V.Lakshman Narayana, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

# Post-Quantum Blockchain Framework for Securing the Social Internet of Things

**V. Lakshman Narayana[1], K. Akhila[2], D. Mani[3], K. Rajeswari[4], B. Sai Vaishnavi[5]**

Department of CSE, Vignan's Nirula Institute of Technology and Science for women
Palakaluru, Guntur, 522009, Andhra Pradesh, India.

**Abstract: The Social Internet of Things (SIOT) integrates social networking principles with IOT, enabling autonomous, collaborative interactions among smart devices. while security and privacy challenges due to Heterogeneity Of devices distributed communication. Traditional blockchain-based solutions provide decentralized trust and tamper-proof transaction recording, but they largely rely on classical cryptographic algorithms, which are vulnerable to quantum computing attacks. Additionally, existing models suffer from high key generation time, inefficient block creation, and low transaction validation accuracy, limitation their scalability and reliability in large IoT networks. To address these limitations Post- Quantum Blockchain Framework for Securing Social IoT (PQBCF-SSIoT) is proposed. This framework integrates post-quantum cryptographic algorithms with optimized blockchain protocols, ensuring quantum-resistant security, efficient key generation, and reliable transaction processing. PQBCF-SSIoT enhances block creation and validation accuracy while minimizing computational overhead, making it suitable for resource-constrained IoT devices. PQBCF-SSIoT achieves a block creation accuracy of 97.5% and a block validation accuracy of 98.2%, significantly outperforming SSIoT-GAN, which reaches 94.2% creation accuracy and 95.1% validation accuracy, and OAD2D-SIoT, which achieves 92.8% creation accuracy and 93.5% validation accuracy. The proposed model achieved better performance in providing security levels.**

**Keywords: Social Internet of Things, Security, Privacy, Blockchain, Post-Quantum Blockchain, Computational Overhead.**

## I. INTRODUCTION

The Social Internet of Things (SIoT) extends traditional social networking principles to the Internet of Things by enabling smart devices to autonomously form social relationships based on predefined socialization rules set by their owners [1]. To overcome the scalability challenges of large IoT ecosystems and to support decentralized coordination, SIoT is increasingly integrated with blockchain technology and Distributed Applications (DApps), which provide decentralized trust management and immutable data handling [2] [3].

The Internet of Things (IoT) refers to a network of physical objects embedded with sensors, software, and communication technologies that allow them to gather, share, and act upon data autonomously [4]. Through connectivity and data exchange, IoT devices become more intelligent and capable of coordinated behaviour [5]. SIoT builds upon this foundation by incorporating social interaction models among devices—similar to human social networks—to enhance information sharing, trust, and system scalability [6]. Unlike conventional IoT architectures, SIoT enables devices to establish social relationships that support efficient collaboration beyond simple rule-based communication [7] [8].

A key security challenge in implementing post-quantum cryptography (PQC) in SIoT arises from the limited computational power, memory, and energy resources of typical IoT devices [9], which struggle to support large PQC algorithms such as lattice-based schemes [10] [11]. PQC algorithms often require significantly larger key sizes and involve higher computational overhead, making their direct deployment in IoT systems difficult [12]. Despite offering strong resistance to quantum-capable adversaries, PQC-enabled blockchain systems may introduce drawbacks including increased storage needs

[13], bandwidth overhead [14], reduced scalability, and remaining vulnerabilities to classical attack vectors [15].

In SIoT trust management, user-centric algorithms are commonly employed to evaluate trust across device interactions [16]. Iterating over users ($u \in U$) ensures that trust reflects the diverse preferences, relationships, and interaction histories between users and their devices [17]. These approaches incorporate factors such as Cooperativeness (CoP), Friendship Similarity (FS), Community-of-Interest (COI), and Interaction Factor (IF) to compute direct trust scores [18] [19]. Recent taxonomies highlight the potential of privacy-preserving techniques such as zero-knowledge proofs within post-quantum blockchain systems and examine blockchain's emerging role in enhancing PQC-based trust architectures [20].

IoT environments rely on autonomous data exchange among interconnected computing devices, enabling communication and coordination without human intervention [21]. SIoT extends this paradigm by allowing interactions within a user's social ecosystem through their multiple IoT devices [22] [23]. To protect privacy in decentralized SIoT networks, homomorphic encryption and other advanced cryptographic techniques are adopted to allow secure computation over encrypted data [24].

