International Journal of Basic and Applied Sciences, 14 (1) (2025) 216-221

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/9f4z3q54
Research paper

An adaptive learning model for secure data sharing in decentralized environments using blockchain technology

Thupakula Bhaskar [1], Hema N. [2], R. Rajitha Jasmine [3] , Pearlin [4], Uma Patil [5], Madhava Rao Chunduru [6], P. Saravanan [7], Venkatesh Kanna T. [8], R. G. Vidhya [9] *

[1] Department of CSE, Sanjivani College of Engineering, Savitribai Phule Pune University, Maharashtra , India
[2] Department of ISE, RNS Institute of Technology, Bangalore, Karnataka, India
[3] Department of CSE, R.M.K. Engineering College, Kavaraipettai, Tamil Nadu, India
[4] Department of English, Panimalar Engineering College, Chennai, Tamil Nadu, India.
[5] Department of CSE, PCET'S & NMVPM'S Nutan College of Engineering and Research, Pune, Maharashtra, India
[6] Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India
[7] Department of ECE, Sri Sairam Institute of Technology, Chennai, Tamil Nadu, India
[8] Department of ECE, Velammal College of Engineering and Technology, Madurai, Tamil Nadu, India
[9] Department of ECE, HKBK College of Engineering, Bangalore, India
**Corresponding author E-mail: nehamunjal982@gmail.com*

Received: March 21, 2025, Accepted: April 30, 2025, Published: May 7, 2025

Abstract

Blockchain technology has rapidly emerged as a vital skillset, reshaping digital infrastructure with its decentralized, transparent, and secure characteristics. These core features have driven its integration across various industrial applications, establishing it as a foundation for modern computing paradigms such as cloud and edge computing. Recognizing this potential, the present study introduces a novel and disruptive approach utilizing an adaptive learning model to enhance security within data-sharing ecosystems through decentralized access control mechanisms. The proposed framework was implemented using Python and rigorously evaluated through experimentation. A comprehensive performance analysis compared the proposed Adaptive Learning Model (ALM) against conventional cryptographic techniques, specifically RSA and AES algorithms. Multiple performance metrics were analysed, and the outcomes demonstrated that the proposed method significantly improves security, scalability, and processing time.

Keywords: *Blockchain Technology; Decentralized Systems; Data Security; Adaptive Learning; Cloud Computing; Edge Computing.*

1. Introduction

In recent years, blockchain technology has garnered significant attention across a variety of domains, ranging from cryptocurrencies to enterprise-level services [1]. This widespread adoption signals the transformative potential of blockchain as a foundational innovation for the next wave of developments in the financial and industrial sectors. With increasing research and exploration in this space, blockchain is gradually reshaping critical aspects of our lives, including finance, energy, and public services [2]. From a technological perspective, blockchain is a form of distributed ledger technology (DLT), first popularized by its use in Bitcoin for recording digital financial transactions. It functions as a decentralized, real-time, and openly accessible data system [3]. Rather than being controlled by a centralized authority, blockchain relies on a peer-to-peer network in which all transactions are securely stored in an immutable chain of blocks [4,5]. Each block is verified using cryptographic techniques and consensus algorithms, which ensure the integrity and authenticity of recorded data, making it highly resistant to tampering or unauthorized modifications [6]. The essential attributes of blockchain—namely decentralization, transparency, and security—position it as a valuable tool for improving operational efficiency while reducing overhead costs [7]. These features have accelerated the development of various blockchain-based applications, emphasizing the relevance of ongoing research in this dynamic field [8], [9]. Simultaneously, advancements in information and communication technologies have opened new avenues for emerging paradigms such as the Internet of Things (IoT) and cloud computing. IoT has fundamentally transformed both personal and industrial environments by enabling interconnected devices to communicate and interact in real time [10], [11]. These devices—ranging from sensors to smart appliances—can collect, transmit, and respond to data through embedded systems, thereby enabling intelligent services in areas like smart cities and smart manufacturing [12], [13]. Given the limited processing power and storage capabilities of IoT devices, many operations are offloaded to cloud platforms, leading to the integration known as the Cloud of Things (CoT). CoT provides a scalable and robust environment for managing IoT applications, thereby enhancing service efficiency and overall system performance [14], [15]. However, conventional CoT architectures often face limitations due to their reliance on centralized communication models, such as main cloud servers [16], [17]. This centralization can lead to bottlenecks, reduced scalability, and increased vulnerability, especially as

