Blockchain-Enabled Security for Distributed Cyber-Physical Systems Using Practical Byzantine Fault Tolerance (PBFT)

[1]Mr.Sidharth Sharma

[1]*Vice President – IT Projects/Audits, JP Morgan Chase. Inc, 545 Washington Blvd Jersey City, NJ 07310 – US.*

Abstract. Distributed Cyber-Physical Systems (DCPS) are increasingly vulnerable to security threats due to their complex, interconnected nature. Traditional security mechanisms struggle to ensure trust, integrity, and resilience against malicious attacks and system failures. Blockchain technology, with its decentralized and immutable ledger, offers a promising solution to enhance security in DCPS. This paper explores the integration of blockchain with Practical Byzantine Fault Tolerance (BFT) to address security challenges in DCPS. PBFT consensus mechanisms enable systems to function reliably even in the presence of malicious nodes, ensuring fault tolerance and data integrity. By leveraging blockchain and BFT, this approach mitigates single points of failure, enhances trust among distributed components, and secures communication against cyber threats. This paper presents a detailed analysis of blockchain-based PBFT models for DCPS security, evaluating their performance, scalability, and resilience. The findings demonstrate that integrating blockchain with PBFT enhances system reliability, improves data authenticity, and strengthens overall cybersecurity in DCPS environments.

Keywords. Blockchain, Distributed Cyber-Physical Systems (DCPS), Practical Byzantine Fault Tolerance (PBFT), Practical Byzantine Fault Tolerance (PBFT), Consensus Mechanisms, Cybersecurity, Fault Tolerance, Decentralized Security, Smart Grids, Industrial Automation, Secure Communication, Data Integrity, Resilience, Tamper-Resistant Ledger, Trustless Networks.

1. INTRODUCTION

Distributed Cyber-Physical Systems (DCPS) are critical infrastructures that integrate computational and physical processes, enabling real-time monitoring, control, and automation across various domains such as smart grids, industrial automation, healthcare, and autonomous transportation. As these systems grow in scale and complexity, they become increasingly vulnerable to cyber threats, data tampering, and system failures. Ensuring security, integrity, and resilience in DCPS is paramount to maintaining reliable operations and preventing malicious attacks. Traditional security measures, such as cryptographic techniques and centralized authentication, often fail to address the challenges posed by distributed environments. A single point of failure in centralized security models can compromise the entire system, making it susceptible to adversarial attacks. To overcome these limitations, blockchain technology emerges as a promising solution due to its decentralized, transparent, and tamper-resistant nature. By leveraging blockchain, DCPS can achieve enhanced data integrity, secure communication, and improved trust among distributed components. However, achieving consensus in distributed networks while ensuring security and fault tolerance remains a significant challenge. Practical Byzantine Fault Tolerance (BFT) techniques provide a robust mechanism to maintain system reliability even when a portion of the network behaves maliciously or fails. Practical BFT-based consensus protocols enable DCPS to operate securely by mitigating threats such as Sybil attacks, data manipulation, and node failures. When combined with blockchain, Practical BFT enhances the security and fault tolerance of distributed systems by ensuring consensus is reached even in adversarial environments.

This paper explores the integration of blockchain with Practical BFT techniques to enhance security in DCPS. It analyzes different Practical BFT-based consensus mechanisms, their applicability in blockchain networks, and their impact on the performance and security of DCPS. The proposed approach aims to strengthen system resilience, prevent unauthorized access, and ensure secure communication among distributed entities. The rest of the paper discusses the architecture, implementation challenges, and potential improvements in utilizing blockchain with BFT for securing DCPS.

2. LITERATURE SURVEY

The evolution of BFT consensus algorithms has been pivotal in addressing the security and reliability challenges of DCPS. Zhong et al. (2023) provide a comprehensive survey of BFT consensus algorithms, analyzing their performance and applicability in distributed systems. Their work categorizes various Practical BFT protocols and discusses their strengths and limitations, offering insights into selecting appropriate algorithms for specific applications.

