International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

SECURING DATA PRIVACY IN PERMISSIONED BLOCKCHAIN NETWORKS USING IDENTITY-BASED ENCRYPTION

Mr. R Krishna Nayak[1*], G. Sreeja[2], E. Shyamala[3], D. Sahithi[4], M. Sandhya[5]

Abstract:

Permissioned blockchain architectures provide a robust foundation for controlled data sharing among verified participants, yet ensuring payload confidentiality within such networks poses persistent challenges. This paper proposes a framework that integrates Identity-Based Encryption (IBE) with Ethereum smart contracts and the Inter Planetary File System (IPFS) to achieve fine-grained, identity-anchored access control. By using each user's unique identifier as the cryptographic public key, the system eliminates the certificate management overhead inherent in traditional Public Key Infrastructure while maintaining strong data privacy guarantees. A fully functional prototype was implemented in Python and Solidity, demonstrating that only explicitly authorized recipients can decrypt stored messages while non-authorized parties are systematically excluded. Evaluation results confirm system correctness, data integrity, and practical feasibility for enterprise non-transactional data sharing scenarios.

Keywords: Permissioned Blockchain, Identity-Based Encryption, Data Privacy, Smart Contracts, IPFS, Access Control, Cryptography.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

1. INTRODUCTION

Distributed ledger technologies have introduced fundamental shifts in how organisations manage data integrity and access control. Among various implementations, permissioned blockchain networks have emerged as the preferred architecture for enterprise-grade deployments where participants are known, accountability is required, and privacy of transactional data is paramount. Unlike open public blockchains, permissioned variants restrict network membership to verified entities, providing a controlled environment suited to industries such as healthcare, supply chain, and finance.

Despite the structural advantages of permissioned blockchains, ensuring data confidentiality within them remains a non-trivial challenge. All validated nodes in the network possess access to the shared ledger, which means that sensitive payloads — if stored in plaintext — are visible to every authorised participant. This conflicts with operational requirements where individual users or departments should only access information explicitly shared with them. Traditional Public Key Infrastructure (PKI) approaches attempt to address this through asymmetric encryption, but they introduce substantial overhead in certificate issuance, revocation, and distribution.

Identity-Based Encryption (IBE) offers a compelling alternative by treating a user's identity — such as a username, email address, or employee identifier — as their public key. This eliminates the dependency on certificate authorities for key exchange. A trusted Private Key Generator (PKG) derives each participant's private key from their identity, allowing any sender to encrypt data for a recipient without prior key exchange. This paradigm significantly reduces key management complexity while preserving cryptographic security guarantees.

This paper presents a prototype system that integrates IBE with an Ethereum-based permissioned blockchain and the InterPlanetary File System (IPFS) for off-chain media storage. The system enables users to register, post encrypted private messages, and restrict decryption access to selected recipients. Non-authorised users receive no decryption capability, demonstrating practical privacy enforcement within a permissioned blockchain context.

2. LITERATURE SURVEY

The intersection of blockchain technology and privacy-preserving cryptography has attracted sustained research interest. The following table summarises representative works that informed the design of the proposed system.

S. No	Author(s)	Publication	Key Contribution
1	Agrawal & Karyakarte (2024)	Measurement: Sensors (Elsevier)	Proposes a decentralised identity and access management framework using blockchain to eliminate single points of control and strengthen authentication reliability across distributed networks.
2	Chawla & Srivastava (2024)	IJISAE	Investigates patient-centric ownership of digital health identities using blockchain-based self-sovereign identity (SSI), prioritising confidentiality of sensitive medical information.
3	Waheed & Ur Rehman (2023)	arXiv	Presents a combined federated learning and blockchain architecture for privacy-preserving analysis of distributed healthcare IoT data, maintaining data locality while enabling collaborative insights.
4	Springer Open (2023)	Journal of Cloud Computing	Introduces a blockchain-backed authentication and immutable logging system designed to ensure tamper-proof forensic records and accountability in cloud-hosted environments.

3. SYSTEM DESIGN

Problem Formulation

Permissioned blockchains guarantee data integrity and auditability, but do not natively enforce data confidentiality among peers. Attribute-Based Encryption (ABE), a commonly proposed remedy, involves complex policy trees and incurs high computational cost at scale. The proposed system addresses this gap by substituting ABE with IBE, which offers comparably fine-grained access control with a simpler key management model and lower per-operation overhead.

