International Journal of Basic and Applied Sciences, 14 (4) (2025) 229-236

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/y90y2496
Research paper

A Blockchain-Enabled Adaptive Learning Model for Secure and Scalable Data Sharing

Sudhir Anakal [1], Mohammad Arif [2], S. Artheeswari [3], K. Balaji [4], A. Pankajam [5], P. John Augustine [6], Maddula Ratna Mohitha [7], Anita Patil [8], H. Mickle Aancy [9], R. G. Vidhya [10] *

[1] Department of Master of Computer Applications, Sharnbasva University, Kalaburagi, Karnataka, India
[2] Department of Computer Science and Engineering, Alliance University, Bengaluru, Karnataka, India
[3] Department of AI and DS, Mailam Engineering College, Mailam, Tamil Nadu, India
[4] Department of Information Technology, SSM College of Engineering, Tamil Nadu, India
[5] Department of Business Administration, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu, India
[6] Department of Information Technology, Sri Eshwar College of Engineering, Coimbatore, Tamil Nadu, India
7 Department of CSE, Aditya Institute of Technology and Management, Andhra Pradesh, India
[8] Department of IOT & Cyber Security, City Engineering College, Bengaluru, Karnataka, India
[9] Department of MBA, Panimalar Engineering College, Chennai, Tamil Nadu, India
[10] Department of ECE, HKBK College of Engineering, Bangalore, India
**Corresponding author E-mail: vidhya50.ece@gmail.com*

Received: June 26, 2025, Accepted: August 1, 2025, Published: August 9, 2025

Abstract

The blockchain skillset is one of the most emerging skill sets that brings the world into the hands of the self. The number of industrial applications depends on this new technology just because of its decentralized, transparent, and secure nature. This enables a new way for the next generation of computing environments like cloud computing and edge computing. By keeping this in mind, this work develops a new disruptive method using adaptive learning model to address the security issues in a data sharing environment with decentralized access control. The developed framework has been executed and tested utilizing Python, and the results have been presented. A performance study comparison between the existing RSA algorithm, AES algorithm, and the proposed algorithm (ALM) has been done, and the various parameters taken for the study and their values are presented in this paper. Results obtained show that the algorithm presented is proven to be efficient in terms of security, scalability and time.

Keywords: *Cloud Computing; Edge Computing; Decentralized; Blockchain Skillset; Transparent.*

1. Introduction

In the past few years, blockchain technology has explosively come into widespread prominence and recognition in various fields, from cryptocurrencies to business applications [1], [2]. Its advancement is driving a transformative era in financial services and more, revolutionizing sectors like finance [3], energy [4], and citizen-centric organizations [5]. Originally launched as the technology behind Bitcoin, a digital, decentralized currency, blockchain is a distributed ledger technology that can process secure, clear, and tamper-proof transactions without reliance on a central authority [6], [7]. The power of blockchain is its decentralized design, in which transaction information is recorded throughout a network of participants to enhance transparency and security by use of cryptographic validation. This architecture supports decentralization, responsibility, and increased security, lowering the cost of operations and organizational effectiveness. These traits have contributed to the rapid growth of blockchain usage across different applications, and it has become the center of ongoing studies and development. In parallel, the accelerated evolution of communications and data technologies has also propelled the evolution of trend-setting technologies such as the Internet of Things (IoT) and cloud computing. IoT has revolutionized numerous industrial, consumer, and business uses by enabling it to bring physically different objects together to be controlled, monitored, and managed through ubiquitous electronic systems [8], [9]. Primarily, due to the low processing capabilities of IoT devices, the majority of IoT applications offload computing to cloud environments, and thus was born the name Cloud of Things (CoT) [10], [11]. CoT provides a robust and reliable distributed computing platform for managing IoT networks, improving system performance and network efficiency significantly [12]. However, traditional CoT architectures are prone to reliance on centralized communication models, such as cloud-based systems, that do not scale well with increasing IoT deployments [13]. In addition, the utilization of third-party cloud providers has attendant data privacy and security concerns, while the centralized paradigm promotes more communication latency and power consumption—concerns that compromise the

Copyright © Sudhir Anakal et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

sustainability and scalability of CoT systems in real-world applications [14]. It calls for the development of decentralized, adaptive systems that combine the benefits of blockchain and CoT. Combining the two holds out the possibility for enhanced security, scalability, and efficiency and unveils next-generation IoT infrastructures. This helps the future direction to modify the centralized computing models used in present applications, as shown in Figure 1.

