

ATM USING EYE CONTACT LENS (IRIS RECOGNISATION)

1.Mrs. A. Rajini Devi, 2.S. Bhavana, 3.K. Shreethisahasra, 4.S. Bhavya Sri, 5.S. Shravani

¹Assistant Professor, Department of Information Technology,
(2,3,4,5)^{B.Tech 2nd Year Students, Department of Information Technology,}

Vignan's Institute of Management and Technology for Women, Hyderabad, Telangana - 501301, India
avularajinidevi@gmail.com, shakaribhavana@gmail.com, kshreethisahasra@gmail.com, somabhavyasri@gmail.com
, suraboinashravani07@gmail.com.

ABSTRACT

In the present digital era, banking systems play a very important role in everyday life. Automated Teller Machines (ATMs) are widely used for cash withdrawal, balance enquiry, fund transfer, and other banking services. Traditional ATM systems mainly depend on ATM cards and Personal Identification Numbers (PINs) for authentication. Although this method is simple, it suffers from many security issues such as card loss, card theft, PIN guessing, skimming attacks, and unauthorized access. To overcome these problems, biometric authentication systems are introduced in ATM technology. Biometrics uses unique biological characteristics of humans for identification and verification. Among different biometric techniques, iris (eye contact lens) recognition is considered highly secure and reliable. An ATM system that uses eye contact lens (iris recognition) provides a multi-level security system, which ensures that only the genuine user can access the bank account. This approach eliminates the need for carrying ATM cards and significantly reduces fraud and identity theft.

1. INTRODUCTION:

In today's rapidly evolving digital era, ensuring secure and reliable authentication methods has become a critical concern in banking systems. Traditional automated teller machine (atm) authentication techniques, such as personal identification numbers (pins) and debit cards, are increasingly vulnerable to security threats including card skimming, phishing, and unauthorized access.

These limitations highlight the urgent need for advanced, user- friendly, and highly secure authentication mechanisms. Biometric authentication has emerged as a promising solution to address these challenges by utilizing unique physiological characteristics of individuals.

Among various biometric technologies, iris recognition stands out due to its high accuracy, stability, and resistance to forgery. The iris, a colored ring surrounding the pupil, possesses intricate patterns that are unique to each individual and remain unchanged throughout life, making it an ideal candidate for identity verification.

This paper proposes an innovative approach to atm security by integrating iris recognition technology with advanced wearable devices, specifically smart contact lenses.

The concept of using eye contact lenses embedded with micro- sensors enhances the convenience and efficiency of the authentication process, enabling seamless and contactless user verification. By capturing and analyzing iris patterns in real time, the system ensures a higher level of security while reducing the dependency on physical cards and memorized pins.

The proposed system aims to revolutionize conventional atm operations by providing a secure, fast,

and user-centric authentication method. Additionally, it addresses key concerns such as identity theft and unauthorized transactions, thereby improving overall trust and reliability in banking services.

2. LITERATURE SURVEY:

The study by Smith and Rao (2022) focuses on the use of iris scanning technology integrated with contact lenses for ATM login systems. Their methodology involves capturing iris patterns through specially designed lenses that enable biometric authentication even in low-light conditions. The major achievement of this system is its ability to provide enhanced security while maintaining functionality in challenging environments. However, the approach has certain limitations, including high implementation costs and issues related to proper lens alignment, which may affect accuracy and user convenience.

Lee et al. (2023) proposed an improved authentication system that combines iris scanning with an additional identification layer using smart lenses. This dual-layer verification significantly enhances security and helps in reducing fraudulent activities. Their system demonstrates better reliability compared to single-factor biometric methods. Despite these advantages, the system is implement and manage in real-world scenarios..

Patel and Singh (2024) introduced an advanced AI-based iris recognition system using smart lenses. Their approach leverages artificial intelligence to improve the speed and accuracy of iris detection and authentication. The system enables fast and secure transactions, making it highly suitable for modern banking applications. However, the method demands high computational power and raises concerns regarding user privacy, as sensitive biometric data is processed and stored.

Kumar et al. (2025) developed a smart lens system equipped with sensors for real-time iris scanning. This system emphasizes user convenience and high security, offering an easy-to-use interface for authentication. The integration of sensors allows continuous and accurate monitoring of iris patterns. Nevertheless, the technology is expensive and not widely available, limiting its adoption in large-scale applications.

