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

TRUST-BASED PRIVACY PRESERVING PHOTO SHARING IN ONLINE SOCIAL NETWORKS

KANCHI GAYATRI DEVI
Department of MCA
SKBR PG COLLEGE, AMALAPURAM, A.P
gayatrikanchi84@gmail.com

Abstract
The explosive growth of Online Social Networks (OSNs) has made photo sharing a primary means of social interaction. However, sharing co-owned photos often leads to serious privacy violations because current OSN privacy policies are user-centric and fail to consider the privacy preferences of all individuals appearing in the photo.

Trust-Based Privacy Preserving Photo Sharing in Online Social Networks is a novel framework that leverages trust relationships among users to dynamically control the visibility and anonymization of co-owned photos. The system computes trust scores based on social interactions, relationship strength, and user feedback. It then applies selective anonymization techniques such as face blurring, region masking, or pixelation on sensitive parts of the image according to the minimum trust threshold set by co-owners.

By integrating trust evaluation with image processing and access control mechanisms, the framework effectively reduces privacy leakage while preserving the usability and visual quality of shared photos. The proposed system supports multi-user decision-making for co-owned content and provides a scalable, user-friendly solution for secure photo sharing in platforms like Facebook, Instagram, and Twitter. Experimental results demonstrate significant reduction in privacy risk with minimal impact on photo utility and social engagement.

Keywords: Online Social Networks, Photo Sharing Privacy, Trust-Based Access Control, Co-Owned Photos, Privacy Preservation, Image Anonymization, Trust Computation.

I.Introduction
Online Social Networks (OSNs) have transformed how people connect, communicate, and share life moments through photos. Millions of photos are uploaded and shared daily, many of which contain multiple individuals (co-owned photos). While this fosters social bonding, it raises critical privacy concerns. A user may unintentionally expose sensitive information about others in the photo, leading to unauthorized identification, stalking, or misuse of personal images.

Traditional OSN privacy settings are primarily owner-centric and do not adequately protect the privacy preferences of co-owners. Existing solutions often rely on crude methods such as complete denial of sharing or heavy anonymization, which reduce the social value of the photo.

To address these challenges, we propose a Trust-Based Privacy Preserving Photo Sharing framework. The system evaluates trust levels between the uploader and other individuals in the photo using social graph analysis, interaction history, and explicit user preferences. Based

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

on computed trust scores, the framework automatically applies appropriate anonymization techniques only to the portions concerning low-trust co-owners, while keeping the photo visually meaningful for high-trust viewers.

This approach provides fine-grained, dynamic privacy protection for co-owned photos in OSNs, balancing privacy preservation with social utility.

II. Literature Survey

Several studies have addressed privacy issues in photo sharing on OSNs:

- Xu et al. (2018) proposed a trust-based privacy-preserving mechanism for co-owned photos by selectively anonymizing images based on trust relationships.
- Li et al. introduced HideMe, a system that extracts privacy-sensitive factors from photos and enforces personalized privacy policies.
- Ra et al. (2013) developed P3, a privacy-preserving photo encoding scheme that splits images into public and secret parts.
- Various works on access control in OSNs highlight the importance of trust computation using friendship strength, interaction frequency, and common interests.
- Studies on image anonymization techniques (face detection, blurring, and region-specific masking) show their effectiveness in reducing re-identification risks while maintaining perceptual quality.

Most existing approaches either ignore trust dynamics or apply uniform anonymization, leading to over-protection or under-protection. Our work builds upon these foundations by integrating dynamic trust evaluation with adaptive image anonymization.

III. Existing System & Proposed System

A.ExistingSystem

Current OSNs such as Facebook and Instagram allow the photo uploader to set basic privacy levels such as public, friends, friends of friends, or custom. Co-owners have limited or no control over how their images are shared. Once uploaded, photos can be viewed, downloaded, or tagged by anyone within the chosen audience.

