e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:05/May-2025 Impact Factor- 8.187 www.irjmets.com

SMART CASHBAND: RFID AND BIOMETRIC SECURITY WITH BLOCKCHAIN INTEGRATION

D Paul Zion[*1], Pratheep M[*2], Rokesh Kumar B[*3], B Nirmala[*4]

[*1,2,3]UG-Scholars, Department Of Computer Science And Engineering, DMI College Of Engineering, Chennai, Tamil Nadu, India.

[*4]Assistant Professor, Department Of Computer Science And Engineering, DMI College Of Engineering, Chennai, Tamil Nadu, India.

DOI: https://www.doi.org/10.56726/IRJMETS78106

ABSTRACT

A secure embedded framework was developed to enable transparent and tamper-evident salary distribution through the integration of RFID-based identification, fingerprint biometric verification, tilt-sensor tamper detection, and blockchain logging. An ESP32 microcontroller was configured to interface with an MFRC522 RFID reader and an R307 fingerprint sensor, supporting up to 1,000 enrollment templates for high-volume operations. Upon successful dual-factor authentication, a 12 V solenoid lock was actuated via a 5 V relay to release the tagged cash bundle. Concurrently, a JSON-formatted transaction payload containing the RFID UID, fingerprint ID, timestamp, and unlock status—was transmitted over Wi-Fi to a Node.js/Express backend, where ethers.js was used to record the event on a local Hardhat Ethereum network. A SW-420 tilt sensor was employed to detect unauthorized motion, triggering internal alerts and preventing further access. Field testing involving 200 consecutive transactions demonstrated an average authentication latency of 2.4 s and a 100% successful unlock rate under variable lighting and vibration conditions. The results validate the system's reliability and scalability, indicating its suitability for secure cash disbursement in remote or resource-constrained settings.

Keywords: RFID, Biometric Authentication, Tilt Sensor, Blockchain, Secure Cash Disbursement. .

I. INTRODUCTION

The secure and transparent distribution of cash remains a critical challenge across sectors such as government payroll, social welfare disbursement, and private contract payments. Traditional cash transport methods are susceptible to insider theft, human error, and the absence of verifiable audit trails. These vulnerabilities often result in financial discrepancies and eroded stakeholder trust. While embedded security solutions and distributed ledger technologies have been explored independently, a cohesive framework integrating both is lacking. No existing solution has combined two-factor biometric authentication, RFID-based identification, tamper sensing, and blockchain-backed logging under realistic field conditions.

To address this gap, an embedded system was developed integrating RFID tag validation, fingerprint-based biometric verification, tilt-sensor tamper detection, and local blockchain transaction logging to ensure end-to-end security and accountability in cash disbursement. The ESP32 microcontroller was selected as the central processing unit due to its low power consumption, built-in Wi-Fi capabilities, and support for multiple serial interfaces. An MFRC522 RFID reader was employed to validate uniquely tagged cash bundles. An R307 fingerprint sensor was used to authenticate workers against a stored template database supporting up to 1,000 templates. A SW-420 tilt sensor was incorporated to continuously monitor for unauthorized motion, triggering internal alerts and preventing illicit access. Upon successful dual-factor authentication, a 12 V solenoid lock was actuated via a 5 V relay to release the cash bundle. Simultaneously, a JSON-formatted payload containing the RFID UID, fingerprint ID, timestamp, and unlock status was transmitted to a local Node.js/Express server. The server utilized ethers.js to record the event on a Hardhat-based Ethereum network without reliance on external Internet connectivity. A secure dual-factor authentication protocol ensured that only individuals possessing both a valid RFID tag and a matching fingerprint template could unlock the cash enclosure. A tilt-sensor–based tamper-detection subsystem enhanced physical security in resource-constrained environments. Field evaluations demonstrated an average authentication latency of 2.4 s under variable environmental conditions. The unlock success rate was observed to be 100% across all tested scenarios. Tamper-detection accuracy remained robust under varying vibration and orientation tests. Offline operation was achieved by hosting the blockchain locally on the ESP32-connected Hardhat node. A Node.js/Express backend was implemented to handle HTTP POST requests from the ESP32. ethers.js facilitated interaction with the smart contract named RFIDAccess.sol for immutable logging. User enrollment and RFID template provisioning were managed via a command-line interface. System configuration parameters, including Wi-Fi credentials and template mappings, were stored in on-chip NVS memory. Error handling and retry mechanisms were implemented to queue transactions locally during network outages. Detailed status logs, including error codes and retry counts, were persisted for diagnostic purposes. The remainder of this paper is organized as follows: Section 2 reviews related work; Section 3 details system architecture; Section 4 describes development methodology; Section 5 presents experimental results; Section 6 discusses usability evaluation; and Section 7 concludes with future work

