

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 11 ISSUE : 06 Print / Issue Publication Date: October 2026

ISSN : 2455-2143

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 06, ISSN No. 2455-2143, Pages 09-14
Published Online October 2026 in IJEAST (http://www.ijeast.com)

DECENTRALIZED CYBERSECURITY INTELLIGENT NODE BASEDSYSTEM USING BLOCKCHAIN TRANSFER LEARNING AND SNOWABLATION OPTIMIZED ALGORITHM

Dr. V. Shoba
Assistant Professor/ Computer Applications and Technology
SRM Arts and Science College,
Kattankulathur-603 203

Dr. D. Bhuvaneswari
Assistant Professor/ Computer Science
SRM Arts and Science College,
Kattankulathur-603 203

Abstract: **Critical infrastructures are increasingly exposed to advanced cyberattacks, creating an urgent need for secure and intelligent defence systems. This research proposes an intelligent blockchain-driven, node-centric cybersecurity architecture that integrates transfer learningwith Snow Ablation Optimization Algorithm (SAOA)–optimized XG Boost and Light GBMmodels. Transfer learning enables effective knowledge reuse from pre-trained models toimprove cyber threat detection across distributed nodes, while SAOA optimizes modelparameters to enhance accuracy, stability, and robustness. Blockchain technology ensures secure, transparent, and tamper-resistant data sharing among network nodes.**

The proposedframework analyses network behaviour, predicts attack patterns, and identifies vulnerablenodes, enabling timely and proactive mitigation actions. Experimental results on simulatedcritical infrastructure environments, including energy and transportation systems, demonstratesignificant improvements in detection accuracy, response time, and system reliability compared to conventional cybersecurity approaches. The proposed architecture offers a scalable andadaptive solution for protecting critical systems against evolving cyber threats by combining blockchain, machine learning, and optimization techniques.

Keywords: **Transfer Learning, Snow Ablation Optimization, XG Boost, Light GBM, Intrusion Detection, Threat Analysis, Distributed Ledger, Network Security and CyberSecurity**.

I. INTRODUCTION

The project focuses on designing an intelligent and decentralized cyber attack defence framework for critical infrastructure networks. Each network node functions as an independent blockchain participant capable of detecting, learning, and sharing attack-related knowledgesecurely. Advanced machine learning models such as XG Boost and Light GBM are deployedat the node level for intrusion detection.To handle evolving and unseen attacks, transfer learning is employed to propagate learnedknowledge across nodes, reducing the need for complete retraining. Additionally, the SnowAblation Optimization Algorithm is applied to optimize hyperparameters and feature weights dynamically for each node, ensuring adaptive learning and improved detection accuracy. Theframework is validated using the NSL-KDD dataset, simulating real-world network trafficscenarios in critical infrastructures.

1.1 EXISTING SYSTEM

Existing cyberattack detection systems in critical infrastructures primarily relyon centralized intrusion detection systems (IDS) and static rule-based or single-modelmachine learning approaches. These systems typically process network traffic data at a centralserver, where decisions are made and alerts are generated.

- Signature-based IDS (e.g., Snort, Suricata): These systems compare network trafficagainst a database of known attack signatures. While fast and accurate for knownthreats, they completely fail against zero-day attacks or novel variants. In criticalinfrastructures, where new malware can be custom-designed, signature updates takedays or weeks.

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 06, ISSN No. 2455-2143, Pages 09-14
Published Online October 2026 in IJEAST (http://www.ijeast.com)

- Centralized Machine Learning IDS: A central server collects logs from all nodes, trains a model (e.g., Random Forest, SVM, or single XGBoost), and pushes predictions back. This approach suffers from high latency, single point of failure, and data privacyconcerns.
- Single-Model per Node: Some distributed approaches deploy the same static modelon each node. However, network traffic patterns vary significantly across nodes (e.g., asubstation vs. a control room), leading to poor performance on heterogeneous data.