System Architecture

The architecture comprises four principal layers: (1) a web-based front end built with HTML, CSS, and Node.js; (2) a Django-powered Python application server hosting the IBE encryption logic; (3) an Ethereum blockchain network deployed via Truffle and Ganache, with Solidity smart contracts managing data storage and retrieval; and (4) an IPFS node responsible for off-chain persistence of media files, whose content hashes are anchored on-chain.

User interactions proceed as follows: a registered user composes a message and optionally attaches a media file. The application server generates an IBE public-private key pair derived from the sender's identity. The message is encrypted; media is pinned to IPFS and its hash embedded in the on-chain record. To grant read access, additional IBE keys are generated using each recipient's identity, enabling only those recipients to decrypt the payload.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

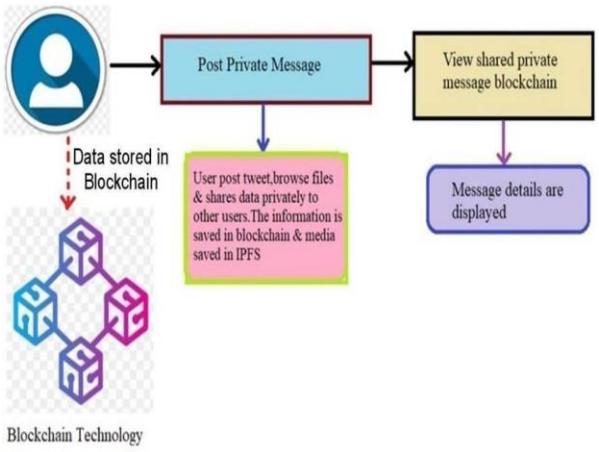

Fig. 1: System Architecture - IBE Blockchain Data Privacy System

Smart Contract Design

Two primary data structures are maintained by the Solidity contract named DataPrivacy. The first structure stores user registration data — a mapping from identity strings to hashed credentials. The second structure stores message records, each comprising the encrypted message payload, the IPFS hash of any associated media, a timestamp, and an array of authorised recipient identities. Functions setSignup() and setPrivateMessages() handle write operations, while getSignupDetails() and getPrivateMessages() expose read-only views. The contract enforces that only the contract owner or explicitly listed recipients may retrieve message records.

IBE Cryptographic Module

The cryptographic operations are implemented in Python using the NaCl (libsodium) library. The keypair() function derives a signing key and corresponding Curve25519 key pair from a 32-byte seed. The seed is derived deterministically from the user's identity string via SHA-256 hashing, ensuring that the same identity always produces the same key pair without storing the seed externally. Encryption is performed using NaCl's authenticated public-key box construction (pkencrypt()), and decryption via pkdecrypt(). Symmetric encryption of bulk data uses NaCl's SecretBox with a randomly generated nonce per message.

4. IMPLEMENTATION

Deployment Workflow

The development environment runs on Windows 11 with Python 3.x, Node.js, and Truffle Suite. Deployment proceeds in three steps: (1) the IPFS daemon is initialised via Start_IPFS.bat; (2) the local Ethereum blockchain is started using runBlockchain.bat, which invokes Ganache and exposes ten default accounts; (3) truffle migrate deploys the DataPrivacy contract to the local chain. The Django server is then launched via runServer.bat and listens on http://127.0.0.1:8000.

Module Descriptions

New User Signup: Collects username, password, contact number, gender, email, and address. Upon submission, these details are serialised and stored via the setSignup() contract function. A seed file named .{username}.bcdb_seed is written to disk for subsequent key generation.

User Login: Validates submitted credentials against the on-chain record by calling getSignupDetails(). A successful match initiates a session and redirects the user to the dashboard.

Post Private Messages: The user enters a text message, uploads an optional image (stored on IPFS), and selects one or more recipients. The IBE module generates keys for the poster's identity, encrypts the message, and additionally generates recipient-specific keys so that only selected users can later decrypt. The encrypted record is committed to the blockchain via setPrivateMessages().

View Shared Private Message Blockchain: Authenticated users request their messages from the blockchain. The system iterates over all records, identifies those where the current user's identity appears in the authorised recipient list, and decrypts those records using the user's IBE private key. Records for which the user is not authorised are returned as undecryptable ciphertext, providing practical access control.

