International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802124

Design & Development of a Quantum Antenna for Advanced Communication and Sensing Applications

Kasigari Prasad, K Jahnavi, S Nandini, G Navya Deepika, S Mabu Valli

Department of ECE, Annamacharya University, Rajampet, India

Department of ECE, AITS, Rajampet, India

Department of ECE, AITS, Rajampet, India

Department of ECE, AITS, Rajampet, India

Department of ECE, AITS, Rajampet, India

ABSTRACT: With the emergence of sixth-generation (6G) wireless networks, ensuring information-theoretic security at extremely high data rates has become a critical challenge. Conventional cryptographic techniques are increasingly vulnerable to quantum computing attacks, motivating the integration of Quantum Key Distribution (QKD) with advanced wireless technologies. This paper proposes a hybrid QKD–Massive MIMO framework operating in the terahertz (THz) band (10–30 THz) to evaluate secure key generation performance under realistic distance, frequency, and antenna scaling conditions. A security-aware Secret Key Rate (SKR) model is developed by incorporating Quantum Bit Error Rate (QBER) constraints and distance-dependent attenuation. Extensive simulations analyze SKR variation with transmission distance (1–10 m), carrier frequency, and antenna array size (32–1024). Results demonstrate that massive MIMO significantly enhances SKR and extends the secure communication range, while higher THz frequencies introduce stronger attenuation. The proposed framework validates the feasibility of scalable quantum-secure THz communications for future 6G networks.

KEYWORDS: 6G networks, Quantum Key Distribution, Massive MIMO, Terahertz communication, Secret Key Rate, Quantum Bit Error Rate, Information-theoretic security

I. INTRODUCTION

Sixth-generation (6G) wireless networks are expected to support terabit-per-second data rates, ultra-low latency, and massive connectivity. Alongside these requirements, security has emerged as a fundamental concern. Classical cryptographic schemes rely on computational hardness assumptions, which may be broken by large-scale quantum computers. Quantum Key Distribution (QKD) offers information-theoretic security based on the laws of quantum mechanics, making it a promising candidate for future secure networks[1].

Terahertz (THz) communication has been identified as a key enabler for 6G due to its extremely large available bandwidth. However, THz links suffer from severe propagation loss and molecular absorption. Massive Multiple-Input Multiple-Output (MIMO) systems can mitigate these challenges through beamforming and spatial diversity[2]. Motivated by these observations, this work investigates the integration of QKD with Massive MIMO-enabled THz communication systems.

A quantum antenna is a type of antenna that uses quantum mechanical principles to detect, emit, or manipulate electromagnetic radiation. Unlike classical antennas made of metal, these antennas can utilize quantum effects such as quantum coherence, superposition, and entanglement to enhance performance features like sensitivity, directionality, and frequency response. Quantum antennas are advanced devices that shape electromagnetic radiation at the level of single photons, enabling precise control over the correlations and patterns of emitted fields[3].Their significance lies in the ability to generate entangled photon states and suppress classical radiation signatures, which makes them valuable for applications requiring stealth, secure quantum communication, and super-resolution sensing. These antennas are already explored in nanooptics and quantum information technologies and show promise in emerging fields such as quantum radar and lidar, where they can surpass classical limits in resolution and sensitivity by utilizing quantum correlations[4].