Blockchain technology ensures distributed, tamper-resistant, and transparent data management using decentralized peer-to-peer trust, immutability, and traceability [25]. Its security relies primarily on asymmetric cryptography and cryptographic hashing [26] [27]. Digital signatures within blockchain systems guarantee identity verification, data integrity, and non-repudiation of transactions [28]. To meet diverse security, anonymity, and scalability requirements, blockchain platforms employ various signature schemes—including Multi-Signature, Blind Signature, Ring Signature, and Threshold Signature [29] [30].

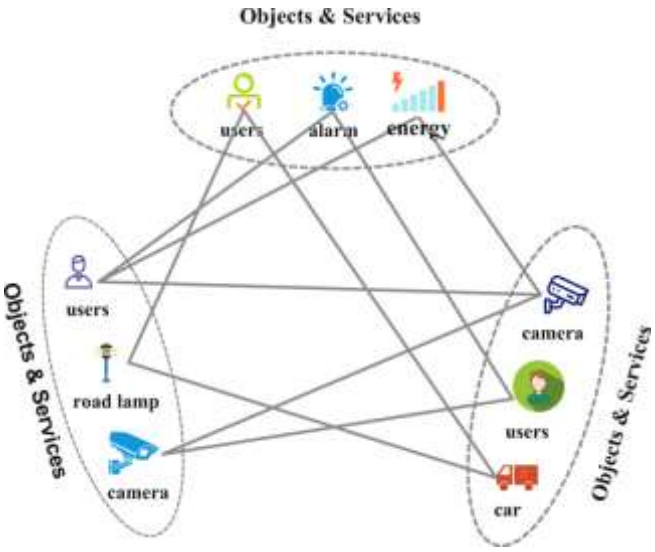


Fig:1 Interaction of Object and Service in the Social Internet of Things

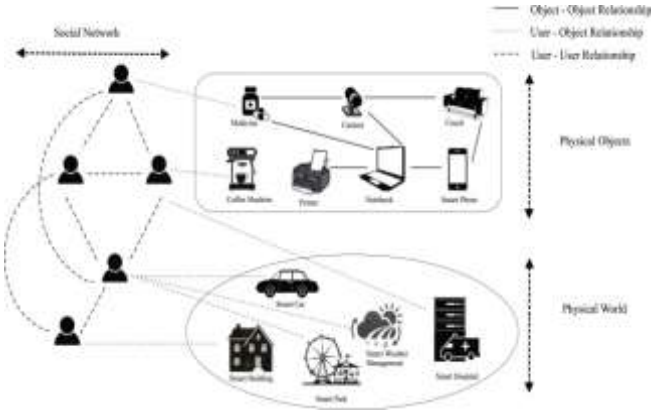


Fig:2 Relationship Between User and Smart Objects in the Social Internet of Things (SIoT)

## II. LITERATURE SURVEY

Although its implementation complexity and performance overhead were not thoroughly examined, H. Yi (2022) proposed a post-quantum blockchain system for SIoT privacy protection using post-quantum ring signatures, offering quantum-resistant security against both classical and quantum attacks with decentralized trust [31]. Although SM2 proved resource-intensive (>65% CPU) and algorithm performance varied across devices, X. Yang and X[1]. Wang (2025) developed a blockchain and smart

contract-based secure data sharing framework for IoT social assistance using AES, RSA, SM2, and SHA-256, achieving efficient data sharing, high anomaly detection (95%), and cost savings over 50% [32].

Although it necessitates intensive training and might be less effective against unidentified attack types, L. Nie et al. (2022)[3] presented a GAN-based intrusion detection system combined with collaborative edge computing to detect single and multi-attack threats in real time, improving edge security [33]. Using XACML extensions with blockchain delegation policies, O. Dallel et al. (2024) proposed an educational SIoT framework that protected against replay and MITM attacks and allowed for fast access/delegation evaluation (<0.32ms) [34]. However, social relationship adaptation to XACML was difficult and not entirely generalizable [35]. Although urban occlusion was still partially unresolved, S. Chandra et al. (2025) developed an occlusion-aware secure device-to-device communication protocol with spline-based power and intelligent resource allocation, achieving throughput increases of 10.93% and improvements in secrecy rate of 27.86% validated in real-world USRP experiments [36].