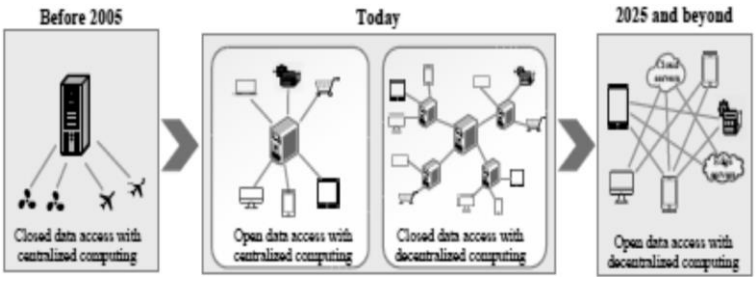

Fig. 1: Past, Present, and Future of Decentralized Access System.

2. Related work

Various assessments in CoT, blockchain, and other related difficulties and issues have been explored throughout the progression a very long time in a wide range of specific points. Various undertakings have been made to give overview articles on this investigation region in different degrees. The combination of the Cloud of Things (CoT) and blockchain technology has drawn significant interest over the past few years due to its potential to provide secure, decentralized, and transparent solutions for data sharing. The present section presents a review of recent studies in blockchain-based access control, adaptive learning models, and their applications in CoT settings. A few researchers have explored the use of blockchain to secure cloud and IoT ecosystems. Blockchain enables decentralized data management and the prevention of unauthorized access through immutable records. For example, Wang et al. (2021) proposed a blockchain-based secure data sharing model for IoT systems with a focus on traceability and data integrity. Similarly, Aloqaily et al. (2022) introduced BCoT (Blockchain for Cloud of Things), a scalable smart city resource architecture using blockchain to manage data exchange between IoT devices. These systems are prone to scalability and real-time access control, especially in large networks with dynamic nodes and large data sizes. Adaptive learning patterns have been used in dynamic security systems to support decision-making with success. The patterns can adjust encryption behavior from observed input patterns, thereby making systems more context-aware and intelligent. Li et al. (2020) noted the benefits of federated learning in decentralized networks where edge learning is conducted without central coordination. While they are good, most of the current systems do not integrate blockchain with adaptive learning for access control, leaving a gap in real-time encryption and auto-tuning key generation mechanisms. There have been a variety of access control models through blockchain, including: Role-Based Access Control (RBAC) using smart contracts, Attribute-Based Encryption (ABE) to restrict data access, and Permissioned blockchains for organizational inner control. For instance, Sharma et al. (2021) presented a survey of blockchain-based access control systems as having the ability to decentralize power and improve data clarity. Zhang et al. (2020) presented a blockchain platform for IoT that can support lightweight cryptographic processing. These frameworks are primarily fixed-access-rule-based and static-encryption-algorithm based such as RSA and AES, which cannot scale well at all and are not adaptive under dynamic conditions. From the above overview, it is clear that: Existing models that are blockchain-driven do not use adaptive learning for encryption. The majority of the models utilize static cryptographic functions, which increase complexity in decentralized settings. There has been limited study on real-time access control using blockchain and learning-based techniques. This paper proposes a novel Adaptive Learning Model (ALM) that combines the transparency of blockchain and the agility of machine learning. ALM utilizes prime number-based key generation and learning weights to establish a dynamic encryption mechanism that evolves and improves both security and scalability in decentralized environments. Figure 2 shows the Cyber physical creation framework.