IoT networks expand [18], [19]. To address these challenges, security and privacy concerns have become key areas of focus [20], [21]. The structure of this paper is organized as follows: Section II reviews related literature, while Section III outlines the proposed framework architecture. In Section IV, we present a novel security algorithm based on an adaptive learning model. Section V discusses the experimental results, and Section VI concludes with insights and directions for future research. Significant efforts have been made in recent years to review the integration of blockchain in diverse technological ecosystems, particularly IoT and cloud computing. Several studies have explored blockchain's capacity to secure IoT infrastructure and its potential application in areas such as smart manufacturing, vehicular networks, autonomous systems, and the next generation 5G wireless networks [22], [23]. Other researchers have examined blockchain's technical underpinnings—such as consensus protocols and networking models—as well as the synergy between blockchain and cloud systems [24], [25]. Further work has highlighted the potential of combining blockchain with edge computing, a more decentralized computing model, to address the scalability and performance issues in distributed environments [26], [27].

2. Proposed methodology

Traditional security frameworks for decentralized access control often rely on separate algorithms for encryption and decryption, which introduces unnecessary complexity and increases system overhead [28], [29]. To address these limitations and simplify secure access control mechanisms, the proposed methodology introduces a streamlined framework that integrates encryption and access management into a unified system with attribute-based security [30], [31]. The architecture of the proposed system—illustrated in Fig. 1—features decentralized access points distributed across multiple organizational levels. This modular design enhances scalability and allows each participating organization to independently manage its access permissions [32], [33]. The system includes key components such as dedicated access points, a suite of microservices, a blockchain-based cluster, an internal user repository, and a hierarchical multi-organization structure.

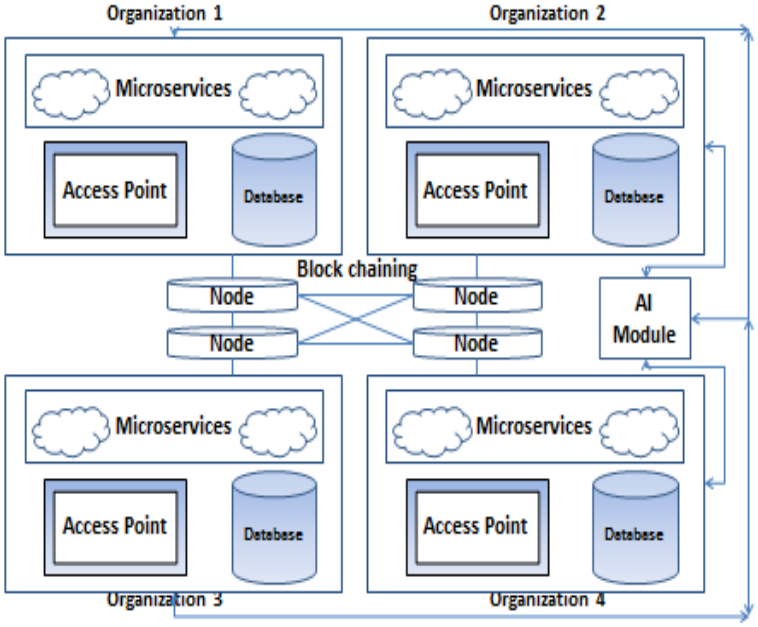

Fig. 1: System Framework for Decentralized Access Control.

Each organization is equipped with its access control unit, enabling local decision-making to approve or deny access requests based on predefined policies. Instead of relying solely on external databases, the system uses a private internal database for operational efficiency [34], [35]. However, the blockchain network ensures distributed data synchronization across nodes, offering redundancy, integrity, and immutability of shared records [36], [37]. The blockchain cluster enforces access rules encoded into smart contracts, maintaining transparency and security while recording the history of all access events. These historical logs enhance auditability and trust in the system [38], [39]. Additionally, the architecture supports reusable microservices that offer specific functionalities [40], [41]. These services operate independently and interact seamlessly with other system components, thereby promoting flexibility and modular development [42], [43]. This integrated and decentralized framework significantly reduces the complexity associated with conventional encryption models and supports secure, scalable, and efficient access control across multiple domains [44], [45].