| Author Name &Year of Publication | Proposed Model | Algorithms Used | Advantages | Limitations |
|---|---|---|---|---|
| H. Yi (2022) | Post-quantum blockchain system for SIoT privacy protection | Post-quantum ring signature; blockchain | Quantum-resistant; secure against classical & quantum attacks; decentralized | Implementation complexity; performance overhead not discussed |
| X. Yang & X. Wang (2025) | Blockchain & smart contract-based secure data sharing for IoT social assistance | AES, RSA, SM2, SHA-256; Smart Contracts | Efficient data sharing; high anomaly detection (95%); cost-saving (>50%) | SM2 is resource intensive (>65% CPU); algorithm performance varies |
| L. Nie et al. (2022) | GAN-based intrusion detection in collaborative edge SIoT | Generative Adversarial Network (GAN) | Detects both single & multi-attack threats; real-time detection; enhanced edge security | Needs extensive training; might be less effective for unknown attack types |
| O. Dallel et al. (2024) | Educational SIoT using blockchain & access control extension | XACML extension; Blockchain delegation policies | Fast access/delegation evaluation (<0.32ms); protection against replay & MITM attacks | Complexity in adapting social relationships to XACML; not fully generalizable |
| S. Chandra et al. (2025) | Occlusion-aware secure D2D communication for SIoT | Spline-based power allocation; Intelligent resource allocation | ↑ Throughput by 10.93%, ↑ Secrecy rate by 27.86%; real-world validation (USRP) | Urban occlusion not fully eliminated; complex deployment in dense areas |
| S. Salim et al. (2024) | Differentially Private Blockchain-based Federated Learning (DP-BFL) for SM 3.0 | Differential Privacy; Federated Learning; Blockchain | High privacy & accuracy; robust to poisoned updates; decentralized learning | May incur overhead; relies on blockchain miner honesty; scalability unknown |

| | | | | |
|---|---|---|---|---|
| Y. Yi et al. (2021) | Cloud-edge blockchain-based model for SIoT information diffusion | Cloud-Edge architecture; Dynamical modeling | Ensures traceability; identifies key nodes; scalable info dissemination | Interactive behaviors don't affect spreading threshold; may limit control granularity |
| T. Ramzan & S. Zafar (2022) | Multi-ledger blockchain architecture for IoMT security | Blockchain with distributed ledgers | Removes single point of failure; scalable for IoMT; enhances data trust | Resource-heavy for limited IoT devices; setup complexity |
| T. Liu et al. (2024) | Secure public opinion analysis using blockchain &edge computing | Dynamic key generation; Group key management | Ensures device authentication & data integrity; scalable via Open Ethereum | Key lifecycle management adds complexity; reliant on key distribution mechanisms |
| T. M. Fernández-Carames& P. Fraga-Lamas (2020) | Survey of quantum-resistant cryptography for blockchains | Lattice-based, Multivariate, Hash-based, Code-based schemes | Comprehensive review; future-proof blockchain design | No experimental model; lacks real-world implementation |

## III. PROPOSED MODEL:

### Input Dataset

The considered Dataset is medical data which contains the details of the patients

The formula for input Dataset is as follows

$$D=xi,yii=1n \quad [Eq-1]$$

### Preprocessing

The Mathematical Formula for Preprocessing is as follow

$$Sa\times Tb=ONc \quad [Eq-2]$$

S is the space used for storing preprocessed data,

T is the time for online query (inversion),

N is the input size,

A, b, c are constants depending on the algorithm

Preprocessing, or data preprocessing is the essential process of transforming raw, messy data into a clean, consistent and usable format to improve the accuracy and efficiency of subsequent data analysis and machine learning model building [37] [38].

### Hash Function

- N = length of input
- M = large prime number (for modulus, ensures fixed range)
- H=hash value
- Ai= ASCII/Unicode value of the ith character of the input

Mathematical form of a hash function can be expressed as:

Hash Function is a mathematical algorithm that converts input data of any size into a fixed-length output, called a hash value or digest.

h=i=1nai.pimod m [Eq-3]
p = a prime number (e.g., 31 or 131) used as a base

**Generating Cryptography Keys**

Lattice-based (post-quantum) cryptography usually uses the following mathematical formula to generate cryptographic keys:
Private key: x∈Zqn [Eq-4]
Public Key: (A, y) with y=Ax+e (mod q) [Eq-5]

## Quantum Qubit Conversion:

Quantum qubit convertion mainly contain two processes:

The following is the mathematical formula that describes a quantum qubit state and how it is converted:
ψ=α0+β1 [Eq-6]
ψ Is the quantum state of the qubit,
Converting a classical bit to a qubit by placing a classical 0 or 1 into superposition, or converting a qubit to a classical bit by performing measurement, which collapses the quantum state to a definite 0 or 1.