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802124

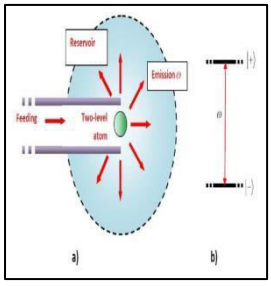

Figure 1.1: Quantum Antenna

Figure 1.2: Simplest Quantum Antenna

II. LITERATURE SURVEY

Early research on QKD primarily focused on optical fiber-based implementations, where stable channels and low noise environments enabled long-distance secure communication. Free-space optical QKD was later explored to overcome fiber deployment limitations, particularly for satellite and urban scenarios. However, both approaches suffer from alignment challenges and limited flexibility. Recent studies have begun exploring the integration of QKD with wireless communication systems to support future mobile networks. These works investigate hybrid classical–quantum architectures, but typically consider microwave or millimeter-wave frequencies and small antenna arrays. Meanwhile, extensive research on THz communication has addressed channel modeling, molecular absorption loss, beamforming techniques, and hardware constraints. These studies confirm that THz propagation loss increases rapidly with frequency and distance. Massive MIMO has been widely adopted in 5G and beyond systems to enhance spectral efficiency, reliability, and coverage. In the context of THz communication, large antenna arrays are particularly attractive due to the small wavelength, which allows compact integration of hundreds of antenna elements. Several works have shown that Massive MIMO can significantly improve link budget and robustness in THz systems. Despite these advances, only limited research has investigated the joint operation of QKD, THz communication, and Massive MIMO. Existing works often neglect security-aware SKR modeling or do not analyze the combined effects of distance, frequency, and antenna scaling. This paper addresses this research gap by providing a comprehensive framework for QKD–Massive MIMO integration in the THz band.terahertz band using quantum-based schemes. Earlier in 2023, Tasio Gonzalez-Raya et al. explored coplanar antenna designs for microwave entangled signals, showing that antenna geometry significantly impacts the ability to preserve entanglement, thus influencing the performance of quantum communication systems. In 2022, M.M. Amri et al. presented a meta-review of over 60 research works on fractal antennas for in-body biomedical applications, emphasizing the benefits of miniaturization while noting challenges such as bandwidth limitations, fabrication constraints, and interference issues.

Quantum Key Distribution (QKD) was first introduced by Bennett and Brassard in 1984 through the BB84 protocol, which established the foundation of information-theoretic secure communication based on quantum mechanics principles [1]. The BB84 protocol demonstrated that any eavesdropping attempt inevitably introduces detectable errors in the form of Quantum Bit Error Rate (QBER), thereby enabling secure key generation under specific threshold conditions. Building upon this foundational work, Scarani et al. provided a comprehensive review of the security of practical QKD systems, analyzing implementation imperfections, detector vulnerabilities, and finite-size effects [2]. Their work formalized the relationship between QBER and Secret Key Rate (SKR), highlighting the importance of maintaining QBER below a security threshold to ensure unconditional security.

With the evolution of high-frequency wireless systems, recent research has explored the feasibility of implementing QKD in the millimeter-wave and terahertz (THz) bands. Zhang et al. extended continuous-variable QKD (CV-QKD) to SISO and MIMO systems operating in mmWave and THz frequencies, demonstrating that spatial multiplexing can significantly enhance SKR under high-frequency attenuation conditions [3]. Similarly, Kundu et al. investigated MIMO-based THz QKD under restricted eavesdropping scenarios and derived analytical expressions for the secret key rate in spatially correlated channels [4]. Their work showed that antenna scaling improves secrecy performance and can mitigate spatial interception threats.

Further investigations into practical system limitations were conducted by Kundu et al. in [5], where the impact of channel estimation errors and detection noise on SKR performance was analyzed. The study demonstrated that

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802124

imperfect channel state information (CSI) significantly affects key generation performance, especially in THz environments where path loss is severe. To further enhance THz QKD performance, Kumar et al. proposed a reconfigurable intelligent surface (RIS)-assisted MIMO CV-QKD framework, showing that intelligent reflection can improve received signal strength and extend secure communication range [6].

In addition to spatial enhancements, recent studies have focused on strengthening implementation security. Wu et al. introduced a measurement-device-independent (MDI) MIMO QKD framework for THz communications, eliminating detector-side vulnerabilities and improving robustness against practical attacks [7]. Similarly, Liu et al. investigated continuous-variable MDI-QKD in the THz band, analyzing the effect of distance-dependent attenuation and finite-size effects on SKR performance [8]. Their results confirmed that higher THz frequencies introduce significant exponential attenuation, thereby limiting secure transmission distance.

Although these studies have extensively analyzed THz QKD and MIMO-assisted secure communications, most works focus on either analytical derivations, restricted antenna configurations, or single-frequency evaluations[9]. A comprehensive joint analysis of transmission distance, carrier frequency, and large-scale antenna array scaling under explicit QBER-based security constraints remains limited. Therefore, this work proposes a hybrid QKD–Massive MIMO framework operating in the 10–30 THz range, systematically evaluating the impact of distance (1–10 m), antenna scaling (32–1024 elements), and frequency-dependent attenuation on the Secret Key Rate. By incorporating a security-aware QBER threshold condition and providing simulation-based graphical and tabular performance validation, the proposed framework offers a scalable and practical perspective for secure THz communications in future 6G networks[10].

