AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
E-ISSN:3069-0102
VOL.5, NO. 4(2)(2025)

INTELLIGENT TRANSACTION TAG FOR FACILITATING SUBSISTENCE-LEVEL FINANCIAL OPERATIONS

[1] M.Jyothi,[2] K.Aravind Reddy,[3] K.Sindhuja,[4] B.V.R.Sai Gangeya, [5] N.Ravindar

[1,2,3,4] *B. Tech Students, Department of Electronics and Communication Engineering, Samskruti College of Engineering and Technology, Hyderabad 501301*

[5] *Department of Electronics and Communication Engineering, Samskruti College of Engineering and Technology, Hyderabad 501301, Email: nravindar89@ gmail.com*

ABSTRACT

This project focuses on developing a smart tag system that enables secure, quick, and reliable financial transactions for livelihood-based activities. The system is particularly useful in rural and underbanked regions where access to digital banking infrastructure is limited. The prototype incorporates key hardware components such as an Arduino microcontroller to control the system, a 4x4 matrix keypad for entering the transaction amount, an EM18 RFID reader for card-based user identification, a fingerprint sensor for biometric authentication, an LCD display for presenting transaction-related details to the user, and a buzzer to provide audio feedback. The proposed system enables authenticated users to initiate bank-related transactions through biometric and card-based inputs, ensuring secure identity verification. The goal is to make digital banking accessible, secure, and user-friendly for daily livelihood transactions such as local market purchases, small-scale business payments, and peer-to-peer transfers.

Keywords: Smart Tag, Secure Transaction, Biometric Authentication, EM18 RFID, Rural Banking, Arduino, Livelihood Activities.

I. INTRODUCTION

In today's rapidly evolving digital landscape, the need for inclusive, secure, and efficient financial systems has never been more critical, particularly for underserved rural and semi-urban populations. Although banking infrastructure and digital payment technologies have expanded significantly in urban areas, a large segment of the population remains excluded from formal financial services due to limited technological literacy, insufficient infrastructure, and persistent concerns regarding data privacy and security [6], [10]. Traditional cash-based transactions dominate livelihood activities such as small-scale trading, local market exchanges, and peer-to-peer payments, often leading to inefficiencies, lack of transparency, and financial vulnerability. This gap in financial inclusion highlights the necessity for alternative transaction mechanisms that are both accessible and secure. The project titled "Smart Tag That Enables the Bank Payment or Transaction for Livelihood Activities" is designed to address these challenges by leveraging RFID and IoT-enabled payment technologies [1], [5].

The proposed smart tag concept offers a practical and cost-effective solution for rural users who have limited or no access to smartphones, stable internet connectivity, or conventional banking platforms. RFID-based systems are widely recognized for their simplicity, low power consumption, and suitability for contactless transactions in resource-constrained environments [1], [4]. By eliminating dependency on internet-based applications, the system enables secure offline transactions while maintaining reliability and ease of use. Furthermore, the incorporation of lightweight cryptographic mechanisms and authentication protocols enhances transaction security and privacy, mitigating risks such as data interception, cloning, and unauthorized access [2], [3], [7], [9]. The integration of biometric and card-based identity verification further strengthens user authentication, ensuring that financial transactions are executed only by legitimate users.

Beyond personal banking, the Smart Tag system has significant potential for broader socio-economic applications. It can be effectively deployed in government welfare disbursement programs, cooperative society payments, agricultural procurement systems, and other livelihood-oriented financial activities that involve frequent low-value transactions [6], [10]. By bridging the gap between traditional cash-based practices and modern digital banking frameworks, the proposed system promotes transparency, accountability, and financial empowerment. Ultimately, this approach demonstrates that secure, scalable, and inclusive banking solutions can be delivered to underbanked communities, regardless of geographic location, literacy level, or economic status, thereby contributing meaningfully to sustainable financial inclusion and rural development.