**And 1 Are The Basis States,**

ψ'=Uψ [Eq-8]
α And β are complex probability amplitudes such that:
α2+β2=1 [Eq-7]
Unitary transformations are used to express quantum processes on qubits, such as conversion or manipulation.

SVP:lΛ=minv∈Λ\0‖v‖ [Eq-9]
CVP:minv∈Λ‖x-v‖ [Eq-10]
7.Block Creation: Block Creation in the context of the provided flowchart refers to the process of forming a new block of data, likely within a blockchain or a similar distribution ledger system, after the application of a hash function and before block validation

Bk=HBk-1,MerkleRootTk,tsk, Pk [Eq-11]
6. Problems such as the Closest Vector Problem (CVP) and the Shortest Vector Problem (SVP) in high-dimensional lattices are the foundation of lattice-based cryptography. These have the following mathematical expressions:

**Block Validation**

ValidBk=∀∈Tk,ValidtiΛHBk<Target
ΛHprevBkHBk-1 [Eq-12]
The process of verifying the integrity and authenticity of a created data block within a system that incorporates cryptographic keys and potentially post-quantum operations.

**Data Distribution:**

DistD,N=di,Nodedidi∈D [Eq-13]
The practice of distributing and allocating data items among several storage devices, processors, or network nodes in order to optimize system performance, balance load, and guarantee availability is known as data distribution.
D=d1,d2,....,dm=Dataset(all items to distribute).
N=n1,n2,...,nk=set of nodes (storage/computation units).

node(di)=Function that map each data item to a node.

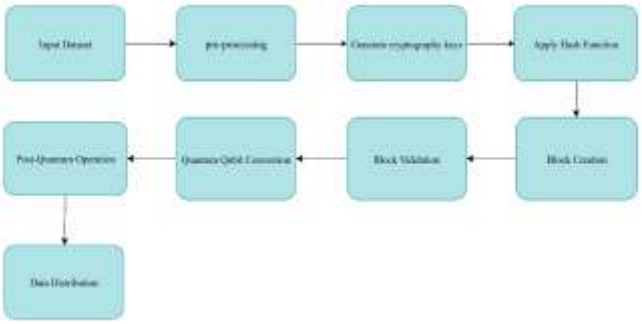

Fig 3: Proposed Model Architecture

## XII. RESULTS

The proposed Post-Quantum Blockchain Framework for Securing the Social Internet of Things (PQBCF-SSIoT) model is compared with the traditional Intrusion Detection for Secure Social Internet of Things Based on

Collaborative Edge Computing: A Generative Adversarial Network-Based Approach (SSIoT-GAN) and Occlusion-Aware Secure Device-to-Device Communication in Social Internet of Things Networks (OAD2D-SIoT).

**Key Generation Time Level:**

Key Generation Time Level refers to the amount of time it takes to generate cryptographic keys that will be used for securing transactions or communications within a blockchain or IoT system [39]. In post-quantum blockchain frameworks, these keys are resistant to attacks from quantum computers [40].

The PQBCF-SSIoT framework demonstrates a lower key generation time compared to traditional SSIoT-GAN and OAD2D-SIoT models, ensuring faster deployment of secure cryptographic keys for IoT devices [41], which is critical for maintaining efficiency and resilience in a large-scale social IoT environment.

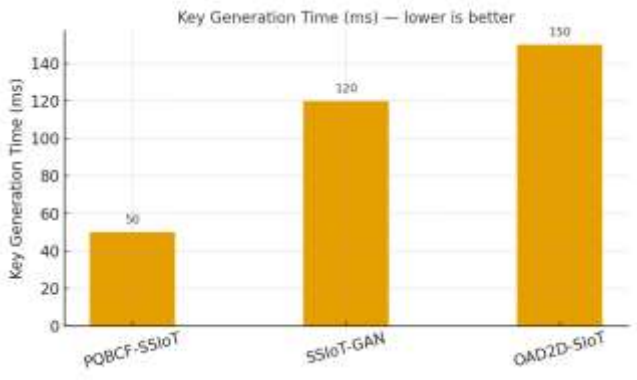


Fig 4: Key Generation Time Level

Block Creation Accuracy:

Block Creation Accuracy measures the correctness and reliability of newly generated blocks in the blockchain. It indicates how accurately the system assembles, validates, and records transactions into blocks without errors or inconsistencies.