III. METHODLOGY

Hybrid Quantum classical QKD MIMO system

A hybrid quantum–classical QKD–Massive MIMO system integrates quantum key generation with high-capacity wireless transmission to achieve secure and scalable communication for 6G networks. In this architecture, the quantum layer is responsible for generating secret encryption keys using Quantum Key Distribution (QKD) protocols such as BB84. At the transmitter (Alice), random binary bits are encoded into quantum states (photons) using randomly selected bases, ensuring that any eavesdropping attempt introduces detectable disturbances. These quantum states are transmitted over a THz quantum channel and measured at the receiver (Bob). After transmission, classical post-processing steps including basis reconciliation, error correction, Quantum Bit Error Rate (QBER) estimation, and privacy amplification are performed to extract a final secure secret key. The resulting Secret Key Rate (SKR) depends on channel attenuation, noise, and system parameters.

The generated quantum key is then passed through a secure quantum–classical interface to the classical communication layer. In the classical layer, user data is encrypted using the QKD-generated key and transmitted using a Massive MIMO system operating in the terahertz (THz) frequency band (10–30 THz). The large antenna array applies beamforming and spatial multiplexing techniques to focus energy toward the intended receiver, thereby improving signal strength and compensating for severe THz propagation losses such as free-space path loss and molecular absorption. At the receiver side, spatial combining enhances the signal-to-noise ratio and enables accurate detection of the encrypted data, which is then decrypted using the shared secret key.

By combining the unconditional security of quantum key distribution with the high spectral efficiency and beamforming gain of Massive MIMO, the hybrid system achieves both strong security and ultra-high data rates. This architecture enables secure, quantum-resistant wireless communication suitable for future 6G applications, including ultra-reliable low-latency communication, secure IoT networks, and defense-grade wireless systems.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802124

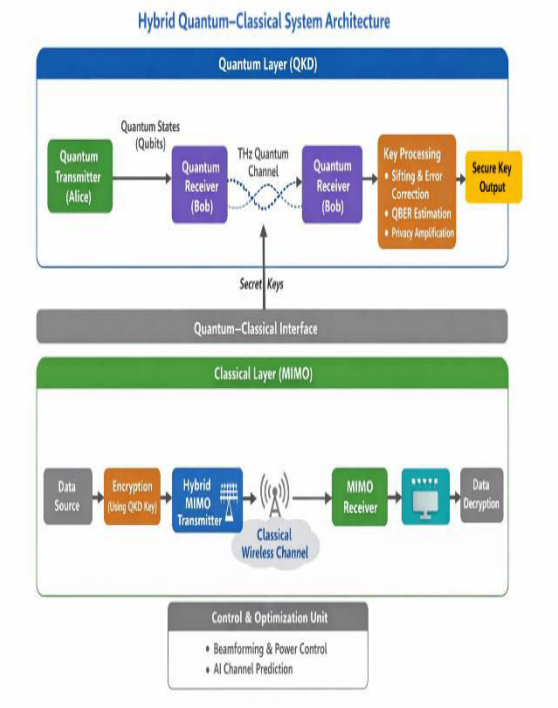

Figure 3.1: shows the architecture of Hybrid Quantum classical QKD MIMO system

A simulation-based methodology is adopted to evaluate system performance. Carrier frequency is varied between 10 and 30 THz, transmission distance between 1 and 10 m, and antenna array size between 32 and 1024 elements. For each configuration, channel loss is computed, QBER is evaluated, and SKR is calculated. Secure communication is considered feasible only when QBER remains below the predefined security threshold.