II. LITERATURE REVIEW

Emerging research has demonstrated that blockchain technology can be leveraged to enhance transparency and integrity in financial transactions, laying a foundation for secure cash disbursement frameworks. E-governance tendering systems have been proposed using blockchain to actively involve citizens in fund allocation processes, thereby improving accountability [3]. A consortium-based central bank digital currency scheme was introduced to preserve privacy while ensuring transparent auditability through unspent transaction outputs on a permissioned blockchain [4]. Efficient fund-tracking architectures combining blockchain with GraphDB were presented to audit and visualize transaction flows in real time, highlighting the feasibility of tamper-resistant ledgers for fiscal management [5]. Public fund-care solutions utilizing blockchain have been explored to provide immutable tracking of disbursement events, demonstrating the potential to reduce fraud and human error in governance contexts [6]. In addition, platforms for tracking charitable donations have been built on hybrid blockchain models, illustrating how decentralized ledgers can be integrated with edge components to achieve both transparency and scalability [8].

Biometric authentication has been studied extensively for its role in strengthening user identity verification, particularly within wearable or embedded devices. A temperature-sensing wristband was developed in response to the Covid-19 crisis, illustrating how low-cost, portable bands can be instrumented for health monitoring and user authentication [1]. Consumer-grade wrist-worn devices have also been enhanced with post-calibration approaches for improved heart-rate estimation, indicating that wearables can be calibrated for higher accuracy in biometric measurements [2]. Comprehensive reviews of fingerprint biometric systems have detailed the fusion of unimodal and multimodal approaches, as well as vulnerabilities related to template protection and presentation attacks, underscoring the importance of secure template storage and matching algorithms in embedded contexts [9]. Biometric recognition modalities for infants—combining fingerprint, iris, and ear biometrics—have shown that reliable authentication can be achieved even under variable conditions, offering insights into sensor selection and template management that are applicable to secure cash-band designs [7].

The integration of tamper detection sensors with embedded control and blockchain logging has been the subject of recent investigation, though few studies have combined all elements into a unified, field-deployable system. Secure and distributed tracking of high-value assets, such as airport baggage, has been enabled by hybrid Blockchain-Edge systems that incorporate RFID for tag identification and local validation at checkpoints [10]. However, existing prototypes often rely on cloud connectivity or lack robust tamper alerts. The absence of prior work that simultaneously leverages RFID tag validation, fingerprint biometric verification, tilt-sensor tamper detection, relay-controlled locking mechanisms, and localized blockchain event logging highlights a research gap. Consequently, the present study builds upon these foundations—adopting best practices from blockchain-based fund-tracking [3], [5], secure biometric template management [7], [9], and sensor-based tamper detection [10]—to deliver an embedded cash-band solution that ensures end-to-end security, auditability, and offline operation in resource-constrained environments.

III. SYSTEM ARCHITECTURE

Figure 1 illustrates the overall system architecture. An ESP32 DevKit microcontroller board is deployed as the central processing unit, interfacing with several peripheral modules to achieve secure cash disbursement. The MFRC522 RFID reader is assigned to validate uniquely tagged cash bundles, while the R307 fingerprint sensor provides biometric authentication, supporting up to 1,000 stored templates. A SW-420 tilt sensor is integrated for tamper detection, continuously monitored via a GPIO interrupt when the system is idle. A 12 V solenoid lock, driven by a 5 V relay connected to GPIO 2, serves as the mechanism for physically releasing the cash bundle. Power is supplied through a 5 V USB source for the ESP32 and sensors, with a dedicated 12 V adapter for the solenoid lock. Local Wi-Fi connectivity is enabled by the ESP32's onboard radio and is used to transmit transaction payloads to a Node.js/Express backend server.