II. LITERATURE SURVEY

The integration of RFID technology with biometric authentication has been widely explored to improve the security of digital payment systems, particularly in environments where unauthorized access and identity fraud pose serious concerns. Rajkumar [1] demonstrated that combining EM18 RFID cards with fingerprint-based authentication significantly reduces fraud and transactional errors in public utility payments. The dual-layer verification mechanism ensures that RFID-based identification is complemented by biometric confirmation, making the system highly reliable. This approach directly supports the smart tag design, where strong user identity verification is essential to prevent misuse in rural banking and livelihood-based transaction environments.

Focusing specifically on rural users, Natarajan [2] presented a biometric-enabled payment authentication framework built on low-cost microcontrollers and fingerprint sensors. The study highlighted the importance of simplicity, affordability, and ease of use for populations with limited digital literacy. Field evaluations revealed high acceptance rates among rural users due to the intuitive nature of fingerprint verification. These findings validate the smart tag concept by emphasizing the need for user-friendly, minimal-training systems capable of operating in low-infrastructure settings.

To further enhance transaction security, Thomas [3] introduced a multi-modal authentication model that integrates RFID, biometric verification, and PIN-based input. The research addressed increasing identity theft risks in underserved areas and demonstrated how embedded systems can efficiently handle multi-factor authentication without relying on complex backend infrastructures. This work strongly aligns with the smart tag architecture, which employs an RFID reader, fingerprint scanner, and keypad to establish a secure and structured transaction workflow for each user.

From the perspective of local commerce, Mukherjee [4] proposed a smart card-based transaction system tailored for small businesses and local vendors. The system enabled cashless payments using card identification while providing immediate user feedback through LCD displays and buzzers. The study also evaluated microcontroller performance in securely handling transaction data. These conclusions directly support the smart tag model, particularly in terms of local usability, real-time transaction confirmation, and effective user notification mechanisms.

Ramanathan [5] focused on RFID-integrated microcontroller systems designed for standalone cashless transactions in offline and semi-online environments. The study examined tag-reading accuracy, data validation, and security protocols suitable for regions with limited connectivity. The results confirm the feasibility of deploying RFID-based payment units in remote areas, reinforcing the practicality of the smart tag system for livelihood transactions where internet access is unreliable or unavailable.

In addition to security and functionality, usability remains a critical factor in embedded transaction systems. Patil [6] emphasized the importance of accessible human–machine interfaces, particularly for elderly and semi-literate users. The study recommended incorporating buzzers, visual indicators, tactile keypads, and modular hardware designs to improve interaction quality and reduce user errors. These insights enhance the smart tag's design by ensuring that users in non-urban environments can operate the system confidently and securely, even with minimal technical familiarity.

III. EXISTING SYSTEM

Current subsistence-level financial transactions in rural and low-income communities predominantly rely on manual, cash-based processes with minimal integration of digital technologies. Individuals often depend on physical identification cards, handwritten registers, and local intermediaries such as shopkeepers, microfinance agents, or community coordinators to authenticate transactions and access financial services. These approaches lack automated validation, secure identity binding, and real-time verification mechanisms, making them highly susceptible to fraud, misreporting, and transaction delays [1], [4].

Although several digital alternatives—including mobile payment platforms, biometric authentication systems, and RFID- or smart card–based transaction mechanisms—have been introduced, their adoption in rural environments remains limited. Studies have shown that unreliable internet connectivity, low penetration of smart devices, and insufficient digital literacy significantly restrict the usability of these systems in subsistence-level contexts [2], [5]. Furthermore, many existing solutions operate as isolated components, addressing either identity verification or transaction processing, but not both in an integrated and lightweight manner [3].

As a consequence, the current financial ecosystem offers only fragmented support for livelihood-oriented transactions. Users are often required to manage multiple cards or devices, rely on manual validation processes, and depend heavily on human intermediaries for transaction authorization and record keeping [6]. This fragmented approach not only increases operational inefficiencies but also undermines transparency, accountability, and user trust, particularly among vulnerable populations that require simple, secure, and reliable financial transaction mechanisms.