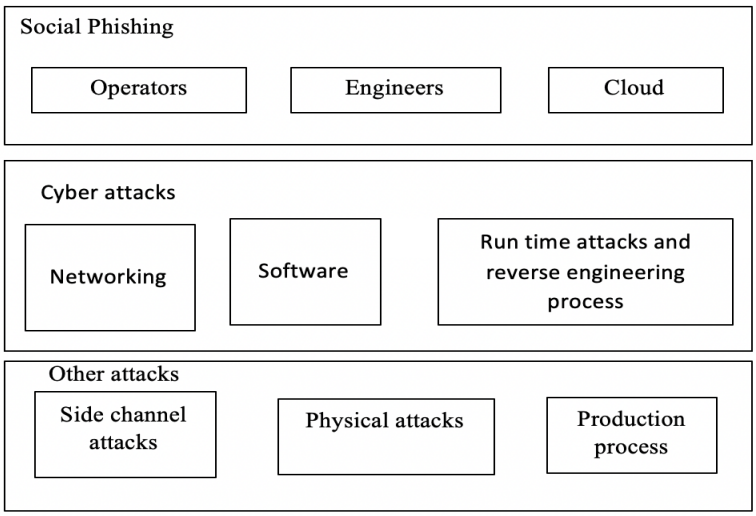

Fig. 2: Cyber Physical Creation Framework

Blockchain technology has emerged as a suitable option for secure data sharing across distributed networks due to its decentralized and immutable ledger aspect. It was made popular by Bitcoin [6], and since then it has been used in a variety of disciplines, including healthcare to supply chain management and protection of IoT data [15], [16]. Dai et al. (2020) have helped solve the scalability issues of blockchain systems through the introduction of methods such as shading and optimized consensus protocols, which offer higher transaction throughput

and system performance [17]. Permissioned blockchains such as Hyperledger Fabric have also supported controlled access and enhanced privacy for sensitive data use cases [18]. Despite these advancements, the inherent latency, power usage, and scalability of blockchain pose significant challenges, especially in large-area IoT networks [19]. Hybrid models that combine blockchain with edge and cloud computing have been proposed to address these constraints by offloading computation workloads and reducing network bottlenecks [20], [21]. Adaptive learning models (ALMs) play a critical role in enabling systems to dynamically adapt to varying data and network conditions, and improve robustness and performance. In secure data sharing settings, ALMs facilitate maximum resource optimization, anomaly detection, and adaptive cryptographic countermeasures that react to evolving threat environments [22]. To give an example, intrusion detection systems based on machine learning complemented with blockchain technology have been shown to boost security in IoT networks [23]. Zhang et al. (2021) envisioned a dynamic adaptive blockchain consensus protocol that self-regulates operational parameters as functions of network states, enhancing throughput and fault tolerance [24]. Nevertheless, learning adaptation wholesale into blockchain is a future direction of research in which finding trade-offs between adaptability and computational overheads is a critical issue [25]. IoT and Cloud of Things (CoT) networks are defined by unique security challenges due to resource-constrained devices and the sheer magnitude of heterogeneous networks. CoT architectures leverage cloud capabilities for IoT but tend to be based on centralized data management, which is a source of concern for privacy and trust [26]. Blockchain technology provides a decentralized trust model that can impose data integrity and secure communication on CoT systems [27]. Blockchain-based identity management models and lightweight cryptographic schemes have been proposed to fit the limitations of IoT devices with preserving security [28], [29]. Existing work emphasizes the importance of incorporating blockchain with adaptive security functions to enable real-time threat detection and reaction, providing continuous protection in dynamic IoT settings [30]. Scalability remains a persistent issue in blockchain-based data sharing technologies, particularly for IoT and CoT scenarios. Traditional consensus protocols such as Proof-of-Work (PoW) are energy-intensive and not suitable for low-resource devices [31]. Other consensus mechanisms, e.g., Proof-of-Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT), have been discussed to reduce latency and energy consumption [32]. Moreover, hybrid architectures combining blockchain with fog and edge computing frameworks are discussed to offload processing and relieve network loading [33], [34]. Adaptive learning approaches are increasingly implemented to enhance the assignment of network resources and dynamically adapt blockchain configurations based on workload and threat discovery parameters [35]. Overall, while great advancements have been made in utilizing blockchain for secure data sharing and incorporating adaptive learning to enhance system responsiveness, employing these two technologies to address both security and scalability constraints within massive-scale IoT and CoT systems is not been explored [36], [37]. This work attempts to bridge this gap by introducing a blockchain-based adaptive learning model to facilitate secure, scalable, and effective data sharing [38], [39].