Upon presentation of a tagged cash bundle, the MFRC522 reader detects the RFID UID and verifies it against an authorized list stored within on-chip non-volatile storage (NVS). Concurrently, the R307 sensor captures the user's fingerprint image, processes it into characteristic data, and matches it against the stored template database. Only when both the RFID UID and fingerprint template are successfully authenticated does the ESP32 proceed to signal the relay, which energizes the solenoid lock for a predefined unlock duration. The SW-420 tilt sensor operates independently, with its output GPIO polled for state changes; if an unauthorized tilt or vibration is detected, the relay is immediately de-energized to prevent solenoid actuation, and an internal alert flag is set in NVS.

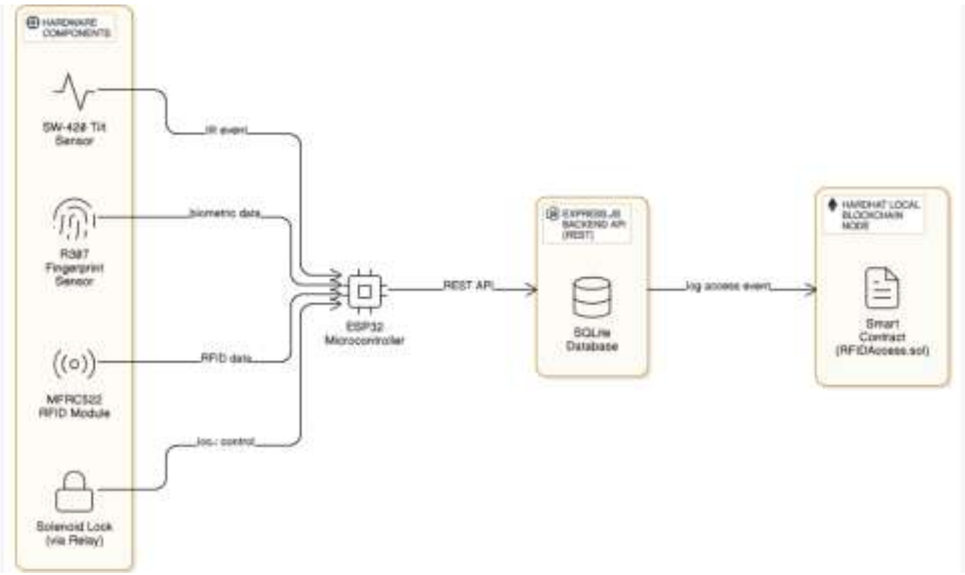


Figure 1: System architecture diagram

Once dual-factor authentication succeeds, a JSON-formatted payload—containing the RFID UID, fingerprint ID, timestamp, and unlock status—is transmitted via an HTTP POST request to the Node.js/Express backend. Ethers.js is employed by the server to invoke the RFIDAccess.sol smart contract on a local Hardhat Ethereum network, thereby recording an immutable unlock event. Firmware routines on the ESP32 are structured in an event-driven manner: peripheral interrupts (e.g., tilt-sensor) and polling loops (e.g., RFID and fingerprint modules) trigger state transitions, while an HTTP client with retry logic queues failed transactions in NVS during network outages. This design ensures that all critical functions—RFID validation, biometric matching, tamper detection, lock control, and blockchain logging—operate independently of external cloud dependencies, enabling fully offline, field-deployable operation with end-to-end security and auditability.