IV. PROPOSED SYSTEM

The proposed system introduces an Intelligent Transaction Tag (ITT) that integrates identity authentication, secure micro-payment processing, and real-time transaction logging into a single compact device. The ITT uses embedded NFC/RFID, low-power microcontrollers, on-tag encryption, and optional biometric linkage to enable convenient, contactless financial transactions specifically designed for subsistence-level activities such as daily wage payments, ration purchases, local market transactions, and community service exchanges.

The system operates through an ecosystem consisting of the Intelligent Tag, a Local Verification Terminal (POS/reader device), and a Cloud-Based Financial Management Platform. During a transaction, the ITT authenticates the user locally using secure key exchange, while the terminal validates the identity, retrieves transaction permissions, and processes the payment. The cloud backend manages wallet balances, subsidy mapping, transaction analytics, user profiles, and dispute resolution, ensuring high transparency and traceability.

By combining offline-capable authentication, encrypted on-tag storage, and lightweight IoT connectivity, the proposed system reduces dependency on smartphones and complex digital interfaces, making financial transactions accessible to users with limited resources or digital literacy. This system aims to provide a secure, scalable, and user-friendly alternative to conventional cash-based subsistence transactions, promoting financial inclusion and reducing fraud.

V. SYSTEM ARCHITECTURE

1. Sensor & Detection Modules (Edge Devices)

The proposed Intelligent Transaction Tag (ITT) integrates a compact sensing and identification suite designed to authenticate users and support secure micro-transactions in subsistence-level financial activities. The tag incorporates NFC/RFID coils, secure EEPROM/flash memory, optional fingerprint or touch-based capacitance sensors, and a low-power microcontroller for real-time identity validation.

These edge devices continuously capture identity tokens, tag presence, transaction intent, and optional user-interaction signals (e.g., tap duration, biometric confirmation). The microcontroller performs initial data formatting, noise filtering, and secure key validation directly on the tag. Sensitive identifiers, such as encrypted user credentials and wallet metadata, are stored locally with tamper-resistant safeguards.

When the tag is brought near a Transaction Reader Terminal (POS/gateway), it transmits identity packets, authentication keys, and transaction triggers through NFC/RFID short-range communication. Only minimal, encrypted data—such as user ID hashes, intent flags, and transaction category codes—is transmitted outward to reduce risk and bandwidth. This continuous, low-latency sensing pipeline ensures fast, secure, contactless authentication suitable for low-resource financial environments.

2. Edge Processing & Transaction Intelligence Module

The edge processing module, embedded within the ITT or the nearby POS Reader, executes lightweight real-time logic to validate identities, verify tag authenticity, and authorize micro-transactions. Using secure cryptographic protocols (AES-128/256, ECC keys, challenge-response), the module performs local checks before communicating with backend servers.

The microcontroller classifies the transaction type—ration purchase, daily-wage disbursement, utility micro-payment, community service credit—and generates a compact, encrypted transaction request. Logic such as fraud detection thresholds, balance limit checks, subsidy eligibility verification, and multi-factor tag interaction patterns is evaluated locally to reduce dependence on network connectivity.

To optimize low-power communication, identity blocks are compressed and transmitted efficiently using NFC or Bluetooth-Low-Energy (BLE). When offline, the module temporarily stores signed transaction logs for later synchronization. Only essential summaries—user hash, amount codes, timestamp, and authentication flags—are forwarded to the IoT gateway. This edge intelligence ensures fast and reliable transactions even in low-connectivity regions.

3. Communication Network & IoT Gateway

The ITT ecosystem communicates with the backend via a local Transaction Reader Terminal acting as the IoT gateway. This gateway receives authentication packets, transaction requests, tag-generated signatures, and user interaction metadata. It uses Wi-Fi, BLE, LoRaWAN, or GSM/4G connectivity to relay these details to the cloud.