Similarly, Zhang et al. (2022) present an in-depth review of BFT consensus mechanisms, focusing on their role in achieving consensus in adversarial environments. They dissect the components of each algorithm, providing a qualitative comparison that aids in understanding their operational intricacies and suitability for different DCPS scenarios

The integration of blockchain with Practical BFT has been proposed as a solution to bolster the security and resilience of DCPS. A recent study introduces a credit-driven practical Byzantine Fault Tolerance consensus algorithm tailored for sustainable 6G communication networks. This approach aims to enhance the reliability and security of DCPS by incorporating a reputation-based system that mitigates the impact of malicious nodes

Gandhi et al. (2021) propose REBOUND, an algorithm designed to defend distributed systems against attacks through bounded-time recovery. REBOUND emphasizes rapid system recovery and reconfiguration in the presence of Byzantine faults, ensuring minimal disruption to DCPS operations.

Wu et al. (2024) explore the development and principles of distributed fault-tolerant consensus before and after the advent of blockchain technology. Their work offers a historical perspective and examines the driving needs for future BFT research, shedding light on the evolution of consensus mechanisms in distributed systems.

3. PROPOSED SYSTEM

Tolerance: The blockchain system can withstand the presence of up to one-third of malicious or faulty nodes within the network while still successfully achieving consensus among the remaining honest nodes. This strong fault tolerance property is a fundamental security guarantee of the blockchain, ensuring the overall system can continue to operate reliably and consistently even in the face of a significant portion of compromised participants. Tamper-Resistant Ledger: Blockchain technology utilizes cryptographic techniques and an immutable, distributed data structure to rigorously ensure the integrity and security of the recorded data. The decentralized, peer-to-peer nature of the blockchain network makes it highly resistant to tampering, as any attempt to modify the ledger would require the consensus of the majority of nodes in the network. This tamper-resistant property is a fundamental strength of the blockchain, providing a reliable and trustworthy system for the secure storage and transfer of information. Intrusion Detection and Mitigation: Advanced anomaly detection techniques utilizing machine learning algorithms protect the system against malicious attacks such as Sybil impersonations, replay attempts, and data tampering.

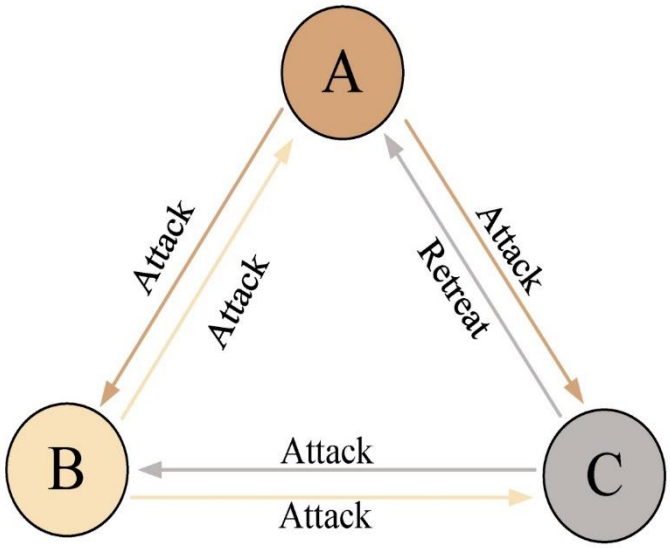

FIGURE 1. Schematic diagram for Practical Byzantine Fault Tolerance (PBFT)

$$m_l = \begin{cases} 2k+1, & \text{if } N(t) = 3k \text{ or } N(t) = 3k+1, \\ 2k+2, & \text{if } N(t) = 3k+2. \end{cases}$$

$$k_l = \begin{cases} k, & \text{if } N(t) = 3k, \\ k+1, & \text{if } N(t) = 3k+1 \text{ or } N(t) = 3k+2. \end{cases}$$

$$\Theta = \{(l,0,0) \mid 0 \le l \le 3L-1\} \cup \left(\bigcup_{k=L}^{N} \text{Level } k \right).$$

Algorithm : Byzantine Fault Tolerance (PBFT).

