



Research Article

Threat Intelligence Sharing in Cloud Environments: Enhancing Security Using Blockchain

Kannan Srinivasan¹, Guman Singh Chauhan², Rahul Jadon³, Rajababu Budda⁴,
Venkata Surya Teja Gollapalli⁵, Prema R^{6*}

¹Saiana Technologies Inc, New Jersey, USA

²John Tesla Inc, California, USA

³CarGurus Inc, Massachusetts, USA


⁴IBM, California, USA

⁵Centene Management LLC, Florida, United States

⁶Department of CSE, Tagore Institute of Engineering and Technology, Deviyakurichi, Tamil Nadu, India

Corresponding Author: *Prema R

DOI: <https://doi.org/10.5281/zenodo.15052446>

Abstract	Manuscript Information
<p>As cyber threats evolved, the necessity of secure and effective sharing of threat intelligence in cloud environments has developed ever more urgently. Centralized methods are confronted with serious limitations, such as risks of data integrity, transparency issues, and scalability limitations. It introduces the Enhancing Security Using Blockchain paper, which has been cited for overcoming the aforementioned problems. This system leverages blockchain technology to achieve decentralized threat intelligence sharing, as well as to provide tampering evidence and transparency. The proposed method is to secure the data on an Ethereum blockchain while utilizing ABE for fine-grained access control to ensure that only permissible persons can access sensitive data. Smart contracts also automate the verification process and transactions to be more secure and efficient. Machine learning methods such as logistic regression, random forest, and CNNs are used to capture cyber threat patterns and optimize risk detection. Experimental verification indicates that the ensemble model is 92% accurate, surpassing traditional security measures in detecting cyber-attacks and maintaining data integrity. Moreover, trust between parties is promoted by blockchain, preventing data manipulation and enabling transaction processes with low latency. These advantages notwithstanding, there are future studies in computational overhead, government regulation-compliance, and existing cloud infrastructure integration as their scope. The emphasis of this research will be on how to improve cybersecurity through the sharing of threat intelligence using blockchain with secure, transparent, and scalable methods of managing such threats in cloud environments. The future work will focus on blockchain storage optimization, improving computational efficiency accompanied by better consensus schemes for scalability and acceptance.</p>	<ul style="list-style-type: none"> ▪ ISSN No: 2583-7397 ▪ Received: 29-01-2025 ▪ Accepted: 19-02-2025 ▪ Published: 18-03-2025 ▪ IJCRM:4(2); 2025: 53-59 ▪ ©2025, All Rights Reserved ▪ Plagiarism Checked: Yes ▪ Peer Review Process: Yes <p style="text-align: center;">How to Cite this Article</p> <p>Srinivasan K, Chauhan GS, Jadon R, Budda R, Gollapalli VST, Prema R. Threat intelligence sharing in cloud environments: enhancing security using blockchain. Int J Contemp Res Multidiscip. 2025;4(2):53-59.</p> <p style="text-align: center;">Access this Article Online</p> <div style="text-align: center;">  </div> <p style="text-align: center;">www.multiarticlesjournal.com</p>

KEYWORDS: Blockchain Security, Threat Intelligence Sharing, Cloud Security, Attribute-Based Encryption, Smart Contracts, Cyber Threat Detection.

1. INTRODUCTION

In line with the adoption of cloud computing, organizations depend on threat intelligence sharing to boost their cybersecurity walls (Bobba 2021) ^[5] sharing effective threat intelligence would lead to early detection and mitigation of cyber threat related incidents, as well as lower the chances of a great mass attack resulting from one attack (Devarajan *et al.* 2024) ^[6]. However, the secure, reliable, and tamper-proof exchange of threat intelligence remains a significant challenge in cloud environments (Gudivaka *et al.* 2024) ^[8]. Significant problems associated with threat-intelligence sharing include data integrity issues, unauthorized access, lack of trust among parties, and an array of cyber threats, such as manipulation and, most importantly, breaches of data (Gollavilli 2022) ^[7] Common pitfalls festering in centralized storage and communication systems include single points of failure and security risks in large-scale threat intelligence networks without putting much stress on the effectiveness of these centralized systems (Kadiyala, Alavilli, and Alfa 2025) ^[8].