Disadvantages of Existing Systems:

1. No support for co-owner privacy preferences in multi-person photos.
2. Static and coarse-grained privacy settings.
3. High risk of privacy leakage through tagging and re-sharing.
4. Lack of trust-aware decision making.
5. No automatic anonymization based on viewer relationships.
6. Poor balance between privacy and photo utility.

B. Proposed System

The proposed Trust-Based Privacy Preserving Photo Sharing system introduces a collaborative and intelligent privacy mechanism. When a user uploads a photo containing multiple people, the system:

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

- Detects faces and identifies potential co-owners via tagging or face recognition.
- Computes trust scores between the uploader and each co-owner using social metrics.
- Allows co-owners to set minimum trust thresholds.
- Applies selective anonymization such as face blurring or masking only for viewers whose trust level falls below the threshold.
- Generates multiple versions of the photo dynamically based on viewer trust.

Advantages of the Proposed System:

1. Fine-grained, trust-aware privacy protection for co-owned photos.
2. Dynamic and adaptive anonymization.
3. Respects individual privacy preferences without ruining social value.
4. Reduced privacy leakage risk.
5. Improved user control and satisfaction.
6. Scalable for real-world OSN platforms.

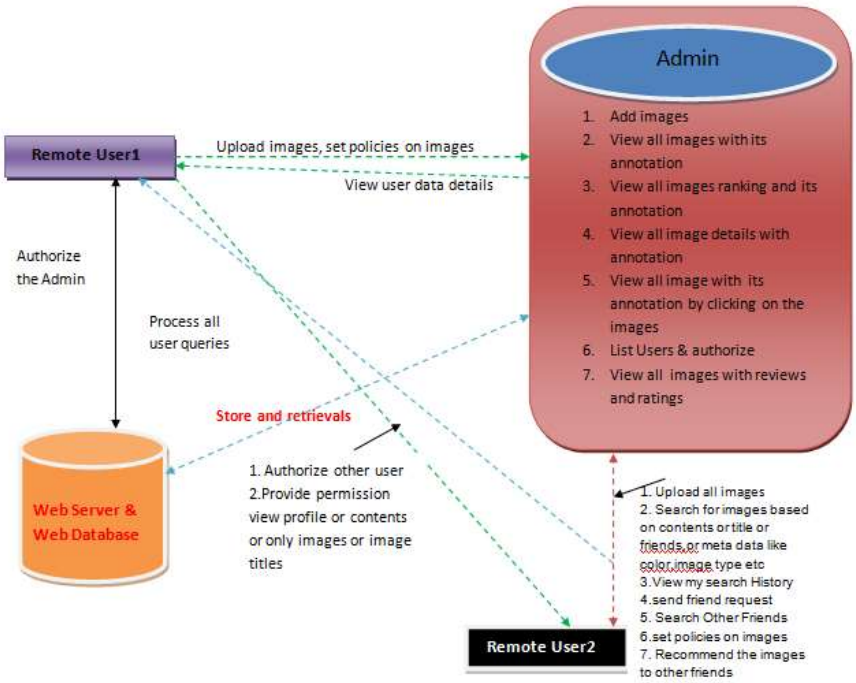
IV. System Design & Architecture

A. System Architecture

The architecture consists of a user-friendly web or mobile interface, trust computation engine, face detection and anonymization module, access control layer, and secure storage. Data flows from photo upload to co-owner identification, then to trust evaluation, followed by selective anonymization, and finally viewer-specific photo rendering.