Step 1. INPUT: Client (C) sends a request M to Primary (P0) to enable service operation

Step 2. P0 multicast the Pre-Prepare messages to all Replicas/nodes

Step 3. All Replicas send Prepare messages

Step 4. All nodes send Commit messages

Step 5. All nodes send Reply messages to C

Step 6. OUTPUT: C waits for an f + 1 Reply messages

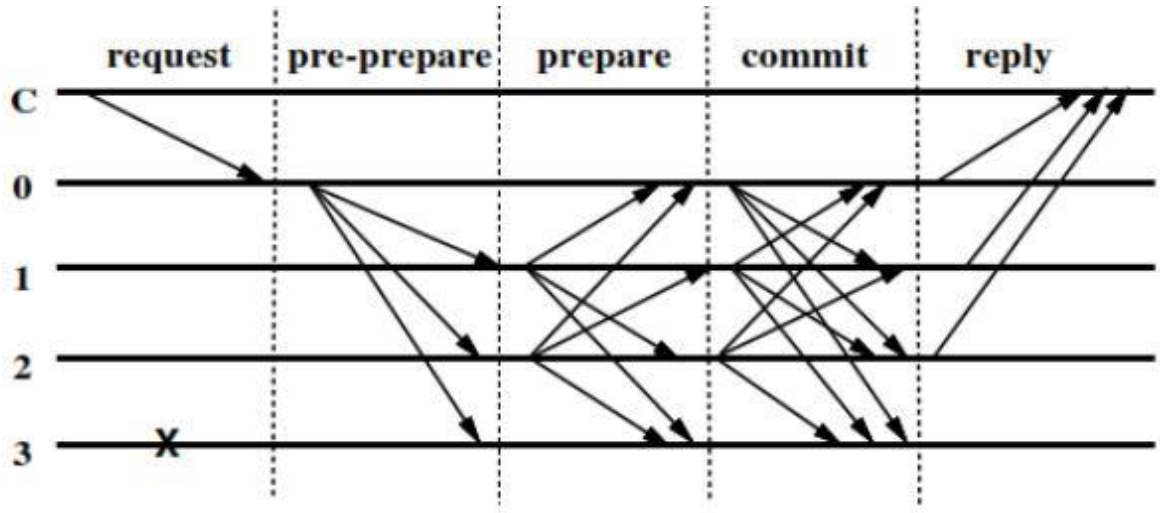

FIGURE 2. PBFT Consensus Algorithm

To enhance blockchain scalability, two key factors must be considered: network structure and blockchain protocol. The most promising approach utilizes two-layer network architecture. In terms of blockchain scaling solutions, they can be categorized into two groups: on-chain and off-chain. On-chain solutions involve modifying the blockchain protocols, such as implementing sharding and increasing block size. Off-chain solutions, on the other hand, are built upon blockchain protocols and involve processing certain transactions externally while only recording the significant ones on the blockchain.

- **Performance Analysis for the Dynamic PBFT Consensus Process**
  In this section, we first derive the stationary probability vector of the QBD process as applied to the PBFT-based blockchain consensus. Then, we analyze the performance of the dynamic PBFT voting process to evaluate its efficiency in securing distributed cyber-physical systems.
- **The Stationary Probability Vector**
  The QBD (Quasi-Birth-Death) process used in modeling the PBFT consensus mechanism is irreducible and contains a finite number of states, ensuring it is positive recurrent. Let π be the stationary probability vector of the QBD process Q. Based on Figures 1 to 4, we represent the stationary probability vector as follows:

$$\pi=(\pi 0,\pi 3L,\pi 3L+1,\ldots,\pi 3N+2)$$

where:

$$\pi 0=(\pi 0,0,0,\pi 1,0,0,\ldots,\pi 3L-1,0,0) \quad (1)$$

$$\pi 3N+2=(\pi 3N+2,0,0,\pi 3N+2,0,1,\ldots,\pi 3N+2,3N+2,0) \quad (2)$$

To compute $\boldsymbol{\pi}$, we solve:

$$\pi Q=0,\ \pi e=1$$

Using UL-type RG-factorization, we define:

$$Uk=Q(k)1+Q(k)0-Uk+1-1Q(k+1)2,3L\leq k\leq 3N+1 \quad (3)$$

From this, we derive the R-measure:

$$Rk=-Q(k)0(Q(k+1)1+Rk+1Q(k+2)2)-1,3L\leq k\leq 3N \quad (4)$$

Similarly, the G-measure follows:

$$Gk=-Uk-1Q(k)2,3L\leq k\leq 3N+2 \quad (5)$$

These equations define the stationary behavior of PBFT consensus in securing distributed cyber-physical systems.