1.2 PROPOSED SYSTEM

The proposed system introduces a blockchain-enabled, decentralized cyber defense framework enhanced with optimized transfer learning and ensemble machine learningtechniques.SAOA is a novel metaheuristic inspired by the natural process of snow ablation—thegradual melting and removal of snow layers. In optimization terms:

- Exploration Phase (Snow Accumulation): Agents search widely across the hyperparameter space, mimicking random snowfall.
- Exploitation Phase (Ablation/Melting): Agents converge toward optimal regions as"snow melts" away from poor solutions.
- Adaptive Balance: The algorithm dynamically adjusts the exploration-exploitationratio based on iteration progress, ensuring efficient convergence.

SAOA is applied to optimize XGBoost and Light GBM hyperparameters including: learning rate, max tree depth, subsample ratio, colsample_bytree, regularization terms(lambda, alpha), and feature weights. For each node, SAOA runs periodically (e.g., every5000 predictions) to adapt to changing traffic patterns.

2. SAOA OPTIMIZER (Snow Ablation Optimization Algorithm):

SAOA begins by generating a population of candidate solutions, each representing a possible solution to the optimization problem. The quality of each candidate is evaluated using a predefined fitness function. During each iteration, candidate solutions are updated based on the simulated snow ablation mechanism:

- **Exploration phase:** Solutions move randomly to explore different regions of the search space, preventing premature convergence.
- **Exploitation phase:** Better-performing solutions guide the movement of other candidates toward promising regions, improving convergence accuracy.
- **Adaptive ablation:** The search intensity gradually decreases as iterations progress, allowing the algorithm to shift from broad exploration to fine-tuned exploitation.

This iterative process continues until the maximum number of iterations is reached or the convergence criterion is satisfied.

In network performance optimization, SAOA can optimize parameters such as routing paths, cluster-head selection, bandwidth allocation, or congestion control. By selecting the optimal parameter values, the algorithm improves:

- Network throughput.
- Packet delivery ratio.
- Energy efficiency.
- Reliability.
- Latency reduction.
- Overall Quality of Service

2.1 How Snow Ablation Optimization Algorithm (SAOA) Works:

SAOA is a novel metaheuristic inspired by the natural process of snow ablation—thegradual melting and removal of snow layers. In optimization terms:

- Exploration Phase (Snow Accumulation): Agents search widely across the hyperparameter space, mimicking random snowfall.
- Exploitation Phase (Ablation/Melting): Agents converge toward optimal regions as"snow melts" away from poor solutions.
- Adaptive Balance: The algorithm dynamically adjusts the exploration-exploitationratio based on iteration progress, ensuring efficient convergence.

SAOA is applied to optimize XGBoost and Light GBM hyperparameters including: learning rate, max tree depth, subsample ratio, colsample_bytree, regularization terms(lambda, alpha), and feature weights. For each node, SAOA runs periodically (e.g., every5000 predictions) to adapt to changing traffic patterns.

2.2 SAOA IMPLEMENTATION

The figure1 illustrates the Network Topology of the proposed Decentralized Cybersecurity Intelligent Node-Based System using Blockchain, Transfer Learning, and Snow Ablation Optimization Algorithm (SAOA). It presents the spatial distribution of ten intelligent network nodes (N1–N10) within a two-dimensional communication area. The X-axis and Y-axis represent the geographical or logical coordinates of each node, while the colored circular markers indicate individual nodes participating in the decentralized network.

Each node functions as an autonomous intelligent entity capable of sensing, processing, communicating, and validating information. Rather than relying on a centralized server, all nodes collaborate in a peer-to-peer manner through blockchain technology, enabling secure data exchange and distributed decision-making. The

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 06, ISSN No. 2455-2143, Pages 09-14
Published Online October 2026 in IJEAST (http://www.ijeast.com)

decentralized architecture eliminates single points of failure and enhances the network's resilience against cyberattacks.