3. PROBLEM STATEMENT

In today's digital banking environment, Automated Teller Machines (ATMs) play a vital role in providing convenient financial services such as cash withdrawal, balance inquiry, and fund transfer. However, most ATM systems still depend on traditional authentication methods using ATM cards and Personal Identification Numbers (PINs). These methods are increasingly becoming insecure due to the rise in sophisticated cyber threats and fraudulent activities.

One of the major problem is the risk of card-related fraud, where ATM cards can be lost, stolen, duplicated, or misused. Techniques such as skimming and cloning allow attackers to capture card details without the user's knowledge. Additionally, PIN-based authentication is vulnerable to shoulder surfing, guessing attacks, and hacking, which further increases the chances of

unauthorized access. Another issue is user inconvenience and dependency on memory, as users must remember PINs and carry ATM cards at all times. This can lead to difficulties, especially for elderly or less tech savvy users. Moreover, traditional systems provide only a single layer of security, which is not sufficient in the current threat landscape. Therefore, the core problem is to develop a robust, secure, and efficient ATM authentication system that eliminates the drawbacks of card and PIN-based methods.

4. PROPOSED SYSTEM

The proposed system introduces a secure and advanced ATM authentication mechanism based on iris recognition complex in design and requires sophisticated maintenance, making it difficult to technology, replacing the traditional card and PIN-based methods. The system captures the user's iris image using a camera or smart contact lens and processes it through advanced image processing techniques. The extracted iris features are then compared with stored templates in a secure database for user verification.

Unlike conventional systems, this approach eliminates the need for physical ATM cards and memorized PINs, thereby significantly reducing risks such as card theft, skimming, cloning, and unauthorized access. The system ensures that only genuine users can access banking services due to the uniqueness and stability of iris patterns.

Additionally, the proposed system is designed to be highly accurate, reliable, and efficient, providing real-time authentication and improving the overall user experience. It also supports secure data storage using encryption techniques, ensuring the protection of sensitive biometric information.

5. METHODOLOGY:

Step 1: User Enrollment (Registration Phase)

The user registers by providing basic details.

The system captures the iris image using a camera or sensor. Unique iris features are extracted and converted into a biometric template.

The template is securely stored in the database for future authentication.

Step 2: Image Acquisition

During authentication, the system captures the user's live iris image using a webcam or embedded camera.

Proper alignment and lighting conditions are considered to ensure clarity of the image.

Step 3: Preprocessing

The captured image undergoes preprocessing to improve quality.

Techniques used include:

Noise reduction Image normalization

Contrast enhancement

This step removes unwanted variations and prepares the image for accurate analysis

Step 4: Feature Extraction

The system extracts unique iris patterns using image processing techniques.

These features represent distinct characteristics of the iris and are converted into a digital format.

This ensures high accuracy in identification.

Step 5: Template Matching and Authentication

The extracted features are compared with stored templates
in the database.

A matching algorithm calculates similarity between input and stored data.

If the match is successful → Access Granted If not → Access Denied

Multiple failed attempts may result in temporary blocking for security.

Step 6: Transaction Processing

After successful authentication, the user is allowed to perform ATM operations such as:

Cash withdrawal Deposit

Balance inquiry

The system processes transactions securely and updates the database in real-time.

Step 7: Response Generation

The system generates user-friendly outputs such as:

Authentication status

Transaction success/failure messages

Results are displayed on the interface for user interaction.

6. ALGORITHM:

1. Start

The system begins the authentication process and activates the iris scanning system.

2. Capture Iris Image

The camera captures the user's eye (iris) image for identification.

3. Preprocess Image

The captured image is cleaned and enhanced by removing noise and adjusting brightness/contrast for better clarity.

4. Extract Features

Unique patterns from the iris are identified and converted into a digital format (feature template).

5. Compare with Database

The extracted features are compared with stored iris templates in the database.

6. Access Decision

If the features match → Access Granted If not → Access Denied

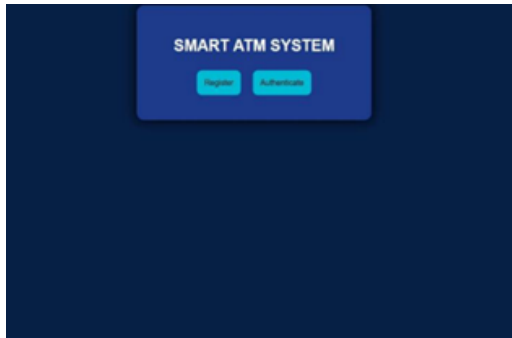
7. Perform Transactions

If access is granted, the user can perform ATM operations like withdrawal or balance check.