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

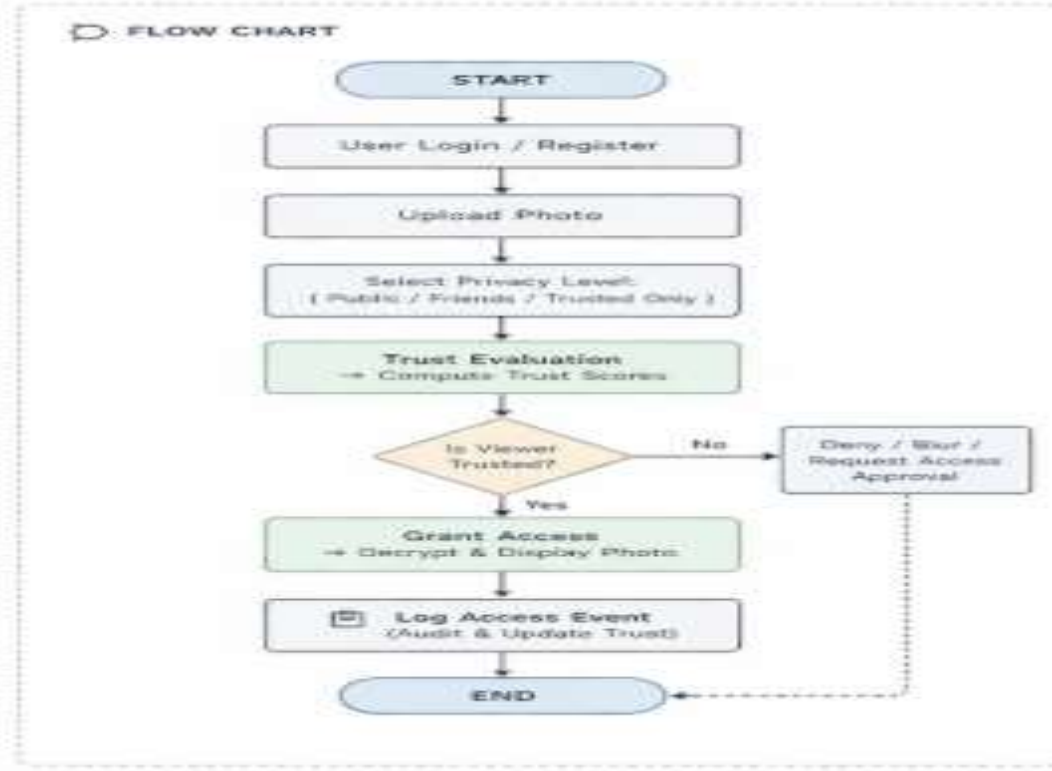
Architecture Diagram



B. System Flowchart

The process starts with user login and photo upload, followed by face detection and co-owner tagging. Then trust score calculation takes place, after which co-owners set approval or thresholds. Based on viewer trust, selective anonymization is applied, and finally secure sharing with dynamic rendering is performed.

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



C. Modules Overview

MODULES:

- ❖ System Construction Module
- ❖ Content-Based Classification
- ❖ Metadata-Based Classification
- ❖ Adaptive Policy Prediction

MODULES DESCSRIPTION:

System Construction Module

The A3P system consists of two main components: A3P-core and A3P-social. The overall data flow is the following. When a user uploads an image, the image will be first sent to the A3P-core. The A3P-core classifies the image and determines whether there is a need to invoke the A3P-social. In most cases, the A3P-core predicts policies for the users directly based on their historical

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

behavior. If one of the following two cases is verified true, A3P-core will invoke A3Psocial: (i) The user does not have enough data for the type of the uploaded image to conduct policy prediction; (ii) The A3P-core detects the recent major changes among the user's community about their privacy practices along with user's increase of social networking activities (addition of new friends, new posts on one's profile etc).

Content-Based Classification

To obtain groups of images that may be associated with similar privacy preferences, we propose a hierarchical image classification which classifies images first based on their contents and then refine each category into subcategories based on their metadata. Images that do not have metadata will be grouped only by content. Such a hierarchical classification gives a higher priority to image content and minimizes the influence of missing tags. Note that it is possible that some images are included in multiple categories as long as they contain the typical content features or metadata of those categories.

Our approach to content-based classification is based on an efficient and yet accurate image similarity approach. Specifically, our classification algorithm compares image signatures defined based on quantified and sanitized version of Haar wavelet transformation. For each image, the wavelet transform encodes frequency and spatial information related to image color, size, invariant transform, shape, texture, symmetry, etc. Then, a small number of coefficients are selected to form the signature of the image. The content similarity among images is then determined by the distance among their image signatures.