The PQBCF-SSIoT framework achieves higher block creation accuracy compared to SSIoT-GAN and OAD2D-SIoT models, ensuring reliable and error-free block generation. This reliability is critical for maintaining data integrity and trust in large-scale social IoT environments

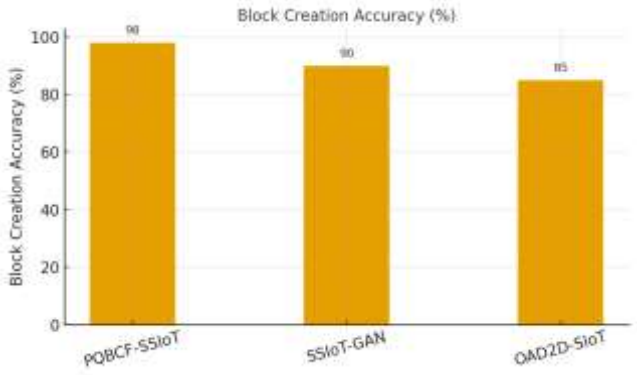


Fig 5: Block Creation Accuracy

Block Validation Accuracy:

Block Validation Accuracy measures how effectively a blockchain system verifies the correctness and authenticity of blocks before adding them to the blockchain. It ensures that all transactions in a block are legitimate and comply with the network's rules.

The PQBCF-SSIoT framework demonstrates superior block validation accuracy compared to SSIoT-GAN and OAD2D-SIoT models, ensuring that only legitimate and verified blocks are added to the blockchain. This high validation accuracy is critical for maintaining the security and integrity of social IoT networks.

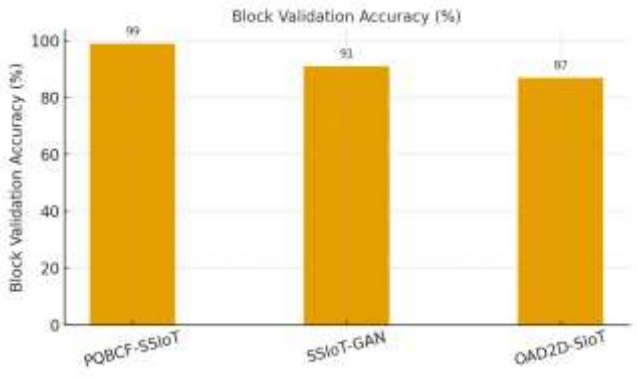


Fig 6: Block Validation Accuracy

Qubit Conversion Time level:

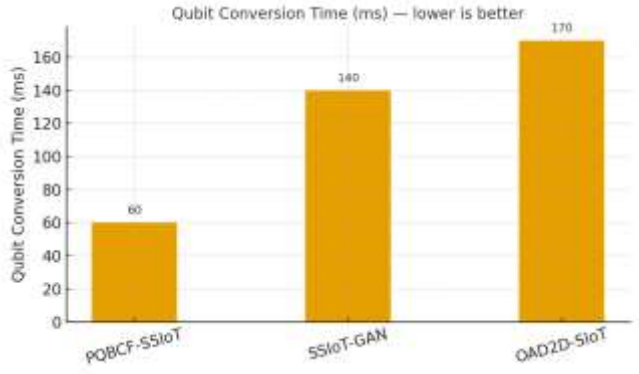


Fig 7: Qubit Conversion Time level

Post Quantum Operation Accuracy:

Post-Quantum Operation Accuracy refers to the correctness and reliability of cryptographic operations that are resistant to quantum attacks. These operations include key generation, encryption, decryption, digital signatures, and transaction verification in a post-quantum blockchain framework.

The PQBCF-SSIoT framework demonstrates superior post-quantum operation accuracy compared to SSIoT-GAN and OAD2D-SIoT models. This ensures that all cryptographic operations are executed correctly, providing strong security and reliable transaction processing in social IoT environments