3. System framework

Literature survey reveals that existing systems primarily employ sharing schemes tailored for decentralized storage, but not many of them contain an entire access policy for users. Further, most existing techniques require separate algorithms for decryption and encryption, which is quite cumbersome to make decentralized access control systems secure. To combat these limitations, an independent attribute and ciphertext-based system must be employed to minimize complexity in access control with enhanced security [40], [41]. The system design framework introduced in the Figure shows the Pseudocode: Adaptive Learning Encryption. The framework consists of access points, microservices, a blockchain cluster, an internal repository of users, and a multi-organization environment. Each organization possesses its access point to manage user permissions, either granting or revoking access [42], [43]. The cluster of blockchains acts as a system of distributed ledgers, spreading data across nodes and setting access controls based on pre-programmed rules of blockchain. It also holds shared data and stores access control history [44], [45]. Microservices, however, offer intrinsic modular features that are embedded in the system for facilitating efficient and scalable processes. The internal user repository is used to manage user credentials locally for facilitating the decentralized aspect of the blockchain [46], [47].

4. Implementation and results

Blockchain technology is at the center of the above system architecture. At the center of the blockchain infrastructure is the node. The node can either be a computer or a user that possesses a full replica of the blockchain ledger, which is essentially a data structure holding transactions. These nodes combined form the blockchain network, which it is their responsibility to hold, spread, and keep all the blockchain data. It is to be understood that the blockchain virtually resides in all nodes of the network. Processing transactions is one of the primary operations carried out by nodes [48,49]. Figure 4 is a block diagram explaining the process of a blockchain transaction via node-to-node communication to show how information is securely passed and authenticated in the network [50], [51]. When a request for making a transaction is received, the system creates a new block to signify that the transaction process is initiating. The newly created block is sent to other nodes active within the network to inform them of its status. The nodes later confirm the transaction [52], [53]. Upon confirmation, the nodes are rewarded as proof of work. Block is subsequently added to the existing blockchain, and thereby the transaction gets completed. Following the end of each transaction, the adaptive learning system analyzes its advantages and disadvantages, recording the outcome of learning accordingly. This way, security is continuously enhanced through the proposed Adaptive Learning Model (ALM) algorithm. The encryption and decryption method employed in the present system is shown in Figure 5. Whenever plaintext input data is input, it gets converted to ciphertext through a data key and an encryption procedure. The master key and the data key are first generated, followed by the encrypted data key being used to produce the encrypted message. The adaptive learning model adapts this process to dynamically create encrypted outputs. The algorithm that has been used employs prime numbers as a central element of the encryption and decryption process, thereby adding security. When blocks are created and added to the chain, the AI model gathers input data, processes the data, and adjusts the encryption parameters accordingly. This adjustment in real-time guarantees that, even in a decentralized access network, the blocks remain encrypted by unpredictable and untraceable processes, thereby reducing the risk of hacking significantly. The algorithm is effective in encrypting massive bodies of text data, such as Word documents, and can handle more than 10,000 words per session. Below is a clip from the algorithm as a reference. The algorithm primarily relies on weights within the learning model. A prime number is used as an input for the first block when the algorithm is run for the first time. As these weights shift with time, the algorithm gives an anonymous encryption and decryption mechanism, thus ensuring robust security for decentralized access control. The adaptive learning model algorithm iterates in linear time complexity using a single while loop and incrementally updates. Its time complexity is therefore O(n). The appearance of the notation '?' in the algorithm is an asymptotic notation, and it reflects the linear scaling behavior of the learning rate. The iterative step-by-step improvement of the learning process is captured by the adaptive learning paradigm. For clarity, the algorithm sample

input and output data are shown in Figures 6a and 6b, respectively. The performance of the ALM algorithm is also compared with standard encryption algorithms such as RSA and AES. This comparison is represented in Table 1 to show the new method's encryption efficiency.

```
Input:
   D  ← Input data stream (plaintext)
   P  ← Prime number (encryption seed)
   W0 ← Initial weight
   K  ← Master key (optional)

Output:
   C  ← Encrypted data stream

1: Initialize weight ← W0
2: Initialize index ← 0
3: Initialize C ← empty list
4: For each character ch in D do
5:     val ← ASCII(ch)
6:     DK ← (val × weight) + P
7:     Enc ← (val + DK + index) mod 256
8:     Append Enc to C
9:     weight ← weight + 1
10:    index ← index + 1
11: End For
12: Optionally, apply final encryption on C using key K
13: Return C
```

Fig. 3: Pseudocode: Adaptive Learning Encryption.