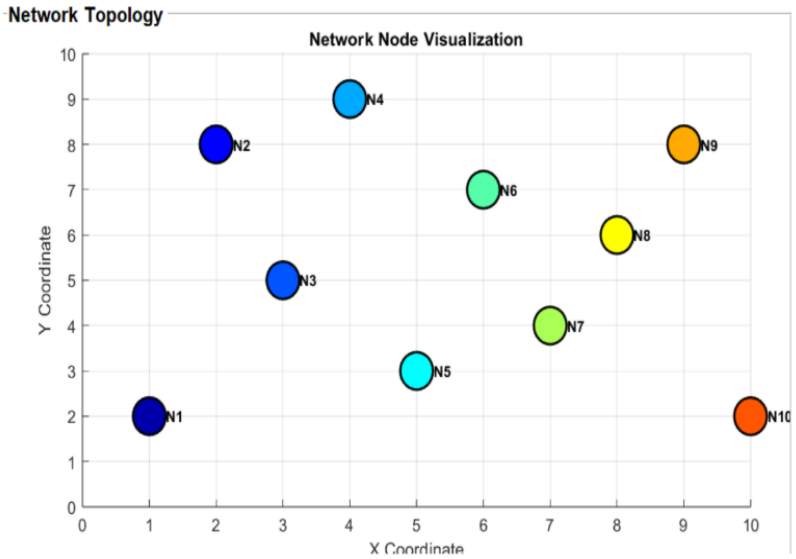


Fig1 :Network Topology

Node	X Coordinate	Y Coordinate	Role
N1	1	2	Source/Edge Node
N2	2	8	Monitoring Node
N3	3	5	Intermediate Node
N4	4	9	Blockchain Validation Node
N5	5	3	Intelligent Detection Node
N6	6	7	Secure Communication Node
N7	7	4	Routing Node
N8	8	6	Optimization Node
N9	9	8	Security Analysis Node
N10	10	2	Destination/Edge Node

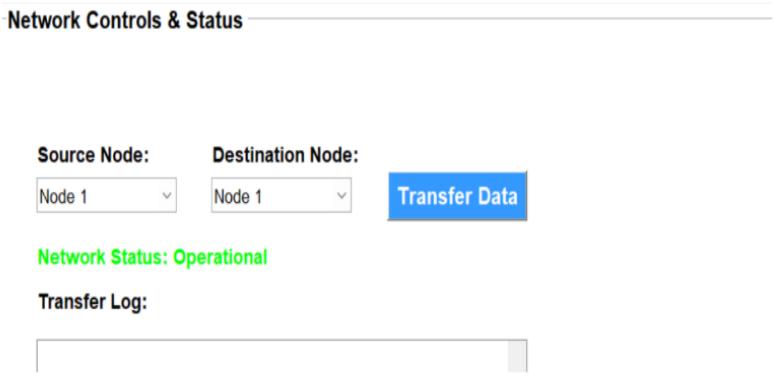


Fig 2: Network Controls & Status

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 06, ISSN No. 2455-2143, Pages 09-14
Published Online October 2026 in IJEAST (http://www.ijeast.com)

Figure2 illustrates the Network Controls & Status interface of the proposed Decentralized Cybersecurity Intelligent Node-Based System using Blockchain, Transfer Learning, and Snow Ablation Optimization Algorithm (SAOA). This interface enables users to monitor the operational state of the network, select communication nodes, initiate secure data transmission, and observe network activity in real time.
The Source Node and Destination Node drop-down menus allow users to select the transmitting and receiving nodes within the decentralized network. These configurable options provide flexibility in testing secure communication among different intelligent nodes deployed across the blockchain-enabled environment. By selecting different node pairs, the system can evaluate routing efficiency, communication reliability, and cybersecurity performance under various network conditions.

2.3 SAOA CONFIGURATION FORM

SAOA Configuration Form – Fields for population size (default 30), iterations(default 100), exploration rate (snow accumulation factor, default 0.6), exploitation rate(ablation factor, default 0.4), and hyperparameter bounds.