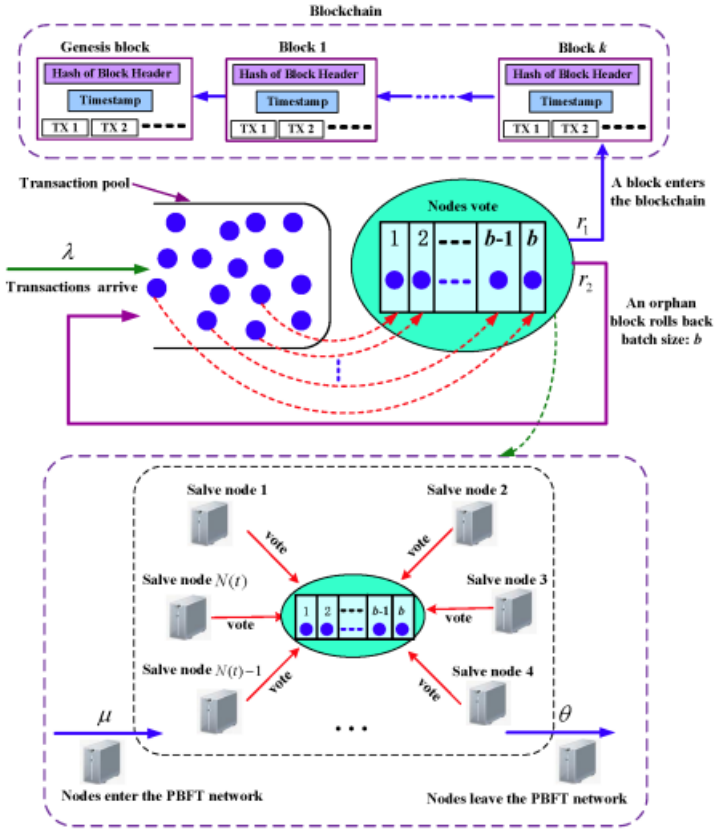

FIGURE 3. The M ⊕ Mb/Mb/1 queue and its dynamic PBFT blockchain system.

Analysis of the M ⊕ Mb /Mb /1 queue Now, we analyze the M ⊕ Mb/Mb/1 queue. It is easy to see that {I(t) : t ≥ 0} is a continuous-time Markov process whose state space is given by Ω = {0, 1, 2, . . . , b − 1, b, b + 1, b + 2, . . .} . Also, the state transition relations of the Markov process {I(t) : t ≥ 0} are depicted as follows.

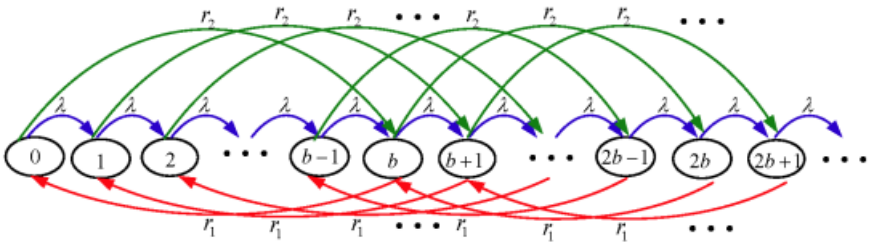

FIGURE 4. The state transition relations of the Markov process.

