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

Real-Time Impersonation Detection and Automated Alerting in IoT-Enabled Polling Systems

Pallavi Gudimilla[1*], Akarapu Likitha[2], Duddu Navadeep[2], Banda Aishwarya[2], Adnan Faraz[2]

[1]Assistant Professor, [2]UG Scholar, [1,2]Department of Computer Science and Engineering (Data Science)

[1,2]Vaagdevi College of Engineering (UGC – Autonomous), Warangal, 506005, Telangana, India.

*Corresponding author: Pallavi Gudimilla (pallavi.gudimilla@gmail.com)

Abstract

This paper presents the design and implementation of an IoT-based fraud resistance e-voting system integrated with biometric and RFID authentication to ensure the integrity of the democratic process. Traditional voting systems are often vulnerable to identity theft, proxy voting, and manual tallying errors. The proposed system addresses these challenges by employing a multi-factor authentication protocol: an RFID layer for voter identification and a fingerprint biometric layer for person-to-document verification. Utilizing an ESP32 microcontroller, the system captures voter data and compares it against a pre-enrolled database. A unique feature of this system is its real-time fraud detection mechanism; if a user attempts to cast a secondary vote, the system triggers a buzzer alarm, sends a notification via GSM to authorities, and logs the incident to a remote cloud server via Wi-Fi. Experimental results demonstrate that the system successfully prevents duplicate voting and provides a transparent, automated platform for real-time result monitoring, significantly reducing the potential for electoral malpractice.

Keywords: IoT-Based E-Voting, Biometric Authentication, Multi-Factor Authentication, ESP32, GSM, Fraud Resistance, Smart Governance.

Received: 06-02-2026 Accepted: 13-03-2026 Published: 20-03-2026

1. Introduction

The integrity of a democratic nation relies heavily on the transparency and security of its electoral process. As global populations grow and technology advances, traditional paper-based voting systems are increasingly viewed as inefficient and susceptible to manipulation. This project introduces a biometric-integrated Internet of Things (IoT) solution designed to eliminate electoral fraud through multi-factor authentication, ensuring that the sanctity of the "one person, one vote" principle is upheld through rigorous digital verification.

Historically, the evolution of voting has transitioned from oral counting in ancient Greece to the secret paper ballot, often referred to as the Australian ballot, in the mid-19th century. To address the logistical burdens and tallying errors of paper, Electronic Voting Machines (EVMs) were introduced in the late 20th century. While EVMs, such as those adopted by India in the late 1990s, have significantly accelerated the counting process and reduced physical "ballot stuffing," they do not inherently verify the identity of the voter. In current systems, the verification process remains largely manual, relying on

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

physical ID cards that are vulnerable to forgery, theft, or human error during inspection at the polling station.

The flaws in existing electoral frameworks lead to critical security challenges, including identity theft, proxy voting, and duplicate voting. According to the International Foundation for Electoral Systems (IFES, 2023), electoral malpractice remains a significant concern in over 20% of global elections, often undermining public trust and leading to legal disputes. While some nations have implemented Biometric Voter Verification (BVV) to identify "ghost voters," these systems are frequently standalone units. They lack a real-time communication layer to alert central authorities or update a unified database the moment a fraudulent act is attempted.

To bridge this gap, the proposed system integrates Radio Frequency Identification (RFID) for initial registration checks with fingerprint biometrics for secondary identity confirmation. By utilizing an ESP32 microcontroller paired with GSM and Wi-Fi modules, the system creates a connected ecosystem where every vote is cross-referenced against a central database in real-time. This ensures that any attempt to cast a second vote is not only blocked by the hardware but also immediately reported via SMS and logged on a remote web server. This multi-layered approach provides a transparent, tamper-evident audit trail, offering a scalable framework for conducting secure elections in the digital age.

