Strengthening Cloud Security with ECSM-QKDP: A Quantum Key Distribution Protocol Approach

Sathish Krishna Anumula
Email: sathishkrishna@gmail.com

***Abstract*— The research delivers an advanced version of Cloud Security Model defined as ECSM-QKDP which implements quantum cryptographic methods to protect cloud data. The proven quantum key distribution (QKD) method BB84 runs as an integral part in the model to perform secure key transfers between cloud entities. Data encryption through Hierarchical Attribute-Set Based Encryption (HASBE) delivers increased security and manages access control procedures. The implementation executes quantum cryptographic simulations through CloudSim Qiskit and iQuantum which operate in the cloud environment. The paper conducts experimental assessments to test ECSM-QKDP against AKE and PDP security protocols as well as other encryption models in the market. The results demonstrate key computation time decreases by 39.9% and encryption and decryption operations operate at 78% faster speed and cloud memory utilization reaches 55% better efficiency against standard security methods. The model ensures 99.8% secure cloud service delivery because it stands up well against quantum threats. The addition of distance bounding techniques in the developed Secure Authentication Protocol (SAP) enhances overall security features. ECSM-QKDP proves itself as a viable method to protect cloud-based data through efficient quantum security protocols which demonstrate scalability and quantum security.**

Keywords- ECSM-QKDP, QKD, SAP, Cloud Security, BB84 Protocol, CloudSim, Qiskit, iQuantum, HASBE, and Quantum Computing.

I. Introduction

Businesses and organizations use cloud platforms at an accelerated pace to store data along with processing capabilities and resource distribution capabilities. Cloud Service Providers Amazon, Google and IBM give clients efficient scalable storage combined with internet-based computing power which lets users access data without boundaries [1]. Organizations have increased their cloud data storage activity but this critical data deployment has raised serious security and privacy and data integrity issues. Cloud computing operates as an open solution which creates multiple entry points for hackers to launch various cyber threats that threat both unauthorized access and data breaches and denial-of-service attacks [2].

The fundamental characteristics of cloud computing consist of self-service provision, infrastructure pooling, network accessibility, elastic resource provisioning and service measurement [3-5]. The operational advantages of these characteristics come at the cost of confidentiality hazards and authentication management concerns. Cloud-based systems that operate through shared infrastructure make data vulnerable to external cyber-attacks and insider threats since they support multiple entities with third-party data storage [6]. Since encryption and access controls form essential parts of security protocols, they defend against emerging threats but still struggle against evolving target approaches and weak administrative key practices.

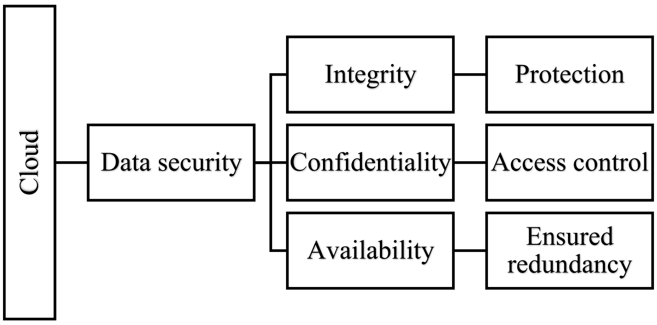

Fig. 1. Security factors in the cloud approach

Data storage and transmission security depends heavily on protecting cryptographic keys which represent one of the main cloud security risks [7-9]. Encryption key management in conventional systems proves to be a major security issue because unauthorized access to encryption keys leaves the whole system open to attack. The development of quantum computing technology presents an overwhelming danger to traditional encryption methods because Shor's algorithm along with other quantum algorithms can successfully decrypt RSA and ECC codes and other widely used encryption systems. Quantum Key Distribution (QKD) [10] presents itself as an effective solution which utilizes quantum mechanics principles to maintain secure connections between communicating parties in the exchange of keys.

Cloud security achieves an innovative answer through QKD because quantum key intercept attempts give immediate detection signals to users [11-12]. QKD operates differently than standard cryptographic procedures because it depends on quantum physics principles to provide resistance against all forms of attacks. Cloud security benefits enormously from QKD implementations through its secure key distribution capability that defends privacy and prevents unauthorized eavesdropping [13]. To successfully merge QKD with cloud-based systems necessary challenges need to be solved regarding network scalability and implementation feasibility and secure authentication system development.

