DETECTING FRAUDULENT STUDENT COMMUNICATION IN A MULTIPLE CHOICE ONLINE TEST ENVIRONMENT

CHELLIBOINA MANIKANTA SWAMY
Department of MCA
SKBR PG COLLEGE, AMALAPURAM, A.P
swamyprince5544@gmail.com

Abstract
Online evaluation systems, pervasive nowadays, are known to be susceptible to higher fraud risks. This work proposes a novel and robust method to detect potential fraud acts in online multiple-choice question (MCQ) exams. For the first time, the communication probability between the examinees is statistically assessed based on the concordance of responses and answer time against null expectations and is subsequently used to identify potential fraud behavior. The model is sensitive to the direction of communication acts, distinguishing content consumption from production, as well as multiwise communication channels. Online remote tests from engineering courses at Tecnico Lisboa are used as a case study. We show that the cumulative contribution of concordant responses between students, when recurrent, offers a way of signaling fraud behavior. Separating content production from consumption reveals the underlying student role played in potential fraud acts. Collusion behavior is assessed against null models of fraud and conformity, and therefore being statistically framed and offering a solid criterion to guide tutors in ascertaining fraud and discouraging communication.

Keywords: Fraudulent Communication Detection, Online MCQ Exams, Collusion Analysis, Statistical Modeling, Network Representation, Null Models, Response Concordance, Answer Time Analysis, Academic Integrity, Remote Proctoring.

I.Introduction

With the rapid adoption of online learning and digital examinations, multiple choice question (MCQ)-based assessments have become a standard evaluation method in educational institutions. However, maintaining academic integrity in such environments has become increasingly challenging due to the ease of digital communication and access to external resources.

In an online MCQ examination environment, students may engage in fraudulent communication using various digital channels such as messaging apps, browser tabs, screen sharing tools, or external devices. These actions compromise the fairness and credibility of the assessment process. Traditional invigilation methods are insufficient in remote settings, making it difficult to detect real-time cheating behavior.

This paper introduces a novel statistical network-based framework for detecting fraudulent student communication in multiple-choice online test environments. The methodology leverages time-stamped answer records and response concordance to identify collusion patterns with strong statistical guarantees.

II.LiteratureSurvey

A. M. Duhaim et al. (2021) investigate data mining techniques for cheating detection during online exams using behavioral patterns such as mouse movements and response times.
R. Bawarith et al. (2017) propose an e-exam cheating detection system integrating biometric authentication and behavior analysis.
B. A. Barr and S. F. Miller (2013) highlight vulnerabilities of remote assessments to academic dishonesty.
R. Matos and J. Barber (2013) examine security flaws in Moodle-based examination environments.
V. Susithra et al. (2021) focus on automated proctoring using computer vision and machine learning for anomalous behavior detection.
G. R. Watson and J. Sottile (2010) explore the prevalence of cheating in digital learning environments.
C. M. Toquero (2020) discusses challenges in higher education during the COVID-19 pandemic.
F. Kamalov et al. (2021) propose machine learning-based cheating detection in online exams.
P. R. Morales and M. L. Verde (2020) examine psychometric techniques for valid remote assessments.
R. K. Ladyshewsky (2015) compares performance in supervised vs. unsupervised online tests.
Z. Zhang et al. (2022) address fraudulent activities using advanced bot detection.
H. Hu et al. (2021) introduce random forest-based test-cheating detection.
J. Ranger et al. (2020) assess cheating detection indicators in e-exams.
M. Li et al. (2021) propose an optimized collusion prevention framework.
G. J. Cizek and J. A. Wollack (2017) provide quantitative methods for detecting cheating.

III. Existing System & Proposed System

A. Existing System

Existing approaches rely on statistical methods such as item response theory, response time analysis, and biometric/proctoring tools. Many systems use rule-based monitoring, machine learning classification, or computer vision for anomaly detection.

Disadvantages of Existing Systems:

1. Assume fixed question orders and reversible answering.
2. Neglect distinguished roles and multiwise cumulative effects from inadvertent content sharing.
3. Do not reliably test deviation against plausible expectations.
4. High dependency on manual proctoring or expensive hardware.
5. Limited ability to detect directional and group-level collusion.