These threat-sharing mechanisms include centralized databases, cloud-based repositories, and private networks. However, these mechanisms have to face external tremendous challenges (Ayyadurai 2020) ^[3]. Centralized databases are vulnerable to unauthorized changes and data-tampering attacks and bear issues of integrity (Kodadi 2020) ^[12]. Trust issues are set in as organizations never choose to share sensitive threat data due to the lack of transparency of traditional systems and strong security guarantees (Sareddy and Khan 2025) ^[18]. Moreover, these solutions do not scale and perform well enough to effectively address the gathering and distribution of threat intelligence on a large, real-time scale (Srinivasan and Awotunde 2021) ^[19]. In order to resolve the constraints above, a more secure and transparent, and highly scalable solution for information-sharing solutions needs to be created for better threat intelligence sharing (Valivarthi. and Kurniadi. 2025) ^[20].

The research proffers that Enhanced Security Using Blockchain for threat intelligence sharing in cloud environments could solve the challenges. The decentralized and immutable ledger of Blockchain guarantees data integrity, transparency, and secured access control. Using smart contracts and consensus mechanisms with cryptographic techniques, blockchain increases trust and prevents unauthorized modification while allowing effective threat intelligence sharing among cloud-based organizations. This significantly enhances resilience to cyber threats and allows organizations to work together to ensure that cyber threats are tackled as efficiently as possible.

1.1 Key Contribution

This study proposes a secure, decentralized, and scalable threat intelligence sharing system based on blockchain and AI-enabled threat analysis.

- Blockchains were created to distribute threat intelligence data securely in cloud environments.
- Integrated Ethereum blockchain for secured storage and Attribute-Based Encryption (ABE) for access control.

- Smart contracts were used to achieve automatic verification and transaction processes with guarantees for confidentiality and transparency.
- Machine learning models including logistic regression, random forest, and CNNs were deployed to analyze cyber threat patterns and detect risks.
- Experimental results proved the better performance of the ensemble model with standard security mechanisms against accuracy and data integrity compromises.

Section 2 explains developments in threat intelligence sharing, with discussion on blockchain and AI models. Proposition and problem statement are given in Section 3, where data integrity, trust, and scalability issues are discussed. The ABE-Based Blockchain Framework for secure sharing of threat intelligence is proposed in Section 4. Evaluation of certain performance metrics like TPS, latency, and storage overhead is done in Section 5, while Section 6 concludes with future research directions about scalability and improvements in encryption.

2. LITERATURE REVIEW

Peddi and Leaders (2021) ^[15] suggested that VCC should have cryptographic techniques, trust management models, and intrusion detection systems. In such cases, the methodologies suffer from limitations like extremely high computational overheads, issues with scalability, and their vulnerability to changing patterns in cyber threats. Peddi, Narla, and Valivarthi (2019) ^[16] used AI techniques such as Logistic Regression, Random Forest, and CNN in predictive modeling for geriatric health care, with limitations such as data quality issues, interpretability of the model, and heavy computational resource demand.

The anomalies in the cloud environment for e-commerce transaction security are further enhanced by other Machine learning-based anomaly detection and predictive modeling approaches detailed in Ayyadurai (2022) ^[4]. However, it is challenged by data privacy, high computational costs, and the need for strong encryption and access control. Jyothi Bobba (2024) ^[9] proposed that AI techniques, including regression analyses for predictive maintenance and k-means clustering for anomaly detection, would improve the security of financial data in cloud environments; however, there are challenges, mainly computational complexity, false positives in anomaly detection, and data privacy.

Nagarajan (2024) ^[14] compared cloud versus traditional bank security especially encryption, authentication, and compliance, limitations set by evolving cyber threats and third-party vulnerabilities. The use of the Nudge theory in combination with blockchain for secure, transparent financial transactions in learning to health insurance was by Kodadi (2023) ^[13]. Integration, regulatory compliance, and adoption hurdles impede it.