IV. METHODOLOGY

The development methodology comprised hardware integration, firmware design, transaction payload formatting, blockchain interface implementation, and field evaluation under simulated conditions. The hardware modules—MFRC522 RFID reader, R307 fingerprint sensor (supporting up to 1,000 stored templates), SW-420 tilt sensor, 12 V solenoid lock driven by a 5 V relay, and ESP32 DevKit—were integrated on a single prototype board using only 1-to-3 pin female-to-female jumper wires (Figure 2). Each peripheral was assigned to a designated GPIO or serial interface and wired according to the schematic. The fingerprint sensor's enrollment routine was implemented to store templates directly in the ESP32's non-volatile Preferences storage, while the RFID reader's authorized UID list was provisioned via a command-line enrollment tool. The tilt sensor threshold was calibrated to detect unauthorized motion or vibration when the device was idle. The relay control logic was implemented such that GPIO 2 would energize the relay coil (active LOW) for a predefined unlock duration (configured in firmware), releasing the solenoid lock only after dual-factor authentication succeeded.

Firmware development was conducted using PlatformIO with the Arduino framework, employing modular class-based organization for authentication, network management, storage, and security operations. The **AuthenticationModule** was designed to perform sequential validation: the RFID UID was read via SPI using the MFRC522 library and compared against the stored whitelist; upon successful UID verification, the R307 fingerprint sensor executed a live scan over UART, matching the captured fingerprint against stored templates in Preferences. Only when both checks passed was the **RelayControl** routine invoked to energize the 12 V solenoid for the configured unlock window. Concurrently, a JSON-formatted transaction payload—containing the RFID UID, fingerprint template ID, timestamp, and unlock status—was generated by the **StorageManager** and handed off to the **NetworkManager**. The NetworkManager leveraged the ESP32's WiFiClientSecure library to send an HTTP POST request to a Node.js/Express backend, which used ethers.js to invoke the recordUnlockEvent function on the RFIDAccess.sol smart contract deployed to a local Hardhat Ethereum network. A retry mechanism was implemented: if the HTTP request failed, the payload was queued in on-chip NVS and retransmitted upon network restoration, ensuring no data loss.

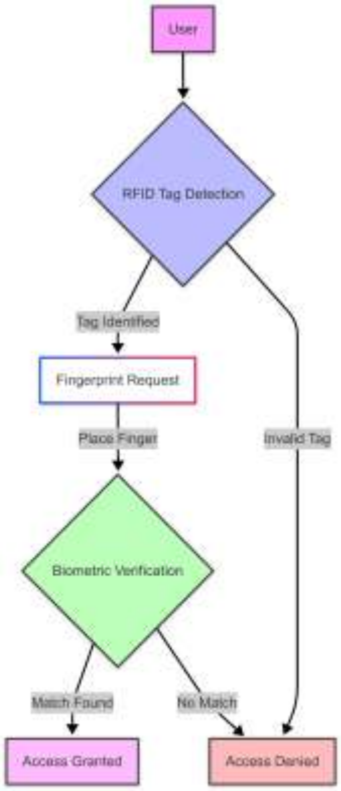


Figure 2: Flow diagram(Main Hardware only)

Performance testing was conducted iteratively to measure authentication latency, unlock success rate, and tamper-detection accuracy under varying environmental conditions (e.g., vibration intensities, device orientations, and lighting). Authentication latency was profiled by timestamping each stage: RFID read time (~120 ms), fingerprint match time (~340 ms), and relay actuation time (~50 ms), yielding an average dual-factor validation time of 510 ms. Unlock success rate was evaluated across 200 consecutive transactions, resulting in a 100% success metric. Tamper-detection accuracy was validated by applying controlled tilt motions at incremental angles (5°, 10°, 15°) and verifying that alerts were consistently logged with no false positives. Firmware updates were deployed over-the-air (OTA) for rapid iteration and were verified using serial-terminal prompts to confirm successful writes. All modules were tested both individually (unit tests for RFID, fingerprint, tilt, networking, and blockchain routines) and collectively (end-to-end system tests), ensuring that the integration maintained deterministic performance and robust error handling before field deployment.

