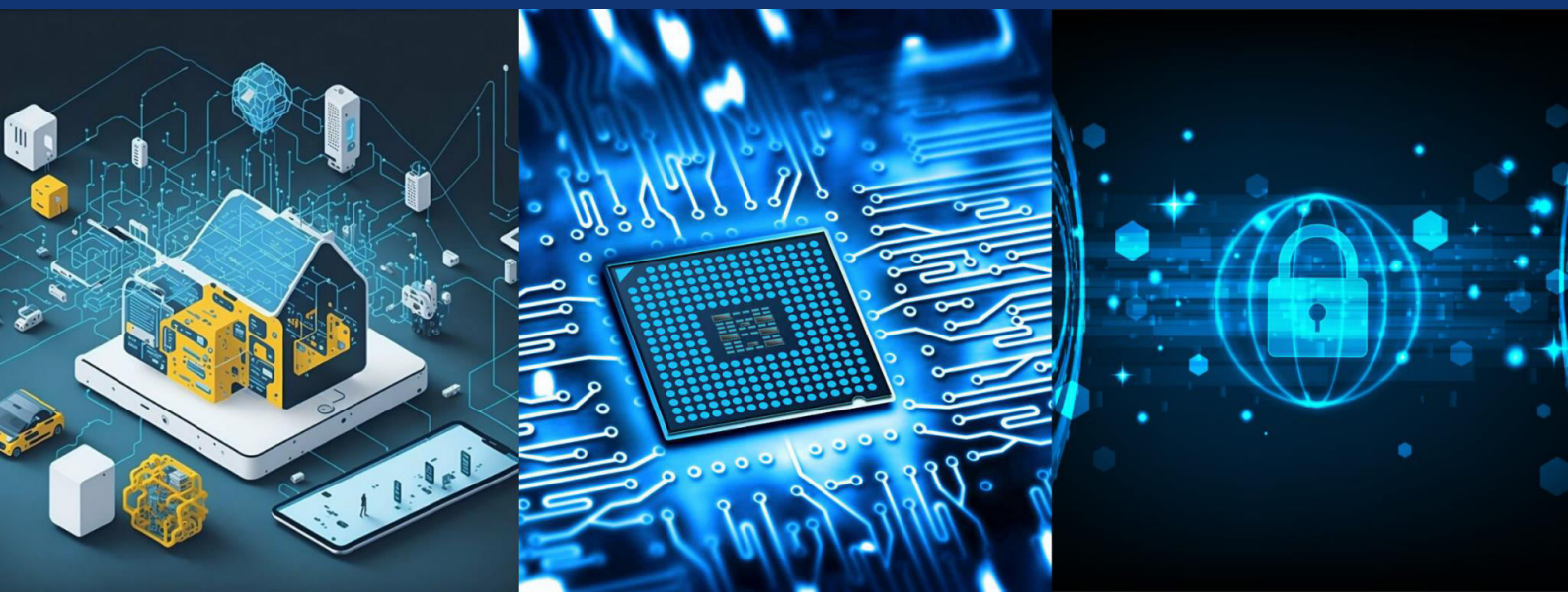
IJIRCCE

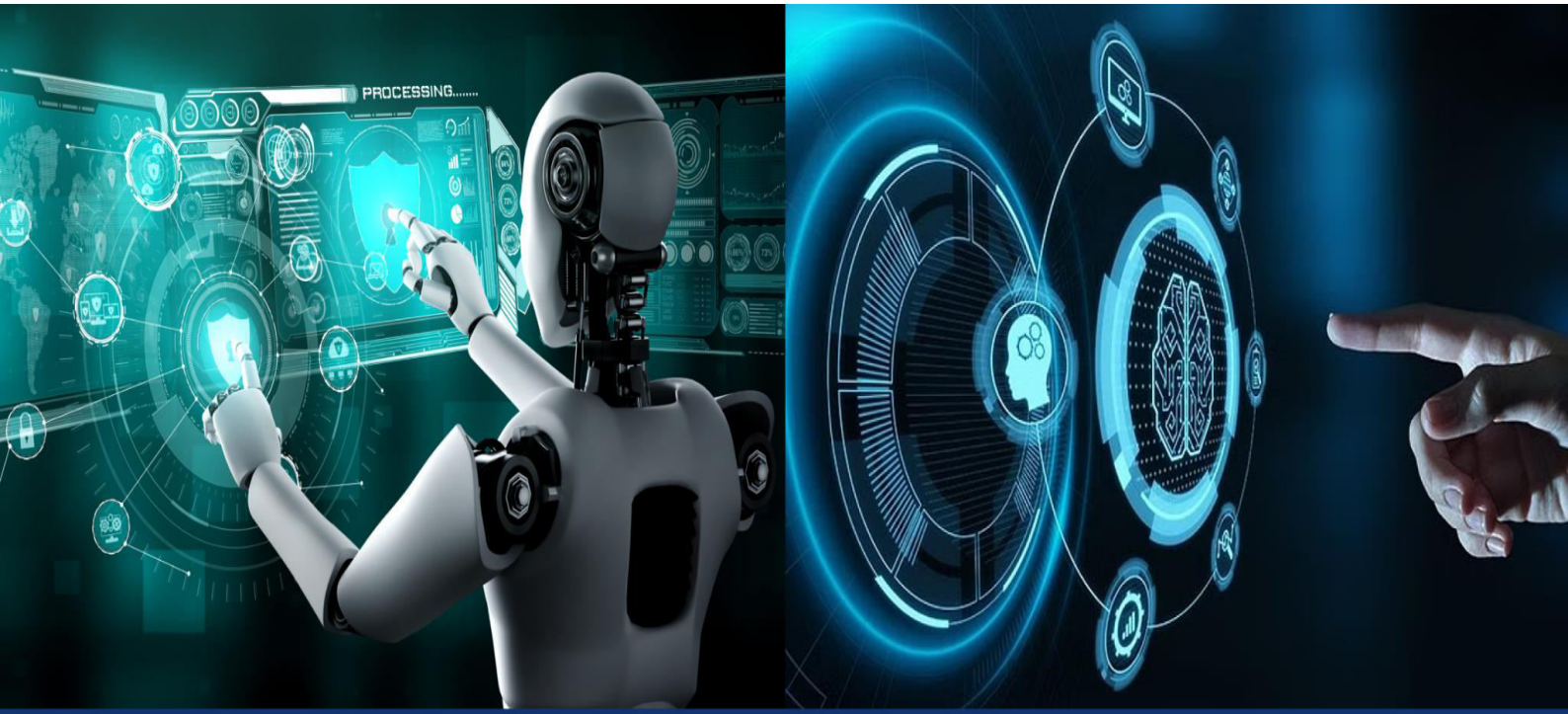
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 10, October 2026

© 2026 IJIRCCE | Volume 14, Issue 10, October 2026 DOI: 10.15680/IJIRCCE.2026.1410015

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Hybrid Blockchain-IoT Architectures for Transparent and Accountable Public Distribution Systems-A Survey

Jueli Chintawar[1], Vishwesh Patil[2], Vansh Barde[3], Himanshu Mire[4], Dr. Kapil Gupta[5]

Department of Computer Engineering, St. Vincent Pallotti College of Engineering and Technology, Nagpur, India[1-4]

Assistant Professor, Department of Computer Engineering, St. Vincent Pallotti College of Engineering and Technology, Nagpur, India[5]

ABSTRACT: The PDS of India feeds more than 800 million people in the total via nearly 500,000 Shops. The Aadhaar seeding, point-of-sale devices, and the portability of One Nation One Ration Card have digitalized the major portion of the pipeline. However the loopholes, diversion, authentication failure, stock manipulation, and lack of realtime monitoring persists. This indicates that the architecture itself has issues and is not the result of lack of digitization. Centralized relational databases maintain the efficient transactional records but since it is possible for the authorized person to modify them at their will, they cannot provide any tamper evident independent verifications. This survey reviews 48 studies in fifteen distinct areas of technologies related to transparent welfare delivery of blockchain ledgers, traceability within food supply chains, Internet of Things based physical verification, digital governance, biometric and token based authentication, hash chains, smart contracts, hybrid blockchain-cloud computing, AI-powered fraud detection, digital wallet, role based access control, and cloud hosted government computing. All the technologies have been individually tested. No surveyed system has more than two or three technologies in use. Even the closest systems are hybrid blockchain-cloud solutions. This gap in integration of technologies inspires the proposed Digital Supervision Layer that integrates hybrid blockchain anchoring, IoT based quantity verification, layered multifactor authentication, blockchain aware role based access control, digital wallet, and anomaly detection in one transaction pipeline.