8. End

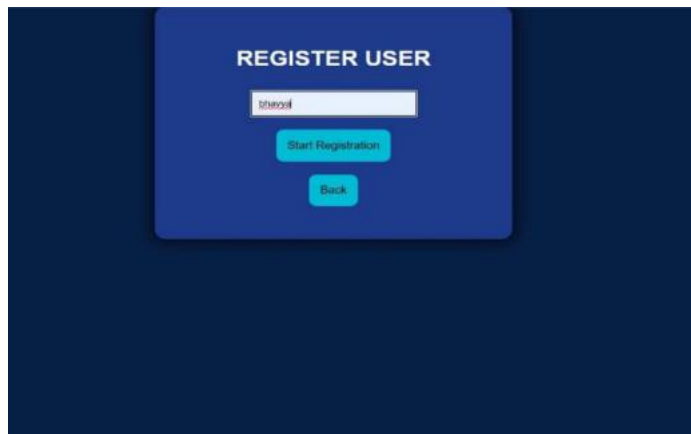
The process completes after authentication and transaction.

7. RESULTS:



Registration Page:

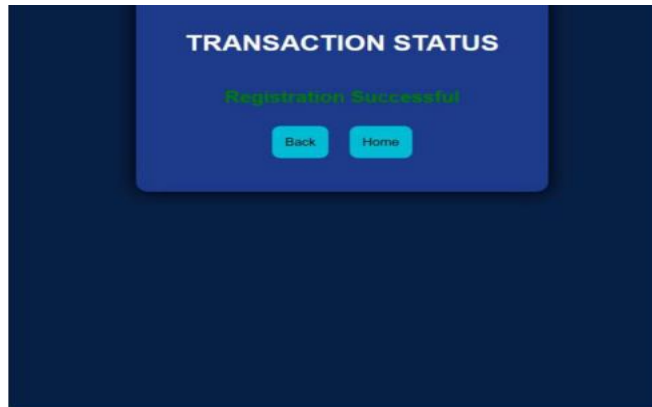
The Registration Page represents the initial step where a new user enrolls into the ATM system using iris recognition. It provides a simple interface for entering basic details such as the username, followed by initiating the registration process. Once started, the system captures the user's iris image through a camera and processes it to extract unique biometric features. These features are then converted into a secure digital template and stored in the database for future authentication. The design ensures ease of use, reduces user errors, and guarantees that only valid and high-quality biometric data is recorded, forming a strong foundation for secure ATM access.



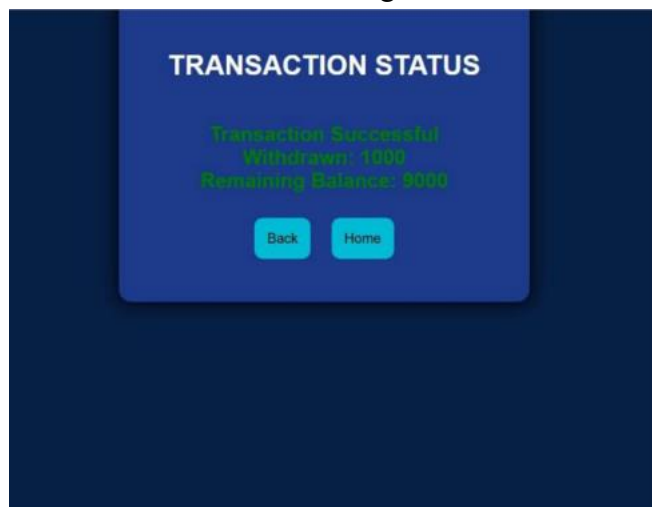
Transaction Status (Registration Successful):

This screen displays the confirmation message after successful registration, indicating that the user's data and iris template have been securely stored. It provides clear feedback such as "Registration Successful," helping users understand that the process has been completed without errors. This improves user confidence and trust in the system, especially since sensitive biometric data is involved. Additionally, navigation options like Back and

Home allow users to move easily within the application, ensuring a smooth and user-friendly experience.



such as balance information or confirmation of an action. It provides clear and concise output to ensure the user understands the result without confusion. The interface emphasizes readability and simplicity while maintaining secure communication between the system and the user. Navigation options like Back and Home improve usability by allowing users to continue further operations or return to the main menu, making the interaction smooth and efficient.