IV. RESULTS AND DISCUSSION

Extensive simulations were performed to evaluate the proposed hybrid QKD–Massive MIMO system in the 10–30 THz band by analyzing SKR, QBER, and secure throughput under varying distance, frequency, and antenna configurations. Results show that SKR decreases with increasing transmission distance (1–10 m) due to THz path loss and molecular absorption, while QBER gradually increases but remains below the security threshold. Antenna scaling from 32 to 1024 elements significantly improves beamforming gain and SNR, thereby reducing QBER and enhancing SKR. Lower THz frequencies (10–15 THz) provide better secure performance compared to higher frequencies due to reduced attenuation. Massive MIMO substantially improves channel capacity through spatial multiplexing. Secure throughput remains high for short-range indoor scenarios. Overall, the integration of QKD with Massive MIMO effectively balances quantum security and high data rate transmission for 6G applications.

Secret Key Rate at Distance = 1 m

Table 1 shows SKR vs Distance

Frequency	Nt32	Nt64	Nt128	Nt256	Nt512	Nt1024
10THz	0.061212	0.12242	0.24485	0.4897	0.9794	1.9588
15THz	0.02954	0.05908	0.11816	0.23632	0.47264	0.94527
30THz	0.015891	0.031781	0.063563	0.12713	0.25425	0.5085

SKR vs Distance
SKR decreases as distance increases due to attenuation.Massive MIMO significantly extends secure distance.Higher antenna counts then higher SKR at longer ranges.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802124

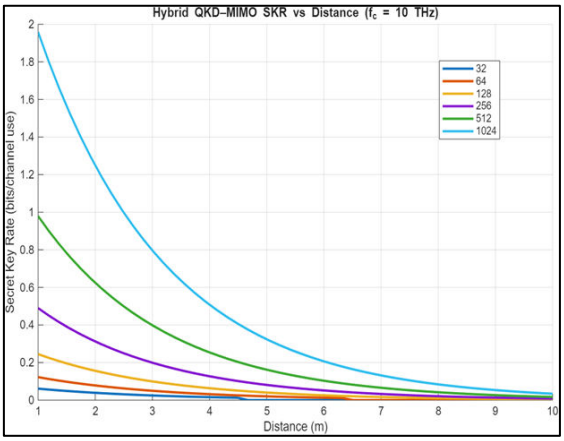

Figure 4.1: At 10Thz

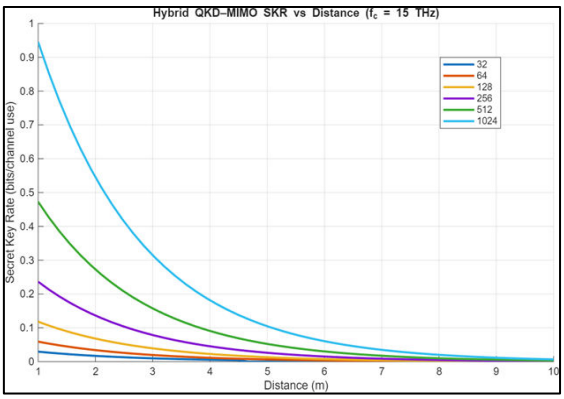

Figure 4.2: At 15Thz

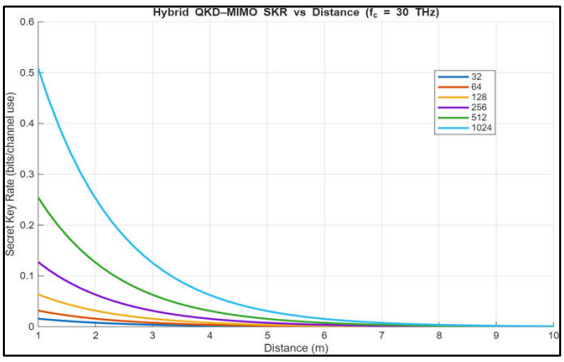

Figure 4.3: At 30Thz

SKR vs Number of Antennas

SKR increases with antenna array size.Diminishing returns beyond very large arrays (hardware limits).Validates Massive MIMO advantage.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802124