KEYWORDS: blockchain, Internet of Things, public distribution system, hash-linked ledger, anomaly detection, role-based access control, multi-factor authentication, digital wallet.

I. INTRODUCTION

India's Public Distribution System is one of the world's largest food-security program, moving subsidized rice, wheat, sugar, and kerosene to more than 800 million beneficiaries through roughly half a million Fair Price Shops run jointly by state civil supply departments and the Food Corporation of India [1]. Built originally on the paper ration cards and manual stock registers, and the system has stayed most nontransparent exactly where diversion is easiest, warehouse dispatch, transport, and the shop counter [14]. The National Food Security Act of 2013 turned entitlements into the legal right for roughly two-thirds of the population, multiplying the audit burden on the infrastructure never designed for that scale [1, 3]. Digitization efforts end-to-end computerization of TPDS operations, Aadhaar seeding, ePoS devices, and ONORC portability responded to a simple fact: manual records could not be reconciled against real allocations anywhere near real time [16, 13]. But ePoS rollout only strengthened point-of-sale authentication. It never produced a tamper-evident record running from godown to household, because ePoS logs sit on state-run servers that the departments operating them can still edit [14]. That gap between "digitized" and "trustworthy" is what draws attention to cryptographically verifiable, IoT-instrumented PDS architectures.

Two decades of computerization have left several structural weaknesses unresolved: grain still leaks between warehouse and shop despite ePoS adoption [3]; deliveries can be logged as complete while being redirected to the open market 2025, with foundational papers retained where they remain because records remain editable [5]; biometric authentication continues to mismatch, especially for elderly and manual labour beneficiaries[18]; recorded and physical stock diverge because systems record what a transaction claims rather than what was actually dispensed[12];

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

beneficiaries and auditors have no practical way to confirm a stored record has stayed unchanged [21]; and state platforms rely on periodic batch uploads, so fraud surfaces only after the fact [15]. These problems look operationally different but share one root of the cause, existing systems record transactions without guaranteeing the records cannot be altered undetected. A centralized database, however carefully administered, remains editable by whoever holds the authorized access. Blockchain anchoring, cryptographic hash chaining, and IoT-based physical verification exist precisely to close the gap. This work does not propose replacing the existing PERN or PostgreSQL operational stack; it strengthens that stack with a hybrid blockchain based supervision layer, keeping conventional efficiency everywhere it already works while adding cryptographic integrity where fraud is most likely to occur. Fifteen technology areas are covered: blockchain in public distribution and food supply chains, IoT-based smart-ration hardware, digital governance, Aadhaar and QR-based authen-tication, cryptographic hash chains, Ethereum smart contracts, hybrid blockchain architectures, AI/ML fraud and anomaly detection, digital wallets, supply-chain transparency, role-based access control, and cloud-based government computing. Priority goes to work published between 2020 and the primary reference for a technique.

II. LITERATURE REVIEW

A. Blockchain in Public Distribution Systems

Research in using blockchain and IoT technology in India's public distribution system agree that centralization of information leads to short-weighting, diversion of food grains and unreliable audit trails, yet the extent of progress differs drastically between the two. Malathi et al. [4] created a private Ethereum network on Raspberry Pi using QR code-based authentication and a Tamil voice or text user interface; an 80 participant pilot study found complete immutability, average response time of 130 ms and 90% user satisfaction, yet throughput decreased beyond 40 transactions per second and multi-state implementation is still not tested. Shwetha and Prabodh [5] and Singh et al.
[6] remain theoretical, the former discusses IoT-tracked distribution without any specifics on throughput or consensus algorithm, whereas the later suggests the use of a consortium blockchain that segregates on-chain and off-chain data without constructing a prototype. None combines ledger anchoring with realtime IoT-based quantity validation or scales up to a nationwide solution gap which the proposed solution bridges by anchoring transaction hash codes on Ethereum Sepolia and adding load cell validation and streaming anomaly detection.