3. Results and discussion

As detailed in the previous section, blockchain technology forms the backbone of the proposed system architecture. Central to this structure are nodes, which can be any computing device or user that maintains a complete replica of the blockchain ledger [46]. These nodes serve essential functions such as storing, validating, and propagating transaction data throughout the network. In essence, the existence of blockchain is distributed across these interconnected nodes, making the system robust, transparent, and decentralized. One of the primary responsibilities of a node is to process transactions. A typical blockchain transaction workflow begins with a request, which is validated through node-to-node communication—illustrated in Fig. 2. Upon successful validation, the transaction is confirmed, and nodes receive a reward for their participation through consensus mechanisms like Proof of Work. Once verified, the transaction is recorded in a new block, which is then appended to the existing chain.

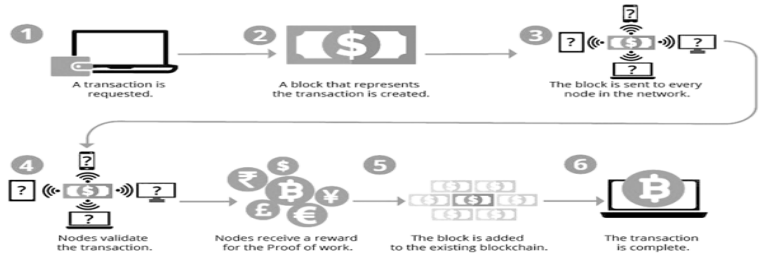

Fig. 2: An Example Blockchain Transaction.

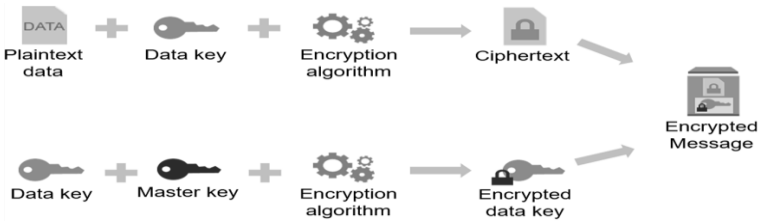

Fig. 3: Methodology Used for Encryption and Decryption.

At this stage, the adaptive learning model (ALM) is activated to evaluate the transaction process, documenting observations to continuously refine its performance. The ALM plays a crucial role in dynamically reinforcing the security protocols by learning from ongoing operations. The encryption and decryption mechanisms employed by the proposed system are depicted in Fig. 3. Every time a plaintext input is processed, it undergoes encryption through a combination of a data key and a master key. The encrypted data key generates a secure ciphertext, which is transmitted securely within the network. The ALM integrates this encryption process and utilizes it to generate output that adapts to evolving access conditions. A unique feature of this encryption strategy is the use of prime numbers during the initial block generation. The system's security increases as the ALM adjusts the encryption model based on learned parameters from previous block weights. Each new block's encryption mechanism is influenced by dynamic weight values derived from previous operations, ensuring each encryption is distinct and difficult to trace. This design allows the system to support high-volume encryption, such as securing documents with over 10,000 words, without compromising speed or performance. The ALM algorithm itself is based on a linear loop structure, ensuring time complexity remains at O(n)—indicating efficient scalability. The symbol '?' in the algorithm denotes an asymptotic equivalent for a linearly scaled learning rate, reflecting the model's ability to adapt continuously. To illustrate how the ALM operates in practice, sample inputs and corresponding outputs are provided in Fig .4a and 4b. These examples help visualize how the algorithm securely processes and encrypts data in real-time. Overall, the results demonstrate that the proposed ALM algorithm significantly enhances the security, adaptability, and efficiency of decentralized access control systems. Its capability to evolve encryption techniques based on real-time input and prior activity sets it apart from traditional static methods.

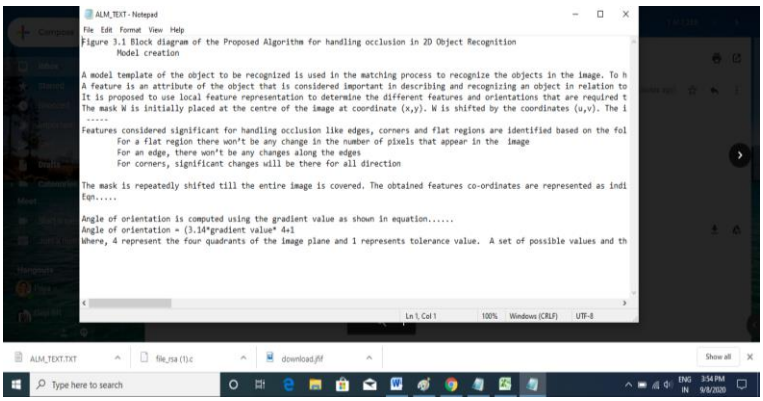

Fig 4: A) Sample Input for Algorithm Testing.