B. Proposed System

The proposed system introduces a disruptive methodology to assess fraud communication using four major principles:

1. Statistical frame to assess pairwise communication probability (matched answers, choice probability, response times, recurrence).
2. Network representation of potential communication acts.
3. Null models of compliance and fraud for statistical significance.
4. Scoring, clustering, and visualization to support tutor actionability.

The framework distinguishes content production from consumption and detects multiwise channels while providing strict statistical guarantees.

Advantages of the Proposed System:

1. Statistically robust detection with null models.
2. Directional and multi-participant collusion analysis.
3. No dependency on expensive proctoring hardware.
4. Actionable insights with scoring and clustering.
5. Effective in dynamic question-order environments.

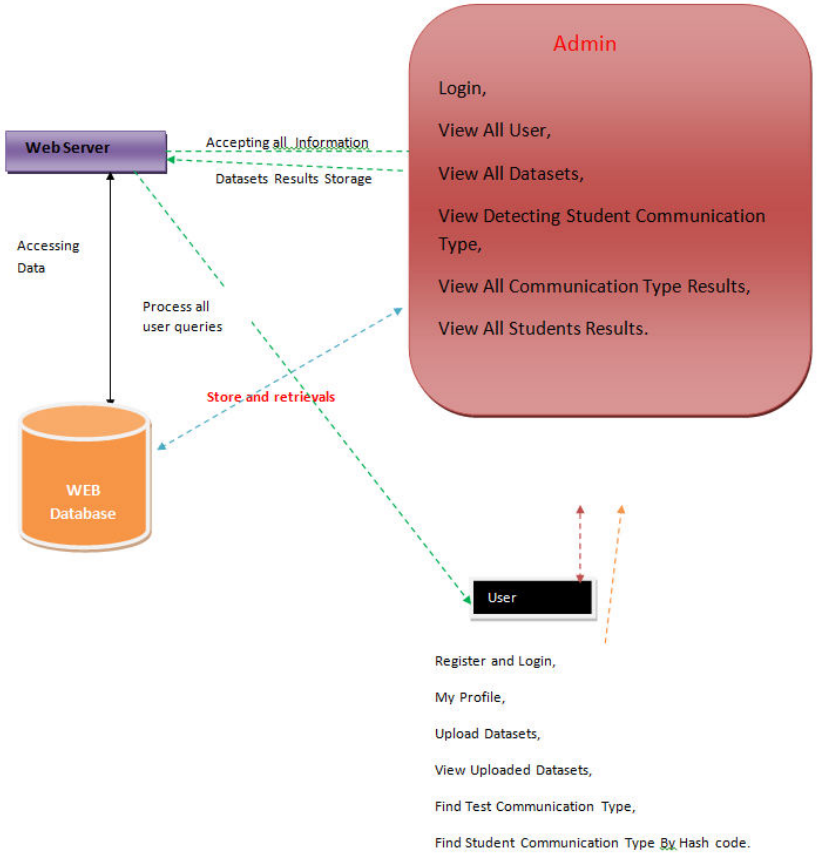
IV. System Design & Architecture

A. System Architecture

The architecture follows a layered model:

- **Frontend Layer** — User interface for students and admins (JSP).
- **Monitoring Layer** — Real-time data collection (response time, answers).
- **Processing Layer** — Statistical analysis and network construction.
- **Fraud Detection Engine** — Null model comparison and scoring.
- **Backend Layer** — MySQL database for logs and results.

