American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

Software Solutions to Identify Users Behind Social Media Based Drug Trafficking

[1] Dr. D. Shanthi, [2]O. Sanyogitha, [3]B. Akhila, [4]A. Anushka
[1]Professor, HOD, [(2,3,4)] B. Tech 4th year Student,
Department of Information Technology,
Vignan's Institute of Management and Technology for Women, Hyderabad, India
[1.]drshanthicse@gmail.com,[2.]ollalasanyogitha@gmail.com,[3.]akhilabolla42@gmail.com,
[4.]anurishi20051315@gmail.com

ABSTRACT

With the fast evolution of social media websites, criminal behavior like drug trafficking can now be performed discreetly using those platforms. Manual detection of such activities becomes challenging owing to huge amounts of unstructured data being generated every single day. This research paper introduces a Drug Trafficking Detection System which automatically analyses tweets for detecting suspicious activities. It utilizes some simple text pre-processing techniques, along with keyword search and risk assessment mechanism, in order to analyze individual tweets. Using a specific risk score generated for each tweet, the tweets are categorized into three types - Low Risk, Medium Risk, and High Risk. This system will generate alerts for risky tweets that police can act upon immediately. The system minimizes human labor, increases accuracy, and makes detection quick. The system is easy to use, inexpensive, and scalable; therefore, it is applicable in real-life settings. Despite its reliance on the current model where detection is based on keywords, this system can be improved through time to include sophisticated machine learning models and real-time data analysis. All in all, this system serves as an efficient method of monitoring social media to fight drug abuse.

Keywords:

Drug Trafficking Detection, Social Media Analysis, Tweet Analysis, Risk Analysis, Keyword-Based Detection, Text Processing, Crime Detection System

INTRODUCTION:

In recent years, the expansion of social media websites has revolutionized ways of human interaction, but there is one more significant aspect that must be noted, namely the opportunity for criminal organizations to use social networks for their purposes including drug trafficking. Such criminals tend to employ coded speech and indirect language, thus making detection through manual monitoring challenging. Given the huge amount of unstructured data collected each day, such processes take much time, are inefficient, and may cause errors. Thus, in order to provide an effective solution, this paper suggests designing a Drug Trafficking Detection System which will enable automated data analysis for identifying suspicious cases among tweet data. In particular, such an algorithm will include such stages as text preprocessing, keyword-based detection, and risk scoring. Depending on the obtained

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

score, tweets will be sorted according to specific criteria to low-risk, medium-risk, and high-risk ones. High-risk tweets will then be flagged and shown to police users via a dashboard. The proposed system is quite easy to use, scalable, and cheap, yet there is an option to improve its functioning by means of advanced techniques.

LITERATURE SURVEY:

There have been several researches carried out on the development of techniques that can be used to monitor drug related activities on social media platforms. For instance, Raval and Patel (2021) proposed a novel technique that uses AI based monitoring system that detects suspicious behaviors based on texts and user interactions and provides instant alerts. However, it suffers from various drawbacks like false positives and privacy concerns [1]. Sridevi et al. (2020) have proposed a semi-supervised deep learning technique that focuses on detecting activities through analyzing hashtag metadata. It helps improve detection accuracy by identifying slang terms; however, it is constrained by data constraints and variations in language [2]. Robin et al. (2018) carried out interviews to investigate risks involved with law enforcement officers and users. However, their findings are limited due to small samples and self-reported behavior [3]. While these techniques have helped address various concerns regarding detection of drugs on social media platforms, they have several limitations. These include the inability to scale up, data dependency and detection accuracy. That is why the proposed solution takes a different path by implementing simple yet practical techniques [4].