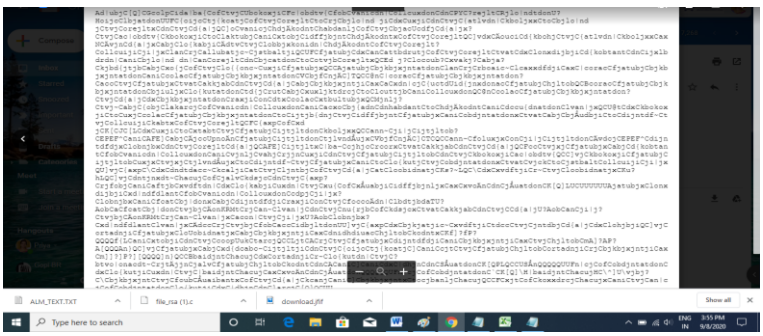

Fig 4: B) Sample Encrypted Output.

To evaluate the effectiveness of the proposed Adaptive Learning Model (ALM) in terms of encryption performance, a comparative analysis was conducted against conventional RSA and AES algorithms. The results of this comparison are summarized in Table 1, offering a clear perspective on the encryption standards and performance metrics of each approach.

Table 1: Feature Comparison of AES vs RSA vs ALM Algorithms

S. No	Features	AES	RSA	ALM
1	Type of cryptography	Symmetric	Asymmetric	Both symmetric and asymmetric
2	Keys are defined throughout the process	Single key	Different key	Multiple keys for each block were created
3	Throughput	Very high	Low	Very high
4	Confidentiality	High	Low	Very high

The Adaptive Learning Model (ALM) algorithm was developed and executed using the Python programming language. The performance outcomes of the implementation are presented in Table 2. These results indicate that the ALM algorithm achieves a significantly higher encryption rate within a shorter processing time compared to the widely used RSA and AES algorithms when tested on identical input document sets.

Table 2: Comparison of AES, RSA and ALM Algorithms -Time Taken to Complete Encryption

S. No	Number of words	Time in (ms)		
		RSA	AES	ALM
1	1000	9.858	0.243	0.084
2	2500	12.091	0.249	0.085
3	5000	16.940	0.343	0.101
4	10000	30.272	0.421	0.115

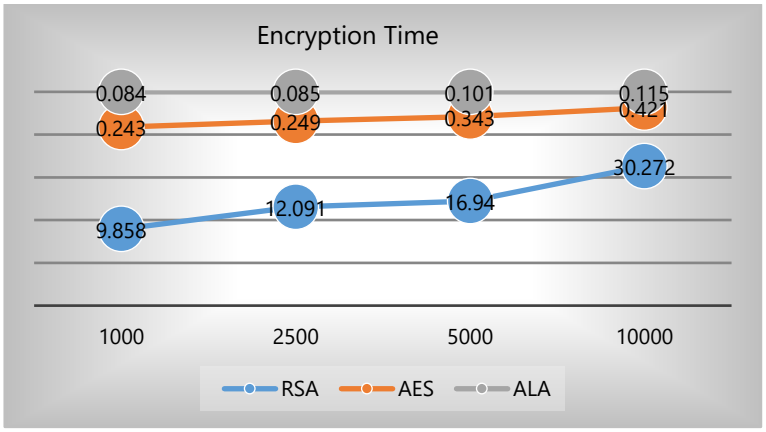

Fig. 5: Encryption Time AES vs RSA vs ALM Algorithm.