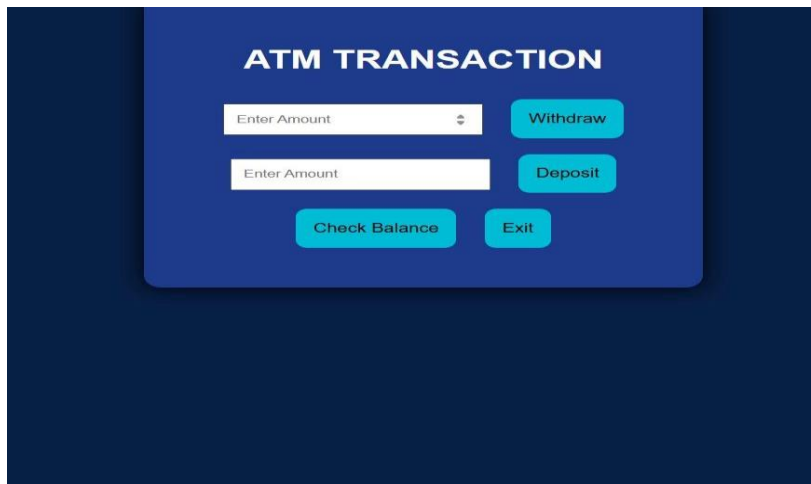


ATM Transaction Screen:

The ATM Transaction screen is the main interface where authenticated users perform banking operations such as withdrawal, deposit, and balance enquiry. It allows users to input the desired amount and choose the corresponding action, making transactions quick and efficient. The system processes these requests securely after verifying the user's identity through iris recognition. The interface is designed to be simple and intuitive, enabling users to easily understand and execute operations. Features like Exit ensure safe termination of the session, enhancing both usability and security.

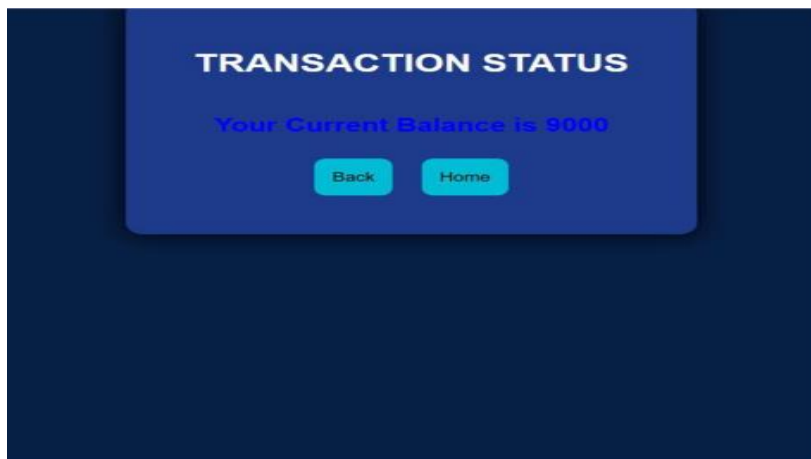
Transaction Successful Screen:

The Transaction Successful screen confirms that a financial operation, such as withdrawal or deposit, has been completed successfully. It displays key details like the amount transacted and the remaining account balance, ensuring transparency and clarity. This immediate feedback reassures users that their transaction has been securely processed. The interface also includes navigation controls for further actions or exiting the system, enhancing user convenience and overall experience while maintaining a high level of security and reliability.



Transaction Status (General Output):

This screen displays the result of a performed transaction,



8. CONCLUSION:

The proposed atm system using iris recognition demonstrates a significant advancement over traditional card and pin-based authentication methods. By leveraging unique and stable iris patterns, the system ensures highly accurate and secure user identification, effectively reducing risks such as card theft, skimming, and unauthorized access. The integration of image processing techniques and biometric verification enhances the reliability and efficiency of atm transactions while eliminating the need for physical cards and memorized passwords. This not only strengthens security but also improves user convenience, making the system more accessible and user-friendly for a wide range of users.

Furthermore, the project highlights the practical implementation of modern technologies such as computer vision, machine learning, and secure database management in real-world banking applications. Despite challenges like cost, hardware requirements, and privacy concerns, continuous advancements in technology are expected to address these limitations. Overall, the system presents a scalable, efficient, and future-ready solution for **secure** banking, emphasizing the potential of biometric authentication to transform ATM security and provide a safer, faster, and more reliable financial transaction experience.