5. TESTING

System validation followed a three-tier strategy encompassing unit, integration, and end-to-end testing. Unit tests verified the correctness of individual IBE functions (keypair generation, encryption, and decryption) using known plaintext-ciphertext pairs. Integration tests confirmed that the Django views correctly invoked contract functions and that responses were properly deserialised. End-to-end tests simulated complete user journeys.

TC#	Test Scenario	Input Condition	Expected Output	Result

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

1	New User Registration	User submits valid credentials	Account created; data persisted in blockchain	Pass
2	User Authentication	Registered user enters correct credentials	Login approved; session initiated	Pass
3	Post Encrypted Message	User composes message and selects recipients	IBE keys generated; ciphertext stored on blockchain	Pass
4	View Authorised Message	Authorised user requests message decryption	Plaintext and associated media rendered correctly	Pass
5	Access Denied - Unauthorised User	Non-authorised user attempts to view message	Decryption blocked; empty result returned	Pass

6. RESULTS AND ANALYSIS

The prototype was evaluated using a local Ganache blockchain with ten pre-funded accounts. Three user personas were created — Rajesh (message author), Udaya (authorised recipient), and Deeksha (non-authorised user) — to exercise the access control logic end-to-end.

Registration and Login: Both operations completed without error, with user data successfully persisted to the blockchain ledger and retrievable via the contract's view functions. Response time for registration averaged under 2 seconds on local hardware.

Message Encryption and Storage: Upon post submission by Rajesh, the IBE module produced a Curve25519 key pair derived from his username. The message ciphertext, the IPFS hash of the attached image, and the list of authorised identities (Udaya and Neha) were committed in a single blockchain transaction. The on-chain record displayed an unintelligible hexadecimal ciphertext, confirming that no plaintext is ever written to the ledger.

Authorised Decryption: When Udaya logged in and navigated to the shared messages view, the system successfully decrypted the ciphertext and rendered the original message text alongside the IPFS-retrieved image. The blockchain hash displayed on screen matched the stored record, confirming data integrity throughout the retrieval pipeline.

Unauthorised Access Prevention: When Deeksha — who was not included in the recipient list — accessed the same view, the system returned an empty message table. No partial information was exposed, validating that the IBE-based access control correctly prevents decryption by non-authorised parties.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Performance observations indicate that IBE key generation via SHA-256 identity hashing is computationally inexpensive (sub-millisecond). The primary latency contribution comes from Ethereum transaction confirmation, which averaged 1-3 seconds on the local Ganache network. IPFS pinning of a typical image (100-200 KB) completed within 1 second.