4. NUMERICAL ANALYSIS

In this section, we use two groups of numerical examples to verify the validity of our theoretical results and to show how some key system parameters influence performance measures of the dynamic PBFT voting process and its dynamic blockchain system. Group one: The dynamic PBFT voting process Now, we are going to observe the impact of the key parameters μ, θ, γ, p, β on the performance measures of the dynamic PBFT voting process. In Figure 7(a), we take the parameters as follows: θ = 2, β = 2, γ = 10, p ∈ [0.4, 0.7] and μ = 1.85, 2, 2.5. In Figure 7(b), we take the parameters as follows: μ = 2, β = 2, γ = 10, p ∈ [0.3, 0.75], and θ = 2, 2.5, 3

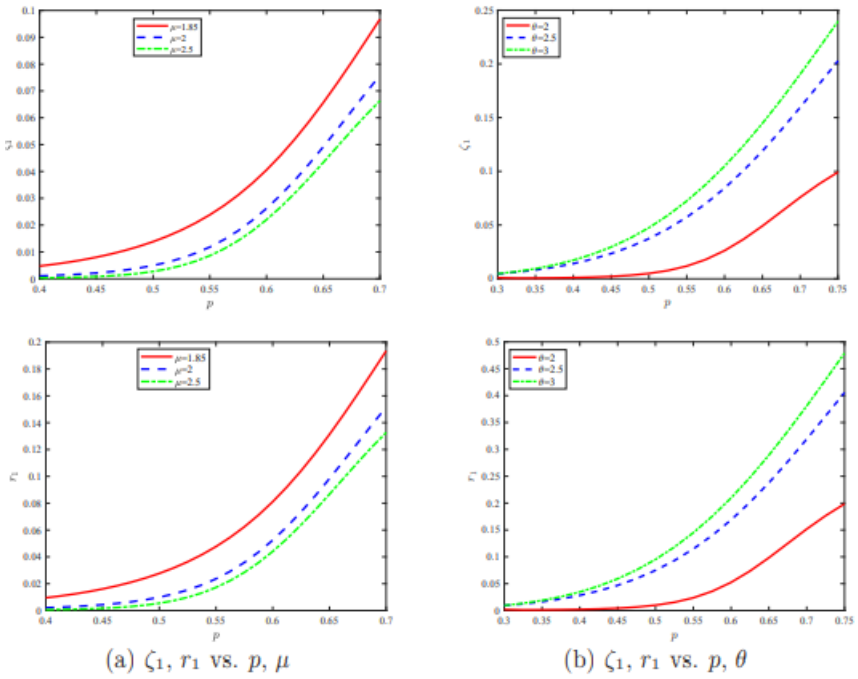

FIGURE 5. Two performance measures ζ1 and r1 vs. three parameters p, μ, and θ.

It is seen that all ζ1 and r1 increase as p increases, which indicates that the stationary probability ζ1 (or rate r1) that a transaction package becomes a block can increase as the probability p that a transaction package is approved by each node increases. In addition, we can observe that ζ1 and r1 decrease as μ increases in Figure 7(a); while ζ1 and r1 increase as θ increases in Figure 5(b). These numerical results indicate that as μ increases, more and more external nodes enter the dynamic PBFT network, such that the stationary probability ζ1 (or rate r1) that a transaction package becomes a block can decrease; while as θ increases, more and more external nodes leave the dynamic PBFT network, such that the stationary probability ζ1 (or rate r1) that a transaction package becomes a block can increase. This shows that the number of votable nodes in the dynamic PBFT network significantly affects the stationary probability ζ1 (or rate r1) that a transaction package becomes a block. Thus, they are consistent with our intuitive understanding.