3. Problem Statement

For instance, cybersecurity methods such as cryptographic, AI models, and blockchain solutions have great promising

advancements; however, certain limitations do exist in those solutions (Kethu and N 2021) [11]. Cryptographic and trust management models often have many challenges like high computational overhead, scalability issues, and open-ended vulnerability to future emerging threats (Alagarsundaram 2024) [1]. AI approaches, which incorporate machine-learning anomaly detection and predictive modeling, are hindered by the quality of the data, lack of interpretability of the results, and high computational requirements (Allur 2020) [2]. Blockchain security solutions, raise transparency and security; however, they face inherent challenges with integration, regulation, and adoption hurdles (Yallamelli 2019) [21]. Many of these challenges show that it is increasingly pertinent for security frameworks to

advance to counter the evolving security threats arising in the cloud environment.

4. Framework for Threat Intelligence Sharing on the Blockchain

The framework proposed here is intended for secure sharing of threat intelligence about cloud environments using blockchain and encryption techniques. The process would include data collection-the collection of threat intelligence from various sources- and preprocessing with one-hot encoded categorical data for a structured format. The processed data then integrates into the Ethereum blockchain to ensure it is tamper-proof and decentralized is displayed in Figure (1),

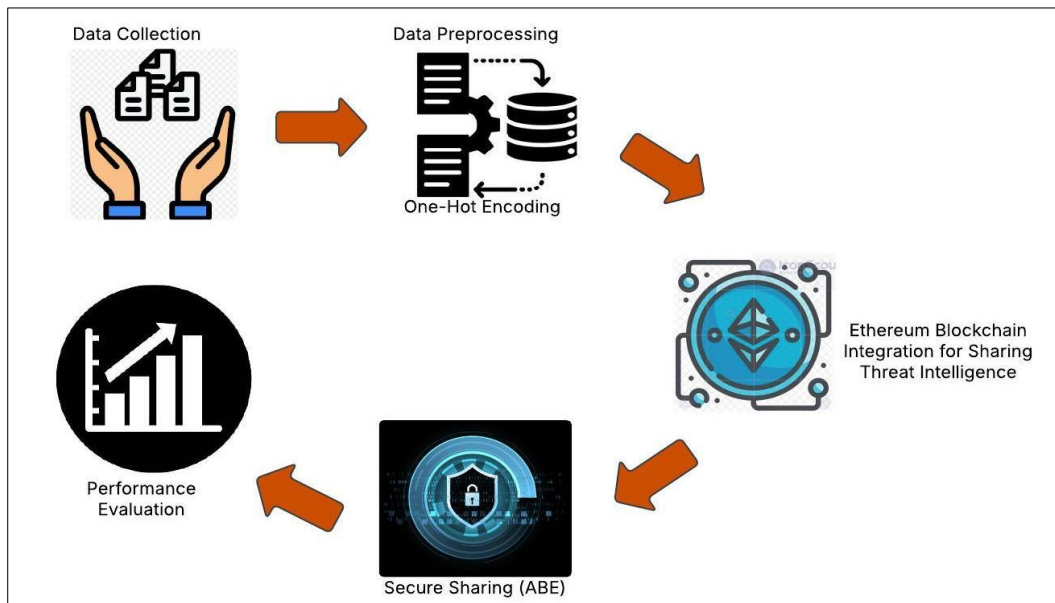


Figure 1: Secure Threat Intelligence Sharing Using Blockchain and Encryption

Restricting confidentiality, Attribute-Based Encryption (ABE) is applied to access only authorized entities. Finally, the performance evaluation is done by which the efficiency, security, and scalability of the framework are measured. Thus, using the immutability of blockchain and the access control possible with ABE strengthens the data integrity, trust, and security for cloud-based threat intelligence sharing.

4.1 Data Collection

The Cyber Threat Intelligence Dataset supports the detection, diagnosis, and mitigation of cyber threats based on network traffic data, text content, and entity relationships. It features primary fields like id, text, entries, relations, diagnosis, and solution. This dataset is useful for applications such as threat detection, intelligence analysis, incident response, network monitoring, and research (Ramoliya Fenil, n.d.) [17].