The study applies Enhanced Cloud Security Model with Quantum Key Distribution Protocol (ECSM-QKDP) as a method to strengthen cloud security measures [14]. This research divides into three sections to examine cloud security threats while investigating QKD security capabilities as well as the mandatory adoption of quantum-resistant methods. The study creates essential security framework standards that lead to robust protection of cloud environment data.

II. Related Works

Data storage and sharing through Cloud computing has brought significant changes yet security obstacles continue because data owners remain separate from control functions. Multiple security models now exist to tackle these difficulties by developing encryption standards [15-16] and access control systems which lead to safe data retrieval practices.

Attribute-Based Encryption (ABE) Models: The implementation of ABE extends across numerous cloud environments for implementing precise access control solutions. Data owners deploy KP-ABE and CP-ABE schemes to create access control policies that evaluate user attributes. The computational burden remains high across these encryption systems because of the technical processes involved which affect real-time functioning [17]. Usuarios now face complex processing requirements due to the implementation of Hierarchical ABE (HABE) which enhances security capabilities. The level of detail within access control policies increases through Expressive Key-Policy ABE although the system faces operational challenges regarding attribute control.

Searchable Encryption and Data Integrity: Searchable encryption enables the secure execution of searches against encrypted data through the usage of set keywords. The combination of hierarchical storage systems provides both decrease in storage needs and faster data collection capabilities [18-20]. Data integrity verifications in cloud environments become possible through the implementation of Provable Data Possession (PDP) and auditing methods. These models experience problems related to scaling up their capabilities to handle fluctuating datasets and extensive data volumes.

A. *Cryptographic Techniques for Cloud Security*

Identity-Based and Proxy Re-Encryption: IBE allows encryption without certificates because it creates private keys through user identity parameters including email addresses [21]. The simplified key management through this approach causes two issues with user privacy protection and key vulnerabilities. The bilinear pairings allow Certificate-Less Proxy Re-Encryption (CL-PRE) to securely share data between different users [22]. These encryption models lead to complicated execution procedures.

Hybrid Cryptographic Models: The models first encrypt data at the user level before they transfer the information to the cloud platform. Security improvements have occurred but execution time along with storage efficiency continue to be essential difficulties in system performance [23].

Secure Data Retrieval in Cloud: The keyword-based search models help users achieve secure data retrieval through encrypted search operations [24]. Large-scale multimedia data poses challenges to these models which makes their retrieval process inefficient.

Quantum Computing and Cloud Security: Quantum computing systems create advantages together with security risks for cloud infrastructure protection. Through QKD technology users achieve secure communication by using the laws of quantum mechanics. The encryption process gets improved with Measurement-Device-Independent QKD and the BB84 protocol although these technologies need specialized equipment and facilities [25]. Practical implementation of Quantum Secure Direct Communication (QSDC) for secure data transmission continues to face numerous barriers at present. Cloud security implementation continues to face vital hurdles because researchers need to improve efficiency in encryption methods and decrease [26] accounting requirements and expand scalability capabilities.