9. FUTURE SCOPE:

The future scope of the proposed ATM system using iris recognition focuses on enhancing security, usability, and system intelligence through advanced technologies. One of the major improvements includes integrating multi-factor authentication along with iris recognition to provide an additional layer of security against unauthorized access. The system can also be extended with cloud-based databases to enable centralized data storage and access across multiple ATM networks, improving scalability and efficiency. Further advancements in artificial intelligence and machine learning can enhance the accuracy and speed of iris recognition, enabling real-time authentication with minimal errors. Additionally, incorporating anti-spoofing techniques such as liveness detection can strengthen the system's ability to distinguish between real users and fraudulent attempts.

Another important direction for future development is improving user interaction and accessibility. The system can be enhanced by adding multilingual support and voice-based interfaces, making it more user-friendly for people from diverse linguistic backgrounds and for visually impaired users. Integration with mobile applications can allow users to perform pre-authentication and manage transactions remotely, reducing waiting time at ATMs. Moreover, features like predictive analytics and AI-based dashboards can help monitor user behavior and detect suspicious activities in advance, improving overall system security and performance. By reducing implementation costs and addressing privacy concerns, the system can be widely adopted in real-world banking environments, making it a practical and next-generation solution for secure financial transactions.

10. REFERENCES:

1. Daugman , J. (2004), *How Iris Recognition Works*, IEEE Transactions on Circuits and Systems.
2. Bowyer, K., Hollingsworth, K., & Flynn, P. (2008), *Image Understanding for Iris Biometrics*, Computer Vision Journal.
3. Jain, A.K., Ross, A., & Prabhakar, S. (2004), *An Introduction to Biometric Recognition*, IEEE Transactions.
4. Divya, C.D., & Rajendra, A.B. (2023), *An Investigation of Iris Recognition Techniques: A*

- Literature Survey*, Journal of Applied Engineering.
5. Farouk, R.H., Mohsen, H., & Abd El-Latif, Y.M. (2022), *A Proposed Biometric Technique for Improving Iris Recognition*, Springer Journal.
 6. Mascarenhas, M. et al. (2020), *ATM Security System using Iris Recognition by Image Processing*, IJERT.
 7. Vincy, A.D., & Sathana, S. (2019), *Recognition Technique for ATM based on Iris Technology*, IJERT.
 8. Fathima et al. (2019), *A Review on Iris Recognition Systems*, IJERT.
 9. Ashraf, I. (2023), *Enhancing ATM Security System using Iris Recognition*, American Journal of Geospatial Technology.
 10. Koteswari, S. et al. (2016), *Fusion of Iris and Fingerprint Biometric Identifier for ATM Services*, International Journal of Communications.
 11. Minaee, S. et al. (2015), *Iris Recognition Using Scattering Transform and Textural Features*, IEEE Research.
 12. Todupunuri, A. (2025). IMPROVING CUSTOMER EXPERIENCE WITH MODERN BANKING SOLUTIONS. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.5120615>
 13. Babburi, S. (2024). Explainable AI Framework for Policy-Compliant Anomaly Detection in Data Pipelines.
 14. Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
 15. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
 16. Poojari, R. INTELLIGENT SYSTEMS+B108 AND APPLICATIONS IN ENGINEERING.
 17. 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.
 18. 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](https://doi.org/10.64751/ajaccm.2026.v6.n1(2).pp1-8)
 19. 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.
 20. 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>
 21. 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>
 22. Viswanathan, V. (2024). Pioneering Ethical AI Integration in Enterprise Workflows: A

Framework for Scalable Team Governance. Available at SSRN 5375619.

23. 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).
24. Viswanathan, V. (2025). Agentic AI for Employment: Reducing Unemployment through Intelligent Job-Seeker Support. *LEX LOCALIS–Journal of Local Self-Government*.
25. Mudusu, S. K. (2026, February 9). AI-augmented data quality engineering. *InfoWorld (Foundry Expert Contributor Network)*.
26. 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.
27. 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.
28. 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.
29. 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.
30. DEVARASETTY, N. (2023). SCALABLE DATA ENGINEERING APPROACHES FOR AI-DRIVEN INDUSTRIAL IOT APPLICATIONS. *INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH AND MANAGEMENT*, 11(06), 954-968.
31. 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.
32. 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).
33. 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.
34. 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*.
35. 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).

36. Ravishankara, M. (2026, February). CircuChain: Disentangling Competence and Compliance in LLM Circuit Analysis. In SoutheastCon 2026 (pp. 1-7). IEEE.
37. Sruthi, M. V., Sree, V. U., & Soundararajan, K. (2012). Specific removal of motion artifacts in medical image processing. IJECCE, 3(3), 227-229.