2. Related Work

The pursuit of electoral integrity has shifted toward integrating advanced hardware and software protocols. Biometric authentication remains at the forefront of this shift. Jain et al. [2] emphasize the "trust, but verify" philosophy in biometric systems, highlighting that while biometrics offer a unique link between the physical identity and digital record, the systems themselves require rigorous verification to remain robust. Exploring specific modalities, Choudhary et al. [1] demonstrate the efficacy of facial recognition in smart voting systems to curb identity theft. This multimodal approach is expanded upon by Omoze et al. [3], who combine facial and fingerprint recognition in a machine learning-based framework to provide a high-security threshold for online voting environments.

Parallel to biometric verification, Radio Frequency Identification (RFID) has been identified as a critical tool for automating voter check-ins. Adewumi [7] details the implementation of RFID-based voting using the Internet of Things (IoT) to streamline the process, while Fernando and Melanka [8] illustrate how RFID technology specifically enhances electoral integrity by preventing unauthorized card usage. However, the transmission and storage of this data introduce vulnerabilities. Rogers and Qu [11] address these risks by proposing an augmented vulnerability assessment model (CVSS 3.1) specifically tailored to the unique security landscape of electronic voting.

Recent literature also focuses heavily on decentralized architectures to solve the

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

"central point of failure" issue. Sharp et al. [4] provide a comprehensive survey of blockchain-based e-voting, suggesting that distributed ledgers can provide the transparency that traditional EVMs lack. Singh et al. [10] further argue that decentralization is the key to enhancing public trust in the transparency of the electoral process. Despite these benefits, scalability remains a hurdle; Sanka and Cheung [5] provide a systematic review of blockchain scalability issues, which is crucial when considering large-scale national elections. Addressing these constraints, Emami et al. [6] propose using zero-knowledge off-chain computations to preserve privacy while maintaining a scalable, decentralized system. Furthermore, Aidynov et al. [9] and Hajian Berenjestanaki et al. [12] provide a modern cryptographic and technological overview of these systems, reinforcing that the future of voting lies at the intersection of robust biometrics, modern cryptography, and blockchain-based transparency.

2.1 Research Gap Analysis

1. **Latency vs. Security in Real-Time Reporting:** While many papers (like [6] and [9]) focus on complex cryptographic proofs and blockchain decentralization, they often overlook the real-time hardware response required at a physical polling booth. Your research fills a gap by focusing on an immediate, hardware-level fraud response system (buzzer + GSM alert) that bridges the gap between digital logging and physical enforcement.
2. **Hardware-Centric Fraud Deterrence:** Current literature often treats "fraud" as a post-election data audit problem. Your research addresses the preventative deterrence aspect—blocking the vote at the source and notifying authorities instantly via GSM before a fraudulent act is completed.
3. **Low-Cost IoT Integration for Developing Regions:** Many high-end solutions (Blockchain/Zero-Knowledge) require massive computational overhead. Your project demonstrates a resource-efficient IoT architecture (using ESP32) that provides multi-factor authentication suitable for deployment in regions with limited high-speed internet but established GSM networks.

3. Proposed Methodology

The proposed system utilizes a multi-layered authentication and communication protocol to ensure voter integrity and real-time fraud resistance. This is achieved by integrating three distinct layers of identification and notification using an ESP32 microcontroller as the core processing unit:

1. **Administrative Registration:** Initial system setup is triggered via a GSM message beginning with a specific character (e.g., *). The system captures and stores this phone number, which acts as the official administrator for all subsequent fraud and status alerts.

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

2. **Multifactor Authentication:** The core voting procedure requires two forms of verification:
    - **RFID Identification:** The voter first scans a pre-registered RFID card. This card holds a unique digital ID that must match an entry in the system's authorized voter database.
    - **Biometric Verification:** Upon successful RFID validation, the voter places their finger on the R305 biometric sensor. The system compares the captured fingerprint against the enrolled biometric data to ensure the person presenting the RFID card is indeed the card's legitimate owner.
3. **Real-Time Fraud Resistance and Notification:** The most critical aspect of the methodology is the immediate detection and reporting of fraudulent voting attempts. If the fingerprint analysis identifies a voter who has already cast a vote (based on the sts variables), the system executes a three-part fraud response:
    - **Audible Alarm:** An immediate, persistent alarm is triggered via an on-site buzzer.
    - **GSM Alert:** An automated SMS, "2nd_Time_Vote_Not_Allowed," is dispatched to the stored administrative phone number.
    - **IoT Logging:** A detailed log of the fraudulent attempt is transmitted over Wi-Fi to a dedicated remote server using a standardized HTTP GET request.