B. Blockchain for Food Supply Chains

Tian's system design [7] uses RFID along with blockchain for end-to-end traceability, but there is no analysis on the system's implementation and scalability issues. The next step would be AgriBlockIoT [8] by Pincheira Caro et al., which includes performance evaluation of the system on the Ethereum and Hyperledger Sawtooth platforms, even though validation is limited to testing in a testbed environment, and beneficiary identification is not within the scope of the work. The most efficient solution as for the throughput is offered by Prashar et al. [9], which shows throughput up to 161 tx/s; still, it is aimed at the market traceability, no ration card entitlement, just like the other two solutions.

C. IoT-based Smart Ration Distribution

Shukla et al. [10] utilized RFID cards that were crosschecked with the backend database. We are eliminating duplication of cards but without any proof regarding the actual dispensed quantity as per the record. Gaikwad & Nikumbh [11] took another stride by utilizing the SMS through the GSM technology, inheriting the vulnerability of being cellular, with no binding of the biometrics whatsoever. Indirani et al. [12] took it a level higher by using the fingerprint biometrics along with Aadhar number to automate the dispensation but recorded the transactions on an ordinary spreadsheet, making it a retrogressive step for the integrity of the data being recorded.

D. Digital Governance in Welfare Systems

Through the study based on around 1,600 below poverty line families, Nagaraj and Prakash [13] reveal that Aadhaar-based PDS is unaware of the social relations prevailing locally, leading to the authentication problems which force frontline workers into behavior that adversely impacts the poor households. Hundal and Chaudhuri
[14] describe the same phenomenon in terms of the digital exclusion in two states, whereas through her ethnography, Chaudhuri [15] explains that the algorithm behind the system gets designed due to the continuous human infrastructure interface rather than the logic alone. No one suggests any other design, the proposed layer does not disturb the present ePoS or Aadhaar route but adds an extra layer of authentication via OTP or QR.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

E. Aadhaar Authentication

Muralidharan, Niehaus, and Sukhtankar [16] used a combination of a randomized experiment and a natural experiment conducted in Jharkhand state and found that the biometric authentication reduced leakages effectively and however, there were around 1.5 to 2 million recipients who lost their access either temporary or permanent due to seeding problems and inefficient grievance redressal system. In the field survey conducted in Ranchi district, Menon [18] found that nearly 52% of the transaction completion took place. Further, Nagaraj and Prakash [17] claim that the architecture employs a single strategy without considering the different local relationships.

F. QR-based Authentication Systems

Kao et al. [19] provide single use QR-coded OTPs for the access control purposes in a physical world but assume reliable mobile network connectivity, something fragile in the case of rural fair price shops. Gangurde et al. [20] on the other hand, AES encrypts the QR based credential without providing key rotation or ledger lookup to prevent the reuse. Neither considers the linking of the QR code to a tamper proof ledger or the physical validation, which is provided by the proposed solution through QR validation result and weight checking.

G. Cryptographic Hash Chains

The digital time stamping approach developed by Haber and Stornetta [21] connects the hash value of each entry with its predecessor in such a way that any change to the past entries renders subsequent links invalid the light-weight and dependent on a custodian who is partially trusted but lacks the consensus. In the case of EngraveChain [22] created by Shekhtman and Waisbard, the hash values of the logs are anchored within the Hyperledger Fabric, which solves the problem of dependency on a single custodian but still operates in a permissioned environment. The proposed layer uses the approach of combining append only chains with Ethereum anchoring on a regular basis.