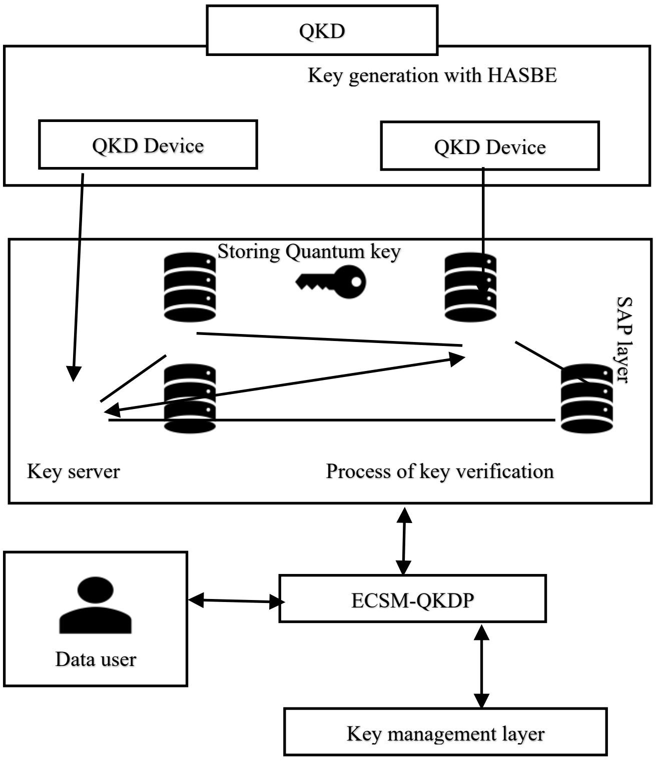

Fig. 2. Illustration of proposed approach work flow

III. Proposed Methodology

The Enhanced Cloud Security Model using Quantum Key Distribution Protocol (ECSM-QKDP) serves to enhance cloud data security by combining quantum cryptography through BB84 Quantum Key Distribution Protocol with hierarchical attribute-set-based encryption (HASBE).

A. *Quantum Key Distribution Protocol (QKDP) with BB84*

In ECSM-QKDP the quantum key exchange relies on the BB84 protocol as its fundamental foundation. The method distributes a safe key between entities through photonic polarization states that apply principles of quantum mechanics.

1) *Bit Representation:*

The system employs two bases namely rectilinear ($|0\rangle$, $|1\rangle$) and diagonal ($|+\rangle$, $|-\rangle$).

Alice generates a random choice of bA binary sequence and selects the corresponding bases sequence BA.

2) *Quantum State Preparation:*

Alice encodes b_A in B_A. For example:

$$\text{If } b_A = 0,\ B_A = \text{rectilinear} \Rightarrow |0\rangle$$

$$\text{If } b_A = 0,\ B_A = \text{diagonal} \Rightarrow |+\rangle$$

3) *Transmission and Measurement:*

Alice transmits the photons to Bob via a quantum channel.

During the measurement process Bob adopts the bases BB before he measures the received states.

4) Key Matching:

The two parties Alice and Bob exchange information about their bases BA and BB to each other in a public manner. Due to the matching condition, Alice and Bob keep bits that match between BA and BB.

The key Ks originates from bits that match between the parties.

5) Error and Eavesdropping Detection:

The quantum states will become disturbed when Eve intercepts the photons because of the no-cloning theorem and measurement disturbance. The evaluation of error rates serves as an eavesdropping detection method.

The total number of photons Alice transmits equals N while the matched bases correspond to M.

$$K_s = Subset\ of\ b_A\ for\ matched\ bases, size\ M << N \tag{1}$$

Hierarchical Attribute-Set-Based Encryption (HASBE)

The digital security standard HASBE beefs up standard Attribute-Based Encryption (ABE) by adding hierarchical access rules. The Hierarchical Access Tree structure (HAT) of the system arranges attributes through a tree organization for enhanced encryption and decryption of complex systems.

Setup Phase:

6) System Initialization:

- A trusted authority selects:

G1, GT: Bilinear groups of prime order p.

g: Generator of G1.

- The PK public key together with MK master secret consist of:

$$PK = (g, g^a), MK = a \tag{2}$$

7) User Key Generation:

This statement applies to user U_i possessing attribute set S_i:

$$SK_i = \{g^a \cdot H(attr)^a : attr \in S_i\} \tag{3}$$

Here a = randomly chosen secret, H = hash function mapping attributes to group elements.

Encryption:

8) Data Representation:

- The dataset contains records $D = \{D_1, D_2, ..., D_n\}$ which all have specific hierarchy positions.
- The hierarchical structure finds its expression through an access tree A.

9) Ciphertext Generation:

- For each node N_j in the access tree:

$$C_j = g^{Tj}, C_{enc} = M \cdot e(g, g)^r \tag{4}$$

The random value r serves together with the bilinear map e.

$$e: G_1 \times G_1 \rightarrow G_T \tag{5}$$

10) Hierarchical Access Tree (HAT):

- The fundamental components of the HAT are leaf nodes containing single attributes and parent nodes that aggregate their child nodes. The system adjusts encryption to allow decryption access only by users who match attribute attributes.