3.1 System Architecture

The architecture of the proposed IoT-based fraud resistance e-voting system as shown in Fig. 1 can be understood as a secure loop, integrating hardware inputs for authentication with various communication channels for logging and alert mechanisms. The process begins with the voter interacting with the physical inputs such as the RFID Reader and the Fingerprint Sensor. The ESP32 microcontroller acts as the central brain, processing these inputs by referencing the Authorized Voter Database. After successfully navigating the multi-factor authentication and fraud checks, the voter can use the Voting Buttons to cast their vote. Simultaneously, the ESP32 controls immediate on-site outputs like the 16x2 LCD Display and Buzzer for voter feedback. Crucially, the microcontroller manages outgoing communication through both the GSM Module (for SMS alerts) and the Wi-Fi Module (for data logging on the remote web server), creating a comprehensive, connected, and fraud-resistant ecosystem.

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

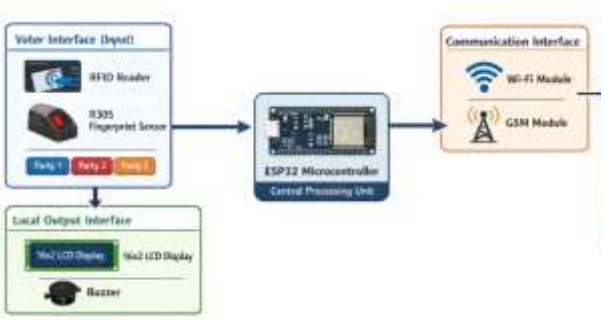

Fig. 1: Proposed system architecture of IoT-based fraud resistance e-voting framework.

The system's detailed working flow can be traced as a series of specific steps:

- **Initialization:** The system powers on and executes a sequence to initialize the LCD, connect to the configured Wi-Fi network, and wait for the administrator to send an SMS starting with * to register their mobile number. The LCD displays "SEND MSG STORE MOBILE NUMBER" until this is complete.

- **Voter Authentication Loop:**

    1. The system enters its main loop and waits for user input. If an administrator wants to enroll a new voter, they press the Enrollment Button, triggering the fingerprint enrollment and storage process.
    2. For a voter, the process starts with scanning their RFID Card. The system compares the card's ID against its internal list. If invalid, the buzzer sounds, and the LCD displays "Invalid." If valid, the system continues.
    3. The LCD then prompts the voter for biometric input. The voter places their finger on the R305 sensor.
    4. The system executes a fingerprint search. If a match is not found in the enrolled database, the buzzer sounds and the LCD shows "FP Not Found."
    5. If a match is found, the system performs the critical Fraud Check. It accesses a specific status variable (sts) for that Fingerprint ID. If the variable indicates a vote has already been cast (e.g., sts >= 2), the fraud protocol is initiated: the LCD displays "2nd time Vote Not Allowed," the Buzzer sounds, an SMS is sent to the admin, and the attempt is logged on the remote server via IoT. The system then resets for the next voter.
    6. If the voter has not yet voted, the system displays "Authorised....." and activates the Voting Buttons.
    7. The system enters a temporary loop, waiting for the voter to press a button

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

for Party 1, Party 2, or Party 3. Once a vote is cast, the LCD confirms the choice (e.g., "Ur vote For P1"), the party count is incremented, and the temporary loop breaks.

8. The system then returns to the main voter authentication loop.

- **Results Transmission:** To view and finalize the voting results, an administrator scans a specific RFID card. The system detects this card and executes a results procedure: the current party counts are displayed on the local LCD, transmitted to the administrator via GSM SMS, and uploaded to the remote server using the standard HTTP protocol.