H. Ethereum Smart Contracts

Sahi et al. [24] integrate a public Ethereum identity layer with a permissioned Hyperledger Fabric exchange layer and validate only via an example in the healthcare sector without any gas or the latency measurements. Yigit and Dag [25] design a Solidity solution for supply chain events but identify gas cost and EVM scalability as open issues, confirmed by Ta and Do [26] by testing the gas usage and throughput on different chains under generic loads. None of these studies examines the issue of welfare distribution, where sensitive data and budget constraints come into play and our layer stores only hashes, timestamps, and IDs on Sepolia, motivated directly by the [26].

I. Hybrid Blockchain Architecture

On-chain or off-chain segregation was introduced by Singh et al. [27] for Indian PDS systems but the research is limited to the architecture design without a functional system implementation. While extending this approach to the healthcare services via hOCBS model by Miyachi and Mackey [29], the empirical validation of the framework is yet again being ignored. Sharmin et al. [28] fill in the gap using AES encryption, IPFS storage, and Merkle batched hashing on Sepolia testnet with 99.85% gas savings, but this is the only one of the three that includes the real test net validation, although IPFS causes most latency in it.

J. AI-Based Fraud Detection

Kumar et al. [30] achieve the 99.3% accuracy in identifying the income statement of the manipulation using Random Forest, yet their learning is purely offline through the use of self-reported data. Alexopoulos et al. [31] model the network of VAT transactions using a weighted graph and classify using the algorithm XGBoost, well-fitted for the fraud but requires a fairly complete history of the network. Mienye and Jere [32] provide an overview of deep learning models used for card fraud detection while not addressing any welfare specific challenges.

K. ML for Anomaly Detection

immutable and auditable but validated only on a single known node testbed. Dadhania and Patel's e-DRBAC-HC [44] layers IoT sourced data and token verification on a ledger for healthcare. None targets the welfare distribution; the proposed layer adapts the role hierarchy for Admin, Shopkeeper, and Beneficiary architecture, and does not validate any of those approaches in the context of the domain data. The work of De Medeiros et al. However, Darban et al. [33], though categorizing the anomalies detection papers by the objectives and [34] limits its scope to IoT and sensor networks, emphasizing on the practical challenges relevant to the implementation on a load cell level on a constrained platform. In their paper, Alarfaj et al. [35] test different classifier models on an imbalanced credit card dataset having accuracy of close to 99.9%, but validation is only on the finance.

© 2026 IJIRCCE | Volume 14, Issue 10, October 2026 DOI: 10.15680/IJIRCCE.2026.1410015

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

L. Digital Wallet Systems

According to Jaffer et al., [36], about USD 60 billion is expected from welfare subsidies out of which around 40% is estimated to have been lost to the inefficiencies, and they suggest the use of a permissioned blockchain with Aadhar number hashing into entitlement tokens. Similarly, Bakare et al.
[37] use the same concept for subsidies for agriculture. In a more advanced application, Pawar et al. [38] adopt an approach based on stakeholder methodology and a pilot solution, but without the quantity verification.

M. Supply Chain Transparency

Hash chains have been incorporated into RFID tags on the Hyperledger Fabric platform by Wang et al. [39]. This approach has been tested in the context of beverages, though it is limited by RFID memory and consensus overhead. The work of the Wanget al. [40] combines microservices with domain driven design, opting to sacrifice interoperability for the storage efficiency. The effort by Omar et al. [41] seeks to address the traceability of PPE in times of COVID-19 on Ethereum, while only managing its 15 transactions-per-second limit at less than $1.70 per transaction.

N. Role-Based Access Control

Sandhu et al. RBAC0–RBAC3 models [42] established the vocabulary later; the systems still use it, though purely as an abstract reference model. Ri, Kim, and Jong [43] encode the role assignment as a smart contract on Hyperledger Fabric, making the constraints panels with the contract enforced, role gated ledger writes it.

III. COMPARATIVE ANALYSIS

Table I and Table II combined the surveyed literature. No row in either table represents a paper combining hash chaining, smart contracts, hybrid synchronization, and cloud hosting for the welfare distribution specifically and each building block is individually mature but never assembled for this purpose.