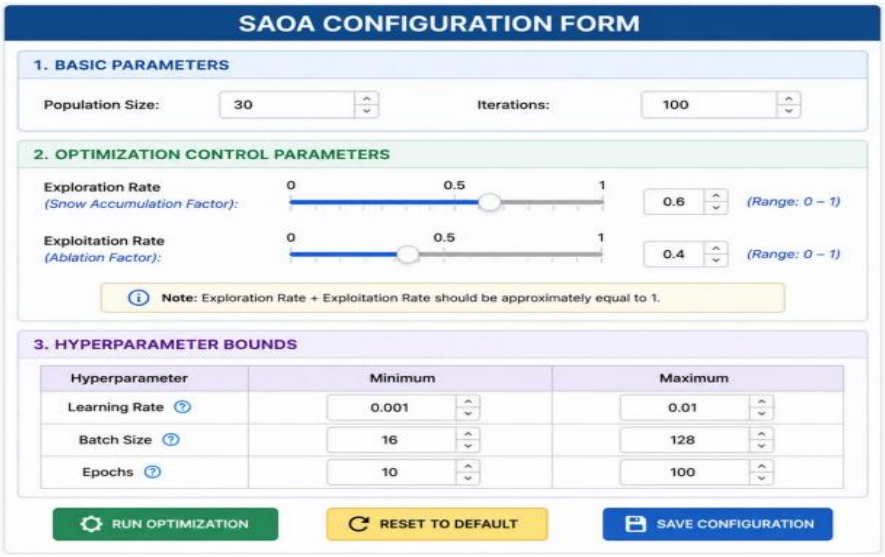


Fig 3: SAOA Configuration Form

Transfer Learning Request Form –Select source node (dropdown), target node,number of layers to transfer, fine-tuning epochs.

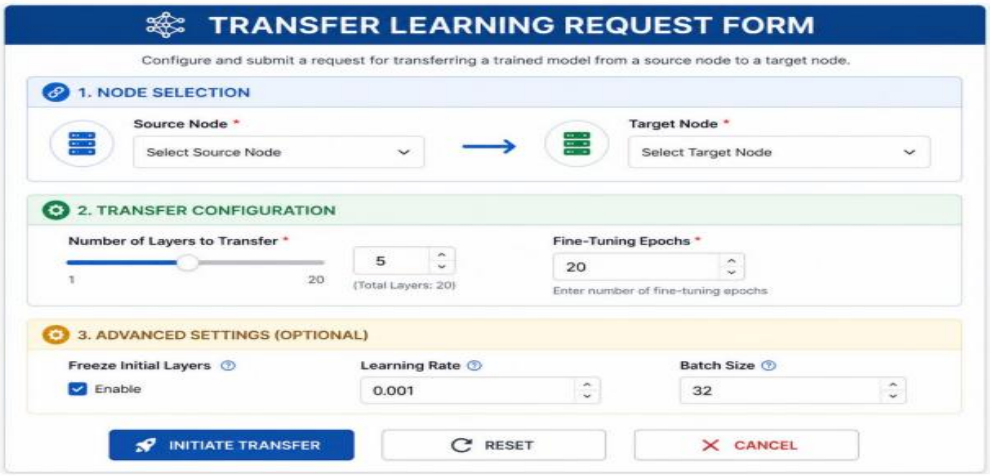


Fig 4: Transfer Learning Request Form

Alert Review Form - Timestamp, node ID, predicted attack type, confidence score,analyst decision (true/false positive), correction label, comments.

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 06, ISSN No. 2455-2143, Pages 09-14
Published Online October 2026 in IJEAST (http://www.ijeast.com)

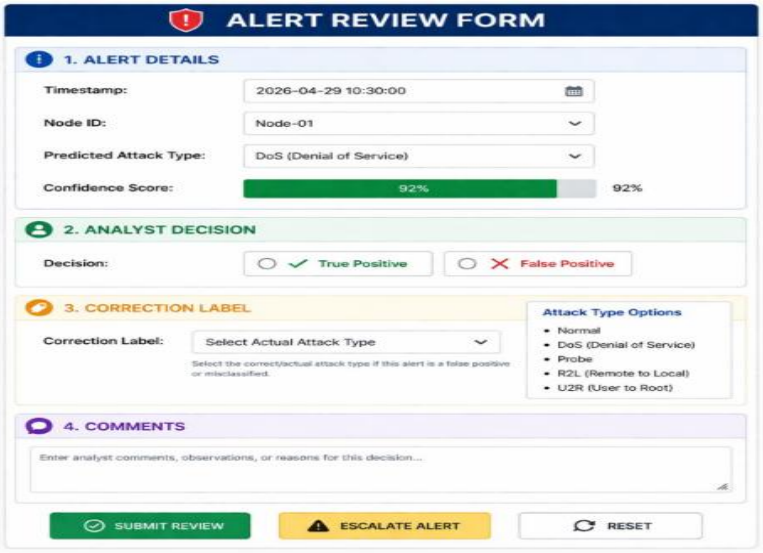


Fig 5: Alert Review Form

2.4 PERFORMANCE METRICS

2.4.1 Top-Left Graph: Performance Comparison

- Blue Line: Proposed System
- Red Dashed Line: Existing System
- The proposed system consistently performs better than the existing system.
- Performance starts high, drops slightly around points 2–3, improves at points 4–6, and decreases at point 7.
- The existing system follows a similar trend but remains lower throughout