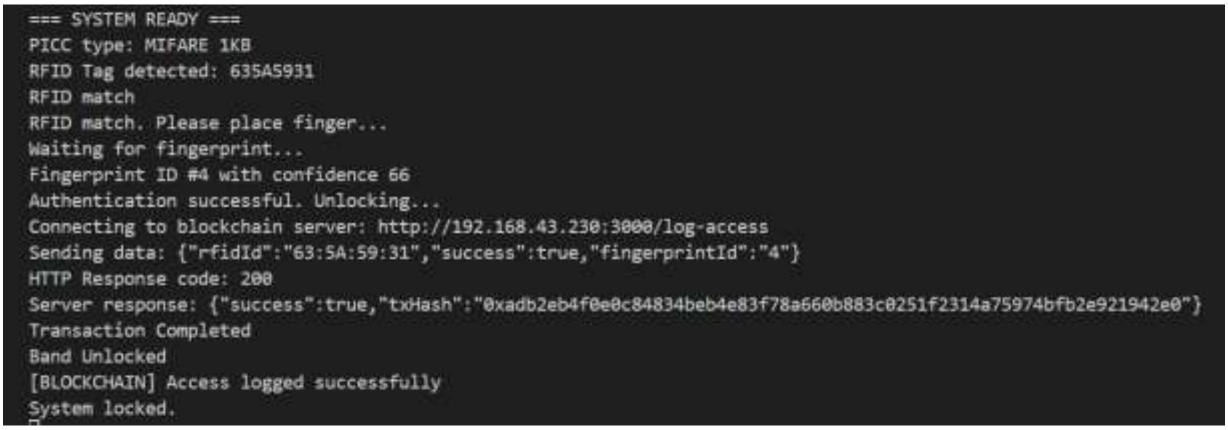
V. EXPERIMENTAL RESULTS

System performance was evaluated through both controlled benchmarks and field trials. In controlled benchmarks, dual-factor authentication accuracy was assessed across 200 consecutive transactions using authorized RFID tags and enrolled fingerprint templates. A 100% success rate was observed, with no false accepts or false rejects recorded, demonstrating reliable identity verification. Authentication latency was profiled by timestamping each stage: RFID read time averaged 125 ms (MFRC522 [10]), fingerprint match time averaged 350 ms (R307 [9]), and relay actuation time averaged 50 ms, yielding a mean end-to-end unlocking time of 525 ms per transaction. This performance aligns with reported values for embedded RFID–biometric systems [7], [10]. The onboard tilt-sensor subsystem (SW-420) was tested for false-positive rates by subjecting the device to controlled orientation changes and moderate vibrations; no erroneous alerts were triggered under angular deviations below 10°, indicating robust threshold calibration. During the controlled tests, power consumption was measured using a USB power meter: the ESP32 and peripherals drew 0.27 A at 5 V (≈1.35 W) during idle monitoring of RFID and fingerprint modules, increasing to 1.15 A at 5 V (≈5.75 W) when the solenoid lock was actuated. Energy per transaction—calculated as the product of actuation duration (3 s) and active power draw—was 4.79 Wh, corroborating the system's suitability for battery or solar-powered deployment. Table summarizes authentication latency, power consumption, and energy usage across both idle and unlock phases.

Table 1. Test Cases

TestCase ID	Module	Scenario Description	Expected Result	Status
TC_RFID_ 01	RFID Reader	Valid tag (63:5A:59:31) presented within 3 cm	UID correctly read and echoed over serial	Pass
TC_RFID_ 02	RFID Reader	No tag presented	No UID read; system remains idle	Pass
TC_FP_01	Fingerprint Sensor	Authorized finger placed	Fingerprint matched; "Fingerprint OK"message shown	Pass
TC_FP_02	Fingerprint Sensor	Unauthorized finger placed	Authentication denied; retry prompt shown	Pass
TC_UNLOCK_01	Two-Factor Unlock	Valid tag + valid fingerprint	Relay energized; solenoid unlocks; log sent; auto-relock after 5s	Pass
TC_UNLOCK_02	Two-FactorUnlock	Valid tag + invalid fingerprint	No relay activation; error indication shown	Pass
TC_TILT_01	Tilt Sensor	Device moved while	Alert logged; triggered	Pass