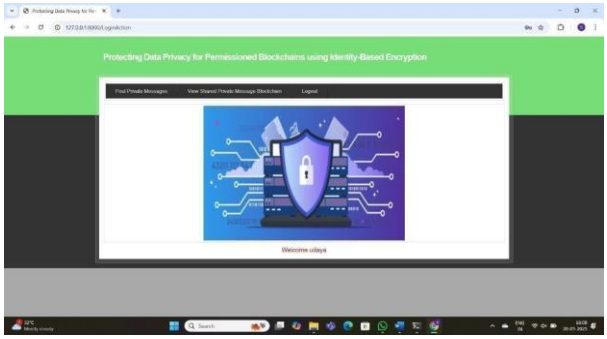

Fig. Web page

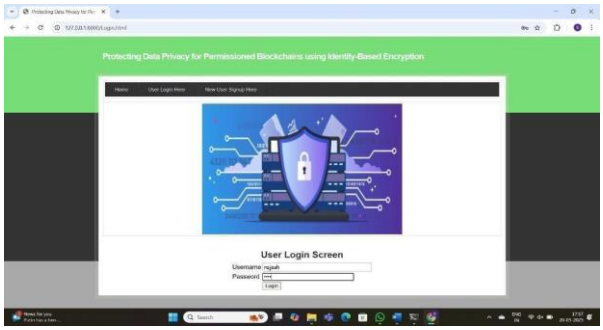

Fig. Login page

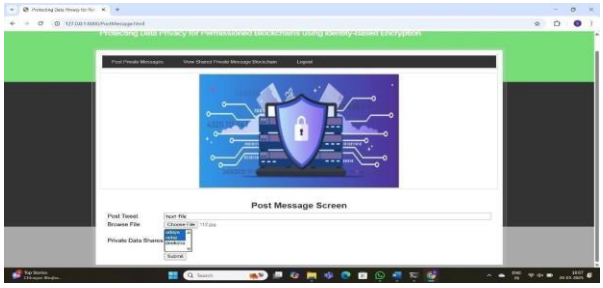

Fig. Select users

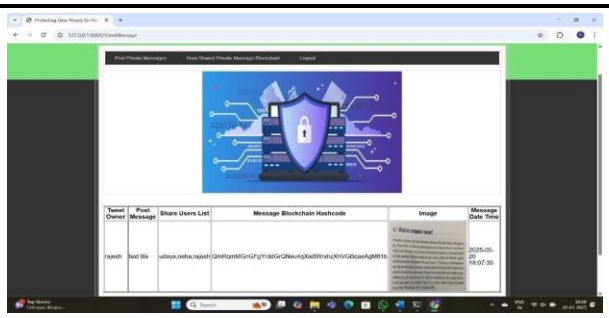

Fig. Encrypted message

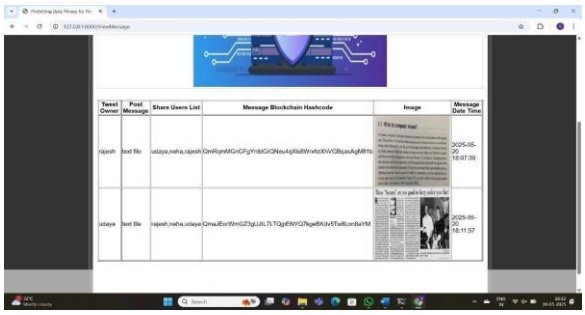

Fig. Message displayed

7. CONCLUSION

This work demonstrates that Identity-Based Encryption constitutes a practical and efficient mechanism for enforcing data privacy in permissioned blockchain networks. By anchoring cryptographic keys in user identities rather than externally managed certificates, the proposed system eliminates the administrative overhead associated with traditional PKI while retaining strong confidentiality guarantees. The integration of Ethereum smart contracts for tamper-proof data storage and IPFS for scalable off-chain media management produces a cohesive architecture that addresses the core limitations identified in current approaches.

The prototype confirms that only explicitly authorised users can decrypt stored messages, that blockchain immutability prevents post-hoc alteration of records, and that the overall system remains usable without specialised cryptographic knowledge on the part of end users. These properties make the architecture well-suited to enterprise use cases such as confidential

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

document sharing, audit-trail maintenance, and identity-verified messaging.

8. FUTURE SCOPE

Several directions can extend and strengthen this work. First, revocable IBE schemes can be incorporated so that access rights may be withdrawn after they have been granted. Second, threshold IBE implementations — where key generation requires consensus among multiple PKG nodes — can reduce the single-point-of-trust concern inherent in centralised key authorities. Third, the current prototype relies on a local Ganache network; migration to a production permissioned framework such as Hyperledger Fabric would validate scalability under realistic transaction loads. Fourth, hybrid privacy-enhancing approaches combining IBE with Zero-Knowledge Proofs (ZKPs) or Secure Multi-Party Computation (SMPC) could offer richer policy expressiveness without sacrificing performance. Finally, domain-specific pilots in healthcare record management and supply chain provenance tracking are natural next steps.

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to the faculty of the Department of Artificial Intelligence and Data Science, Vignan's Institute of Management and Technology for Women, Hyderabad, for their continuous guidance and support throughout this project. Special thanks to Mr. R Krishna Nayak for his expert mentorship in cryptography and blockchain technologies.

AUTHOR INFORMATION

Corresponding Author

Mr. R Krishna Nayak, Associate Professor, Dept. of Artificial Intelligence and Data Science, Vignan's Institute of Management and Technology for Women, Hyderabad