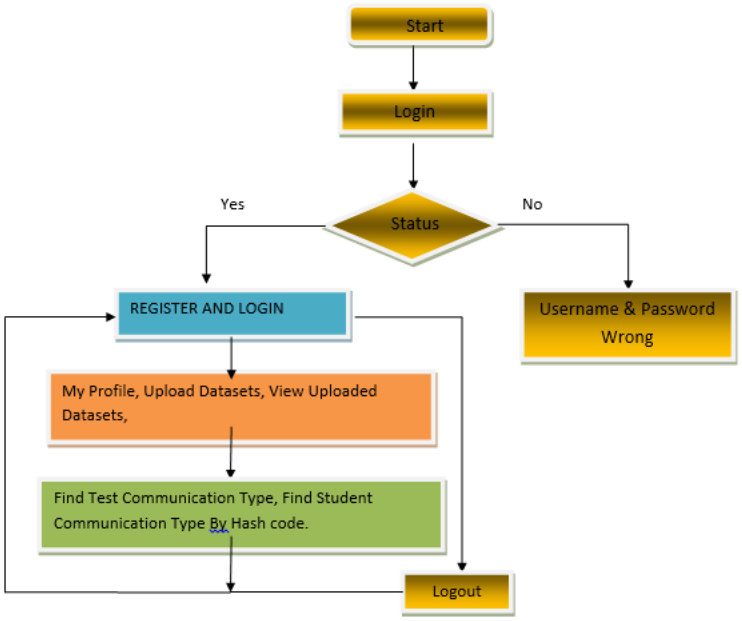
Data flows from exam session → real-time monitoring → statistical network building → fraud scoring → alert generation.



B. System Flowchart

The process starts with student login → exam initialization → real-time response collection → statistical probability calculation → network representation → null model comparison → fraud scoring → clustering and visualization → alert generation and report.

➢ **Flow Chart : User**



C. Modules Overview

1. Admin Module — User management, dataset view, fraud reports.
2. User (Student) Module — Registration, login, exam participation, profile management.
3. Monitoring & Data Collection Module.
4. Statistical Analysis & Network Construction Module.
5. Fraud Detection & Scoring Module.
6. Visualization & Reporting Module.

Table I: Technology Stack

Component	Technology / Tool
Language	Java / J2EE (JSP + Servlet)
Web Framework	JSP + Servlet
Database	MySQL
Development Tool	NetBeans 7.2.1
Server	Apache Tomcat
Hardware	Pentium IV 2.4 GHz, 40 GB HDD, 512 MB RAM
Operating System	Windows 7

Table II: Performance / Evaluation Summary

Metric / Component	Proposed System	Existing Systems	Remarks
Collusion Detection Accuracy	High	Moderate	Statistical null models
Directional Analysis	Yes	No	Production vs Consumption
Multiwise Channel Detection	Yes	Limited	Network representation
False Positive Rate	Low	High	Strict statistical guarantees
Tutor Actionability	Excellent	Low	Scoring + Clustering
Real-Time Capability	Yes	Partial	Response-time analysis