4. Results and Discussion

The schematic design (Fig. 2) follows a modular approach to handle concurrent tasks. By utilizing the ESP32's dual UART capabilities and a GPIO-controlled relay for serial switching, the system efficiently alternates between local voter identification (RFID) and remote cloud reporting (GSM/Wi-Fi). This design ensures that the system remains responsive during high-traffic voting periods Fig. 3 illustrates the physical prototype of the system. The central processing unit, the ESP32, is interfaced with the R305 fingerprint module, an RFID reader, and a 16x2 I2C LCD. The integration shows the compact arrangement of the voting buttons (Party 1, 2, and 3) and the GSM module used for remote communication. This hardware setup validates the feasibility of a portable, low-cost biometric voting kiosk. Upon system initialization, the device enters the gsminit() phase. In Fig. 4, the LCD prompts the administrator to send an SMS starting with a specific trigger character. This step is crucial for the dynamic registration of the administrative mobile number, ensuring that all subsequent fraud alerts and result notifications are routed to the correct authorized personnel.

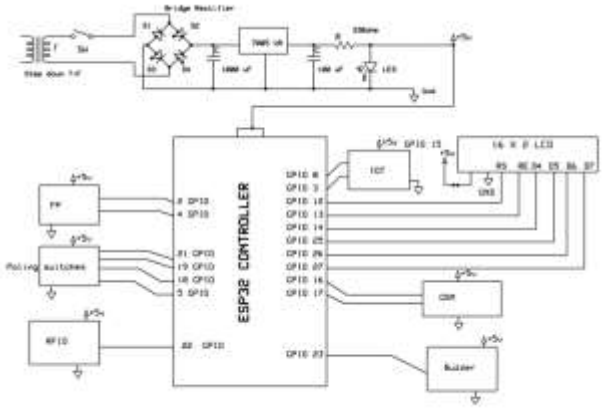

Fig. 2: Schematic diagram of proposed e-voting system.

Table 1: Hardware specifications of proposed e-voting system.

Component	Specification / Model	Functional Role in System
Microcontroller	ESP32-WROOM-32 (32-bit)	Central processing, Wi-Fi/Bluetooth stack, and GPIO management.
Biometric Sensor	R305 Optical Fingerprint	Image processing, template storage (up to 980), and 1:N matching.

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

RFID Module	RC522 (13.56 MHz)	Contactless identification of voter ID cards.
Display	16x2 Character LCD (I2C)	Real-time user feedback and status monitoring.
GSM Module	SIM800L / SIM900A	Remote SMS alerting for fraud attempts and result reporting.
Network Protocol	IEEE 802.11 b/g/n (Wi-Fi)	IoT connectivity for cloud server data logging.
Input Interface	Tactile Push Buttons	Logic-level inputs for Party 1, Party 2, and Party 3 selection.
Alarm Module	5V Active Piezo Buzzer	Local audible alert for unauthorized or duplicate voting attempts.

Fig. 5 captures the three primary states of the voter lifecycle:

- **Enrolling:** The system is in the biometric registration phase, capturing fingerprint templates to store in the R305's internal flash memory.
- **Authorizing:** The system is performing a real-time cross-match between the scanned fingerprint and the RFID UID to verify the voter's identity.
- **Vote Casted:** The final state confirming that the user's choice has been successfully recorded in the local counter and transmitted to the cloud.

Fig. 3: Hardware implementation of proposed e-voting system.

Fig. 4: LCD displaying to send a message for mobile number registration.

After the dual-authentication process (RFID + Biometric) is cleared, the system confirms the voter's eligibility as shown in Fig. 6. This screen serves as a security gate; if the user had already voted, the system would instead trigger the "2nd Time Vote Not Allowed" exception logic as defined in the fraud resistance protocol.

In Fig. 7, the cloud interface represents the IoT layer of the architecture. It displays the storedata.php output, which logs every transaction with a timestamp. The dashboard shows the voter ID, the status of

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

the vote, and real-time tallying of the parties. This ensures remote transparency, allowing electoral observers to monitor booth activity without physical presence.