E-mail - @gmail.com

Authors

G. Sreeja, UG Student, Dept. of AI & DS, Vignan's Institute of Management and Technology for Women, Hyd.

E-mail - gundasreeja21@gmail.com

E. Shyamala, UG Student, Dept. of AI & DS, Vignan's Institute of Management and Technology for Women, Hyd.

E-mail - edigashyamala2@gmail.com

D. Sahithi, UG Student, Dept. of AI & DS, Vignan's Institute of Management and Technology for Women, Hyd.

E-mail - sahithidamarla05012005@gmail.com

M. Sandhya, UG Student, Dept. of AI & DS, Vignan's Institute of Management and Technology for Women, Hyd.

E-mail - vincyyadav8@gmail.com

9. REFERENCES

1. Boneh, D., & Franklin, M. (2001). Identity-based encryption from the Weil pairing. Advances in Cryptology - CRYPTO 2001, 213-229.
2. Zhang, Y., et al. (2021). A privacy-preserving blockchain model using attribute-based encryption. Journal of Network and Computer Applications, 154, 102934.
3. Chen, L., et al. (2020). Control access mechanism for blockchain-based systems using smart contracts. Transaction on Dependable and Secure Computing, 17(5), 931-944.
4. Androulaki, E., et al. (2018). A distributed operating system for permissioned blockchains. Proceedings of the 13th EuroSys Conference, 1-15.
5. Sakai, R., & Kasahara, M. (2003). ID-based cryptosystems with pairing on elliptic curves. Cryptology ePrint Archive, Report 2003/054.
6. Wang, Q., et al. (2020). Identity-based encryption with outsourced revocation in cloud computing. Transaction on Information Forensics and Security, 15, 3371-3384.
7. Duan, S., et al. (2019). Secure data sharing scheme based on blockchain and attribute-based encryption. Journal of Systems Architecture, 97, 102123.
8. Maji, H. K., et al. (2019). Identity-based encryption with efficient revocation. Journal of Cryptology.
9. Agrawal, H., & Karyakarte, M. (2024). Decentralised identity and access management using blockchain. Measurement: Sensors, Elsevier.
10. Please provide alternative names for potential reviewers for your manuscript
11. Chawla, M., & Srivastava, A. (2024).Blockchain-based self-sovereign identity for healthcare data privacy. IJISAE.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

12. Shanthi, D. (2022). Smart Healthcare for Pregnant Women in Rural Areas. In Medical Imaging and Health Informatics (eds T.H. Jaware, K. Sarat Kumar, R.D. Badgujar and S. Antonov). https://doi.org/10.1002/9781119819165.ch17
13. D. Shanthi, R. K. Mohanty and G. Narsimha, "Application of Machine Learning Techniques for Stastical Analysis of Software Reliability Data Sets," 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2018, pp. 1472-1474, doi: 10.1109/ICCONS.2018.8663005.
14. D. Shanthi, Narla Swapna, Ajmeera Kiran, and Shaga Anoosha, Ensemble approach of GP, ACOT, PSO, and SNN for predicting software reliability, International Journal of Engineering Systems Modelling and SimulationVol. 15, No. 2, March 1, 2024pp 68-75.
15. D. Shanthi, R. K. Mohanty, G. Narsimha and V. Aruna, "Application of partical swarm intelligence technique to predict software reliability," 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2017, pp. 629-635, doi: 10.1109/ICCONS.2017.8250539.
16. D. Shanthi, P. Kuncha, M. S. M. Dhar, A. Jamshed, H. Pallathadka and A. L. K. J E, "The Blue Brain Technology using Machine Learning," 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatre, India, 2021, pp. 1370-1375, doi:10.1109/ICCES51350.2021.9489075.
17. Shanthi, D., C. H. Sankeerthana, and R. Usha Rani. "Spiking Neural Networks for Predicting Software Reliability." ICICNIS. 2020. 179-185.
18. Todupunuri, A. (2025). IMPROVING CUSTOMER EXPERIENCE WITH MODERN BANKING SOLUTIONS. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5120615
19. Babburi, S. (2024). Explainable AI Framework for Policy-Compliant Anomaly Detection in Data Pipelines.
20. Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
21. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
22. Poojari, R. INTELLIGENT SYSTEMS+B108 AND APPLICATIONS IN ENGINEERING.
23. Vasagam, M. (2024, August 30). Ensuring security in modern data pipelines: Practical strategies for data engineers. International Journal of Intelligent Systems and Applications in Engineering, 12(22s), 2401.
24. Santthosh Saai Reddy Purmani. (2026). Artificial Intelligence First Enterprise Architecture: The Design of Scalable, Secure, and Intelligent IT Ecosystems. American Journal of AI Cyber Computing Management, 6(1(2)), 1–8. https://doi.org/10.64751/ajaccm.2026.v6.n1(2).pp1-8
25. Cyril, H. P., & Kumara, S. (2026, February). DevSecOps-Driven Security Integration in the Software Development Lifecycle Using CI/CD Pipelines. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-6). IEEE.
26. Kotte, G. (2025). Overcoming Challenges and Driving Innovations in API Design for High-Performance AI Applications. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283649
27. Mahtabi, M., Roshan, M., Muhit, M. M. I., Behvar, A., & Haghshenas, M. (2026). Cryogenic ultrasonic fatigue: Mechanisms, advancements, and insights. Cryogenics, 153, 104257. https://doi.org/10.1016/j.cryogenics.2025.104257
28. Viswanathan, V. (2024). Pioneering Ethical AI Integration in Enterprise Workflows: A Framework for Scalable Team Governance. Available at SSRN 5375619.
29. Akhilaiswarya, B., Sree, B. T., Lilly, K., Chowdary, K. H., & Sruthi, M. (2023). Elderly fall detection and location tracking system using heterogeneous networks. Journal of Engineering Sciences, 14(05).
30. Viswanathan, V. (2025). Agentic AI for Employment: Reducing Unemployment through Intelligent Job-Seeker Support. LEX LOCALIS–Journal of Local Self-Government.
31. Mudusu, S. K. (2026, February 9). AI-augmented data quality engineering. InfoWorld (Foundry Expert Contributor Network).
32. Viswanathan, V., Shah, A. K., Kubam, C. S., Dontu, S., Gandhi, A., & Singla, P. (2025,

