bandwidth Allocation and Performance in 5G Network", *IEEE Access*, Vol. 13, pp. 173081-173095, 2025.
 - [26] L. Manjunath, N. Prabakaran, S.V. Aswin Kumer, E. Mohan, Balaji Natarajan and G. Sambasivam, "QoS Aware Integrated Management Technique for 5G mmWave-based Hetnets", *IEEE Access*, Vol. 11, pp. 103394-103405, 2023.
 - [27] Abbas Al-Thaedan, Zaenab Shakir, Ahmed Yaseen Mjhoor, Ruaa Alsabah, Ali Al-Sabbagh, Fitzroy Nembhard and Monera Salah, "A Machine Learning Framework for Predicting Downlink Throughput in 4G-LTE/5G Cellular Networks", *International Journal of Information Technology*, Vol. 16, pp. 651-657, 2023.
 - [28] Arjun Ray, Manish Yadav, R. Babu Dawadi and R. Krishna Bhandari, "Game Theoretic Approach to QoS Oriented Machine Learning Model Development Toward 5G Network Migration Planning", *IEEE Access*, Vol. 13, pp. 73949-73974, 2025.
 - [29] Wael AlZoubi and Hazem Hatamleh, "Multicasting Strategies for Increasing Network Efficiency in 5G using Deep Learning", *The International Arab Journal of Information Technology*, Vol. 22, No. 2, pp. 327-345, 2025.
 - [30] Ziyu Pan and Jie Yang, "Deep Reinforcement Learning-based Optimization Method for D2D Communication Energy Efficiency in Heterogeneous Cellular Networks", *IEEE Access*, Vol. 12, pp. 140439-140455, 2024.