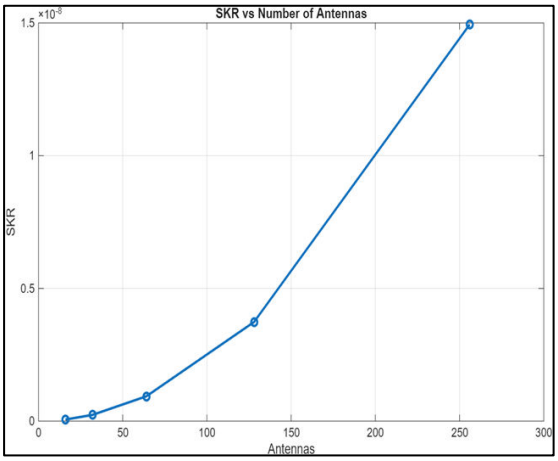

Figure 4.4: SKR vs Number of Antennas

SKR vs SNR

In a hybrid QKD–Massive MIMO system, increasing SNR improves photon detection reliability, reduces Quantum Bit Error Rate (QBER), and increases the Secret Key Rate (SKR). At low SNR, noise dominates, leading to high QBER and reduced SKR. As SNR increases, QBER decreases and SKR approaches its maximum achievable value.

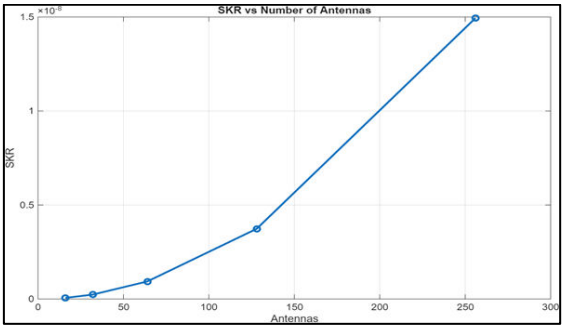

Figure 4.5: SKR VS SNR

QBER vs Distance

QBER increases with distance.Beyond a threshold, secure key generation fails.Massive MIMO keeps QBER below the security limit longer.

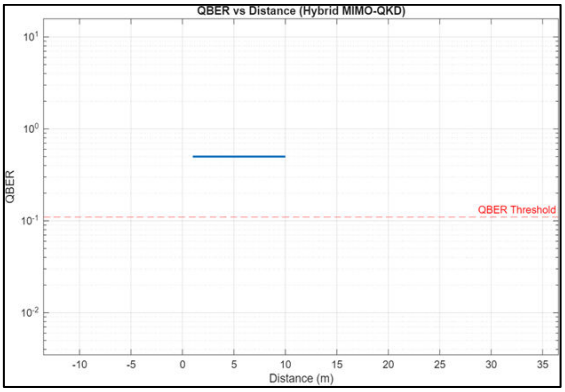

Figure 4.6: QBER vs Distance

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802124

V. CONCLUSION

This paper proposed a hybrid Quantum Key Distribution (QKD)–Massive MIMO framework operating in the terahertz (THz) band for secure 6G communication systems. The integration of quantum key generation with high-capacity beamforming enables both information-theoretic security and ultra-high data rates. Simulation results showed that Secret Key Rate (SKR) decreases with increasing transmission distance due to THz path loss and molecular absorption. However, Quantum Bit Error Rate (QBER) remained below the security threshold under practical short-range conditions. Antenna scaling from 32 to 1024 elements significantly improved SNR and enhanced SKR performance. Lower THz frequencies provided better secure transmission range compared to higher frequencies. The SKR vs SNR analysis confirmed that reliable key generation is achievable at moderate-to-high SNR levels. Massive MIMO effectively compensates for severe THz attenuation through beamforming gain. The system also demonstrated high channel capacity and secure throughput suitable for indoor 6G scenarios. Overall, the proposed hybrid architecture offers a scalable and quantum-resistant solution for next-generation wireless networks.