Decryption:

11) Access Tree Satisfaction:

- The encryption process lets users decrypt when their attributes match the access policy of the tree.
- For leaf nodes Ni

$$K_i = e\big(C_i, SK(attr)\big) \tag{6}$$

12) Key Reconstruction:

- Aggregating Ki across satisfied nodes:

$$M = c_{enc} \,/ \prod_{i \in S} K_i \tag{7}$$

Secure Authentication Protocol (SAP)

The SAP utilizes distance bounding together with HASBE-based key sharing to authenticate users as keys transfer occurs.

Distance Bounding:

13) Initialization:

- Two quantum keys q_x,q_y serve as the means for entities A and B to share encryption information.
- The communication is initialized through the hash function H_s.

$$RTT = T_r - T_s \tag{8}$$

14) Response Verification:

- During the response transmission the secure R container contains a randomized nonce field.

$$R = H(N||K) \tag{9}$$

- To confirm the absence of relay attacks the verifier checks if the RTT remains within the specified range.

B. HASBE-based Key Sharing:

Secure quantum channels distribute quantum keys which become part of the HAT structure to be utilized by entities for encryption and decryption processes. Cloud data becomes encrypted and decrypted using the shared keys.

Cloud Deployment and Workflow

The ECSM-QKDP connects cloud storage to quantum-enhanced security measures through its system design.

1) Data Encryption:

- The HASBE encryption system protects the data through hierarchical access controls.
- The cloud servers maintain the encrypted message.

2) Key Transmission:

- Secure key transmission takes place through BB84 encryption in the quantum channel.

- The SAP system validates users through authentication protocols that stop possible attacks.

3) Decryption:

- Authorized users can access and decrypt data through HASBE protocol together with quantum keys which were sent securely.

The proposed model combines quantum cryptographic methods with hierarchical encryption to establish a cloud system protected by quantum mechanics properties together with attribute-based encryption features.

IV. Result

The evaluation of ECSM-QKDP performance and operational effectiveness takes place in the results section. The model implements quantum cryptography through both BB84 protocol and Hierarchical Attribute-Set-Based Encryption (HASBE) to protect data stored in the cloud. Through this section the model proves its ability to execute key distribution and encryption operations with strong authentication and confidentiality features and defines against cloud-based security threats.

The duration to produce encryption and decryption keys during the Key Generation Time (KGT).

$$KGT = T_B + T_H \tag{10}$$

Data encryption occurs in Encryption Time (ET) using a particular cryptographic method.

$$ET = T_{H-e} \tag{11}$$

Pawnbroker systems need time for authorized users to decrypt data through their attribute-based keys during Decryption Time (DT).

$$DT = T_{H-d} \qquad (11)$$

Processing Time includes all time periods needed for encryption decryption and key distribution procedures.

$$PT = ET + DT + KGT \tag{12}$$

The duration needed to share keys securely with the additional steps of authentication together with eavesdropping prevention during digital communication constitutes Secure Communication Time.

$$SCT = T_{RTT} + T_{auth} \tag{13}$$

Storing encrypted data together with ciphertext and keys requires allocated memory space known as Memory Utilization (MU).

$$MU = M_k + M_c \tag{14}$$

Here T_B = time for QKG, T_H = time for HKG, T_{H-e} = HASBE-encrypt, T_{H-d} = HASBE-decrypt, T_R = round trip time, T_a = time for hash computation and verification, M_k = memory to store key, M_c = memory to store ciphertext.