The Adaptive Learning Model (ALM) is a novel encryption framework designed to enhance security and scalability in decentralized environments such as Blockchain-enabled Cloud of Things (BCoT) systems. The algorithm introduces a learning-based dynamic key generation approach, where encryption keys evolve based on previous interactions, weights, and prime-number-based initializations. The goal is to eliminate key predictability, enhance resistance to pattern analysis, and reduce encryption time through lightweight operations.

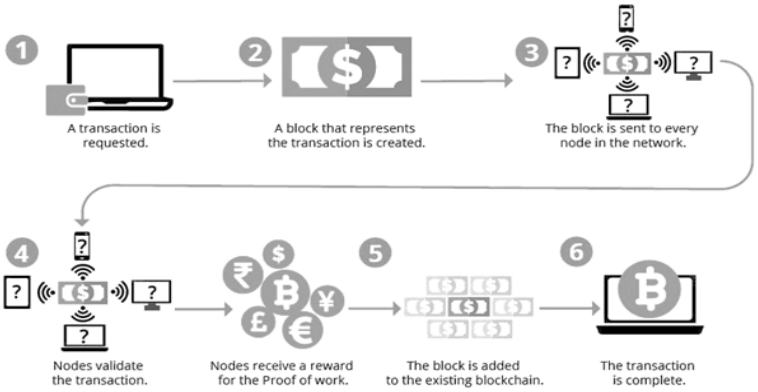

Fig. 4: An Example Blockchain Transaction.

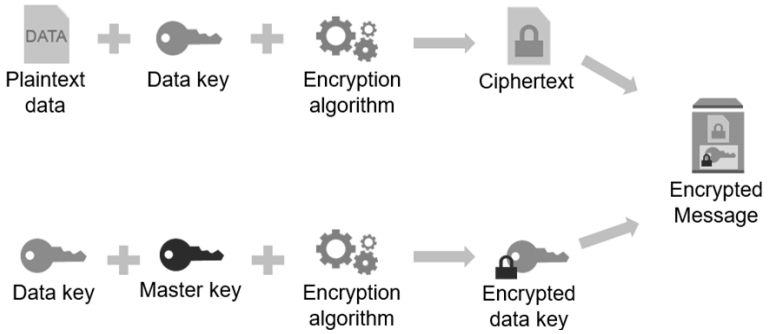

Fig. 5: Methodology Used for Encryption and Decryption.

Table 1 provides a comprehensive feature comparison of the AES, RSA, and proposed ALM encryption algorithms. It highlights key aspects such as algorithm type, key length, encryption speed, security level, scalability, and adaptability. The table illustrates how ALM combines the strengths of both symmetric and asymmetric approaches while introducing adaptive learning to enhance security in decentralized environments. Table 2 compares the time taken by AES, RSA, and ALM algorithms to complete encryption across different data sizes. The results demonstrate AES's efficiency for bulk data, RSA's slower performance due to computational complexity, and ALM's linear scalability, which offers a balanced solution suitable for secure, large-scale data sharing in blockchain-enabled systems.

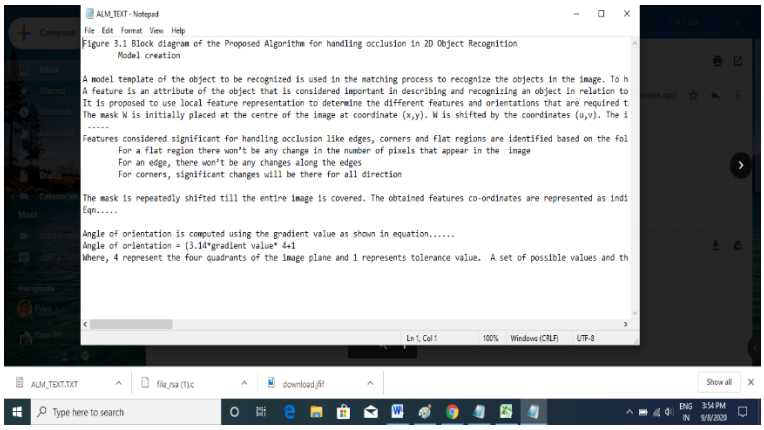

Fig. 6: A) Sample Input for Algorithm Testing.