Metadata-Based Classification

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

The metadata-based classification groups images into subcategories under aforementioned baseline categories. The process consists of three main steps. The first step is to extract keywords from the metadata associated with an image. The metadata considered in our work are tags, captions, and comments. The second step is to derive a representative hypernym (denoted as h) from each metadata vector. The third step is to find a subcategory that an image belongs to. This is an incremental procedure. At the beginning, the first image forms a subcategory as itself and the representative hypernyms of the image becomes the subcategory's representative hypernyms.

Adaptive Policy Prediction

The policy prediction algorithm provides a predicted policy of a newly uploaded image to the user for his/her reference. More importantly, the predicted policy will reflect the possible changes of a user's privacy concerns. The prediction process consists of three main phases: (i) policy normalization; (ii) policy mining; and (iii) policy prediction.

Table I: Technology Stack

Table I: Technology Stack

Component	Technology / Tool
Programming Language	Java / Python
Frontend	HTML, CSS, JavaScript, JSP
Backend	Java Servlets / Flask
Database	MySQL
Image Processing	OpenCV, TensorFlow / Keras
Development Tool	NetBeans / Eclipse / PyCharm
Operating System	Windows / Linux

Table II: Performance / Evaluation Summary

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

Metric / Component	Proposed System	Traditional OSN Sharing	Remarks
Privacy Leakage Risk	Low	High	Trust-aware anonymization
Photo Visual Quality	High (for trusted users)	Full / Over-anonymized	Selective masking
Co-owner Control	Excellent	Limited	Threshold-based decisions
User Satisfaction	High	Moderate	Balanced privacy & utility
Computational Overhead	Acceptable	Low	Real-time face processing

Fig 1:-Home page

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

Fig 2:-uploaded photodetails

Fig 3:- View All users trust parameter

Fig 4:- passing phtosharing permission parameters

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

VI.Conclusion

This project presented a Trust-Based Privacy Preserving Photo Sharing framework for Online Social Networks. By combining trust computation with adaptive image anonymization, the system effectively protects the privacy of co-owners while maintaining the social value of shared photos.

The modular design and dynamic rendering approach make it highly suitable for modern OSNs. The framework reduces privacy risks associated with co-owned content and empowers users with fine-grained control. This work contributes to the growing field of privacy-aware social media technologies and sets a foundation for more intelligent and user-centric photo sharing mechanisms in the future.

References

1. L. Xu et al., Trust-Based Privacy-Preserving Photo Sharing in Online Social Networks, IEEE Transactions on Dependable and Secure Computing, 2018.
2. M. R. Ra et al., P3: Toward Privacy-Preserving Photo Sharing, NSDI, 2013.
3. F. Li et al., HideMe: Privacy-Preserving Photo Sharing on Social Networks, IEEE INFOCOM.
4. Studies on trust computation and access control in Online Social Networks.
5. Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
6. Purmani, S. S. R. (2024). Aligning IT investment decisions with overall business strategy from an enterprise program management perspective, focusing on the integration of IT leadership in strategic decision-making processes. International Journal of Communication Networks and Information Security, 16(5), 1213–1219
7. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
8. Mahimalur, R. K., Vasgam, M., & Manoharan, D. Devops Lifecycle Management And Cloud Migration Assessments: A Security-Driven CICD Perspective.
9. Purmani, S. S. R. (2025). Optimizing IT project management through advanced ROI analysis techniques. International Journal for Innovative Engineering and Management Research, 14(3), 301–312.
10. 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
11. Kotte, G. (2025). Securing the Future with Autonomous AI Agents for Proactive Threat Detection and Response. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283830
12. Purmani, S. S. R. (2025). Streamlining IT operations and service management with agile frameworks. European Journal of Advances in Engineering and Technology, 12(4), 76–81.
13. Mudusu, S. K. (2025). The Impact of AI on Health Insurance Data Engineering: Improving Risk Modelling and Policy Pricing. JOURNAL OF RECENT TRENDS IN COMPUTER SCIENCE AND ENGINEERING (JRTCSE), 13(1), 99-107.