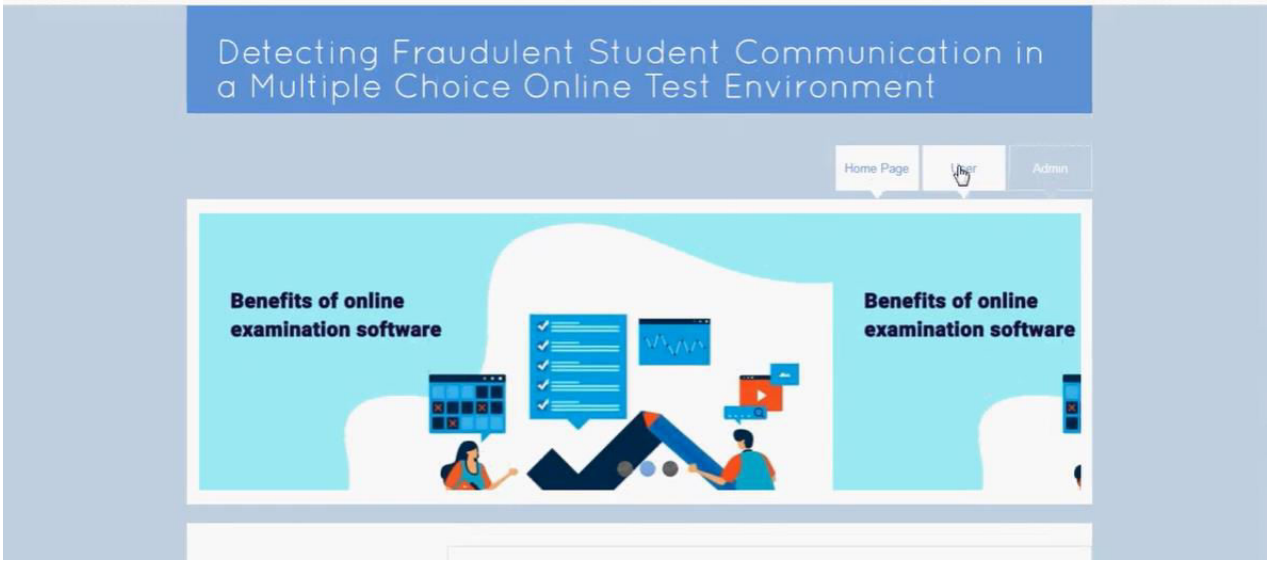


Fig :- Home page