Table 1: Comparative Summary of Blockchain and Ledger-Based Approaches to PDS

Paper / Topic Area	Year	Technology	Advantages	Limitations / Gap	Relevance to Proposed System
Blockchain in PDS [4]–[6]	2019–2022	Permission	Demonstrates tamper-evidence feasibility	Not evaluated at NFSA scale; no national throughput data	Validates ledger-anchoring concept; scale must be addressed
Blockchain for food supply chains [7]–[9]	2016–2020	Consortium blockchain	Improves upstream transparency	Focuses on logistics, not last-mile dispensation	Informs upstream traceability layer only
Cryptographic hash chains [21]–[23]	1991–2023	Hash-linked ledgers	Lightweight, low compute cost	No consensus mechanism; single-writer trust	Basis for proposed hash-linked ledger design
Ethereum smart contracts [24]–[26]	2023–2024	EVM-based contracts	Enforceable, auditable business logic	High gas cost, limited throughput	Justifies selective on-chain anchoring, not full storage
Paper / Topic Area	Year	Technology	Advantages	Limitations / Gap	Relevance to Proposed System
Hybrid blockchain architecture [6], [28], [29]	2021–2025	Blockchain + relational DB	Balances performance and tamper-evidence	Synchronization layer is new trust point	Direct architectural precedent for proposed system
Cloud-based government systems [45]–[48]	2012–2024	Gov cloud / hybrid cloud-blockchain	Establishes shared-infrastructure baseline	Institutional adoption risk, not technical	Confirms PostgreSQL-cloud + Ethereum pattern feasibility

© 2026 IJIRCCE | Volume 14, Issue 10, October 2026 DOI: 10.15680/IJIRCCE.2026.1410015

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Table 2: Comparative Summary of Authentication, IoT, and AI-Based Monitoring Approaches

Paper / Topic Area	Year	Technology	Advantages	Limitations / Gap	Relevance to Proposed System
IoT-based smart ration distribution	2021 – 2024	Load-cell/weight sensors	Independent physical verification of quantity	Rarely integrated with authentication or ledger	Provides ground-truth input for dispensation records
Aadhaar authentication	2021 – 2024	Biometric (fingerprint/iris)	Strong identity binding	False rejection among elderly/manual-labour users	Retained as primary factor needs fallback layer
QR-based authentication	2021 – 2024	QR code + mobile scan	Low hardware cost, offline-tolerant	Vulnerable to replay without OTP binding	Basis for proposed multifactor authentication flow
Digital wallet systems	2021 – 2024	App/DB-based wallet ledger	Simplifies subsidy accounting	Wallet integrity depends entirely on backend trust	Wallet balance changes anchored via hash-linked ledger
Role-based access control	2021 – 2024	RBAC on web application layer	Mature, well-understood pattern	Disconnected from ledger-write permissions	Extended to govern who may trigger ledger writes
AI/ML fraud & anomaly detection	2021 – 2024	Supervised / unsupervised ML	High classification accuracy (85–99%)	Not deployed on live/streaming data	Proposed as streaming layer over live transaction feed

IV. DISCUSSION

Across all fifteen areas there is one problem that keeps coming up again. The problem is making a system that gives out a lot of things like food to people who do not have a lot of money and also making sure that this system is fair and works well. The blockchain is being used in this system to make it work better. At first people were just testing the blockchain with projects but now they are using it in bigger and more complicated ways. They are only using the blockchain for the important parts of the system because it is too expensive to use it for everything. This is like what CloudGuardian does. The other problem is that the blockchain cannot solve everything on its own. For example if the system says that 5kg of food were given out but really 4kg were given out then the system is not working correctly. This is a problem that IOT is trying to solve. The blockchain and IOT both are used here to make the system work better to make sure that it is fair and make sure that people are getting the things they need. Hybrid blockchain and the hash chain and the cloud government research all have one thing in common. They all are using a database for everyday things. It also has a layer that is only for keeping track of important events. This extra layer is special because you can only add things to it you cannot change what is already there. What is the difference about these systems is where they draw the line between what is in the database and what goes in the special layer when we have a lot of data like the NFSA has. Government studies show the deployment success depends on institutional acceptance and on the technical capability. Some departments do not want to use the systems because they like being in control of records. On the security side, Aadhaar biometrics is the main identity, some older people and people who are in labor are having trouble with it. So now people are looking at it using ways to prove who they are like QR code and OTP. These are the new ways not meant to replace the biometric but to help when they are not in working. This is called RBAC, it is not often used with the blockchain of a device. In the fraud detection literature, there is an emphasis on high accuracy when looking at the past transactions but this is almost never tested in the live streams while the growth problem consistently points to the throughput and gas fees as the two major limiting factors. The success of the pilots on the other hand does not translate to implementation due to lack of rural connectivity, organizational pushback, and the absence of standards for interoperability of the state of systems.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. RESEARCH GAPS