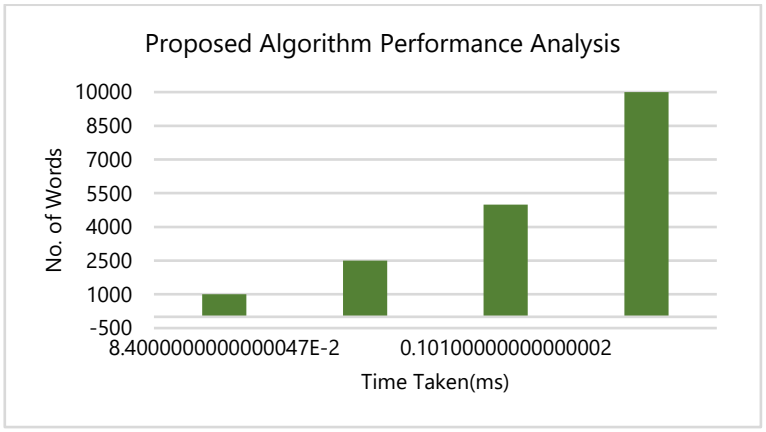

Fig. 6: Performance Analysis of Proposed Algorithm.

As illustrated in Figure 5, the proposed Adaptive Learning Model (ALM) algorithm demonstrates a significantly faster encryption time compared to the conventional AES and RSA algorithms. Furthermore, the ALM consistently maintains a high encryption accuracy while operating within reduced time frames. To validate its scalability and robustness, the algorithm was tested on varying input sizes, ranging from 1,000 to 10,000 words. The outcomes of these tests are depicted in Figure 6, providing a clearer understanding of the algorithm's performance across different data volumes.

4. Conclusion

This study presents a novel solution to the security challenges inherent in decentralized access control systems by introducing a blockchain-based framework integrated with an Adaptive Learning Model (ALM) algorithm. The proposed approach enhances data protection by dynamically adjusting encryption strategies, significantly outperforming conventional RSA and AES algorithms in terms of processing time and encryption efficiency. The ALM's capability to employ multiple encryption keys further strengthens its resistance to unauthorized access and potential cyber threats. While the current model demonstrates promising results, it does not yet address scenarios involving multiple master nodes, which could further enhance decentralized control and load distribution. This limitation opens a direction for future work, where support for multiple master configurations and the incorporation of advanced intelligence can be explored. Additionally, the model can be further evaluated and trained using real-world datasets to validate its applicability in diverse security-critical environments.

References

[1] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," Int. J. Web Grid Serv., vol. 14, no. 4, pp. 352–375, Dec. 2018. https://doi.org/10.1504/IJWGS.2018.095647.

[2] D. Zuehlke, "SmartFactory: From vision to reality in factory technologies," 17th IFAC World Congr., Seoul, Korea, Jul. 2008. https://doi.org/10.3182/20080706-5-KR-1001.02391.

[3] J. Choi, "Secure multiparty computation and trusted hardware: Examining adoption challenges and opportunities," Secur. Commun. Netw., Article ID 1368905, 2019. https://doi.org/10.1155/2019/1368905.

[4] T. Al-Shehari, M. Kadrie, T. Alfakih, H. Alsalman, T. Kuntavai, et al., "Blockchain with secure data transactions and energy trading model over the internet of electric vehicles," Sci. Rep., vol. 14, no. 1, p. 19208, Jan. 2024, https://doi.org/10.1038/s41598-024-69542-w.

[5] R. Vidhya, D. Banavath, S. Kayalvili, S. M. Naidu, et al., "Alzheimer's disease detection using residual neural network with LSTM hybrid deep learning models," J. Intell. Fuzzy Syst., vol. 45, no. 6, pp. 12095–12109, 2023. https://doi.org/10.3233/JIFS-235059.

[6] P. Selvam, N. Krishnamoorthy, S. P. Kumar, K. Lokeshwaran, M. Lokesh, et al., "Internet of Things Integrated Deep Learning Algorithms Monitoring and Predicting Abnormalities in Agriculture Land," Internet Technol. Lett., Nov. 2024, https://doi.org/10.1002/itl2.607.

[7] S. S. F. Begum, M. S. Anand, P. V. Pramila, J. Indra, J. S. Isaac, C. Alagappan, et al., "Optimized machine learning algorithm for thyroid tumour type classification: A hybrid approach Random Forest, and intelligent optimization algorithms," J. Intell. Fuzzy Syst., pp. 1–12, 2024.

[8] K. Maithili, A. Kumar, D. Nagaraju, D. Anuradha, S. Kumar, et al., "DKCNN: Improving deep kernel convolutional neural network-based covid-19 identification from CT images of the chest," J. X-ray Sci. Technol., vol. 32, no. 4, pp. 913–930, 2024. https://doi.org/10.3233/XST-230424.