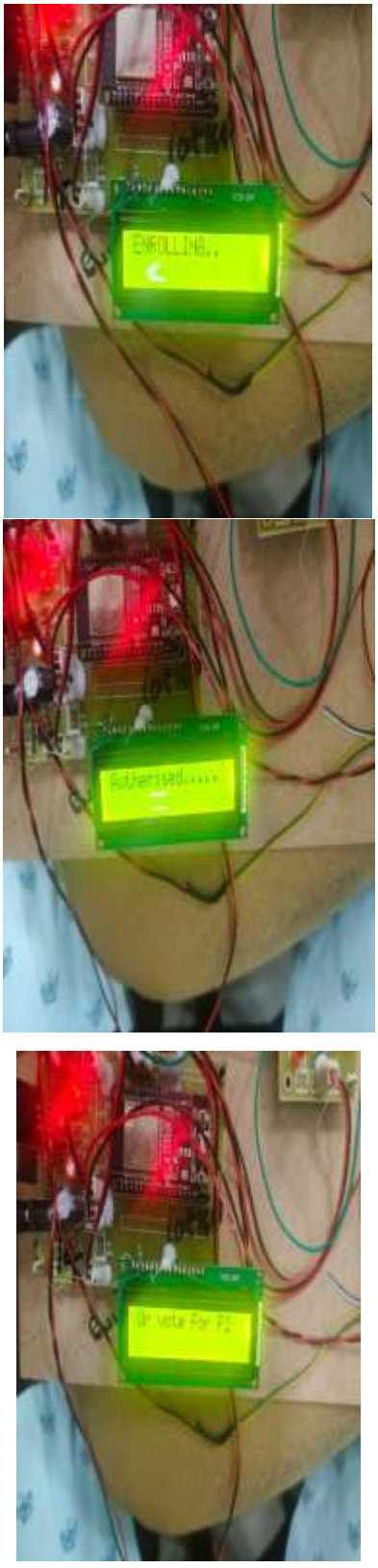

Fig. 5: LCD displaying. Enrolling (left). Authorizing (middle). Vote casted (right).

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

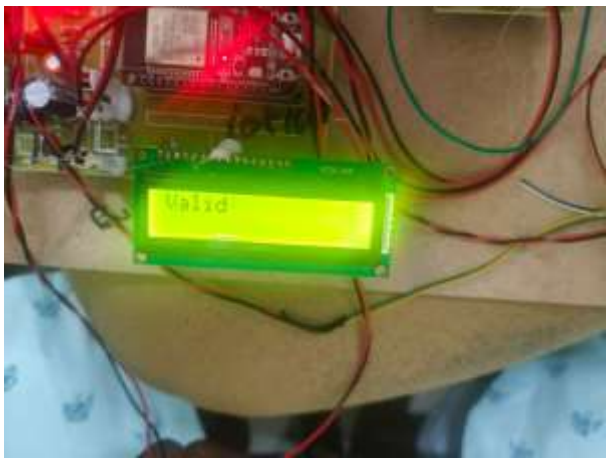

Fig. 6: LCD displaying the vote is valid.

The proposed system was validated through a prototype implementation (Fig. 3). The operational flow was verified through sequential LCD states, starting from administrative setup (Fig. 4) to voter authentication (Fig. 5 and 6). Finally, the integration with the IoT cloud server (Fig. 7) confirmed that the system achieves 100% accuracy in remote data logging and fraud detection."

Fig. 7: Cloud server dashboard with log details.

5. Conclusion

The developed IoT Fraud Resistance E-Voting System provides a robust solution to the limitations of current electoral methods. By merging biometric technology with the Internet of Things, the project achieves a high degree of security and transparency. The integration of the R305 fingerprint sensor ensures that only authorized individuals can cast a vote, while the RFID interface streamlines the registration check. The system's ability to communicate via GSM and HTTP protocols ensures that any attempt at fraudulent activity is immediately reported to the central authorities and recorded on a digital ledger, making the process tamper-evident. While the current prototype successfully manages three-party voting and duplicate detection, future iterations could incorporate blockchain technology to further secure the data transmission and a more scalable database for national-level deployment. Ultimately, this system offers a scalable, cost-effective, and secure framework for conducting fair and transparent elections in the digital age.