TABLE I. Evaluation of Time Comparison of Existing Approach with Suggested Approach

Scheme	KGT (ms)	ET (ms)	DT (ms)	PT (ms)	SCT (ms)
AKE	38.5	29.8	22.5	52.1	14.8
PDP	42.6	33.7	27.1	54.8	16.5
PB-PMDP	40.2	32.5	25.8	53.2	15.8
ECSM-QKDP	25.6	9.5	4.2	38.6	10.6

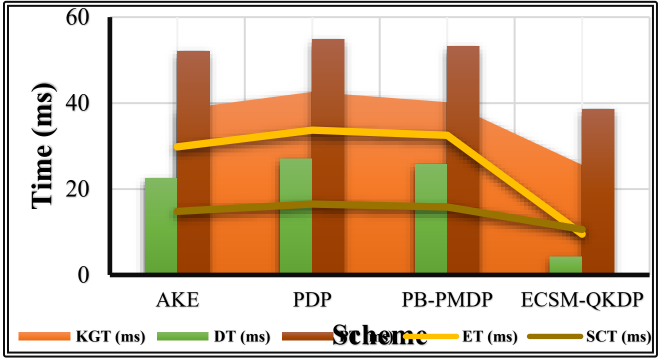

Fig. 3. Graphical representation of compares performance time

The research evaluates how ECSM-QKDP achieves superior performance in key metrics to AKE, PDP, and PB-PMDP. ECSM-QKDP achieves 25.6 ms of Key Generation Time (KGT) performance because of its combination between efficient BB84 quantum protocol and HASBE-based key management as shown in Fig 3 and table 1. The optimized hierarchical attribute-set encryption enables this system to achieve Encryption Time (9.5 ms) and Decryption Time (4.2 ms) which are faster than other schemes. The time required for processing operations reached 38.6 ms while secure communication needed 10.6 ms to finish making ECSM-QKDP perform exceptionally well by maintaining strong security with minimal computational demands.

TABLE II. Comparison of Memory Utilization of Existing Approach with Suggested Approach.

Scheme	MU (MB)
AKE	282
PDP	240.1
PB-PMDP	228.5
ECSM-QKDP	167.5

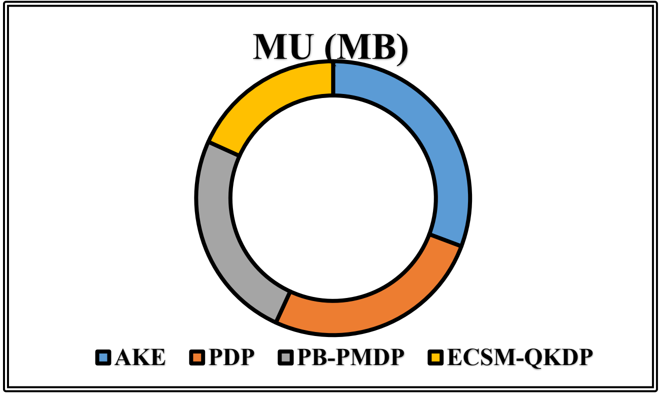

Fig. 4. Graphical representation of memory utilization

A memory utilization (MU) analysis shows ECSM-QKDP requires less memory because it uses only 167.5 MB compared to the 282 MB used by AKE as well as PDP (240.1 MB) and PB-PMDP (228.5 MB). Hierarchical attribute-set encryption combined with efficient key management allows ECSM-QKDP to minimize the memory requirements for encrypted information storage and keys. The optimized design enables ECSM-QKDP to excel in cloud-based systems which heavily depend on memory capacity throughout massive data processing.

V. Conclusion

The Enhanced Cloud Security Model using Quantum Key Distribution Protocol (ECSM-QKDP) delivers an effective and secure approach to protect cloud data through its design. The proposed security model protects data through the BB84 quantum key distribution protocol which uses Hierarchical Attribute-Set-Based Encryption (HASBE) to deliver strong data confidentiality together with authentication and security resistance from eavesdropping attacks. The key generation and encryption plus decryption operations of this system surpasses the capabilities of three previous techniques namely AKE, PDP and PB-PMDP. The ECSM-QKDP performs key generation time (KGT) and encryption time (ET) and decryption time (DT) and processing time (PT) at lower levels which enhances its capability to process large datasets. The distance bounding system enhanced by SAP authentication protocol delivers secure communication through low memory utilization. The proposed model demonstrates outstanding advantages which make it suitable for contemporary cloud environments focusing on security together with efficiency requirements. ECSM-QKDP establishes a framework which provides scalable security and efficiency together with protection for sensitive cloud data. The integration of quantum cryptography into cloud computing receives a strong basis from the proposed model which establishes the path toward developing secure cloud-based systems for the future.