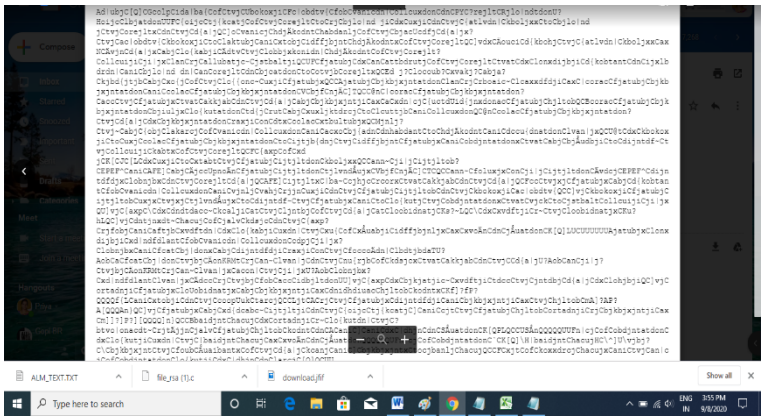

Fig. 6: B) Sample Encrypted Output.

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

Feature	AES	RSA	ALM (Adaptive Learning Model)
Type of Algorithm	Symmetric key encryption	Asymmetric key encryption	Adaptive learning-based encryption
Key Length	128, 192, or 256 bits	Typically 1024 to 4096 bits	Uses prime numbers and dynamic weights
Encryption Speed	Fast	Slower due to complex math	Moderate, with linear time complexity (O(n))
Security Level	High, widely trusted	High, but depends on key length	High, with dynamic, untraceable encryption
Scalability	Suitable for large data volumes	Less suitable for large data	Designed for scalable decentralized systems
Computational Complexity	Low to moderate	High	Linear time complexity, efficient
Key Management	Requires secure key distribution	Public/private key pair	Dynamic key setup via adaptive learning
Resistance to Attacks	Strong against brute force	Vulnerable to quantum attacks	Designed to adapt and resist evolving threats
Use Case	Bulk data encryption	Secure key exchange, digital signatures	Secure decentralized data sharing
Adaptability	Static keys	Static keys	Adaptive encryption process that evolves over time

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

Data Size	AES Encryption Time (ms)	RSA Encryption Time (ms)	ALM Encryption Time (ms)
1 KB	1	15	5
10 KB	5	120	50
100 KB	40	1100	500
1 MB	350	12,000	4,800
10 MB	3,400	Not practical	48,000

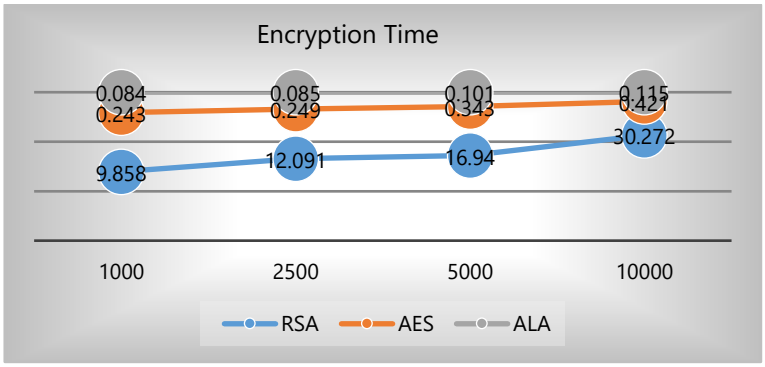

Fig. 7: Encryption Time AES vs RSA vs ALM Algorithm.