[9] K. Mannanuddin, V. R. Vimal, A. Srinivas, S. D. U. Mageswari, G. Mahendran, et al., "Enhancing medical image analysis: A fusion of fully connected neural network classifier with CNN-VIT for improved retinal disease detection," J. Intell. Fuzzy Syst., vol. 45, no. 6, pp. 12313–12328, 2023. https://doi.org/10.3233/JIFS-235055.

[10] T. A. Mohanaprakash, M. Kulandaivel, S. Rosaline, P. N. Reddy, S. S. N. Bhukya, et al., "Detection of Brain Cancer through Enhanced Particle Swarm Optimization in Artificial Intelligence Approach," J. Adv. Res. Appl. Sci. Eng. Technol., vol. 33, no. 3, pp. 174–186, 2023. https://doi.org/10.37934/araset.33.2.174186.

[11] Wange N. K., Khan I., Pinnamaneni R., Cheekati H., Prasad J., et al., "β-amyloid deposition-based research on neurodegenerative disease and their relationship in elucidate the clear molecular mechanism," Multidisciplinary Science Journal, vol. 6, no. 4, pp. 2024045–2024045, 2024. https://doi.org/10.31893/multiscience.2024045.

[12] Anitha C., Tellur A., Rao K. B. V. B., Kumbhar V., Gopi T., et al., "Enhancing Cyber-Physical Systems Dependability through Integrated CPS-IoT Monitoring," International Research Journal of Multidisciplinary Scope, vol. 5, no. 2, pp. 706–713, 2024. https://doi.org/10.47857/irjms.2024.v05i02.0620.

[13] Balasubramani R., Dhandapani S., Sri Harsha S., Mohammed Rahim N., Ashwin N., et al., "Recent Advancement in Prediction and Analyzation of Brain Tumour using the Artificial Intelligence Method," Journal of Advanced Research in Applied Sciences and Engineering Technology, vol. 33, no. 2, pp. 138–150, 2023. https://doi.org/10.37934/araset.33.2.138150.

[14] Chaturvedi A., Balasankar V., Shrimali M., Sandeep K. V., et al., "Internet of Things Driven Automated Production Systems using Machine Learning," International Research Journal of Multidisciplinary Scope, vol. 5, no. 3, pp. 642–651, 2024. https://doi.org/10.47857/irjms.2024.v05i03.01033.

[15] Saravanakumar R., Arularasan A. N., Harekal D., Kumar R. P., Kaliyamoorthi P., et al., "Advancing Smart Cyber Physical System with Self-Adaptive Software," International Research Journal of Multidisciplinary Scope, vol. 5, no. 3, pp. 571–582, 2024. https://doi.org/10.47857/irjms.2024.v05i03.01013.

[16] Vidhya R. G., Surendiran J., Saritha G., "Machine Learning Based Approach to Predict the Position of Robot and its Application," Proc. Int. Conf. on Computer Power and Communications, pp. 506–511, 2022. https://doi.org/10.1109/ICCPC55978.2022.10072031.

[17] Sivanagireddy K., Yerram S., Kowsalya S. S. N., Sivasankari S. S., Surendiran J., et al., "Early Lung Cancer Prediction using Correlation and Regression," Proc. Int. Conf. on Computer Power and Communications, pp. 24–28, 2022. https://doi.org/10.1109/ICCPC55978.2022.10072059.

[18] Vidhya R. G., Seetha J., Ramadass S., Dilipkumar S., Sundaram A., Saritha G., "An Efficient Algorithm to Classify the Mitotic Cell using Ant Colony Algorithm," Proc. Int. Conf. on Computer Power and Communications, pp. 512–517, 2022. https://doi.org/10.1109/ICCPC55978.2022.10072277.

[19] Sengeni D., Muthuraman A., Vurukonda N., Priyanka G., et al., "A Switching Event-Triggered Approach to Proportional Integral Synchronization Control for Complex Dynamical Networks," Proc. Int. Conf. on Edge Computing and Applications, pp. 891–894, 2022. https://doi.org/10.1109/ICECAA55415.2022.9936124.

[20] Vidhya R. G., Rani B. K., Singh K., Kalpanadevi D., Patra J. P., Srinivas T. A. S., "An Effective Evaluation of SONARS using Arduino and Display on Processing IDE," Proc. Int. Conf. on Computer Power and Communications, pp. 500–505, 2022. https://doi.org/10.1109/ICCPC55978.2022.10072229.