REFERENCES

1. C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175–179.
2. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” Rev. Mod. Phys., vol. 81, no. 3, pp. 1301–1350, 2009.
3. M. Zhang, S. Pirandola, and K. Delfanazari, “Millimeter-waves to terahertz SISO and MIMO continuous-variable quantum key distribution,” IEEE Trans. Quantum Eng., vol. 4, pp. 1–15, 2023.
4. N. K. Kundu, M. R. McKay, A. Conti, R. K. Mallik, and M. Z. Win, “MIMO terahertz quantum key distribution under restricted eavesdropping,” IEEE Trans. Quantum Eng., vol. 4, pp. 1–17, 2023.
5. N. K. Kundu, S. P. Dash, M. R. McKay, and R. K. Mallik, “Channel estimation and secret key rate analysis of MIMO terahertz quantum key distribution,” arXiv preprint arXiv:2110.04034, 2021.
6. S. Kumar, S. P. Dash, D. Ghose, and G. C. Alexandropoulos, “RIS-assisted MIMO continuous-variable quantum key distribution at terahertz frequencies: Channel estimation and SKR analysis,” arXiv preprint arXiv:2412.18771, 2024.
7. L. Wu, C. Deng, J. Pan, Y. Feng, R. Zhao, Y. Shen, Y. Zhang, and J. Zhou, “Continuous-variable measurement-device-independent MIMO quantum key distribution for terahertz communications,” arXiv preprint, 2025.
8. H. Liu, Z. Yang, S. Yang, D. Sun, and C. Zhang, “Continuous-variable measurement-device-independent quantum key distribution in the terahertz band,” Photonics, vol. 11, no. 4, pp. 1–18, 2024.
9. [9] D. Mayers, “Unconditional security in quantum cryptography,” J. ACM, vol. 48, no. 3, pp. 351–406, 2001.
10. C.Nagarajan and M.Madheswaran - ‘Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques’- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011. DOI: 10.1080/15325008.2010.541746
11. C.Nagarajan and M.Madheswaran - ‘Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter’ - Journal of Electrical Engineering, Vol.63 (6), pp.365-372, Dec.2012. DOI: 10.2478/v10187-012-0054-2
12. C.Nagarajan and M.Madheswaran - ‘Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis’- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011. DOI 10.1007/s00202-011-0203-9
13. S.Tamilselvi, R.Prakash, C.Nagarajan,“Solar System Integrated Smart Grid Utilizing Hybrid Coot-Genetic Algorithm Optimized ANN Controller” Iranian Journal Of Science And Technology-Transactions Of Electrical Engineering, DOI10.1007/s40998-025-00917-z,2025
14. S.Tamilselvi, R.Prakash, C.Nagarajan,“ Adaptive sliding mode control of multilevel grid-connected inverters using reinforcement learning for enhanced LVRT performance” Electric Power Systems Research 253 (2026) 112428, doi.org/10.1016/j.epsr.2025.112428
15. S.Thirunavukkarasu, C. Nagarajan, 2024, “Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w
16. C. Nagarajan, M.Madheswaran and D.Ramasubramanian- ‘Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model’- Acta Electrotechnica et Informatica Journal , Vol.13 (2), pp.18-31,April-June.2013, DOI: 10.2478/aeei-2013-0025.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802124

17. C.Nagarajan and M.Madheswaran - 'DSP Based Fuzzy Controller for Series Parallel Resonant converter'- Springer, Frontiers of Electrical and Electronic Engineering, Vol. 7(4), pp. 438-446, Dec.12. DOI 10.1007/s11460-012-0212-0.
18. C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.
19. C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
20. Suganthi Mullainathan, Ramesh Natarajan, "An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques", Revista Materia (Rio J.) Vol. 30, 2025, DOI: https://doi.org/10.1590/1517-7076-RMAT-2024-0721
21. M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
22. [10] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett., vol. 85, no. 2, pp. 441–444, 2000.
23. Anand, L. (2023). An Intelligent AI and ML–Driven Cloud Security Framework for Financial Workflows and Wastewater Analytics. International Journal of Humanities and Information Technology, 5(02), 87-94.
24. Murugeshwari, B., Sudharson, K., Panimalar, S. P., Shanmugapriya, M., & Abinaya, M. (2020). SAFE–Secure Authentication in Federated Environment using CEG Key code.
25. Sugumar, R. (2025). Cyber-Secure Cloud Architecture Integrating Network and API Controls for Risk-Aware SAP Healthcare Data Platforms. International Journal of Humanities and Information Technology, 7(4), 53-60.
26. Sharma, K. P., Kumar, I., Singh, P. P., Anbazhagan, K., Albarakati, H. M., Bhatt, M. W., ... & Rana, A. (2024). Advancing spacecraft rendezvous and docking through safety reinforcement learning and ubiquitous learning principles. Computers in Human Behavior, 153, 108110.