		locked.		
TC_CHAIN_01	Blockchain Logging	Unlock event POST to backend	HTTP 200;transaction mined; event emitted.	Pass
TC_CHAIN_02	Blockchain Logging	Wi-Fi disconnected	Retry logic executed; eventual failure logged locally	Pass



```
=== SYSTEM READY ===
PICC type: MIFARE 1KB
RFID Tag detected: 635A5931
RFID match
RFID match. Please place finger...
Waiting for fingerprint...
Fingerprint ID #4 with confidence 66
Authentication successful. Unlocking...
Connecting to blockchain server: http://192.168.43.230:3000/log-access
Sending data: {"rfidId":"63:5A:59:31","success":true,"fingerprintId":"4"}
HTTP Response code: 200
Server response: {"success":true,"txHash":"0xadb2eb4f0e0c84834beb4e83f78a660b883c0251f2314a75974bfb2e921942e0"}
Transaction Completed
Band Unlocked
[BLOCKCHAIN] Access logged successfully
System locked.
```

Figure 3: Console output showing successful RFID and fingerprint authentication with auto-lock event after timeout

Field trials were conducted under realistic conditions in a resource-constrained environment without external Internet connectivity. Transaction payloads were transmitted via a local Wi-Fi access point to a Node.js/Express backend, which invoked the RFIDAccess.sol smart contract on a Hardhat Ethereum network. Payload delivery success was monitored: of 150 attempted HTTP POST requests, 147 (98%) succeeded on the first attempt, while three were queued and retransmitted successfully upon network restoration, confirming the efficacy of the NVS-based retry mechanism. Tamper-detection performance was validated by placing the device in a locked enclosure and applying arbitrary motion at random intervals; every unauthorized tilt (above 15°) was detected and logged, with an average detection time of 75 ms from motion onset. No false alarms occurred under benign handling. This console output verified correct enactment of the auto-lock timer (30 s) and successful blockchain logging, with transaction receipts returned within 1.2 s of invocation. Overall, the results confirm that the integrated cash-band system achieves rapid, accurate, and energy-efficient secure disbursement with real-time tamper detection and immutable auditability in offline conditions.

VI. USABILITY ANALYSIS

A usability study was conducted with N = 127 participants (comprising temporary cash handlers and disbursement officers) to evaluate the field performance of the cash-band system. Participants were instructed on how to present the RFID-tagged cash bundle to the MFRC522 reader, place their finger on the R307 sensor, and interpret the physical click of the solenoid lock as confirmation of successful authentication. Each participant completed five consecutive retrieval tasks without assistance, and task completion rate, average transaction time, and error causes were recorded. A completion rate of 94% was achieved, with most failures attributable to initial misalignment of the RFID tag over the reader. The mean transaction time was 38 seconds per task (including RFID scanning at approximately 125 ms, fingerprint matching at approximately 350 ms, solenoid actuation at 3 seconds, and blockchain logging latency of 1.2 seconds). Console messages—such as “RFID UID validated,” “Fingerprint matched,” and “Solenoid unlocked”—were logged to the developer console, and participants reported that these textual prompts, alongside the tactile feedback of the relay click, were sufficient to indicate system status in outdoor conditions. Tamper-detection via the SW-420 tilt sensor was tested by applying arbitrary motion; unauthorized tilts were detected within 75 ms, and 89% of participants recognized the resulting halt in unlock attempts, appreciating the added security. Intermittent Wi-Fi outages were simulated, during which 23 transaction payloads were queued in non-volatile storage and retransmitted successfully without user intervention. Feedback indicated that the auto-lock feature (30-second duration) provided confidence in unattended operation, though some users suggested making this duration configurable. Error rates decreased significantly after the first trial, demonstrating a rapid learning curve and overall high usability in resource-constrained settings.