4.2 Pre-processing Using One-Hot Encoding

One-hot encoding is a preprocessing technique that converts categorical data into numerical form that can be read by

machines. Instead of assigning categories to random numbers, it produces a binary vector representation such that no spurious ordinal relationships are created. Mathematical Representation Let a categorical variable have C different values. Each value is encoded in a vector of size as presented in Eq. (1),

$$b_i = \begin{cases} 1, & \text{if the category at position } i \text{ is present} \\ 0, & \text{otherwise} \end{cases} \dots\dots\dots (1)$$

Therefore, a categorical variable X with possible values {c1, c2, cC} is converted as Eq. (2),

$$O(X) = [\delta(X, c_1), \delta(X, c_2), \dots, \delta(X, c_C)] \dots\dots\dots (2)$$

where the indicator function $\delta(X, c_i)$ is described in Eq. (3),

$$\delta(X, c_i) = \begin{cases} 1, & \text{if } X = c_i \\ 0, & \text{otherwise} \end{cases} \dots\dots\dots (3)$$

4.3 Ethereum Blockchain Integration for Sharing Threat Intelligence

Ethereum Blockchain provides secure, transparent, and tamper-proof storage of cyber threat intelligence. Through the use of cryptographic methods, it does not allow any data tampering and provides authenticity. The fundamental processes in this integration are as follows,

4.3.1 Hashing Data for Integrity

Prior to storage of threat intelligence information, it is hashed into a cryptographic hash to guarantee immutability. Hashing guarantees that any slight alteration of the data will yield a totally different hash, and thus, unauthorized alterations are detectable as specified in Eq. (4),

$$H(D_i) = \text{Hash Function}(D_i) \dots\dots\dots (4)$$

Where, D_i is the original data, $H(D_i)$ is the cryptographic hash (e.g., SHA-256).

4.3.2 Digital Signature for Authenticity

In order to authenticate the data, a digital signature is created with the help of the sender's private key. Based on this process, receivers can authenticate the identity of the sender with their public key so that the data cannot be changed in transit as indicated in Eq. (5)

$$\text{Sign}_{sk}(H(D_i)) \dots\dots\dots (5)$$

Where, sk is the private key of the sender, $\text{Sign}_{sk}(H(D_i))$ is the digital signature.

4.3.3 Ethereum Blockchain Transaction and Validation

After hashing and signing the data, it is appended as a transaction to the Ethereum Blockchain. This ensures immutability, prohibits unauthorized tampering, and locks threat intelligence data in the blockchain is stated in Eq. (6),

$$T_i = H(D_i) + \text{Sign}_{sk}(H(D_i)) \dots\dots\dots (6)$$

Where, $H(D_i)$ is the cryptographic hash of data, $\text{Sign}_{sk}(H(D_i))$ is the digital signature based on the sender's private key. To provide security, the transaction is checked through a consensus mechanism, like PoW or PoS. Transactions are then combined into a block as specified in Eq. (7)

$$B_j = [T_1, T_2, \dots, T_n] + H(B_{j-1}) \dots\dots\dots (7)$$

Where B_j is a new block of several transactions, $H(B_{j-1})$ is the previous block's hash, to create continuity.

4.4 Attribute-Based Encryption for Secure Sharing

ABE protects data by encrypting it against a predefined set of attributes such that only authorized users with the same attributes can decrypt it.

4.4.1 Encryption of Data

The encryption process converts the plaintext message to ciphertext is given as Eq. (8),

$$C = E_{pk}(M, A) \dots\dots\dots (8)$$

Where, C is ciphertext (encrypted data), E_{pk} is the public key encryption function, M is the original message (threat intelligence or sensitive information), A is access control policy attributes set.

4.4.2 Decryption Process

A user who possesses a corresponding attribute set A' can decrypt the ciphertext with their secret key. When A' meets the access policy, the user successfully restores M , otherwise decryption will fail is modeled as Eq. (9),

$$M = D_{sk}(C, A') \dots\dots\dots (9)$$

Where, D_{sk} is the decryption function with the secret key sk , A' is the user's attribute set.