5. RESULTS AND DISCUSSIONS

The X-axis represents the growing number of nodes in the blockchain network. The left Y-axis shows that the number of consensus or D messages increases gradually with the number of nodes for both Practical Byzantine Fault Tolerance and Decentralized Lightweight Byzantine Fault Tolerance consensus protocols. However, the DLBFT consensus requires significantly more D messages compared to PBFT, following a similar increasing trend. This suggests that the DLBFT protocol generates a substantially higher message overhead as the network size scales up. The right Y-axis depicts the percentage difference in the number of D messages between DLBFT and PBFT. This difference starts at 87.5% for smaller networks and steadily increases, reaching around 90% for the largest network size examined. This indicates that DLBFT consistently requires nearly double the number of consensus messages compared to PBFT, with the relative difference growing as the number of nodes increases. The higher message overhead of DLBFT compared to PBFT has important implications for blockchain scalability. As the network expands, the DLBFT protocol will generate a significantly larger volume of consensus-related traffic, potentially leading to higher latency, bandwidth consumption, and energy expenditure. This tradeoff should be carefully considered when selecting a consensus mechanism for large-scale blockchain deployments. For the BFT algorithm, the number of messages exchanged is 364 for a peer-to-peer single-layer node structure with 13 nodes, increasing to 47,124 messages for 153 nodes, whereas for the DLBFT algorithm, the number of exchanged messages starts at 157—for a double-layer network structure with 13 nodes—and increases to 4602 messages for 153 nodes

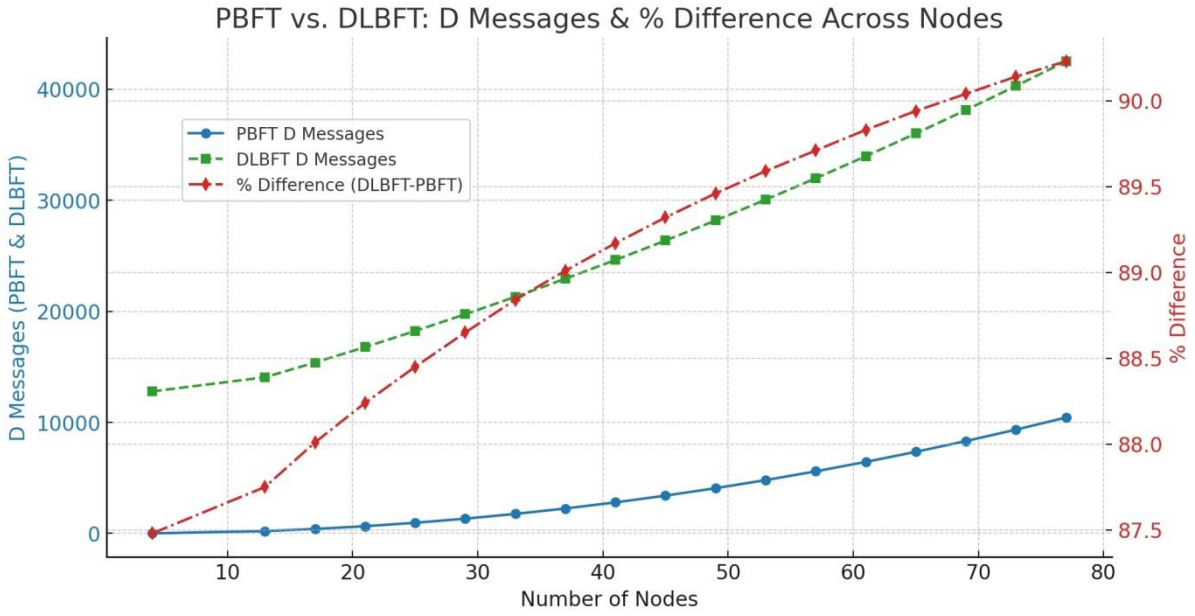

FIGURE 6. PBFT VS DLBFT Difference Across Nodes

6. CONCLUSION

The proposed blockchain-integrated Byzantine Fault-Tolerant framework enhances the security, scalability, and fault tolerance of DCPS. While PBFT remains a viable solution for small-scale networks, DLBFT's trade-off between security and communication complexity must be carefully evaluated for large-scale, real-time applications. Future research should focus on optimizing consensus mechanisms to balance security, efficiency, and scalability in cyber-physical infrastructures.