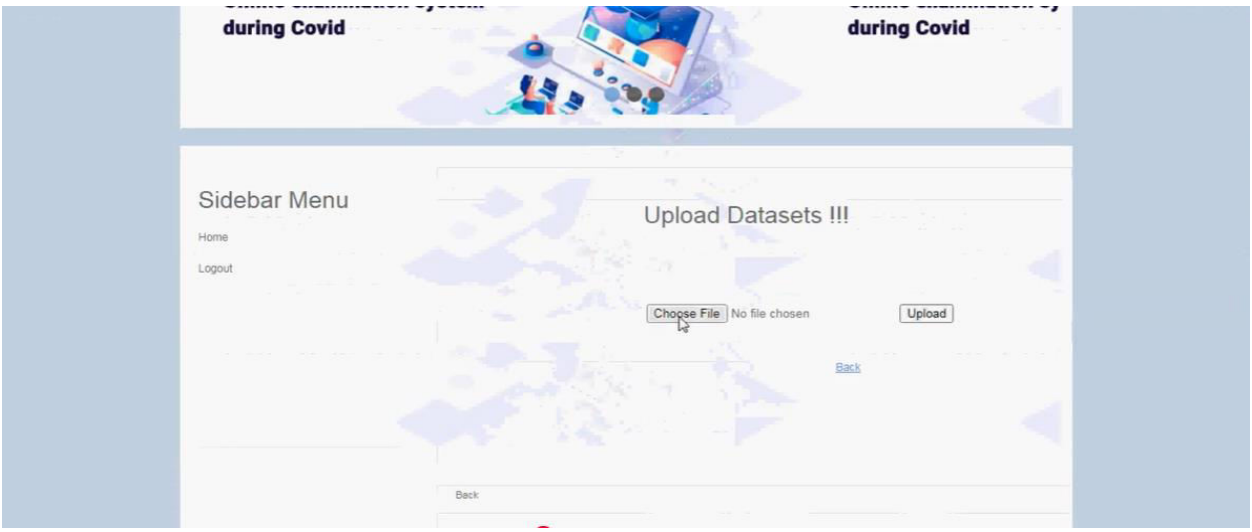
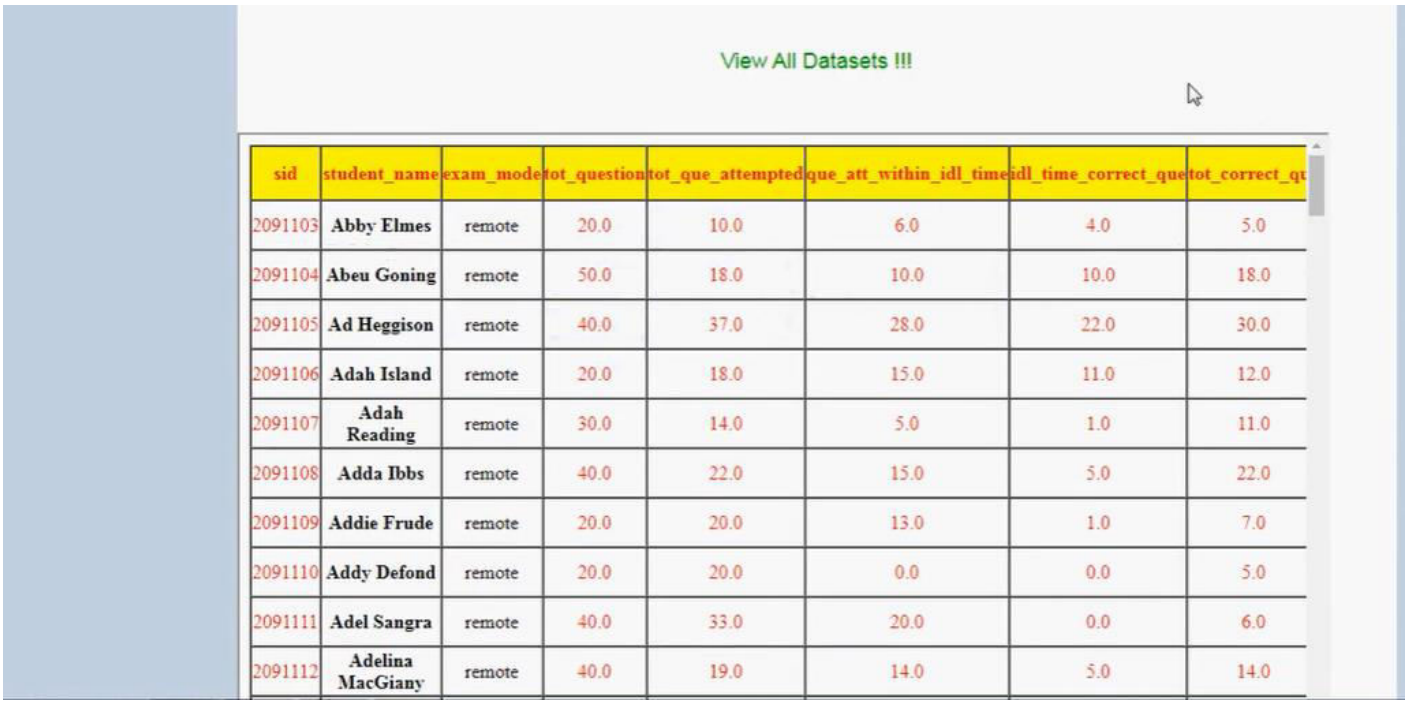