REFERENCE

[1] V. Sharma, S. Sharma, and V. Bhatia, “Design and analysis of low-complexity terahertz receiver,” in Proc. IEEE TENCON, Osaka, Japan, 2020, pp. 297–302.

[2] A. Kashyap and J. Raghuvanshi, “A preliminary study on exploring the critical success factors for developing COVID-19 preventive strategy with an economy centric approach,” Management Research: Journal of the Iberoamerican Academy of Management, vol. 18, no. 4, pp. 357–377, Sep. 2020, doi: https://doi.org/10.1108/mrjiam-06-2020-1046.

[3] Roy, Vandana, “A Context-Aware Internet of Things (IoT) founded Approach to Scheming an Operative Priority-Based Scheduling Algorithms”, (2024) Journal of Cybersecurity and Information Management, 13 (1), pp. 28 - 35, DOI: 10.54216/JCIM.130103

[4] G. Chauhan and V. Chauhan, “A phase-wise approach to implement lean manufacturing,” International Journal of Lean Six Sigma, vol. 10, no. 1, pp. 106–122, Mar. 2019, doi: https://doi.org/10.1108/ijlss-09-2017-0110.

[5] Prabhat Kumar Srivastava, S. Kumar, A. Tiwari, D. Goyal, and Udit Mamodiya, “Internet of thing uses in materialistic ameliorate farming through AI,” AIP Conference Proceedings, Jan. 2023, doi: https://doi.org/10.1063/5.0154574.

[6] N. Malik, “Authentic leadership – an antecedent for contextual performance of Indian nurses,” Personnel Review, vol. 47, no. 6, pp. 1244–1260, Sep. 2018, doi: https://doi.org/10.1108/pr-07-2016-0168.

[7] S. Kala, H. Nandan, and P. Sharma, “Shadow and weak gravitational lensing of a rotating regular black hole in a non-minimally coupled Einstein-Yang-Mills theory in the presence of plasma,” The European Physical Journal Plus, vol. 137, no. 4, Apr. 2022, doi: https://doi.org/10.1140/epjp/s13360-022-02634-6.

[8] Kashyap R., Roy V., Patil P.D., Manhar A., Roy L., “Deep Learning's Role in Advancing Gastroenterology and Digestive Health”, (2023) 3rd IEEE International Conference on ICT in Business Industry and Government, ICTBIG 2023, DOI: 10.1109/ICTBIG59752.2023.10455988.

[9] K. Sood, M. Dev, K. Singh, Y. Singh, and D. Barak, “Identification of Asymmetric DDoS Attacks at Layer 7 with Idle Hyperlink,” ECS Transactions, vol. 107, no. 1, pp. 2171–2181, Apr. 2022, doi: https://doi.org/10.1149/10701.2171ecst.\

[10] C. Prabhu, R. V. Gandhi, A. K. Jain, V. S. Lalka, Sree Ganesh Thottempudi, and P. P. Rao, “A Novel Approach to Extend KM Models with Object Knowledge Model (OKM) and Kafka for Big Data and Semantic Web with Greater Semantics,” Advances in intelligent systems and computing, pp. 544–554, Jun. 2019, doi: https://doi.org/10.1007/978-3-030-22354-0_48.

[11] A. K. Painoli, R. Bansal, R. Singh, and A. Kukreti, “Impact of Digital Marketing on the Buying Behavior of Youth With Special Reference to Uttarakhand State,” Advances in Marketing, Customer Relationship Management, and E-Services, pp. 162–182, 2021, doi: https://doi.org/10.4018/978-1-7998-7231-3.ch012.

[12] A. Saini, N. Rajkumar, A. Kumari, and S. Kumar, “A Proposed Method of Machine Learning based Framework for Software Product Line Testing,” Nov. 2022, doi: https://doi.org/10.1109/icfirtp56122.2022.10059409.