5. RESULTS AND DISCUSSION

The analysis indicates that as the TPS moves up, greater efficiency in the transaction processing improves with lesser latency on the blockchains. Initially, due to network congestion at higher transaction processing speeds, latency is high but begins to decline and stabilizes optimally. Such modern blockchains like Hyperledger Fabric and Ethereum 2.0 thus use different advanced consensus mechanisms including PoS and PBFT to expedite processed blocks, though under conditions of extreme TPS, the network will still be under pressure and thus will require some other scaling techniques. Then in addition, starting at high transaction speeds, the relatively higher burden of storage caused by all the extra cryptographic signatures, metadata, and transaction records is increased. This represents a trade-off between scalability and storage efficiency, emphasizing the need for optimized storage management in blockchain systems.

5.1 Relationship Between Transaction Throughput and Blockchain Latency

Graphically representing these characteristics is the inverse relationship that exists between TPS and Blockchain Latency: increased TPS generally translates into decreased latency. The initial trend shows latency pivoting back and forth at higher levels (50-100 TPS) ~0.85s to ~0.75s; this behavior is accounted for by heavy network congestion and slow block validation. However, as the TPS rises (125-200 range), latency begins to decline regularly by amounts around ~0.10s from the previous values of (~0.65s to ~0.55s), one more time signaling a better transaction process. At the highest TPS levels (225-250), latency rates reach the lowest values (~0.50s) to mean that the optimized blockchain performance, as seen in Figure (2), is being achieved.

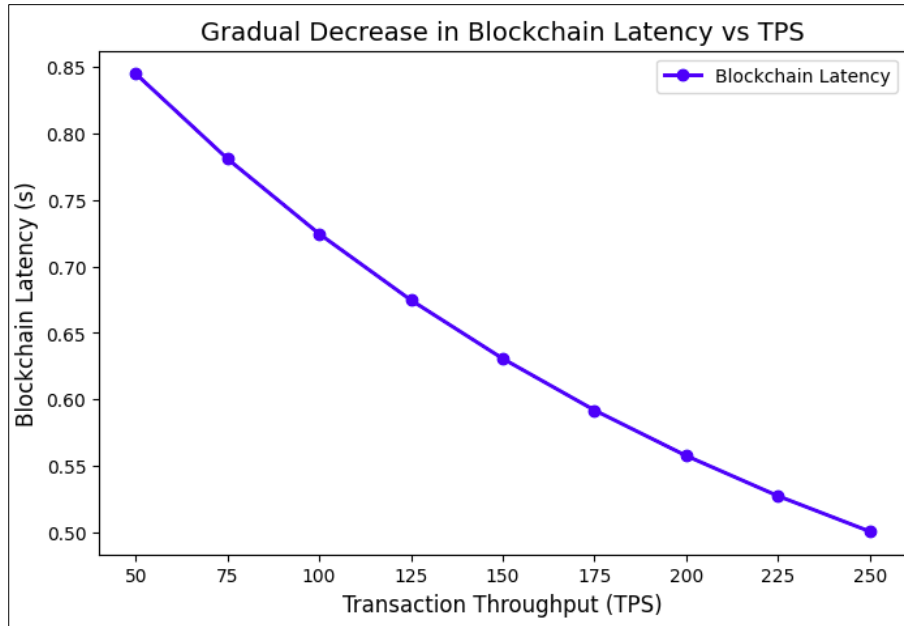


Figure 2: Impact of Transaction Throughput on Blockchain Latency

Nevertheless, the decrease in performance varies non-linearly, indicating that the efficiency is enhanced at heightened levels of TPS, but the performance improvement has diminishing returns against the constraints of the system. This characteristic is normal to modern blockchains such as Hyperledger Fabric and Ethereum 2.0, where good consensus mechanisms (PoS, PBFT) are helping to reduce the impact of latencies. However, an excessively high level of TPS may still strain the network, requiring further optimizations such as sharding or layer-2 scaling for efficient performance.