The analysis above identifies twelve important gaps which still need attention: (1) there is no real-time quantity verification which integrated with authentication, ledger based flow; (2) no tamper-proof audit trail validated on a national NFSA scale; (3) interoperability across state systems is weak even through ONORC require portability; (4) full on chain storage struggles with scalability, with off-chain boundaries which are rarely defined; (5) public-chain transactions generally cost high, with not having PDS-specific cost comparison across consortium chains, sidechains and selective anchoring; (6) Biometric authentication failures persist, and there is no validated fallback hierarchy; (7) There is a risk of reidentification from hashed identifiers with no data minimization plan for welfare use; (8) Machine Learning fraud detection is almost never applied against live transaction streams; (9) hybrid synchronization layers introduced that they are themselves new single points of failure; (10) hybrid designs built for generic workloads instead of PDS's high-frequency, low-value and intermittently connected profile; (11) IoT weight validation left disconnected from authentication and ledger writing mechanisms; and (12) monitoring dashboards that only summarize batch uploads instead of offering continuous, AI-alerted. All of this point leads to only one conclusion that the component technologies exist but no combined architecture integrates physical verification, layered authentication, selective anchoring, and continuous analytics into one of the secure and scalable systems.

VI. CONCLUSION AND FUTURE WORK

The literature review indicates that the technologies required to make India's Public Distribution System (PDS) more transparent, secure, and accountable are available. Blockchain technology ensures transaction integrity, the Internet of Things (IoT) enables physical verification of food grain quantities, layered multifactor authentication verifies beneficiaries, digital wallets track monthly entitlements, and Artificial Intelligence (AI) helps detect suspicious transactions. However, most existing studies focus on only a limited combination of these technologies. To address this gap, we propose a PDS Digital Supervision Layer, a hybrid approach that integrates these technologies into the existing PDS infrastructure to improve transparency, accountability, and fraud detection. The next step is to implement a prototype and evaluate it in a controlled environment using real-world transaction scenarios. The evaluation will focus on transaction latency, IoT device reliability, blockchain performance, and overall system security and robustness. Future enhancements may include lightweight AI models for edge devices, Layer 2 blockchain solutions to reduce transaction costs, cryptographic mechanisms to strengthen privacy, and interoperability with nationwide initiatives such as the One Nation One Ration Card (ONORC) scheme.