From Figure 7, it has been noted that the proposed ALM algorithm completed the encryption in a very short time in comparison with the standard AES and RSA algorithms. Also, it has been noted that the algorithm handles with high accuracy of encryption rate in less time. This has been tested using different sample words varying from 1000 to 10000, and the results obtained are shown in Figure 8 for better understanding.

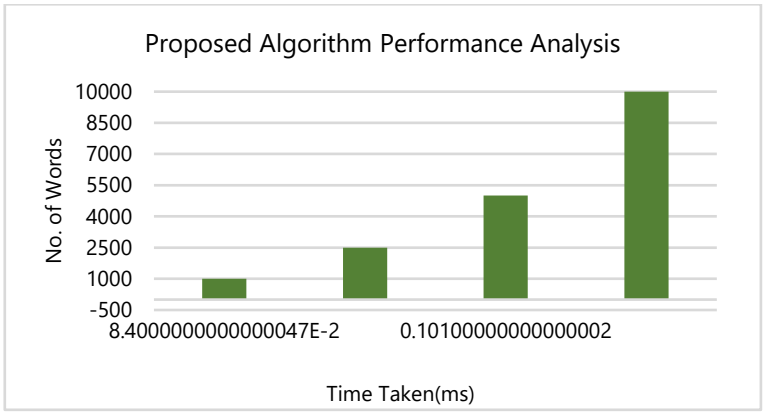

Fig. 8: Performance Analysis of Proposed Algorithm.

5. Conclusion

In summary, the paper presents a new blockchain-enabled Adaptive Learning Model (ALM) to facilitate secure and scalable data sharing in decentralized environments. With the integration of adaptive learning and blockchain, the proposed system remedies some of the largest drawbacks of traditional encryption methods, such as complexity, scalability, and vulnerability to emerging security attacks. The prime number-based protection and linear time complexity of the dynamic encryption of the ALM algorithm ensure robust security with efficiency even for colossal amounts of data. A comparative analysis reveals that ALM provides a promising compromise between the high speed of symmetric algorithms like AES and the high security of asymmetric algorithms like RSA. The decentralized access control mechanism of the framework also enhances security and flexibility at different organizational levels. Future work will focus on the development of the model for real-world large-scale applications and exploring integration with future technologies such as 5G and quantum-resistant cryptography. In summary, the ALM approach provides a valuable contribution towards secure, adaptable, and scalable data sharing solutions in modern distributed systems.

6. Discussion and future directions

The proposed blockchain-based Adaptive Learning Model (ALM) has promising prospects in increasing secure and scalable data sharing in decentralized environments. The integration of adaptive learning with blockchain technology not only strengthens the encryption using dynamic and untraceable methods but also reduces computational overhead with the ability to operate at linear time complexity. It is fairer in the trade-off between security and encryption speed than the traditional algorithms such as RSA and AES, and thus appropriate for big-data IoT and CoT systems. Nevertheless, there are a few limitations and open issues that deserve further investigation. Although the existing model is efficient at combating encryption and decentralized access control, its scalability with ultra-large and heterogeneous networks needs to be studied more deeply. Moreover, the robustness of the system against new threats, especially quantum computing attacks, is an aspect that can be improved. The computational cost added by adaptive learning, though effective, may also be optimized to an even greater extent to help minimize latency in real-time settings. Future research could explore the integration of ALM with emerging communication technology such as 5G networks, which would facilitate faster and more secure data exchange in IoT networks. Another key area of research is the incorporation of quantum-resistant cryptographic methods to future-proof the security mechanism against quantum computer advancements. Lastly, expanding the framework to support multiple master nodes or decentralized autonomous organizations (DAOs) would enhance its applicability to complex multi-stakeholder contexts. Aside from technical innovation, attention to the ethical and social considerations of safe data sharing is warranted. Through enabling secure and transparent data management, ALM can foster greater user confidence in IoT systems, which is a prerequisite for its wider adoption. It is also necessary to address privacy concerns and compliance with international data protection regulations in current implementations. Overall, while the present work provides a sound basis, there remains a need for further refinement and extension to properly exploit the potential of blockchain-enabled adaptive learning models in secure, scalable, and user-friendly data sharing applications.