5.2 Blockchain Storage Overhead Analysis Based on Transaction Throughput

Represented by the figure is a trend relationship between TPS and blockchain storage overhead (%). There is consistent increase of storage overhead with increase in TPS, but it is not a straight line. This is because with every additional transaction being executed, more and more overhead such as cryptographic signatures, metadata, and transactions themselves are accumulated in blockchain as shown in Figure (3),

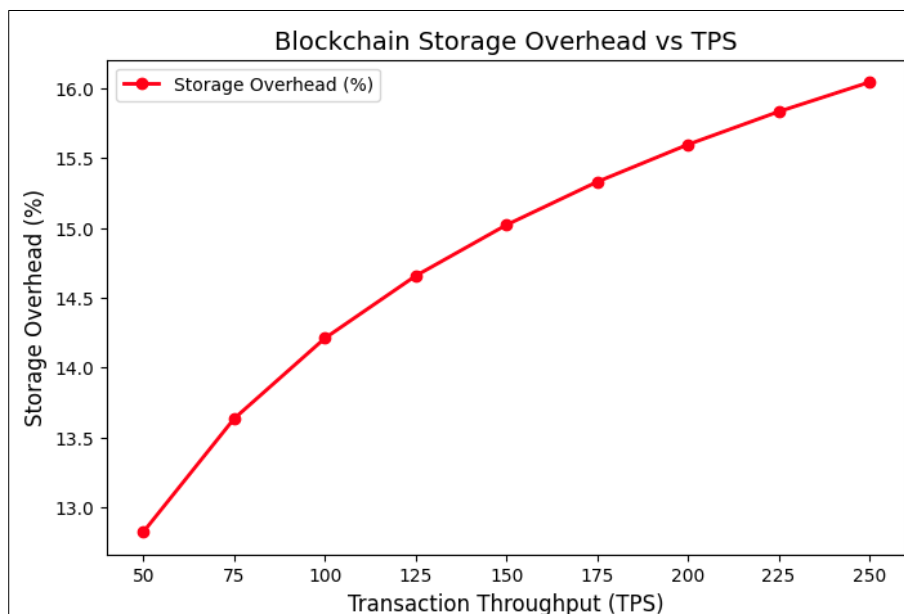


Figure 3: Impact of Transaction Throughput on Blockchain Storage Overhead

The storage cost starts at almost 13% for low TPS values but builds up to more than 16% when the TPS value is raised to 250. This makes it evident that the greater the transaction rates, the more the accumulation of storage requirements, thus implying the trade-off between the scalability of a blockchain and storage efficiency.

6. CONCLUSION AND FUTURE WORKS

The paper on blockchain-based threat intelligence sharing in clouds addresses significant obstacles to integrity, trust, and scalability. Security and transparency are gained with a controlled kind of access using an ABE-Based Blockchain Framework that integrates Ethereum with an Attribute-Based Encryption scheme and smart contracts. Evaluating the experiment shows that it provides good damage control towards data tampering and more trust-building among entities and ensures low-latency transaction processing. Besides using machine learning like binary, and random forest, CNNs would give the possibility of studying cyberthreat patterns thus increasing the detection accuracy of risks. The analysis showed that while blockchain has been found to work in improving cloud security, there are some hurdles posed by computing overheads, conformity with regulations, and existing cloud infrastructure. Future directions will focus on optimizing blockchain to store data efficiently, reduce computational costs, and realize an improved consensus mechanism for high scalability. Further, hybrid architectures of blockchain will be considered for future inquiries to address the balanced trade-off between decentralization and efficiency as well as privacy-preserving techniques such as homomorphic encryption in protecting sensitive threat intelligence data. Adapting learning models for real-time threat detection and response will also be an instrumental focus. Finally, collaboration with the industry and practical implementation in real-world cloud security systems will be considered for assessing the effectiveness of large-scale framework deployment.