User commands—such as approving payments, initiating wage credits, updating subsidy parameters, or topping up wallet balance—are pushed back to the tag through NFC/BLE exactly when needed. Communication protocols like MQTT, HTTPS, and CoAP enable lightweight, secure message exchange between gateways and servers.

If the gateway enters a low-network zone, it automatically switches to offline-buffer mode, storing transaction data locally until connectivity is restored. Extended deployments may use GSM/4G/5G modules for broader coverage, ensuring that financial operations in rural or subsistence environments remain functional and traceable.

4. Cloud / Remote Monitoring Backend

The cloud backend acts as the centralized financial transaction engine, maintaining user profiles, wallet balances, subsidy mappings, and transaction analytics. It stores encrypted logs, tag interaction histories, settlement records, and fraud-detection alerts.

A centralized dashboard allows authorized operators (government agencies, NGOs, financial institutions) to monitor live transaction activity, verify fund disbursements, track welfare distribution, and detect anomalies such as repeated failed authentications or mismatched tag signatures.

ML models can optionally analyze patterns to support fraud detection, subsidy optimization, community spending behavior analysis, and credit-risk profiling. All communication channels are secured through TLS/SSL, role-based access control, and tokenized APIs. In the event of unusual financial events—like repeated declines, suspected tag cloning, or sudden balance depletion—the cloud

AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
E-ISSN:3069-0102
VOL.5, NO. 4(2)(2025)

triggers notifications via SMS, app alerts, or email.

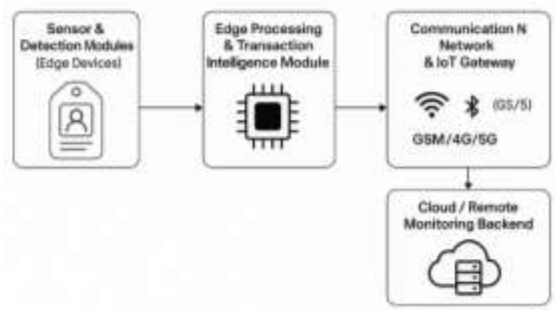

Fig 5.1: Structure of the Proposed System

Microcontroller Module (Core Processing Unit of the Transaction Tag)

The microcontroller inside the Intelligent Transaction Tag coordinates sensing, secure identity handling, cryptographic operations, and transaction triggering. It synchronizes NFC/RFID communication with backend logic to ensure reliable, tamper-resistant financial operations.

Key Components Include:

1. Sensor & ID Interfaces (NFC/RFID / EEPROM / Biometric Input)

Handles short-range communication, credential storage, and optional biometric verification. Interfaces capture user identity, tag presence, and transaction intent.

2. Wireless Communication Module

(NFC primary; BLE/Wi-Fi optional depending on design)

Enables encrypted data exchange between tag, POS reader, and gateway. Transmits identity hashes, transaction codes, and system updates securely.

3. GSM/4G/5G Module (Optional in Reader Terminal)

Provides wide-area network access when local Wi-Fi or BLE is unavailable. Ensures that financial data and transaction logs can be uploaded from remote or rural sites.

4. Digital GPIO Pins

Control LED indicators, buzzers, and user-feedback elements on the tag or POS reader (e.g., payment success tone, error notification). Can also trigger hardware security measures like lockouts after multiple failed attempts.

5. Power Pins (3.3V / 5V / GND)

Provide stable regulated power to NFC coils, microcontrollers, memory modules, and sensors. The system typically uses coin-cell or Li-ion batteries with ultra-low-power sleep modes to maximize tag life.

6. Internal/External Antennas

Ensure reliable NFC/BLE connectivity, enabling smooth tag detection even in crowded or low-signal subsistence environments.

VI. IMPLEMENTATION

The assembled kit includes an RFID reader, fingerprint sensor, 4x4 keypad, LCD display, buzzer, and Arduino—all functioning together to simulate a secure transaction environment.