REFERENCES

1. R. Kumar, L. Ganapathy, R. Gokhale, and M. K. Tiwari, "Scaling up the digitalization of the public distribution system: A COVID- 19 pandemic impetus," IFAC-PapersOnLine, vol. 55, no. 10, pp. 55–60, 2022. N. Nagaraj and A. Prakash, "Digital biometric authentication and citizens' right to food: Neglect of the 'local' in India's Aadhaar-enabled PDS," in Proc. ICEGOV 2021, Athens, Greece, 2021, pp. 1–11.
2. K. Gupta, P. Soni, K. Rautela, and K. Srinivas, "Uptake, imple- mentation, portability, and operability of the one nation one ration card," ADB Briefs, no. 270, Manila, Philippines, Nov. 2023.
3. D. Malathi, V. Ponnusamy, S. Saravanan, D. Deepa, and T. A. Ahanger, "A design framework for smart ration shop using blockchain and IoT technologies," Intell. Autom. Soft Comput., vol. 32, no. 1, pp. 605–619, 2022.
4. A. N. Shwetha and C. P. Prabodh, "Blockchain – bringing ac- countability in the public distribution system," in 2019 4th Int. Conf. RTEICT, Bangalore, India, 2019, pp. 330–335.
5. S. K. Singh, M. Jenamani, D. Dasgupta, and S. Das, "A conceptual model for Indian public distribution system using consortium blockchain," Inf. Technol. Dev., vol. 27, no. 3, pp. 499–523, 2021.
6. F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in Proc. 2016 ICSSSM, Kunming, China, 2016, pp. 1–6.
7. M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, "Blockchain- based traceability in Agri-Food supply chain management," in Proc. IOT Tuscany 2018, 2018, pp. 1–4.
8. D. Prashar, N. Jha, S. Jha, Y. Lee, and G. P. Joshi, "Blockchain- based traceability and visibility for agricultural products," Sus- tainability, vol. 12, no. 8, p. 3497, 2020.
9. S. Shukla, A. M. Patil, and B. Selvin M., "A step towards smart ration card system using RFID & IoT," in Proc. 2018 ICSCET, Mumbai, India, 2018, pp. 1–5.
10. B. G. Priya and S. Nikumbh, "E – Public distribution system us- ing SMART card and GSM technology," in Proc.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

2017 ICISS, Palladam, India, 2017.
11. S. Indirani, S. Subaselvamanikandan, M. Nishanth, and S. Srin- isha, "Smart ration card distribution system," J. Electr. Syst., vol. 20, no. 11s, 2024.
12. N. Nagaraj and A. Prakash, "Digital biometric authentication and citizens' right to food," in Proc. ICEGOV '21, Athens, Greece, Oct. 2021.
13. H. S. Hundal and B. Chaudhuri, "Digital identity and exclusion in welfare: Notes from the PDS in Andhra Pradesh and Karnataka," in Proc. ICTD '20, Guayaquil, Ecuador, Jun. 2020, art. 29, pp. 1–5.
14. B. Chaudhuri, "Programmed welfare: An ethnographic account of algorithmic practices in the PDS in India," New Media Soc., vol. 24, no. 4, pp. 887–902, 2022.
15. K. Muralidharan, P. Niehaus, and S. Sukhtankar, "Identity ver- ification standards in welfare programs: Experimental evidence from India," Rev. Econ. Statist., vol. 107, no. 2, pp. 372–392, 2025.
16. N. Nagaraj and A. Prakash, "Digital biometric authentication and citizens' right to food: Neglect of the 'local'," in Proc. ICEGOV 2021, Athens, Greece, 2021, pp. 338–345.
17. S. Menon, "Aadhaar-based biometric authentication for PDS and food security: Observations from Jharkhand's Ranchi District," Indian J. Human Dev., vol. 11, no. 3, pp. 387–401, 2017.
18. Y.-W. Kao, G.-H. Luo, H.-T. Lin, Y.-K. Huang, and S.-M.
Yuan, "Physical access control based on QR code," in Proc. 2011 Cy- berC, 2011, pp. 285–288.
19. N. Gangurde, S. Ghosh, A. Giri, and S. Gharat, "Ticketing system using AES encryption based QR code," in Proc. 2022 ICSSIT, 2022, pp. 201–206.
20. S. Haber and W. S. Stornetta, "How to time-stamp a digital docu- ment," J. Cryptology, vol. 3, no. 2, pp. 99–111, 1991.
21. L. Shekhtman and E. Waisbard, "EngraveChain: A blockchain- based tamper-proof distributed log system," Future Internet, vol. 13, no. 6, art. 143, 2021.
22. D. Koisser and A.-R. Sadeghi, "Accountability of things: Large-scale tamper-evident logging for smart devices," arXiv:2308.05557, 2023.
23. M. Sahi, A. Liang, W. Van Devanter, K. Oikonomou, and
P. Zhang, "Self-sovereign identity in semi-permissioned blockchain networks," in Proc. 2023 IEEE ICDH, 2023.
24. E. Yigit and T. Dag, "Improving supply chain management pro- cesses using smart contracts in the Ethereum network," Appl. Sci., vol. 14, no. 11, art. 4738, 2024.



INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details