Fig 2:-upload test dataset



View All Datasets !!!

sid	student_name	exam_mode	tot_question	tot_que_attempted	que_att_within_idl_time	idl_time_correct_que	tot_correct_qu
2091103	Abby Elmes	remote	20.0	10.0	6.0	4.0	5.0
2091104	Abeu Goning	remote	50.0	18.0	10.0	10.0	18.0
2091105	Ad Heggison	remote	40.0	37.0	28.0	22.0	30.0
2091106	Adah Island	remote	20.0	18.0	15.0	11.0	12.0
2091107	Adah Reading	remote	30.0	14.0	5.0	1.0	11.0
2091108	Adda Ibbs	remote	40.0	22.0	15.0	5.0	22.0
2091109	Addie Frude	remote	20.0	20.0	13.0	1.0	7.0
2091110	Addy Defond	remote	20.0	20.0	0.0	0.0	5.0
2091111	Adel Sangra	remote	40.0	33.0	20.0	0.0	6.0
2091112	Adelina MacGiany	remote	40.0	19.0	14.0	5.0	14.0

Fig3:- data in dataset

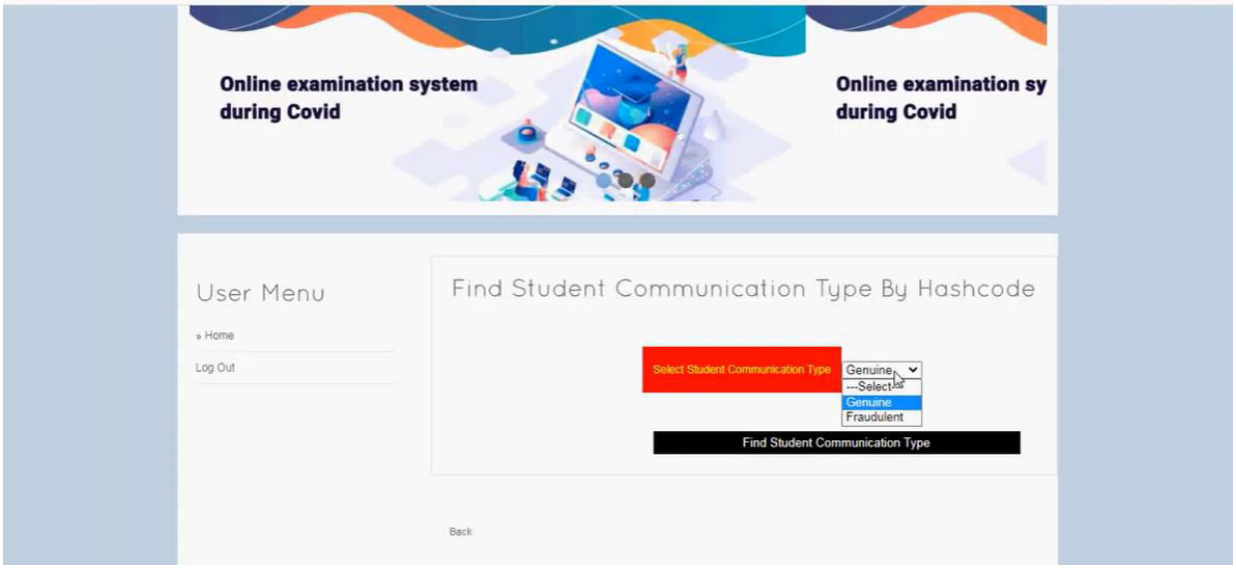


Fig 4:-checking genuine and fake examination

VI. Conclusion

This work introduced a novel methodology to assess likely fraud communication acts in remote online MCQ exams based on the concordance of responses and answer times. Null models are produced to understand regular versus fraud dynamics and to identify collusion

with strict guarantees of statistical significance. Complementarily, clustering algorithms are applied to unravel communication channels between students.

The application of the proposed principles reveals students with a higher fraud likelihood, providing a solid criterion to guide tutors in detecting and discouraging collusion. Future enhancements include AI-based proctoring integration, blockchain for immutable logs, adaptive models, and real-time alerts.

References

1. A. M. Duhaim, S. O. Al-Mamory, and M. S. Mahdi, “Cheating detection in online exams during COVID-19 pandemic using data miningbtechniques,” Webology, vol. 19, pp. 1–26, 2021.
2. R. Bawarith, D. Abdullah, D. Anas, and S. Gamalel-Din, “E-exam cheating detection system,” Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 4, pp. 176–181, 2017.
3. B. A. Barr and S. F. Miller, “Higher education: The online teaching and learning experience,” Fac. School Adv. Stud., ERIC, Univ. Phoenix, Phoenix, AZ, USA, Tech. Rep. ED543912, 2013.
4. R. Matos and J. Barber, “MoodleGate: Securing computer driven exam environments,” in Proc. INTED, 2013, pp. 1–7.
5. V. Susithra, A. Reshma, B. Gope, and S. Sankar, “Detection of anomalous behaviour in online exam towards automated proctoring,” in Proc. Int. Conf. Syst., Comput., Autom. Netw. (ICSCAN), Jul. 2021, pp. 1–5.
6. G. R. Watson and J. Sottile, “Cheating in the digital age: Do students cheat more in online courses?” Online J. Distance Learn. Admin., vol. 13, no. 1, pp. 1–14, 2010.
7. C. M. Toquero, “Challenges and opportunities for higher education amid
8. the COVID-19 pandemic: The philippine context,” Pedagogical Res., vol. 5, no. 4, Apr. 2020, Art. no. em0063.
9. F. Kamalov, H. Sulieman, and D. S. Calonge, “Machine learning based approach to exam cheating detection,” PLoS ONE, vol. 16, no. 8, Aug. 2021, Art. no. e0254340.
10. P. R. Morales and M. L. Verde, “Como asegurar evaluaciones validas y detectar falseamiento en pruebas a distancia sincronas,” Revista Digit.
11. de Investigacion en Docencia Universitaria, vol. 14, no. 2, p. e1240, Nov. 2020.
12. R. K. Ladyshewsky, “Post-graduate student performance in ‘supervised
13. in-class’ vs. ‘unsupervised online’ multiple choice tests: Implications
14. for cheating and test security,” Assessment Eval. Higher Educ., vol. 40, no. 7, pp. 883–897, Oct. 2015.
15. Z. Zhang, S. Zhu, J. Mink, A. Xiong, L. Song, and G. Wang, “Beyond bot detection: Combating fraudulent online survey takers,” in Proc. ACM Web Conf., Apr. 2022, pp. 699–709.
16. H. Hu, Z. Li, and Z. Wang, “Test cheating detection method based on random forest,” in Proc. 3rd Int. Conf. Comput. Sci. Technol. Educ. (CSTE), May 2021, pp. 47–52.