14. 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
15. 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.
16. Purmani, S. S. R. (2025). Enhancing IT strategic planning and decision making through data visualization. International Journal of Enhanced Research in Management & Computer Applications, 14(4), 75–81
17. Maturi, S. Y. (2025). Vulnerabilities in the 802.11 Wireless Client Selection Mechanis.
18. Subramanian, V. K., Bhambri, S., & Gajula, S. (2025, April). Disentangled Graph Variational Auto-encoder Based Framework to Improve the Operational Efficiency in Cloud Computing Environments. In International Conference on Computer Vision and Robotics (pp. 396-407). Cham: Springer Nature Switzerland.
19. Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660
20. Maturi, S. Y. (2025). Blockbond Hardening: Securing Pooled-Hash Protocols Against Traffic Tampering, MITM Hash-Rate Hijacking, and Template Coercion. https://doi.org/10.20944/preprints202512.2064.v1
21. 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.
22. Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660
23. Maturi, S. Y. Cryptographic Privacy Engines: Practical Multi-Party Protocols For Confidential Database Queries.
24. Gajula, S., Bondhala, S., & Margam, M. (2026, February). Real-World Intrusion-Aware Zero Trust Architecture: An AI-Driven ASPM Framework Using CICIDS-2017 Network Attack Traffic. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-7). IEEE.
25. Ranjbareslamloo, S., Dzukeya, G. A., Muhit, M. M. I., & Qattawi, A. (2025). Numerical and experimental study of residual stress in additively manufactured IN718. Manufacturing Letters, 44, 915–927. https://doi.org/10.1016/j.mfglet.2025.915927
26. Maturi, S. Y. Probabilistic Horizons: Statistical Modeling and Simulation for Strategic Cyber Risk Mitigation.
27. Mudusu, S. K. (2026, March 26). A data trust scoring framework for reliable and responsible AI systems. InfoWorld (Foundry Expert Contributor Network).
28. Kotte, G. (2025). Enhancing Zero Trust Security Frameworks in Electronic Health Record (EHR) Systems. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283668
29. Mudusu, S. (2025). Health Insurance Fraud Detection: The Role Of Advanced It Systems In Preventing And Identifying Fraud. International Journal, 16(1), 3769-3777