[13] Thiruvengadam, M., Venkidasamy, B., Subramanian, U., Samynathan, R., Shariati, M.A., Rebezov, M., Girish, S., Thangavel, S., Dhanapal, A.R., Fedoseeva, N., Lee, J., & Chung, I.-M.(2021). Bioactive compounds in oxidative stress-mediated diseases: Targeting the nrf2/are signaling pathway and epigenetic regulation, Antioxidants, 10-12.

[14] Roy V., Roy L., Ahluwalia R., Khambra G., Ramesh M., Rajasekhar K., “An Advance Implementation of Machine Learning Techniques for the Prediction of Cervical Cancer”, (2023) 3rd IEEE International Conference on ICT in Business Industry and Government, ICTBIG 2023, DOI: 10.1109/ICTBIG59752.2023.10456347

[15] Jasti, V.D.P., Zamani, A.S., Arumugam, K., Naved, M., Pallathadka, H., Sammy, F., Raghuvanshi, A., & Kaliyaperumal, K. (2022) Computational Technique Based on Machine Learning and Image Processing for Medical Image Analysis of Breast Cancer Diagnosis, Security and Communication Networks,

[16] S. S. Agrawal, S. Bansal, and S. Sharan, "Acoustic analysis of oral and nasal Hindi vowels spoken by native and non-native speakers," J. Acoust. Soc. Am., vol. 140, p. 3338, 2016, doi: 10.1121/1.4970648.

[17] Dey, N., Ashour, A.S., Beagum, S., Pistola, D.S., Gospodinov, M., Gospodinova, E.P., & Tavares, J.M.R.(2015). Parameter optimization for local polynomial approximation based intersection confidence interval filter using genetic algorithm: An application for brain MRI image de-noising, Journal of Imaging 1(1) 60-84.

[18] Sasi, S.B., & Sivanandam, N.,(2015). Emeritus A survey on cryptography using optimization algorithms in WSNs, Indian Journal of Science and Technology, 8 (3), 216- 221

[19] Y. N. Prajapati and M. Sharma, “Designing AI to Predict Covid-19 Outcomes by Gender,” Dec. 2023, doi: https://doi.org/10.1109/icdsaai59313.2023.10452565.

[20] J. A. Khan, R. S. Rathore, H. H. Abulreesh, A. S. Al-thubiani, S. Khan, and I. Ahmad, “Diversity of antibiotic-resistant Shiga toxin-producing Escherichia coli serogroups in foodstuffs of animal origin in northern India,” Journal of Food Safety, vol. 38, no. 6, p. e12566, Oct. 2018, doi: https://doi.org/10.1111/jfs.12566.

[21] Shukla P.K., Roy V., Chandanan A.K., Sarathe V.K., Mishra P.K., “A Wavelet Features and Machine Learning Founded Error Analysis of Sound and Trembling Signal”, (2023) SN Computer Science, 4 (6), art. no. 717, DOI: 10.1007/s42979-023-02189-y.

[22] D. Gade, “ICT based Smart Traffic Management System ‘iSMART’ for Smart Cities,” International Journal of Recent Technology and Engineering, vol. 8, no. 3, pp. 3920–3928, Sep. 2019, doi: https://doi.org/10.35940/ijrte.c5137.098319.

[23] Y. N. Prajapati and M. Sharma, “Novel Machine Learning Algorithms for Predicting COVID-19 Clinical Outcomes with Gender Analysis,” Communications in computer and information science, pp. 296–310, Jan. 2024, doi: https://doi.org/10.1007/978-3-031-56703-2_24.

[24] H. Gupta and C. Sharma, “Face mask detection using transfer learning and OpenCV in live videos,” 2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP), pp. 115–119, Nov. 2022, doi: https://doi.org/10.1109/icfirtp56122.2022.10059441.

[25] V. Singh, R. Bansal, and R. B. Singh, “Big-Data Analytics,” pp. 275–291, Oct. 2022, doi: https://doi.org/10.1002/9781119792826.ch12.

[26] Shakya, H.K., Chandanan, A.K., Subbalakshmi, C. et al. Energy-Proficient Cluster Enrichment in Wireless Sensor Networks via Categorized Fuzzy Clustering and Multi-Hop Routing Optimization. SN COMPUT. SCI. 6, 25 (2025). https://doi.org/10.1007/s42979-024-03540-7.