[21] Kushwaha S., Boga J., Rao B. S. S., Taqui S. N., et al., "Machine Learning Method for the Diagnosis of Retinal Diseases using Convolutional Neural Network," Proc. Int. Conf. on Data Science, Agents & Artificial Intelligence, 2023, pp. 1–. https://doi.org/10.1109/ICDSAAI59313.2023.10452440.

[22] Maheswari B. U., Kirubakaran S., Saravanan P., Jeyalaxmi M., Ramesh A., et al., "Implementation and Prediction of Accurate Data Forecasting Detection with Different Approaches," Proc. 4th Int. Conf. on Smart Electronics and Communication, 2023, pp. 891–897. https://doi.org/10.1109/ICOSEC58147.2023.10276331.

[23] Mayuranathan M., Akilandasowmya G., Jayaram B., Velrani K. S., Kumar M., et al., "Artificial Intelligent based Models for Event Extraction using Customer Support Applications," Proc. 2nd Int. Conf. on Augmented Intelligence and Sustainable Systems, 2023, pp. 167–172. https://doi.org/10.1109/ICAISS58487.2023.10250679.

[24] Gold J., Maheswari K., Reddy P. N., Rajan T. S., Kumar S. S., et al., "An Optimized Centric Method to Analyze the Seeds with Five Stages Technique to Enhance the Quality," Proc. Int. Conf. on Augmented Intelligence and Sustainable Systems, 2023, pp. 837–842. https://doi.org/10.1109/ICAISS58487.2023.10250681.

[25] Anand L., Maurya J. M., Seetha D., Nagaraju D., et al., "An Intelligent Approach to Segment the Liver Cancer using Machine Learning Method," Proc. 4th Int. Conf. on Electronics and Sustainable Communication Systems, 2023, pp. 1488–1493. https://doi.org/10.1109/ICESC57686.2023.10193190.

[26] Harish Babu B., Indradeep Kumar, et al., "Advanced Electric Propulsion Systems for Unmanned Aerial Vehicles," Proc. 2nd Int. Conf. on Sustainable Computing and Smart Systems (ICSCSS), 2024, pp. 5–9, IEEE. https://doi.org/10.1109/ICSCSS60660.2024.10625489.

[27] Jagan Raja V., Dhanamalar M., Solaimalai G., et al., "Machine Learning Revolutionizing Performance Evaluation: Recent Developments and Breakthroughs," Proc. 2nd Int. Conf. on Sustainable Computing and Smart Systems (ICSCSS), 2024, pp. 780–785, IEEE. https://doi.org/10.1109/ICSCSS60660.2024.10625103.

[28] Sivasankari S. S., Surendiran J., Yuvaraj N., et al., "Classification of Diabetes using Multilayer Perceptron," Proc. IEEE Int. Conf. on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), 2022, pp. 1–5, IEEE. https://doi.org/10.1109/ICDCECE53908.2022.9793085.

[29] Anushkannan N. K., Kumbhar V. R., Maddila S. K., et al., "YOLO Algorithm for Helmet Detection in Industries for Safety Purpose," Proc. 3rd Int. Conf. on Smart Electronics and Communication (ICOSEC), 2022, pp. 225–230, IEEE. https://doi.org/10.1109/ICOSEC54921.2022.9952154.

[30] Reddy K. S., Vijayan V. P., Das Gupta A., et al., "Implementation of Super Resolution in Images Based on Generative Adversarial Network," Proc. 8th Int. Conf. on Smart Structures and Systems (ICSSS), 2022, pp. 1–7, IEEE. https://doi.org/10.1109/ICSSS54381.2022.9782170.

[31] Joseph J. A., Kumar K. K., Veerraju N., Ramadass S., Narayanan S., et al., "Artificial Intelligence Method for Detecting Brain Cancer using Advanced Intelligent Algorithms," Proc. Int. Conf. on Electronics and Sustainable Communication Systems, 2023, pp. 1482–1487. https://doi.org/10.1109/ICESC57686.2023.10193659.