System Architecture:

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

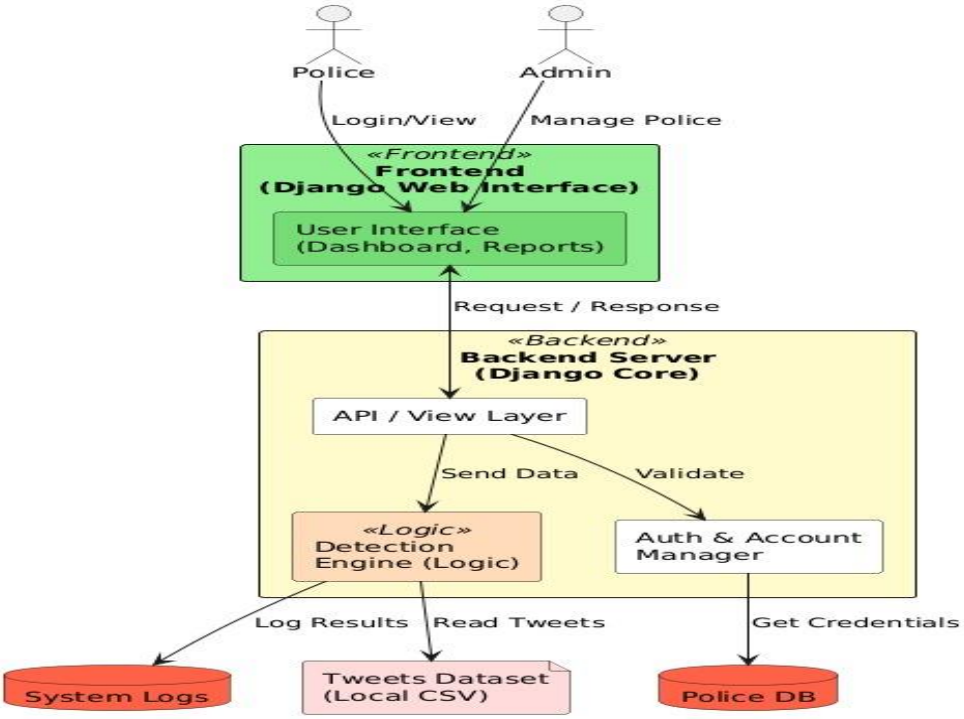


Fig.1: System Architecture

Implementation:

Drug trafficking detection algorithm will be developed using Python language and will have a web-based approach for interaction. The input data will be read from the tweet details stored in a CSV file. The initial process that will be performed on the data is preprocessing, where the data will be converted into lowercase and punctuation marks will be stripped out. .

Drug trafficking detection algorithm will be developed using Python language and will have a web-based approach for interaction. The input data will be read from the tweet details stored in a CSV file. The initial process that will be performed on the data is preprocessing, where the data will be converted into lowercase and punctuation marks will be stripped out.

Additionally, there is the inclusion of user management capabilities, where there are two different roles of Admin User and Police User. The admin user will be responsible for managing accounts and securing access to the system. On the other hand, the police user will be able to login to see the analysis presented in the dashboard. Threatening tweets will be highlighted as an alert.

The design of the system ensures that it will be scalable, capable of processing large amounts of data effectively. Multiple data entries are processed at once in an orderly fashion, guaranteeing quick analysis and reaction times. The design of the system facilitates the addition of new features, including real-time data gathering and more sophisticated analysis

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

methods. Fundamental security features are included, ensuring proper protection of data and access control.

Algorithms:

Keyword-Based Text Classification: The program employs rule-based text classification for detecting any suspicious message. The pre-defined set of keywords that have some relation with drugs like drug, cocaine, weed, heroin, and crack is utilized in checking the generated texts. The message is made lowercase and then checked for the presence of one of the keywords. The message is tagged as suspicious if the check returns positive results.