REFERENCES

1. Jasper Gnana Chandran, J., Karthick, R., Rajagopal, R., & Meenalochini, P. (2023). Dual-channel capsule generative adversarial network optimized with golden eagle optimization for pediatric bone age assessment from hand X-ray image. *International Journal of Pattern Recognition and Artificial Intelligence*, *37*(02), 2354001.
2. Karthick, R., Prabha, M., Sabapathy, S. R., Jiju, D., & Selvan, R. S. (2023, October). Inspired by social-spider behavior for microwave filter optimization, swarm optimization algorithm. In *2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS)* (Vol. 1, pp. 1-4). IEEE.
3. Vijayalakshmi, S., Sivaraman, P. R., Karthick, R., & Ali, A. N. (2020, September). Implementation of a new Bi-Directional Switch multilevel Inverter for the reduction of harmonics. In *IOP Conference Series: Materials Science and Engineering* (Vol. 937, No. 1, p. 012026). IOP Publishing.
4. Kiruthiga, B., Karthick, R., Manju, I., & Kondreddi, K. (2024). Optimizing harmonic mitigation for smooth integration of renewable energy: A novel approach using atomic orbital search and feedback artificial tree control. *Protection and Control of Modern Power Systems*, *9*(4), 160-176.
5. Sulthan Alikhan, J., Miruna Joe Amali, S., & Karthick, R. (2024). Deep Siamese domain adaptation convolutional neural network-based quaternion fractional order Meixner moments fostered big data analytical method for enhancing cloud data security. *Network: Computation in Neural Systems*, 1-28.
6. Sakthi, P., Bhavani, R., Arulselvam, D., Karthick, R., Selvakumar, S., & Sudhakar, M. (2022, September). Energy efficient cluster head selection and routing protocol for WSN. In *AIP Conference Proceedings* (Vol. 2518, No. 1). AIP Publishing.
7. Aravindaguru, I., Arulselvam, D., Kanagavalli, N., Ramkumar, V., & Karthick, R. (2022, September). Space cloud in cubesat-Consigning expert system to space. In *AIP Conference Proceedings* (Vol. 2518, No. 1). AIP Publishing.

8. Karthick, R., Prabaharan, A. M., & Selvaprasanth, P. (2019). A Dumb-Bell shaped damper with magnetic absorber using ferrofluids. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*.
9. Selvan, R. S., Wahidabanu, R. S. D., Karthick, B., Sriram, M., & Karthick, R. (2020). Development of Secure Transport System Using VANET. *TEM (H-Index)*, *82*.
10. Karthick, R., & Sundararajan, M. (2018). Optimization of MIMO Channels Using an Adaptive LPC Method. *International Journal of Pure and Applied Mathematics*, *118*(10), 131-135.
11. Lopez, S., Sarada, V., Praveen, R. V. S., Pandey, A., Khuntia, M., & Haralayya, D. B. (2024). Artificial intelligence challenges and role for sustainable education in india: Problems and prospects. *Sandeep Lopez, Vani Sarada, RVS Praveen, Anita Pandey, Monalisa Khuntia, Bhadrappa Haralayya (2024) Artificial Intelligence Challenges and Role for Sustainable Education in India: Problems and Prospects. Library Progress International*, *44*(3), 18261-18271.
12. Kumar, N., Kurkute, S. L., Kalpana, V., Karuppannan, A., Praveen, R. V. S., & Mishra, S. (2024, August). Modelling and Evaluation of Li-ion Battery Performance Based on the Electric Vehicle Tiled Tests using Kalman Filter-GBDT Approach. In *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)* (pp. 1-6). IEEE.
13. Sharma, S., Vij, S., Praveen, R. V. S., Srinivasan, S., Yadav, D. K., & VS, R. K. (2024, October). Stress Prediction in Higher Education Students Using Psychometric Assessments and AOA-CNN-XGBoost Models. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1631-1636). IEEE.
14. Yamuna, V., Praveen, R. V. S., Sathya, R., Dhivva, M., Lidiya, R., & Sowmiya, P. (2024, October). Integrating AI for Improved Brain Tumor Detection and Classification. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1603-1609). IEEE.
15. Anuprathibha, T., Praveen, R. V. S., Jayanth, H., Sukumar, P., Suganthi, G., & Ravichandran, T. (2024, October). Enhancing Fake Review Detection: A Hierarchical Graph Attention Network Approach Using Text and Ratings. In *2024 Global Conference on Communications and Information Technologies (GCCIT)* (pp. 1-5). IEEE.