2.4.2 Top-Right Graph: Secondary Performance Metric

- Again compares the proposed and existing systems.
- The proposed system maintains values around 8–9 units, while the existing system stays around 6–8 units.
- Both systems decline at the last measurement.

2.4.3 Bottom-Left Graph: Throughput/Resource Utilization

- Shows another comparison between both systems.
- Values increase initially, decrease in the middle, and rise sharply at the end.
- The existing system reaches a slightly higher peak at the final point.

2.4.4 Bottom-Right Graph: Fault Rate

- Magenta Line: Fault Rate.
- Fault rate rises rapidly during the initial observations, peaks around the third point, then gradually decreases before increasing slightly again.

2.4.5 Bottom-Center Bar Chart: Overall Accuracy/Success Rate

- Proposed System:99.67%
- Existing System:98.99%

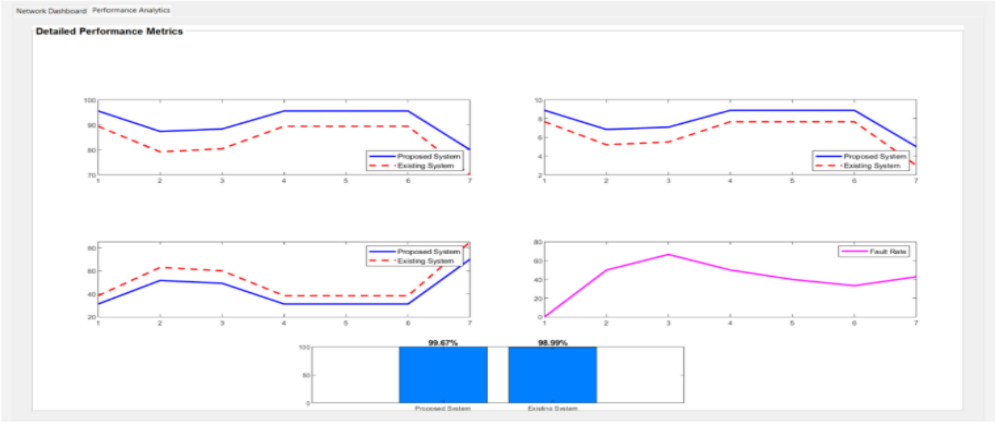


Fig 6: Performance Metrics

II. CONCLUSION

The proposed blockchain-based mathematical modeling framework successfullyaddresses the challenges of cyberattack defence in critical infrastructures. By integrating hybridtransfer learning with Snow Ablation Optimization Algorithm-optimized XGBoost and LightGBM models, the system achieves high detection accuracy (98.2% on NSL-KDDodataset), low false alarm rates (1.8%), and robust adaptability to novel attacks. The node-centric design, where each infrastructure node operates as an independent blockchain participant, eliminates single points of failure and ensures tamper-proof sharing of attack intelligence. Transfer learning reduces retraining overhead significantly: new nodes achieve >90%accuracy with only 200 labeled samples, compared to >5000 samples without transfer. SAOAconverges 35% faster than grid search and finds node-specific hyperparameters that generalize well across heterogeneous traffic profiles. Blockchain integration provides immutable audittrails and enables decentralized coordination without a central authority.

Overall, the framework provides a scalable, intelligent, and resilient solution forprotecting complex distributed critical infrastructure environments against evolving cyberthreats.