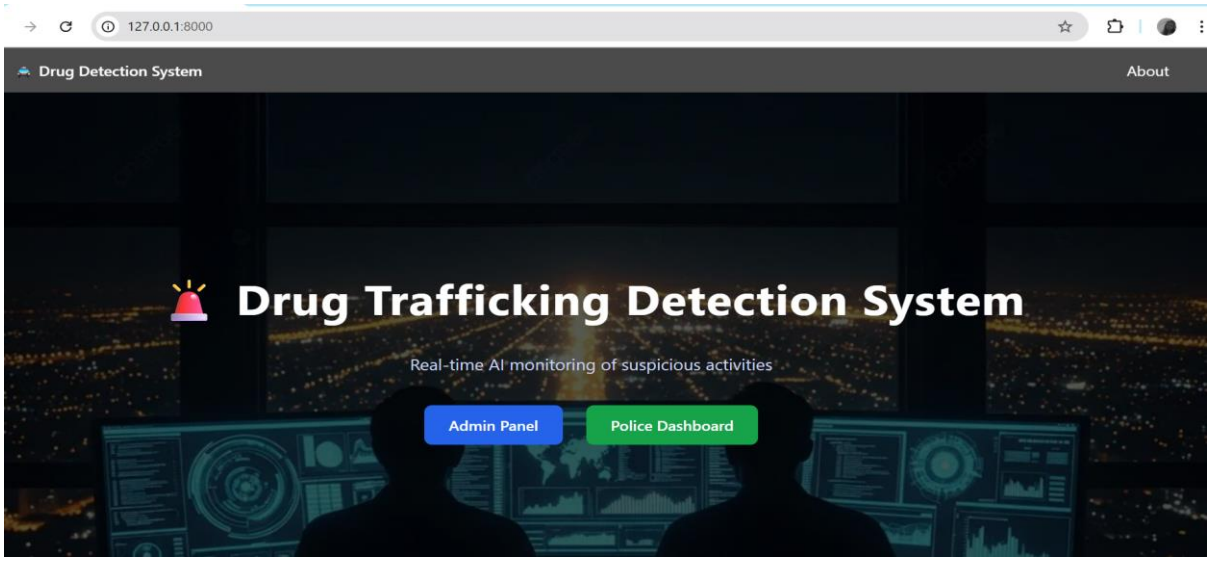
String Matching Algorithm: The string match algorithm is implemented in order to determine whether or not the keyword appears in the given text. The string matching algorithm is done by utilizing the inherent functionality of Python that searches through the messages iteratively.

Risk Scoring Mechanism: The program will assign a risk factor to all detected messages depending on whether any suspicious keywords are found within the text. These messages are classified under varying degrees of risk, such as Low, Medium, and High.

Data Filtering Algorithm: For efficient processing of large databases, the system employs a sequential data filtering algorithm. The filtering is done according to various attributes of messages, including the username, timestamp, and keywords.

Report Generation Algorithm: The system contains a report generation component where all suspect messages for each individual are consolidated. Relevant information is gathered, a case number is assigned, and reports are generated for use by law enforcement agencies.