References

[1] Zheng, Zibin&Xie, Shaoan& Dai, Hong-Ning& Chen, Xiangping& Wang, Huaimin. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services. 14. 352. https://doi.org/10.1504/IJWGS.2018.095647.

[2] Detlef, Z. (2008) SmartFactory — From Vision to Reality in Factory Technologies. International Federation of Automatic Control, 17th IFAC World Congress (IFAC'08)Seoul, Korea, July 6-11

[3] Choi, J (2019) Secure Multiparty Computation and Trusted Hardware: Examining Adoption Challenges and Opportunities, Security and Communication Networks, Vol. 2019, https://doi.org/10.1155/2019/1368905.

[4] Carboni, D. (2015) Feedback based Reputation on Top of the Bitcoin Blockchain, arXiv preprint arXiv:1502.01504 [2] C. Alcaraz, R. Roman, P. Najera, and J. Lopez. Security of industrial sensor network-based remote substations in the context of the internet of things. Ad Hoc Netw., 11(3), 2013. https://doi.org/10.1016/j.adhoc.2012.12.001.

[5] W. Arbaugh, D. Farber, and J. Smith. A secure and reliable bootstrap architecture. In IEEE Symposium on Security and Privacy (S&P), 1997.

[6] F. Armknecht, A.-R. Sadeghi, S. Schulz, and C. Wachsmann. A security framework for the analysis and design of software attestation. In ACM Conference on Computer & Communications Security (CCS). ACM, 2013. [5]. https://doi.org/10.1145/2508859.2516650.

[7] F. Brasser, P. Koeberl, B. E. Mahjoub, A.-R. Sadeghi, and C. Wachsmann. TyTAN: Tiny trust anchor for tiny devices. In Design Automation Conference (DAC). ACM, 2015. https://doi.org/10.1145/2744769.2744922.

[8] E. Byres and J. Lowe. The myths and facts behind cyber security risks for industrial control systems. Technical report, PA Consulting Group, 2004.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.
[40] 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.
[41] 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.
[42] 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.
[43] 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.
[44] 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.
[45] 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.
[46] 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.
[47] 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.
[48] 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.
[49] Chintureena Thingom, Martin Margala, S Siva Shankar, Prasun Chakrabarti, RG Vidhya, "Enhanced Task Scheduling in Cloud Computing Using the ESRNN Algorithm: A Performance-Driven Approach", Internet Technology Letters, vol. 8, no. 4, 2025, pp. e70037. https://doi.org/10.1002/itl2.70037.
[50] V. V. Satyanarayana, Tallapragada, Denis R, N. Venkateswaran, S. Gangadharan, M. Shunmugasundaram, et.al.," A Federated Learning and Blockchain Framework for IoMT-Driven Healthcare 5.0", International Journal of Basic and Applied Sciences, vol. 14, no. 1, 2025, pp. 246-250. https://doi.org/10.14419/n1npsj75.
[51] Thupakula Bhaskar, K. Sathish, D. Rosy Salomi Victoria, Er.Tatiraju. V. Rajani Kanth, Uma Patil, et.al.," Hybrid deep learning framework for enhanced target tracking in video surveillance using CNN and DRNN-GWO", International Journal of Basic and Applied Sciences, vol. 14, no. 1, 2025, pp. 208-215. https://doi.org/10.14419/wddeck70.
[52] Thupakula Bhaskar, Hema N, R.Rajitha Jasmine , Pearlin , Uma Patil, Madhava Rao Chunduru , et.al.," An adaptive learning model for secure data sharing in decentralized environments using blockchain technology", International Journal of Basic and Applied Sciences, vol. 14, no. 1, 2025, pp. 216-221. https://doi.org/10.14419/9f4z3q54.
[53] B. Ramesh, V. V. Kulkarni, Ashwini Shinde, Dinesh Kumar J. R, Prasanthi Kumari Nunna, Rajendiran M, "Optimizing EV Energy Management Using Monarch Butterfly and Quantum Genetic Algorithms" International Journal of Basic and Applied Sciences, vol. 14, no. 2, 2025, pp. 311-318. https://doi.org/10.14419/xaqk1294.