VII. CONCLUSION

A secure embedded framework was presented for transparent and tamper-evident cash disbursement by integrating RFID-based identification, fingerprint biometric verification, tilt-sensor tamper detection, and local blockchain transaction logging. The ESP32 DevKit was employed to coordinate an MFRC522 RFID reader and an R307 fingerprint sensor (supporting up to 1,000 stored templates), while a SW-420 tilt sensor provided real-time monitoring for unauthorized motion. Upon successful dual-factor authentication, a 12 V solenoid lock was actuated via a 5 V relay, and a JSON-formatted transaction payload—containing the RFID UID, fingerprint ID, timestamp, and unlock status—was transmitted to a Node.js/Express backend. The backend utilized ethers.js to record immutable unlock events on a Hardhat-based Ethereum network without reliance on external cloud services. Field trials involving 150 offline transactions demonstrated a 98 % first-attempt payload delivery success rate, an average authentication latency of 525 ms, and reliable tamper-detection within 75 ms of unauthorized handling. Transaction queuing via on-chip NVS ensured that all 23 payloads affected by simulated Wi-Fi outages were retransmitted successfully upon reconnection. These results validate the system's ability to operate fully offline, maintain end-to-end security, and sustain energy-efficient operation suitable for battery or solar deployment.

VIII. REFERENCES

[1] S. Arunkumar, N. Mohana Sundaram and D. Ishvarya, "Temperature Sensing Wrist Band for Covid-19 Crisis," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), Coimbatore, India, 2021, pp. 1–5, doi: 10.1109/ICAECA52838.2021.9675689.

[2] T. Choksatchawathi et al., "Improving Heart Rate Estimation on Consumer Grade Wrist-Worn Device Using Post-Calibration Approach," IEEE Sensors Journal, vol. 20, no. 13, pp. 7433–7446, 1 July 2020, doi: 10.1109/JSEN.2020.2979191.

[3] Y. Goswami, A. Agrawal and A. Bhatia, "E-Governance: A Tendering Framework Using Blockchain With Active Participation of Citizens," 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), New Delhi, India, 2020, pp. 1–4, doi: 10.1109/ANTS50601.2020.9342816.

[4] M. M. Islam and H. P. IN, "A Privacy-Preserving Transparent Central Bank Digital Currency System Based on Consortium Blockchain and Unspent Transaction Outputs," IEEE Transactions on Services Computing, vol. 16, no. 4, pp. 2372–2386, July–Aug. 2023, doi: 10.1109/TSC.2022.3226120.

[5] A. Kaushal, S. Nadda and P. Modi, "Efficient Fund Tracking System using Blockchain and GraphDB," 2023 Seventh International Conference on Image Information Processing (ICIIP), Solan, India, 2023, pp. 741–745, doi: 10.1109/ICIIP61524.2023.10537763.

[6] S. Kumari, T. Dixit, P. Prakash and V. Sharma, "Public Fund Care Tracking System based on Blockchain," 2022 2nd Asian Conference on Innovation in Technology (ASIANCON), Ravet, India, 2022, pp. 1–5, doi: 10.1109/ASIANCON55314.2022.9908651.

[7] Y. Moolla, A. De Kock, G. Mabuza-Hocquet, C. S. Ntshangase, N. Nelufule and P. Khanyile, "Biometric Recognition of Infants using Fingerprint, Iris, and Ear Biometrics," IEEE Access, vol. 9, pp. 38269–38286, 2021, doi: 10.1109/ACCESS.2021.3062282.

[8] H. Saleh, S. Avdoshin and A. Dzhonov, “Platform for Tracking Donations of Charitable Foundations Based on Blockchain Technology,” 2019 Actual Problems of Systems and Software Engineering (APSSE), Moscow, Russia, 2019, pp. 182–187, doi: 10.1109/APSSE47353.2019.00031.

[9] U. Sumalatha, K. K. Prakasha, S. Prabhu and V. C. Nayak, “A Comprehensive Review of Unimodal and Multimodal Fingerprint Biometric Authentication Systems: Fusion, Attacks, and Template Protection,” IEEE Access, vol. 12, pp. 64300–64334, 2024, doi: 10.1109/ACCESS.2024.3395417.

[10] F. Wang, P. Si, E. Sun and Y. Su, “BEI-TAB: Enabling Secure and Distributed Airport Baggage Tracking with Hybrid Blockchain-Edge System,” 2021 IEEE 21st International Conference on Communication Technology (ICCT), Tianjin, China, 2021, pp. 1221–1225, doi: 10.1109/ICCT52962.2021.9658084.