II. RESULTS



Received: 28-03-2026 | Accepted: 06-05-2026 | Published: 13-05-2026

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

Fig.8: Home Page of Drug Trafficking Detection System

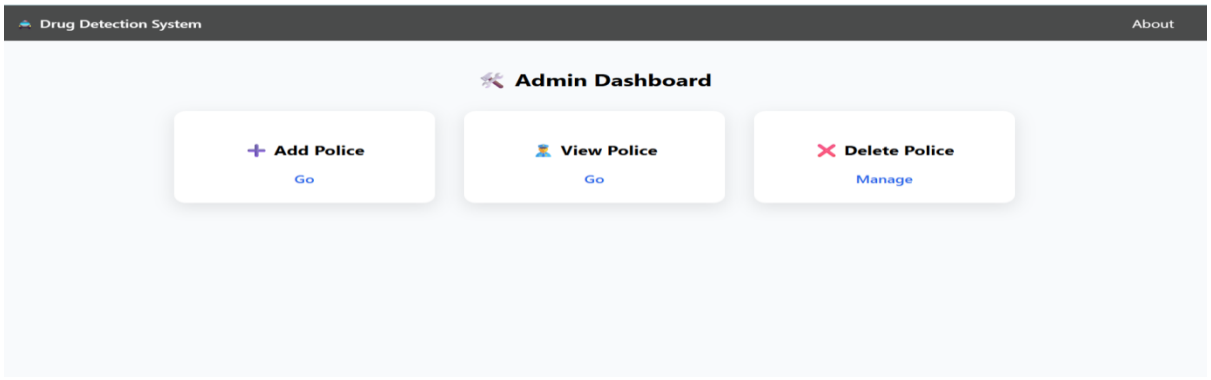


Fig.9: The Dashboard of the Admin

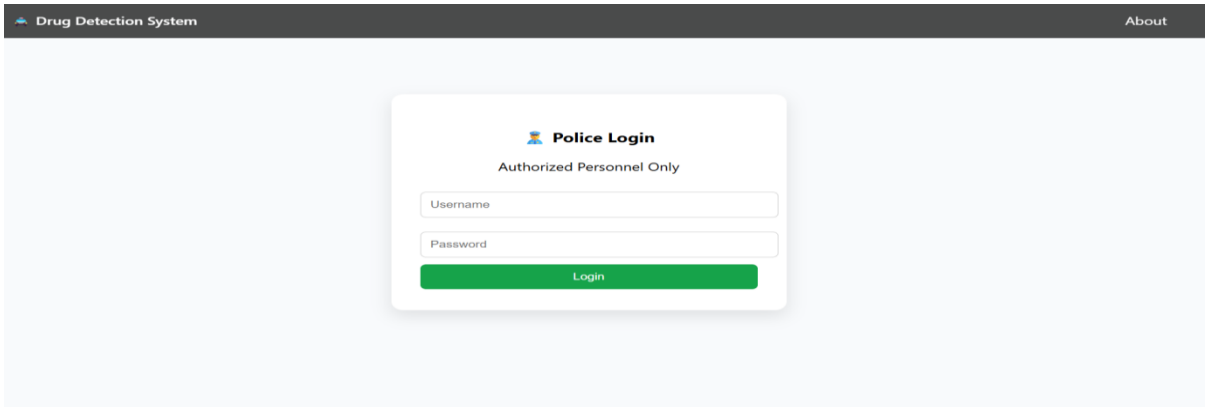


Fig.10: The Dashboard of Police

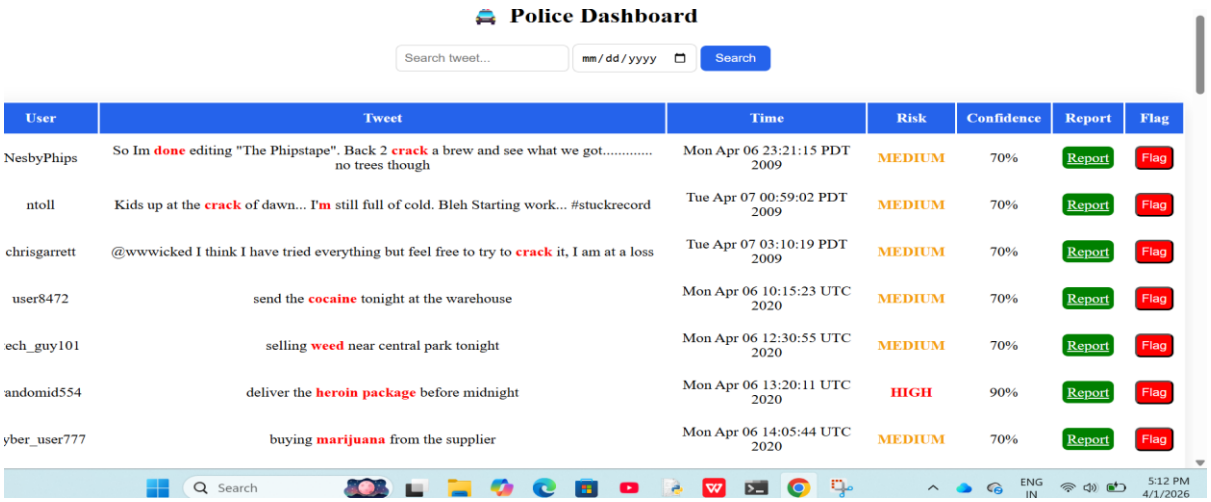


Fig.12: Police Dashboard of Drug Trafficking Detection System

Received: 28-03-2026 | Accepted: 06-05-2026 | Published: 13-05-2026

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

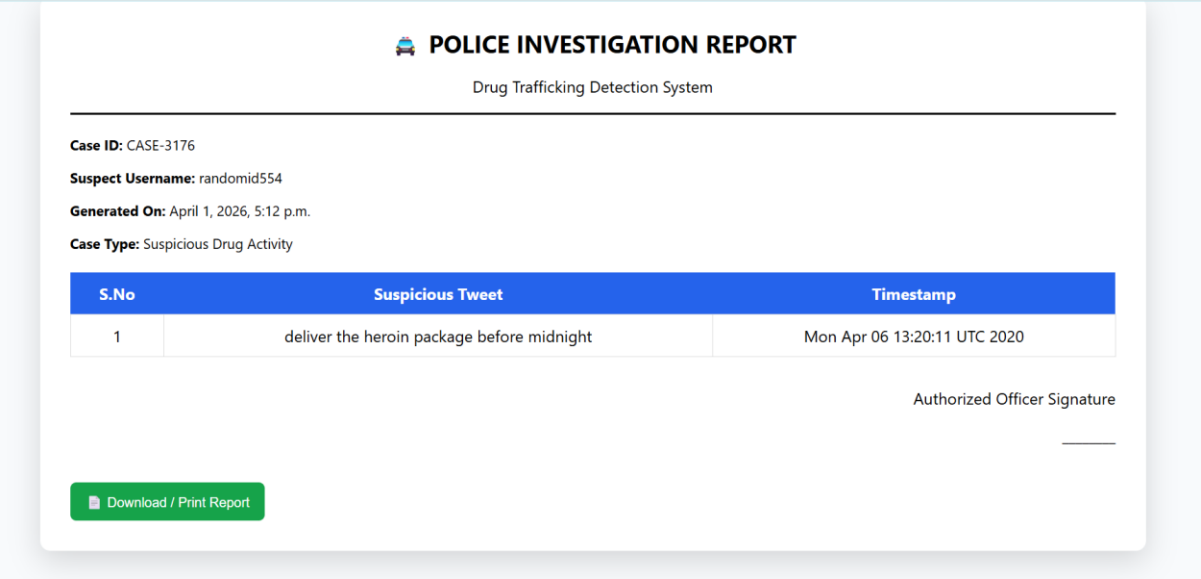


Fig.14: Police Investigation Report Page of Drug Trafficking Detection System.

CONCLUSION:

The suggested Drug Trafficking Detection System is highly efficient in detecting suspicious activity from social media platforms by performing automated analysis of a large number of tweets. This includes the application of text preprocessing, keyword detection, and risk assessment in order to assess each individual tweet. The classification process categorizes tweets as either low risk, medium risk, and high risk. This makes it easier to comprehend any kind of threat. High-risk tweets are emphasized and flagged as an alert for police personnel. This enables prompt and informed decisions to be made. This system saves time and prevents mistakes that might happen with manual processes. It is relatively straightforward, inexpensive, and scalable to adapt to different scenarios. In addition, it features a convenient dashboard display for the police to monitor suspicious activity. Overall, the performance of the system proves to be efficient in detecting any suspicious behavior. However, this system is based on keyword detection which does not detect complicated patterns. Advanced machine learning techniques can be applied for future improvements.

FUTURE SCOPE:

There are various improvements that can be made on the proposed system such as including machine learning and deep learning approaches to increase the efficiency of the process. This system can be improved by incorporating the aspect of collecting real-time data from sources

such as Twitter, Instagram, and Telegram. NLP algorithms can also be included in order to gain an understanding of the context of the communication, the use of slang, and coded messages. It is also possible to incorporate more languages into the system for greater application. Moreover, it can also be used to detect other forms of cybercrimes such as human trafficking, fraud, and terrorism. In addition, improvements can be made in the form of user interface as well as inclusion of charts, maps, graphs, and dashboards for decision-making by law enforcement.