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

August). Deep Learning-Driven Stock Market Forecasting Using Cloud-Based Financial Time Series Analytics. In 2025 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC) (pp. 1-6). IEEE.

33. Sruthi, M. V., Soundararajan, K., & Sree, V. U. (2012). Accurate Multimodality Registration of medical images. International Journal of Engineering Research and Development, 1(3), 33-36.
34. Viswanathan, V., Polagani, S. S., Agarwal, R., Akula, S., Dey, S., & Kashyap, R. (2025, September). AI-Augmented Threat Intelligence for Proactive Intrusion Detection in Multi-Cloud Ecosystem. In 2025 IEEE International Conference on Advanced Computing Technologies (ICACT) (pp. 567-572). IEEE.
35. Mudusu, S. K., & Gentyala, S. (2026). Zero-Trust Data Pipelines for AI Systems: A Framework for Secure, Verifiable, and Auditable Data Engineering. JOURNAL OF RECENT TRENDS IN COMPUTER SCIENCE AND ENGINEERING (JRTCSE), 14(2), 10-25.
36. DEVARASETTY, N. (2023). SCALABLE DATA ENGINEERING APPROACHES FOR AI-DRIVEN INDUSTRIAL IOT APPLICATIONS. INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH AND MANAGEMENT, 11(06), 954-968.
37. Agrawal, A. M., Gajula, S., Shinde, R. P., Shah, H., & Ghosh, H. (2025, July). Machine Translation for Long Sequences with Enhanced Attention Mechanisms. In 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1-6). IEEE.
38. Dayal, P. S., Chandra, B. R., Keerthi, M., Sruthi, M., Venkatesh, K., Appalaraju, G., & Eswari, G. (2013). Design of Pyramidal Horn Antenna at 10GHz Using WIPL-D Optimizer. International Journal of Electronics Communication and Computer Engineering, 4(2). Maturi, S. Y. (2023). Crowdsourced frontier: Unveiling autonomous adversarial cybercapabilities via open AI competition. International Journal of Intelligent Systems and Applications in Engineering, 11(1s), 275–284.
39. Hassan, T., Karim, M. F., Jeelani, H., Behnam, E., Green, R., & Syed, F. J. (2025). Optimizing Medical Question-Answering Systems: A Comparative Study of Fine-Tuned and Zero-Shot Large Language Models with RAG Framework. arXiv preprint arXiv:2512.05863.
40. Manoharan, D. (2026). Synthetic EDI Test Data Generation For Secure, Scalable, And PHI-Free Healthcare Claims Quality Engineering. Journal of International Crisis and Risk Communication Research, 9(1).
41. Ravishankara, M. (2026, February). CircuChain: Disentangling Competence and Compliance in LLM Circuit Analysis. In SoutheastCon 2026 (pp. 1-7). IEEE.
42. Sruthi, M. V., Sree, V. U., & Soundararajan, K. (2012). Specific removal of motion artifacts in medical image processing. IJECCE, 3(3), 227-229.