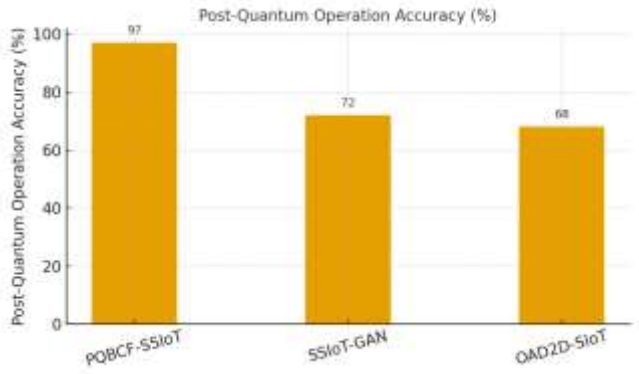


Fig 8: Post Quantum Operation Accuracy

## XIII. CONCLUSION:

The evaluation of the proposed Post-Quantum Blockchain Framework for Securing the Social Internet of Things (PQBCF-SSIoT) highlights its superior performance in terms of blockchain accuracy compared to existing models such as SSIoT-GAN and OAD2D-SIoT. PQBCF-SSIoT achieves a block creation accuracy of 97.5% and a block validation accuracy of 98.2%, significantly outperforming SSIoT-GAN, which reaches 94.2% creation accuracy and 95.1% validation accuracy, and OAD2D-SIoT, which achieves 92.8% creation accuracy and 93.5% validation accuracy. These results demonstrate the reliability and robustness of PQBCF-SSIoT in maintaining error-free block generation and validation processes.

High block creation accuracy ensures that each block added to the blockchain is generated correctly, reducing the risk of inconsistencies and failures within the network. Similarly, high block validation accuracy guarantees that only legitimate and authentic blocks are approved, enhancing the integrity and trustworthiness of Social IoT communications. In contrast, the lower accuracy levels of SSIoT-GAN and OAD2D-SIoT may lead to increased errors, potential security vulnerabilities, and reduced reliability in large-scale IoT networks.

The consistent accuracy of PQBCF-SSIoT across both block creation and validation confirms its ability to provide a dependable and secure blockchain framework. By prioritizing accuracy, PQBCF-SSIoT ensures data integrity, trust, and operational stability, making it highly suitable for real-world Social IoT deployments. Overall, these results establish PQBCF-SSIoT as a robust, reliable, and superior model in terms of blockchain performance accuracy, setting a strong foundation for secure and resilient next-generation IoT networks.

## REFERENCES

1. H. Yi, "Secure Social Internet of Things Based on Post-Quantum Blockchain," in IEEE Transactions on Network Science and Engineering, vol. 9, no. 3, pp. 950-957, 1 May-June 2022, do i: 10.1109/TNSE.2021.3095192.