REFERENCES:

1. J. Devlin et al., “BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding,” 2019.
   A. Alharbi et al., “Automatic Detection of Drug-related Content on Social Media,” 2021.
2. S. Minaee et al., “Deep Learning-based Text Classification: A Survey,” 2021.
3. J. Kowsari et al., “Text Classification Algorithms: A Survey,” 2019.
   A. Pak and P. Paroubek, “Twitter as a Corpus for Sentiment Analysis,” 2010.
4. F. Pedregosa et al., “Scikit-learn: Machine Learning in Python,” 2011.
5. Y. Liu et al., “RoBERTa: A Robustly Optimized BERT Pretraining Approach,” 2019.
6. Shaoqing Ren, Kaiming He, Ross Girshick, and Jian Sun, "Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks," IEEE Transactions on Pattern Analysis and Machine Intelligence,2017.
7. D Shanthi, "Smart Water Bottle With Smart Technology", Handbook Of Artificial Intelligence, Benthem Science Publishers, Pg. No: 204-219, 2023.
8. P. K. Bolisetty And Midhunchakkaravarthy, "Comparative Analysis Of Software Reliability Prediction And Optimization Using Machine Learning Algorithms," 2025 International Conference On Intelligent Systems And Computational Networks (ICISCN), Bidar, India, 2025, Pp. 1-4, Doi: 10.1109/ICISCN64258.2025.10934209.
9. Shanthi, Dr. D., G. Ashok, Chitrika Biswal, Sangem Udharika, Sri Varshini, and Gopireddi Sindhu. 2025. “Ai-Driven Adaptive It Training: A Personalized Learning Framework For Enhanced Knowledge Retention And Engagement”. Metallurgical and Materials Engineering, May, 136-45. https://metall-mater-eng.com/index.php/home/article/view/1567.
10. Shanthi, D., Aryan, S. R., Harshitha, K., & Malgireddy, S. (2023, December). Smart Helmet. In International Conference on Advances in Computational Intelligence (pp. 1-17). Cham: Springer Nature Switzerland.
11. Shanthi, D., G. Narsimha, and R.K. Mohanthy. 2015. Human Intelligence vs. Artificial Intelligence. International Journal of Electronics Communication and Computer Engineering 6 (5): 30–34.
12. 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.

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

13. 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.
14. 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.
15. Shanthi, D., C. H. Sankeerthana, and R. Usha Rani. "Spiking Neural Networks for Predicting Software Reliability." ICICNIS. 2020. 179-185.
16. 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.
17. P. Endla, A. R, S. Suneel, A. P. Singh, P. A and D.Shanthi, "MedSensePathway: A Hybrid Framework for Real-Time Diagnosis of Malarial Parasites using Medical Imaging," 2025 9th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2025, pp. 1972-1978, doi: 10.1109/ICECA66444.2025.11382939.
18. 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
19. Todupunuri, A. (2025). IMPROVING CUSTOMER EXPERIENCE WITH MODERN BANKING SOLUTIONS. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5120615
20. Babburi, S. (2024). Explainable AI Framework for Policy-Compliant Anomaly Detection in Data Pipelines.
21. Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
22. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
23. Poojari, R. INTELLIGENT SYSTEMS+B108 AND APPLICATIONS IN ENGINEERING.
24. 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.
25. 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

26. 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.

27. 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

28. 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

29. Viswanathan, V. (2024). Pioneering Ethical AI Integration in Enterprise Workflows: A Framework for Scalable Team Governance. Available at SSRN 5375619.

30. 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).

31. Viswanathan, V. (2025). Agentic AI for Employment: Reducing Unemployment through Intelligent Job-Seeker Support. LEX LOCALIS–Journal of Local Self-Government.

32. Mudusu, S. K. (2026, February 9). AI-augmented data quality engineering. InfoWorld (Foundry Expert Contributor Network).

33. Viswanathan, V., Shah, A. K., Kubam, C. S., Dontu, S., Gandhi, A., & Singla, P. (2025, 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.
34. 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.

35. 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.

36. 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.

37. DEVARASETTY, N. (2023). SCALABLE DATA ENGINEERING APPROACHES FOR AI-DRIVEN INDUSTRIAL IOT APPLICATIONS. INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH AND MANAGEMENT, 11(06), 954-968.

38. 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.

39. 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).

40. 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.

41. 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.

42. 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).

43. Ravishankara, M. (2026, February). CircuChain: Disentangling Competence and Compliance in LLM Circuit Analysis. In SoutheastCon 2026 (pp. 1-7). IEEE.

44. Sruthi, M. V., Sree, V. U., & Soundararajan, K. (2012). Specific removal of motion artifacts in medical image processing. IJECCE, 3(3), 227-229.