17. J. Ranger, N. Schmidt, and A. Wolgast, "The detection of cheating on E-exams in higher education—The performance of several old and some new indicators," Frontiers Psychol., vol. 11, Oct. 2020, Art. no. 568825.
18. M. Li et al., "Optimized collusion prevention for online exams during social distancing," NPJ Sci. Learn., vol. 6, no. 1, pp. 1–9, Mar. 2021.
19. G. J. Cizek and J. A. Wollack, Handbook of Quantitative Methods for Detecting Cheating on Tests. Evanston, IL, USA: Routledge,2017.
20. Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
21. 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
22. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
23. Mahimalur, R. K., Vasgam, M., & Manoharan, D. Devops Lifecycle Management And Cloud Migration Assessments: A Security-Driven CICD Perspective.
24. 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.
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. 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
27. 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.
28. 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.
29. 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
30. 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.
31. 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

32. Maturi, S. Y. (2025). Vulnerabilities in the 802.11 Wireless Client Selection Mechanis.

33. 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.

34. Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660

35. 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

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. Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660

38. Maturi, S. Y. Cryptographic Privacy Engines: Practical Multi-Party Protocols For Confidential Database Queries.

39. 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.

40. 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

41. Maturi, S. Y. Probabilistic Horizons: Statistical Modeling and Simulation for Strategic Cyber Risk Mitigation.

42. Mudusu, S. K. (2026, March 26). A data trust scoring framework for reliable and responsible AI systems. InfoWorld (Foundry Expert Contributor Network).

43. Kotte, G. (2025). Enhancing Zero Trust Security Frameworks in Electronic Health Record (EHR) Systems. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283668

44. Mudusu, S. (2025). Health Insurance Fraud Detection: The Role Of Advanced It Systems In Preventing And Identifying Fraud. International Journal, 16(1), 3769-3777

45. Kotte, G. (2025). Revolutionizing Stock Market Trading with Artificial Intelligence. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283647

46. Maturi, S. Y. (2025). Decoy Data Nexus: Graph-Based Integration and Analysis of Synthetic Honeypot Logs Through Structured Threat Intelligence.

47. 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.

48. Mudusu, S. K. (2026, April 15). The secure intelligence framework: Architecting AI systems for a data-driven world. CIO (Foundry Expert Contributor Network).

49. 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

50. Manoharan, D. (2026). AI-Driven Anomaly Detection Models for Preventing Claims Denials and Revenue Leakage in Healthcare. Available at SSRN 6385759.

51. 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.

52. 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.

53. Manoharan, D. (2026). Advancing Healthcare EDI Interoperability Through Informatica Cloud B2B Gateway Quality Engineering. Available at SSRN 6385719.

54. 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

55. 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

56. 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.

57. 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.

58. 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.

59. 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).

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

61. 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.

62. Manoharan, D. (2025). Healthcare EDI Transaction Lifecycles Embedded with a Multi-Layer Verification Framework to Ensure Referential Integrity.

63. Mudusu, S. K. (2025, December 22). Cognitive data architecture: Designing self-optimizing frameworks for scalable AI systems. CIO (Foundry Expert Contributor Network).

64. 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

65. 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.

66. 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.

67. 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).

68. Manoharan, D. (2024). Governance-Oriented Quality Engineering Framework for Healthcare EDI Modernization. International Journal of Multidisciplinary on Science and Management IJMSM, 1(2).

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

70. Mudusu, S. K. (2025, April 20). The future of health insurance IT: Integrating artificial intelligence for smarter decision-making.

71. 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.

72. 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.