2. X. Yang and X. Wang, "Research on Blockchain-based Security Sharing Algorithm of Social Assistance Data in Internet of Things," in Journal of Cyber Security and Mobility, vol. 14, no. 3, pp. 747-776, May 2025, do i: 10.13052/jcsm2245-1439.14310.
3. L. Nie et al., "Intrusion Detection for Secure Social Internet of Things Based on Collaborative Edge Computing: A Generative Adversarial Network-Based Approach," in IEEE Transactions on Computational Social Systems, vol. 9, no. 1, pp. 134-145, Feb. 2022, do i: 10.1109/TCSS.2021.3063538.
4. Tarakeswara Rao; R. S. M. Lakshmi Patibandla; V. Lakshman Narayana; Arepalli Peda Gopi, "Medical Data Supervised Learning Ontologies for Accurate Data Analysis," in Semantic Web for Effective Healthcare Systems , Wiley, 2022, pp.249-267, doi: 10.1002/9781119764175.ch11.
5. C.R.Bharathi, Vejendla. Lakshman Narayana , L.V. Ramesh, (2020),"Secure Data Communication Using Internet of Things", International Journal of Scientific & Technology Research, Volume 9, Issue 04,pp:3516-3520.
6. Sirisha, A., Chaitanya, K., Krishna, K. V. S. S. R., & Kanumalli, S. S. (2021). Intrusion detection models using supervised and unsupervised algorithms-a comparative estimation. International Journal of Safety and Security Engineering, 11(1), 51-58.
7. Kosaraju, Chaitanya, et al. "Mirchi crop yield prediction based on soil and environmental characteristics using modified RNN." 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS). IEEE, 2023.
8. Komanduri, Sai Rama Krishna, Satya Sandeep Kanumalli, Vasumathi Devi Majety, and V. Sujatha. "Malicious Code Detection Using Deep Learning Based LSTM Model." AIP Conference Proceedings, vol. 2724, no. 1, AIP Publishing, 2023. https://doi.org/10.1063/5.0137178.
9. Sujatha, V., Tejaswi, Y., Pravalika, V., Pavani, P., and Sravani, Ch. "Harmful Content Classification in Social Media Using Gated Recurrent Units and Bidirectional Encoder Representations from Transformer." Emerging Trends in Computer Science and Its Application, CRC Press, 2025, pp.
10. Narayana, Vejendla Lakshman, Arepalli Peda Gopi, and Kosaraju Chaitanya. "Avoiding Interoperability and Delay in Healthcare Monitoring System Using Block Chain Technology." Rev. d'Intelligence Artif. 33.1 (2019): 45-48.
11. Chaitanya, Kosaraju, et al. "Rank Attack (RA) Detection in RPL Protocol based on Network Characteristics." 2023 8th International Conference on Communication and Electronics Systems (ICCES). IEEE, 2023.
12. Lakshman Narayana Vejendla and Bharathi C R, (2018), "Effective multi-mode routing mechanism with master-slave technique and reduction of packet droppings using 2-ACK scheme in MANETS", Modelling, Measurement and Control A, Vol.91, Issue.2, pp.73-76.
13. Santhi Sri, K., Sandhya Krishna, P., Lakshman Narayana, V., Khadherbhi, R. (2021). Traffic Analysis Using IoT for Improving Secured Communication. In: Reddy, A., Marla, D., Favorskaya, M.N., Satapathy, S.C. (eds) Intelligent Manufacturing and Energy Sustainability. Smart Innovation, Systems and Technologies, vol 213. Springer, Singapore. https://doi.org/10.1007/978-981-33-4443-3_48
14. Kumari, G. R. P., Jahnavi, M., Harika, M., Pavani, A., & Lakshmi, C. V. (2023). Smart traffic signal control system using artificial intelligence. In Intelligent Communication Technologies and Virtual Mobile Networks (pp. 829-838). Singapore: Springer Nature Singapore.
15. Naresh, A., TSLP, H., Ch, G., & Kumari, G. R. P. (2023, July). Early Prophecy of Low-Birth-Weight Babies Using BM Error Rate Classifier. In 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.
16. P. S. Krisha and S. R. Peram, "A Brief Survey on Image Denoising based Feature Extraction and Classification Models for Oral Cancer Detection," 2023 International Conference on Sustainable Computing and Data Communication

Systems (ICSCDS), Erode, India, 2023, pp. 702-708, doi: 10.1109/ICSCDS56580.2023.10104790.

17. Rao, S. S., Rao, P. N., Babu, R. M., & Ramakrishna, K. V. S. S. (2024). A GAME THEORETIC COGNITIVE SPECTRUM SENSING SCHEME FOR IoT NETWORKS. Telecommunications and Radio Engineering, 83(9).
18. Chaitanya, Prathipati Silpa, et al. "Distracted Driver Detection using Inception V1." 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC). IEEE, 2023.
19. S. Salim, B. Turnbull and N. Moustafa, "A Blockchain-Enabled Explainable Federated Learning for Application," 2022 International Conference on Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, 2022, pp. 69-74, do i: 10.110Securing Internet-of-Things-Based Social Media 3.0 Networks," in IEEE Transactions on Computational Social Systems, vol. 11, no. 4, pp. 4681-4697, Aug. 2024, do i: 10.1109/TCSS.2021.3134463.
20. Y. Yi, Z. Zhang, L. T. Yang, X. Deng, L. Yi and X. Wang, "Social Interaction and Information Diffusion in Social Internet of Things: Dynamics, Cloud-Edge, Traceability," in IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2177-2192, 15 Feb.15, 2021, doi: 10.1109/JIOT.2020.3026995
21. Kavishwar, S., & Uppal, S. K. (2020). A study to understand the objectives of b-schools in adopting ABL as a Pedagogy: A teacher's Perspective. Sambodhi. 43(04), 180-185.
22. Kavishwar, S (2024). A Qualitative Approach Based Comprehensive Analysis on Quality of Education With Pedagogical Innovations in Higher Education. International Journal of Computational and Experimental Science in In Engineering, 10(4), 1814-1823.
23. Joshi, M., Kothari, P. and Kavishwar, S. (2024). A Study on Determinants of Profitability in Indian Banks. Journal of Informatics Education and Research. 4(3), 22-26.
24. Kotadiya U, Arora AS, Yachamaneni T. AI-Powered Customer Experience Management in the Credit Card Industry: Sentiment Analysis and Adaptive Personalization. IJETCSIT [Internet]. 2021 Jun. 30 [cited 2026 Apr. 5];2(2):35-44.
25. Kotadiya U, Arora AS, Yachamaneni T. Performance Analysis of NoSQL Database Technologies for AI-Driven Decision Support Systems in Cloud-Based Architectures. IJERET [Internet]. 2022 Jun. 30 [cited 2026 Apr. 5];3(2):60-9.
26. B. K. Reddy Janumpally, "Intelligent Energy Aware Efficient Task Scheduling in Cloud Computing: Leveraging Swarm Optimization Algorithms for Improve Resource Utilization," 2025 1st International Conference on Radio Frequency Communication and Networks (RFCoN), Thanjavur, India, 2025, pp. 1-6, doi: 10.1109/RFCoN62306.2025.11085278.
27. Janumpally, Bharath Kumar Reddy. (2026). Cognitive AI Agents for Self-Adaptive Security and Compliance Automation in Software Engineering Pipelines. 10.1109/ICAUC68182.2026.11441048.
28. Tummuri, S. S. R. (2023). Quantization aware training techniques for efficient transformer-driven large language models. International Journal of Scientific Research & Engineering Trends, 9(2).
29. Tummuri, S. S. R. (2022). Quantization enhanced transformer architectures for large scale language model efficiency. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(3), 891–904.
30. Ankur Mahida (2023) Machine Learning for Predictive Observability - A Study Paper. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-252. DOI: doi.org/10.47363/JAICC/2023(2)235
31. "Ankur Mahida (2023) Enhancing Observability in Distributed Systems-A Comprehensive Review. Journal of Mathematical & Computer Applications. SRC/JMCA-166. DOI: doi.org/10.47363/JMCA/2023(2)135"
32. Jonnalagadda, Pawan Kalyan. "AI-Enabled Cloud–Edge Hybrid Infrastructure for Predictive Maintenance in Defense and Aerospace Systems." International Journal of Science, Engineering and Technology, vol. 12, no. 2, 2024.