[32] Surendiran J., Kumar K. D., Sathiya T., et al., "Prediction of Lung Cancer at Early Stage Using Correlation Analysis and Regression Modelling," Proc. 4th Int. Conf. on Cognitive Computing and Information Processing, 2022, pp. 1–. https://doi.org/10.1109/CCIP57447.2022.10058630.
[33] Goud D. S., Varghese V., Umare K. B., Surendiran J., et al., "Internet of Things-based Infrastructure for the Accelerated Charging of Electric Vehicles," Proc. Int. Conf. on Computer Power and Communications, 2022, pp. 1–6. https://doi.org/10.1109/ICCPC55978.2022.10072086.
[34] Vidhya R. G., Singh K., Paul J. P., Srinivas T. A. S., Patra J. P., Sagar K. V. D., "Smart Design and Implementation of Self-Adjusting Robot using Arduino," Proc. Int. Conf. on Augmented Intelligence and Sustainable Systems, 2022, pp. 1–6. https://doi.org/10.1109/ICAISS55157.2022.10011083.
[35] Vallathan G., Yanamadni V. R., et al., "An Analysis and Study of Brain Cancer with RNN Algorithm-based AI Technique," Proc. Int. Conf. on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2023, pp. 637–642. https://doi.org/10.1109/I-SMAC58438.2023.10290397.
[36] Vidhya R. G., Bhoopathy V., Kamal M. S., Shukla A. K., Gururaj T., Thulasimani T., "Smart Design and Implementation of Home Automation System using Wi-Fi," Proc. Int. Conf. on Augmented Intelligence and Sustainable Systems, 2022, pp. 1203–1208. https://doi.org/10.1109/ICAISS55157.2022.10010792.
[37] Vidhya R., Banavath D., Kayalvili S., Naidu S. M., Prabu V. C., et al., "Alzheimer's Disease Detection using Residual Neural Network with LSTM Hybrid Deep Learning Models," J. Intelligent & Fuzzy Systems, 2023; vol. 45, no. 6, pp. 12095–12109. https://doi.org/10.3233/JIFS-235059.
[38] Balasubramaniyan S., Kumar P. K., Vaigundamoorthi M., Rahuman A. K., et al., "Deep Learning Method to Analyze the Bi-LSTM Model for Energy Consumption Forecasting in Smart Cities," Proc. Int. Conf. on Sustainable Communication Networks and Application, 2023, pp. 870–876 https://doi.org/10.1109/ICSCNA58489.2023.10370467.
[39] Somani V., Rahman A. N., Verma D., et al., "Classification of Motor Unit Action Potential Using Transfer Learning for the Diagnosis of Neuromuscular Diseases," Proc. 8th Int. Conf. on Smart Structures and Systems (ICSSS), 2022, pp. 1–7, IEEE. https://doi.org/10.1109/ICSSS54381.2022.9782209.
[40] Vidhya R. G., Saravanan R., Rajalakshmi K., "Mitosis Detection for Breast Cancer Grading," Int. J. Advanced Science and Technology, 2020; vol. 29, no. 3, pp. 4478–4485.
[41] Gupta D., Kezia Rani B., Verma I., et al., "Metaheuristic Machine Learning Algorithms for Liver Disease Prediction," Int. Res. J. Multidisciplinary Scope, 2024; vol. 5, no. 4, pp. 651–660. https://doi.org/10.47857/irjms.2024.v05i04.01204.
[42] Sudhagar D., Saturi S., Choudhary M., et al., "Revolutionizing Data Transmission Efficiency in IoT-Enabled Smart Cities: A Novel Optimization-Centric Approach," Int. Res. J. Multidisciplinary Scope, 2024; vol. 5, no. 4, pp. 592–602. https://doi.org/10.47857/irjms.2024.v05i04.01113.
[43] Vidhya R. G., Batri K., "Segmentation, Classification and Krill Herd Optimization of Breast Cancer," J. Medical Imaging and Health Informatics, 2020; vol. 10, no. 6, pp. 1294–1300. https://doi.org/10.1166/jmihi.2020.3060.
[44] Carboni D., "Feedback-based Reputation on Top of the Bitcoin Blockchain," arXiv preprint, 2015; arXiv:1502.01504.
[45] Alcaraz C., Roman R., Najera P., Lopez J., "Security of Industrial Sensor Network-Based Remote Substations in the Context of the Internet of Things," Ad Hoc Networks, 2013; vol. 11, no. 3, pp. 1091–1100. https://doi.org/10.1016/j.adhoc.2012.12.001.
[46] Arbaugh W., Farber D., Smith J., "A Secure and Reliable Bootstrap Architecture," Proc. IEEE Symp. on Security and Privacy, 1997, pp. 100–116.