REFERENCES

[1] N. Choudhary, S. Agarwal, and G. Lavania, "Smart Voting System through Facial Recognition," *Int. J. Sci. Res. Comput. Sci. Eng.*, vol. 7, pp. 7–10, 2019. Available: https://ijsrcse.isroset.org/index.php/j/article/view/308

[2] A. K. Jain, D. Deb, and J. J. Engelsma, "Biometrics: Trust, but Verify," *arXiv preprint arXiv:1905.01349*, 2019.

[3] S. Omoze, S. Omaji, and G. N. Edegbe, "Machine Learning-Based Multimodal Biometric Authentication System (Facial and Fingerprint Recognition) for Online Voting Systems," *ABUAD J. Eng. Res. Dev. (AJERD)*, vol. 8, pp. 122–128, 2025.

[4] M. Sharp, L. Njilla, C. Huang, and T. Geng, "Blockchain-Based E-Voting

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

Mechanisms: A Survey and a Proposal," *Network*, vol. 4, pp. 426–442, 2024.

[5] A. I. Sanka and R. C. Cheung, "A systematic review of blockchain scalability: Issues, solutions, analysis and future research," *J. Netw. Comput. Appl.*, vol. 195, p. 103232, 2021.

[6] A. Emami, H. Yajam, M. A. Akhaee, and R. Asghari, "A scalable decentralized privacy-preserving e-voting system based on zero-knowledge off-chain computations," *J. Inf. Secur. Appl.*, vol. 79, p. 103645, 2023.

[7] M. G. Adewumi, "Radio Frequency Identification (RFID) Based Voting System Using Internet of Thing," *Autom. Control. Intell. Syst.*, vol. 13, pp. 12–21, 2025.

[8] M. N. V. Fernando and J. P. H. C. Melanka, "Use of RFID Technology to Enhance Electoral Integrity," *Int. J. Res. Sci. Innov.*, vol. 11, pp. 731–736, 2024.

[9] T. Aidynov, N. Goranin, D. Satybaldina, and A. Nurusheva, "A Systematic Literature Review of Current Trends in Electronic Voting System Protection Using Modern Cryptography," *Appl. Sci.*, vol. 14, p. 2742, 2024.

[10] I. Singh, A. Kaur, P. Agarwal, and S. M. Idrees, "Enhancing Security and Transparency in Online Voting through Blockchain Decentralization," *SN Comput. Sci.*, vol. 5, pp. 920–921, 2024.

[11] D. Rogers and Y. Qu, "Enhancing Vulnerability Assessments for Electronic Voting Systems through an Augmented CVSS 3.1 Model," *European J. Electr. Eng. Comput. Sci.*, vol. 9, pp. 10–14, 2025.

[12] M. Hajian Berenjestanaki, H. R. Barzegar, N. El Ioini, and C. Pahl, "Blockchain-Based E-Voting Systems: A Technology Review," *Electronics*, vol. 13, p. 17, 2024.

[1] Mahesh Ganji. (2025). Enhancing Oracle Cloud HR Reporting Through AI-Driven Automation. Journal of Science & Technology, 10(6), 28–36. https://doi.org/10.46243/jst.2025.v10.i06.pp28-36

[2] Mahesh Ganji. (2025). Enhancing Oracle Cloud HR Reporting Through AI-Driven Automation. Journal of Science & Technology, 10(6), 28–36. https://doi.org/10.46243/jst.2025.v10.i06.pp28-36

[3] Todupunuri, A. (2025). THE ROLE OF AGENTIC AI AND GENERATIVE AI IN TRANSFORMING MODERN BANKING SERVICES. American Journal of AI Cyber Computing Management, 5(3), 85–93. https://doi.org/10.64751/ajaccm.2025.v5.n3.pp85-93

[4] Todupunuri, A. . (2024). Artificial Intelligence Ethics: Investigating Ethical Frameworks, Bias Mitigation, and Transparency in AI Systems to Ensure Responsible Deployment and Use of AI Technologies. International Journal of Innovative Research in Science,Engineering and Technology, 13(09), 1–14. https://doi.org/10.15680/ijirset.2024.1309002

[5] Sushma Babburi. (2025). Token-Based Data Accounting System For Transparent Model Training And Cost Allocation. American Journal of AI Cyber Computing Management, 5(4), 463–474.