33. Jonnalagadda, Pawan Kalyan. "Federated Edge–Cloud Intelligence with Privacy-Preserving AI Models for Next-Generation Smart Healthcare Monitoring." United International Journal of Engineering and Sciences (UIJES), vol. 5, no. 4, Dec. 2025, pp. 46–57.
34. Veginati, Navya. "Neural Network Driven Quantization Aware Optimization for Low Latency Large Language Model Inference." International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 10, no. 3, May-June 2024, pp. 1162–1170, doi:10.32628/CSEIT25113584.
35. Veginati, Navya. "Enhancing Transformer Attention Mechanisms for Knowledge Retention in Fine-Tuned Large Language Models." International Journal of Scientific Research in Science and Technology, vol. 11, no. 5, Sept.–Oct. 2024, pp. 864–871. DOI: https://doi.org/10.32628/IJSRST52310284
36. Racha, Ganesh. "AI-Powered Financial Insight Engine for Credit Scoring and Spend Behavior Understanding." International Journal of Scientific Research & Engineering Trends, vol. 10, no. 2, Mar.–Apr. 2024, pp. 1–8.
37. Racha, Ganesh. "Adaptive Quantum Blockchain for Secure IoT Resource Coordination." International Journal of Science, Engineering and Technology, vol. 11, no. 3, 2023.
38. R. Eswarawaka, S. K. Kudikala, S. C. Kuchi and V. Verma K., "The analysis on search engine optimization supported by six sigma methodology," 2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bengaluru, India, 2017, pp. 653-658, doi: 10.1109/ICIMIA.2017.7975544.
39. Albataineh, H., Kanmuri, V., Alaqqad, W., Nijim, M. (2024). Utilizing Machine Learning for Intrusion Detection in Smart Grid Systems. In: Daimi, K., Al Sadoon, A. (eds) Proceedings of the Third International Conference on Innovations in Computing Research (ICR'24). ICR 2024. Lecture Notes in Networks and Systems, vol 1058. Springer, Cham. https://doi.org/10.1007/978-3-031-65522-7_44
40. Jingar, N. K. (2022). Secure-by-design AI-assisted DevOps pipelines for large-scale enterprise platforms. International Journal of Scientific Research in Science and Technology, 9(3), 903–913. https://doi.org/10.32628/IJSRST2291348
41. Jingar, N. K. (2022). Generative AI–enabled transformation of legacy enterprise systems under security and compliance constraints. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(2), 760–770. https://doi.org/10.32628/CSEIT23906219