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

30. Kotte, G. (2025). Revolutionizing Stock Market Trading with Artificial Intelligence. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283647
31. Maturi, S. Y. (2025). Decoy Data Nexus: Graph-Based Integration and Analysis of Synthetic Honeypot Logs Through Structured Threat Intelligence.
32. Sikder, M. Z., Shakil, M. A. I., Ahad, A., Karim, M. F., Intakhab, B., & Islam, D. A. (2025, June). Microwave-Based Detection of Early-Stage Renal Cell Carcinoma Using UHF Range Antenna. In 2025 International Conference on Computer Systems and Technologies (CompSysTech) (pp. 1-6). IEEE.
33. Mudusu, S. K. (2026, April 15). The secure intelligence framework: Architecting AI systems for a data-driven world. CIO (Foundry Expert Contributor Network).
34. 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
35. Manoharan, D. (2026). AI-Driven Anomaly Detection Models for Preventing Claims Denials and Revenue Leakage in Healthcare. Available at SSRN 6385759.
36. 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.
37. Gajula, S. (2025, December). Ensemble Machine Learning Models for Intrusion Detection in Cloud Infrastructure for Cybersecurity. In 2025 International Conference on Artificial Intelligence, Blockchain, Cloud Computing, and Data Analytics (ICoABCD) (pp. 1-6). IEEE.
38. Manoharan, D. (2026). Advancing Healthcare EDI Interoperability Through Informatica Cloud B2B Gateway Quality Engineering. Available at SSRN 6385719.
39. GIRISH KOTTE. (2025). ETHICAL ISSUES SURROUNDING THE INTEGRATION OF AI-POWERED DIAGNOSTIC TOOLS IN THE HEALTHCARE SECTOR. American Journal of AI Cyber Computing Management, 5(4), 329–334. https://doi.org/10.64751/ajaccm.2025.v5.n4.pp329-334
40. Chowdhury, A. K., Muhit, M. M. I., & Islam, M. M. (2023). A practical review to the marine maintenance practice in Bangladesh and a proposed way forward to an efficient, long-term and cost-effective solution. In Proceedings of the 13th International Conference on Marine Technology (MARTEC 2022). https://doi.org/10.2139/ssrn.4445071
41. Gajula, S., & Margam, M. (2026, February). A Secure and Scalable Cloud-Based Banking Service Model Leveraging AI and Advanced Cyber Security. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-5). IEEE.
42. Mudusu, S. K. (2025). AI-driven data engineering in the Internet of Things: Scaling data pipelines for smart device ecosystems. ISCSITR-International Journal of Data Engineering (ISCSITR-IJDE), 6(1), 1–9.
43. Gajula, S. (2025, December). Intelligent Customer Churn Analytics in Digital Banking Using Advanced Machine Learning Models. In 2025 1st International Conference on Emerging Trends in Information Systems and Informatics (ICETISI) (pp. 1-6). IEEE.
44. 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).

45. Mudusu, S. K. (2026, February 9). AI-augmented data quality engineering. InfoWorld (Foundry Expert Contributor Network).
46. Gajula, S. (2025). Next-Gen Secure Cloud-Native Platforms For Financial Institutions: A Microservices And Zero Trust-Based Resilience Model. Journal of International Crisis & Risk Communication Research (JICRCR), 8.
47. Manoharan, D. (2025). Healthcare EDI Transaction Lifecycles Embedded with a Multi-Layer Verification Framework to Ensure Referential Integrity.
48. Mudusu, S. K. (2025, December 22). Cognitive data architecture: Designing self-optimizing frameworks for scalable AI systems. CIO (Foundry Expert Contributor Network).
49. Ranjbareslamloo, S., Dzukey, G. A., Islam Muhit, M. M., & Qattawi, A. (2025). Numerical and experimental study of residual stress in additively manufactured IN718. Manufacturing Letters, 44, 915–927. https://doi.org/10.1016/j.mfglet.2025.06.108
50. Manoharan, D. (2025). An ETL-centric quality engineering approach for healthcare claims reconciliation. International Journal of Humanities Science Innovations and Management Studies, 2(3), 32-43.
51. Gajula, S. (2026, March). Two Pillars of Banking Intelligence: A Comparative Analysis of AI Techniques for Fraud Prevention and Churn Mitigation. In 2026 14th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.
52. Mudusu, S. K. (2025, June 3). Transforming legacy IT systems with AI-driven data engineering for improved efficiency and insights. Hampton Global Business Review (HGBR).
53. Manoharan, D. (2024). Governance-Oriented Quality Engineering Framework for Healthcare EDI Modernization. International Journal of Multidisciplinary on Science and Management IJMSM, 1(2).
54. DEVARASETTY, N. (2023). SCALABLE DATA ENGINEERING APPROACHES FOR AI-DRIVEN INDUSTRIAL IOT APPLICATIONS. INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH AND MANAGEMENT, 11(06), 954-968.
55. Mudusu, S. K. (2025, April 20). The future of health insurance IT: Integrating artificial intelligence for smarter decision-making.
56. 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.
57. Mudusu, S. K. (2025). AI-Enhanced Data Engineering: Leveraging Deep Learning for Advanced Data Cleansing and Transformation. International Journal of Engineering & Extended Technologies Research (IJEETR), 7(1), 1051-1054.