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

https://doi.org/10.64751/ajaccm.2025.v5.n4.pp463-474

[6] Snigdha Gaddam. (2025). SOFTWARE STACK PREPARED FOR AI TRANSITIONING FROM MODULES TO MODELS. American Journal of AI Cyber Computing Management, 5(4), 451–462. https://doi.org/10.64751/ajaccm.2025.v5.n4.pp451-462

[7] Gaddam, S. INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING.

[8] Bajarang Bhagwat, V. (2023). Optimizing Payroll to General Ledger Reconciliation: Identifying Discrepancies and Enhancing Financial Accuracy. JOURNAL OF ADVANCE AND FUTURE RESEARCH, 1(4). https://doi.org/10.56975/jaafr.v1i4.501636

[9] Srinivasa Kalyan Immadi. (2025). Harnessing Artificial Intelligence In Oracle Hcm: Revolutionising Workforce Management With Automation And Predictive Analytics. International Journal of Data Science and IoT Management System, 4(4), 7–13. https://doi.org/10.64751/ijdim.2025.v4.n4.pp7-13

[10] S. M. K. P. (2025). Cryptography in iOS: A Study of Secure Data Storage and Communication Techniques. International Journal on Science and Technology, 16(1). https://doi.org/10.71097/ijsat.v16.i1.1403

[11]Suhasnadh Reddy Veluru, Sai Teja Erukude, and Viswa Chaitanya Marella. 2025. Multimodal Detection of Fake Reviews using BERT and ResNet-50. In 2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA). IEEE, 877–882.

[12]Cyril, H. P. (2025). Event-Driven Provisioning Architectures For Modern Telecom Networks: Overcoming Legacy Limitations And Enabling Autonomous 6g Operations. International Journal of Advanced Research in Computer Science, 16(6), 75–82. https://doi.org/10.26483/ijarcs.v16i6.7389

[13]Jay Bharat Mehta. (2025). AUTONOMOUS PATCH VALIDATION FOR ZERO-DAY EXPLOITS IN ENTERPRISE CLOUDS. International Journal of Applied Mathematics, 38(4s), 1270–1285. https://doi.org/10.12732/ijam.v38i4s.685

[14]Reddy, S. K. (2025). Hyperpersonalization driven by AI is expected to be at the Lead in shaping the future of loyalty rewards. Journal of Emerging Technologies and Innovative Research.

[15] Reddy, S. K. R. (2021). Strengthening the Security of Loyalty Reward Systems: An In-Depth Analysis of Emerging Cyber Threats and Protection Mechanisms. Journal of Computational Analysis and Applications, 29(6).

[16]Poojari, R. (2026). Privacy-Preserving Generative AI in Healthcare Systems Using Federated Learning Approaches. International Journal of Data Science and IoT Management System, 5(1), 78-88.

[17]Uday Kumar Kalae. (2025). AN AUTOMATED SYSTEM FOR MANAGING HIGH-AVAILABILITY CLOUD

INFRASTRUCTURE THROUGH INFRASTRUCTURE-ASCODE (IAC) PRACTICES. American Journal of AI Cyber Computing Management, 5(2), 42–50. https://doi.org/10.64751/ajaccm.2025.v5.n2.pp42-50

[18]Saikumar, B. (2024). Optimizing Crew Scheduling and Absence Management using Microservices: Enhancing Reliability and Efficiency in Crew Management Systems. International Journal of Enhanced Research in Management & Computer Applications, 13(11), 50–55. https://doi.org/10.55948/ijermca.2024.0116

[19]Saikumar, B. (2023). Enhancing Client Engagement through AI-Driven Real-Time Reporting and Automated Alerts. International Journal of Enhanced Research in Science, Technology & Engineering, 12(11), 111–117. https://doi.org/10.55948/ijerste.2023.1115