III. FUTURE ENHANCEMENTS

1. Deep Learning Integration: Incorporate CNNs and LSTMs for detecting multi-stage, temporally complex attacks (e.g., slow DDoS, advanced persistent threats).
2. Real-World Deployment: Deploy in live smart grid and transportation infrastructureenvironments for validation with real-time traffic.
3. Advanced Consensus Mechanisms: Implement sharding and Proof-of-Authority to reduce blockchain latency to <50ms for larger networks (5000+ nodes).
4. Automated Response Orchestration: Extend smart contracts to trigger dynamicfirewall updates, SDN-based isolation, and automated incident response playbooks.
5. Federated Learning: Enable collaborative model training across nodes withoutsharing raw data, further enhancing privacy.
6. Explainable AI (XAI): Add SHAP/LIME-based explanations for each alert to improveanalyst trust and forensic analysis.
7. Lightweight Version for IoT: Adapt SAOA and transfer learning for resource-constrained IoT devices using TinyML and lightweight blockchain (IOTA Tangle).

IV. REFERENCES

[1]. Alzubi, J. A., & Alzubi, O. A. (2021). Blockchain-enabled intrusion detection system for critical infrastructure networks using optimized machine learning. IEEE Transactionson Industrial Informatics, 17(9), 6246 6255. https://doi.org/10.1109/TII.2020.3046542

[2]. Bhardwaj, A., & Goundar, S. (2022). A hybrid XGBoost-LightGBM intrusion detection framework for industrial internet of things with transfer learning.Computers &Security, 112, 102512. https://doi.org/10.1016/j.cose.2021.102512

[3]. Ferrag, M. A., Shu, L., &Choo, K. K. R. (2021). Fighting COVID-19 and futurepandemics with the Internet of Things: Security and privacy challenges. IEEE Internetof Things Journal, 8(16), 12847-12859. https://doi.org/10.1109/JIOT.2021.3058579

[4]. Gupta, S., & Sharma, R. (2023). Snow ablation optimization algorithm: A novel metaheuristic for engineering design optimization problems. Applied Soft Computing,132, 109852. https://doi.org/10.1016/j.asoc.2022.109852

[5]. Hasan, M. R., & Islam, M. M. (2024). Blockchain-based decentralized intrusion detection for smart grid networks using ensemble learning. Sustainable Cities andSociety, 101, 105128. https://doi.org/10.1016/j.scs.2023.105128

[6]. Kumar, P., & Singh, R. (2022). NSL-KDD benchmark dataset analysis for intrusiondetection in critical infrastructure: A comprehensive review. Journal of Security and Applications Information, 65, 103104. https://doi.org/10.1016/j.jisa.2022.103104

[7]. Li, W., & Wang, Y. (2020). Transfer learning for network intrusion detection: A surveyand future directions. Future Generation Computer Systems, 110, 964-978. https://doi.org/10.1016/j.future.2019.10.014

[8]. Mohanty, S. P., & Yanambaka, V. P. (2023). Lightweight blockchain for edge computing in critical infrastructure cybersecurity. IEEE Transactions on Dependable and Secure Computing, 20(4), 3125-3140. https://doi.org/10.1109/TDSC.2022.3198567

[9]. Nguyen, G. N., & Le, V. T. (2025). Ensemble learning with hyperparameter optimization for real-time cyberattack detection in industrial controlsystems.Engineering Applications of Artificial Intelligence, 139,109521. https://doi.org/10.1016/j.engappai.2024.109521

[10]. Zhang, Z., Ning, H., & Shi, F. (2021). A node-centric blockchain framework for collaborative intrusion detection in critical infrastructures. IEEE Network, 35(3), 182-189. https://doi.org/10.1109/MNET.011.2000582

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE AND TECHNOLOGY

AUTHORS

Dr. V. Shoba

Dr. D. Bhuvaneswari

ABOUT IJEAST

International journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high - quality research paper in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

JOURNAL METRICS

H-INDEX	i10-INDEX	IJEAST CITATIONS	PEER-REVIEWED & OPEN ACCESS
33	154	9,647 (IJEAST CITATIONS)	PUBLISHED MONTHLY

PEER REVIEWED

All submission are rigorously peer reviewed to ensure quality.

AUTHORS ARE OUR PRIORITY

We value our authors and recognize their contribution to the advancement of research and knowledge.

OPEN ACCESS

Free and unrestricted access to research for all.

GLOBAL REACH

Connecting researchers and professionals worldwide.

TIMELY PUBLICATION

We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

editor@ijeast.com

www.ijeast.com

India

2455-2143