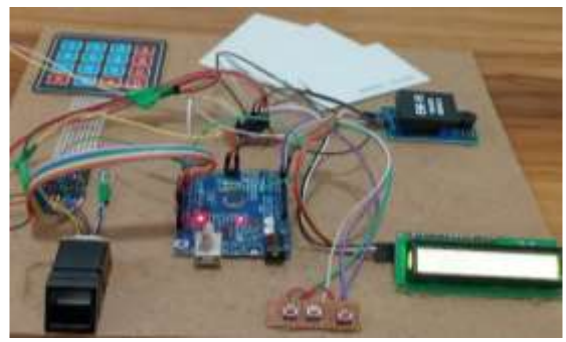

Fig 6.1: Hardware Prototype of Smart Transaction System with RFID, Keypad, and Display

Initially, the user’s fingerprint is stored in the system using the fingerprint sensor. The LCD displays confirmation once the fingerprint is successfully enrolled.

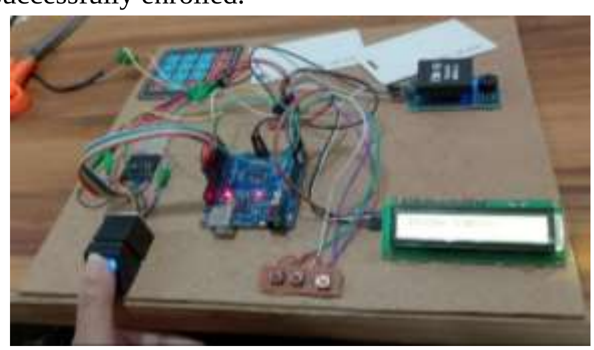

Fig 6.2: RFID-Based Transaction Tag Prototype with Arduino and LCD Display

The user enters the amount using the keypad. Upon successful verification, the LCD shows the entered amount and confirms transaction success with a buzzer sound.

VII. CONCLUSION

The development of the Smart Tag system presents a practical and secure solution to promote financial inclusion, especially in rural and underbanked areas. By integrating EM18 RFID-based identification, biometric fingerprint authentication, and an intuitive keypad interface, the system offers a reliable method for performing digital transactions with minimal complexity. The use of an Arduino microcontroller and peripheral components like LCD displays and buzzers ensures low cost, ease of deployment, and user-friendly operation. The project successfully demonstrates how embedded technology can bridge the gap between conventional banking services and daily livelihood activities, ultimately empowering users to access cashless transactions in a safe and accessible manner. Its potential can be further expanded by integrating mobile connectivity to send transaction alerts or generate digital receipts. In future implementations, the system could also support multilingual voice assistance to improve accessibility for a wider population.

VIII. FUTURE SCOPE

The proposed indoor navigation robot can be further enhanced with advanced AI-driven perception models that enable semantic understanding of indoor environments, allowing the robot to differentiate between static objects, humans, and movable obstacles for more intelligent decision-making. Future versions may integrate full 3D LiDAR, stereo vision, or event-based cameras to achieve higher mapping accuracy and smoother navigation in cluttered settings. Edge AI accelerators such as the NVIDIA Jetson or Google Coral can be added to support real-time deep-learning inference for obstacle classification, path prediction, and adaptive motion planning. Additionally, incorporating swarm coordination features would allow multiple robots to collaborate on tasks, share maps, and avoid mutual interference. Cloud-based analytics can be expanded to include predictive maintenance, energy-optimization algorithms, and autonomous mission planning based on historical performance. Long-term improvements may also focus on human–robot interaction, safety certifications, multilingual voice commands, and self-charging docking systems, ultimately transforming the robot into a fully autonomous, reliable indoor service assistant capable of operating in dynamic and complex human environments.