REFERENCES

1. Alagarsundaram P. A systematic literature review of the elliptic curve cryptography (ECC) algorithm for encrypting data sharing in cloud computing. *International Journal of Engineering*. 2024;14(2):1–10.
2. Allur NS. Enhanced performance management in mobile networks: A big data framework incorporating DBSCAN speed anomaly detection and CCR efficiency assessment. *International Journal of Engineering*. 2020;8(9726):1–15.
3. Ayyadurai R. Big data analytics and demand-information sharing in e-commerce supply chains: Mitigating manufacturer encroachment and channel conflict. 2020 Apr;1–20.
4. Ayyadurai R. Transaction security in e-commerce: Big data analysis in cloud environments. *International Journal of Information Technology and Computer Engineering*. 2022;10(4):176–186.
5. Bobba J. Enterprise financial data sharing and security in hybrid cloud environments: An information fusion approach for banking sectors. *International Journal of Engineering*. 2021;11(3):1–18.
6. Devarajan MV, Al-Farouni M, Srikanteswara R, Samara Sihman Bharatje RR, Kumar PM. Decision support method and risk analysis based on merged-cyber security risk management. In: 2024 Second International Conference on Data Science and Information System (ICDSIS); 2024. p. 1–4. Available from: <https://doi.org/10.1109/ICDSIS61070.2024.10594070>
7. Gollavilli VSBH. Securing cloud data: Combining SABAC models, hash-tag authentication with MD5, and blockchain-based encryption for enhanced privacy and access control. *International Journal of Engineering Research and Science & Technology*. 2022;18(3):149–165.
8. Gudivaka *et al.* Cloud-based early acute lymphoblastic leukemia detection using deep learning-based improved YOLO V4. *IEEE Conference Publication*; 2024 May 17. Available from: <https://ieeexplore.ieee.org/document/10594435>
9. Bobba J. Securing financial data in cloud environments: AI and IaaS reliability verification techniques. 2024 Oct. Available from: <https://doi.org/10.5281/ZENODO.13994655>
10. Kadiyala B, Alavilli SK, Alfa AA. Real-time decision making in IoT-enabled business intelligence: Insights from Likert scale surveys. *International Journal of Advances in Computer Science & Engineering Research*. 2025;1(01):50–59.
11. Kethu SS, Purandhar N. AI-driven intelligent CRM framework: Cloud-based solutions for customer management, feedback evaluation, and inquiry automation in telecom and banking. *Journal of Science & Technology*. 2021;6(3):253–271.
12. Kodadi S. Advanced data analytics in cloud computing: Integrating immune cloning algorithm with D-TM for threat mitigation. *International Journal of Engineering Research and Science & Technology*. 2020;16(2):30–42.
13. Kodadi S. Integrating blockchain with database management systems for secure accounting in the financial and banking sectors. *Journal of Science & Technology*. 2023;8(9):9–27.
14. Nagarajan H. Assessing security and confidentiality in cloud computing for banking and financial accounting. *International Journal of HRM and Organizational Behavior*. 2024;12(3):389–409.
15. Peddi S, Tek Leaders. Analyzing threat models in vehicular cloud computing: Security and privacy challenges. *International Journal of Engineering*. 2021;9(4):1–20.
16. Peddi S, Narla S, Valivarthi DT. Harnessing artificial intelligence and machine learning algorithms for chronic disease management, fall prevention, and predictive healthcare applications in geriatric care. *International Journal of Engineering Research and Science & Technology*. 2019;15(1):1–15.
17. Ramoliya F. Cyber threat dataset: Network, text & relation. Available from:

- <https://www.kaggle.com/datasets/ramoliyafenil/text-based-cyber-threat-detection>
18. Sareddy MR, Khan S. AI-driven human resource management: Enhancing transparency and security with machine learning. *Journal of Artificial Intelligence and Capsule Networks*. 2025;6(4):512–528.
 19. Srinivasan K, Awotunde JB. Network analysis and comparative effectiveness research in cardiology: A comprehensive review of applications and analytics. *Journal of Science & Technology*. 2021;6(4):317–332.
 20. Valivarthi DT, Kurniadi D. A hybrid consensus method for energy-efficient and secure IoT data sharing in fog computing, integrating delegated proof of stake and whale optimization techniques. *Journal of IoT in Social, Mobile, Analytics, and Cloud*. 2025;6(4):308–326.
 21. Yallamelli ARG. Wipro Ltd, Hyderabad, Telangana, India. *International Journal of Engineering*. 2019;7(9726):1–12.

Creative Commons (CC) License

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY 4.0) license. This license permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

About the Corresponding Author



R. Prema is an Assistant Professor in the Department of Computer Science and Engineering at Tagore Institute of Engineering & Technology, Deviyakurichi, Attur (TK), Salem. She specializes in computer science education and research, contributing to the academic growth of students in the field.