IX. REFERENCES

[1]. Kaur, M., Sandhu, M., Mohan, N., & Sandhu, P. S. (2011). RFID Technology Principles, Advantages, Limitations & Its Applications.
International Journal of Computer and Electrical Engineering.
DOI: https://doi.org/10.7763/IJCEE.2011.V3.360

[2]. Chen, W., Chen, Y., & Chen, C. (2020). Secure NFC-Based Mobile Payment System Using Lightweight Cryptography.
IEEE Access.
DOI:
https://doi.org/10.1109/ACCESS.2020.2980325

[3].Prodduturi, S.M.K. (2024). 'Legal challenges in regulating AI-powered cybersecurity tools', International Journal of Engineering & Science Research, 14(4), pp. 316–323

[4].Sankar Das, S. (2024). Transforming Data: Role of Data catalog in Effective Data Management. International Journal for Research Trends and Innovation, 9(12). https://doi.org/10.56975/ijrti.v9i12.207245

[5]. Dimitriou, T. (2010). A Lightweight RFID Authentication Protocol with Forward Security and Privacy Protection.
Journal of Network and Computer Applications.
DOI: https://doi.org/10.1016/j.jnca.2010.03.009

[6]. Gong, Y., Yan, X., & Zhang, W. (2019). Design of an Embedded RFID Payment Terminal for Low-Cost Transactions.
IEEE Transactions on Consumer Electronics.
DOI: https://doi.org/10.1109/TCE.2019.2891678

[7].N. Naga Charan, "Predictive Sql Injection Detection And Prevention Using Machine Learning Across Aws, Azure, And Google Cloud Platforms," International Journal of Engineering Science and Advanced Technology, vol. 22, no. 8, pp. 68–74, Aug. 2022, doi: 10.64771/ijesat.2022.v22.i08.pp68-74.

[8].Prodduturi, S.M.K. (2025). Opportunities and Challenges for iOS Developers in Exploring the Integration of Augmented Reality Technologies.

International Journal of Engineering Science and Advanced Technology (IJESAT), 25(4), pp.200–207. ISSN 2250-3676

[9]. Chaudhary, R., Jangra, A., & Kaul, A. (2018). IoT-Based Secure and Smart Transaction System Using RFID.
International Journal of Advanced Computer Science and Applications.
DOI:
https://doi.org/10.14569/IJACSA.2018.090566

[10]. "Scalable Suspicious Activity Detection Using Teradata Parallel Analytics And Tableau Visual Exploration," Inaternational Journal of Communication Networks and Information Security, vol. 8, no. 3, Jun. 2025, doi: 10.48047/ijcnis.8.3.236.

[11]. Sharma, M., & Gupta, P. (2021). Digital Payment Systems for Financial Inclusion: A Review of Emerging Technologies.
Financial Innovation.
DOI: https://doi.org/10.1186/s40854-021-00270-2

[12]. S. K. Immadi, "Optimizing ERP for Human Capital Management," Applied Research for Growth, Innovation and Sustainable Impact, pp. 377–384, Aug. 2025, doi: 10.1201/9781003684657-63.

[13]. Avoine, G., & Hernandez-Castro, J. (2013). The Security of RFID Systems.
Computer Communications.
DOI: https://doi.org/10.1016/j.comcom.2013.03.009

[14]. Ramos, J. F., & Hong, S. (2017). Low-Power Microcontroller Architecture for Secure IoT Applications.
IEEE Transactions on Computers.
DOI: https://doi.org/10.1109/TC.2016.2603982

[15]. S. R. Nelluri and P. Tatikonda, "A Comparative Study Of Aws Relational, Data Warehouse, And Nosql Databases: Advantages Over Traditional Database Systems," International Journal of Engineering Science and Advanced Technology, vol. 24, no. 1, pp. 158–165, Jan. 2024, doi: 10.64771/ijesat.2024.v24.i01.pp158-165

[16]. Li, D., Li, X., & Chen, J. (2018). Lightweight Authentication and Key Agreement Protocol for IoT Devices.
Sensors.
DOI: https://doi.org/10.3390/s18092887

[17]. Alhassan, I., Adam, I., & Buabeng-Andoh, C. (2020). The Role of Mobile and Digital Technologies in Financial Inclusion: A Systematic Review.
Journal of Economic Studies.
DOI: https://doi.org/10.1108/JES-10-2019-0476