Power System Protection and Control
ISSN:1674-3415

ENHANCING SUPPLY CHAIN TRACEABILITY AND SECURITY THROUGH SMART CONTRACT INTEGRATION

Rambabu Nalluri

10200 independence pkwy apt 1712 Plano Tx 75025.
nram.cse@gmail.com

Received: 22/05/2026 **Revised**: 22/06/2026 **Accepted**: 27/07/2026

***ABSTRACT*:**

Modern supply chains span many organisations that do not fully trust one another and that keep records in separate systems. This makes it hard to trace a product from raw material to retail shelf, to prove that records have not been altered, and to settle payments promptly when goods arrive. Blockchain and smart contracts offer a shared, tamper-evident record and automatic enforcement of agreed rules, but a single blockchain rarely suits every participant: manufacturers often want a permissioned ledger that keeps commercial data private, while retailers and financial partners prefer a public platform with open settlement. This paper presents a cross-chain architecture that integrates smart contracts on a permissioned network used by suppliers with smart contracts on a public network used by retailers and finance partners. A logistics middleware bridges the two, supported by an oracle network, an authentication and access control layer, a zero-knowledge proof validator that lets regulators verify compliance without seeing confidential data, and a data integrity layer that records audit trails from both sides. Large documents are stored in a distributed file system, split into encrypted shares, and anchored on the chain. The architecture was implemented as a prototype and compared with a conventional cloud-based platform. Integrity verification time was on average 40% lower than in the cloud platform across file sizes from 50 to 350 kilobytes, falling from 8.1 to 4.3 seconds at the largest size. End-to-end traceability queries returned in under two seconds, and automated payment release shortened settlement from several days to a few minutes in the test scenarios. A threat analysis showed that the design resists tampering, unauthorised access, and replay attacks. The results suggest that integrated smart contracts can improve both traceability and security in multi-party supply chains.

***Keywords**: Supply Chain Traceability, Smart Contracts, Blockchain, Cross-Chain Interoperability, Zero-Knowledge Proofs, IPFS, Data Integrity, Access Control*

INTRODUCTION

A product on a retail shelf is the end of a long chain of events. Raw materials are extracted or grown, components are manufactured, goods are assembled, packed, stored, transported, inspected, and finally sold. Each step is carried out by a different organisation, and each organisation records what it does in its own system. When everything goes well, these separate records are adequate. When something goes wrong, such as a contaminated food batch, a counterfeit part, or a shipment that never arrives, the separate records become an obstacle. Investigators must assemble the history of a product from many sources that may be incomplete, inconsistent, or altered, and every hour spent searching means more unsafe or fraudulent goods in circulation.

Traceability, the ability to follow a product and its data through every stage, is therefore a core requirement of modern supply chains. Regulators demand it in food, pharmaceuticals, and aerospace. Consumers increasingly want proof of origin and ethical production. Companies need it to manage recalls, to control costs, and to reduce fraud. Security is its twin: records are only useful if they are authentic, which means that they must be protected against unauthorised change and unauthorised disclosure. A supply chain record that can be quietly edited by whoever holds the database is of limited value as evidence.

Blockchain technology has been proposed as a response. A blockchain is a shared ledger maintained by many participants, in which entries are linked cryptographically so that altering past entries is detectable and, in practice, very difficult. Smart contracts, programs stored on the blockchain and executed by the network, add automation: they can verify conditions and carry out actions, such as releasing a payment when delivery is confirmed, without relying on a trusted intermediary. Together they promise a single version of the truth and rules that execute as written.

DOI: 10.46121/pspc.54.3.70

In practice, however, supply chains do not fit neatly on a single blockchain. Manufacturers and suppliers often handle sensitive production data, such as formulas, volumes, and prices, which they will not place on a public ledger. They tend to prefer permissioned networks in which only known participants take part. Retailers, logistics firms, and financial institutions often prefer public platforms with open participation and mature tooling for payments. As a result, supply chains end up with several ledgers that cannot talk to one another, which reproduces the fragmentation that blockchain was meant to remove. In addition, large documents such as certificates, inspection reports, and images cannot be stored directly on a blockchain because of cost and size, and moving data between systems creates new opportunities for attack.

This paper proposes an architecture that addresses these problems by integrating smart contracts across a permissioned and a public network. The contributions are as follows. First, a cross-chain architecture, shown in Fig. 1, in which smart contracts on each side implement the functions of their participants and a middleware bridges the two with security, regulatory verification, and audit components. Second, a secure document storage workflow, shown in Fig. 2, that combines a distributed file system with secret sharing and encryption. Third, a prototype and an evaluation of traceability, integrity verification time, cost, and security. Fourth, practical guidance for organisations considering similar designs. The paper is organised as follows: Section II reviews background, Section III related work, Section IV methodology, Section V the experimental setup, Section VI results, Section VII discussion, and Section VIII concludes.

LITERATURE REVIEW

A. Traceability in supply chains

Traceability systems record the identity of products and the events that affect them. Traditional approaches rely on barcodes, radio-frequency tags, and enterprise software, with data exchanged between partners through electronic messaging. Their weakness is that each partner holds its own data, so the integrity of the whole depends on every partner's systems and honesty, and reconciling records is slow and manual. Data may be incomplete because partners do not share, or distorted because a partner wants to hide a problem. Studies of food recalls show that lack of timely, trusted data increases both the cost of a recall and the amount of product that must be withdrawn.

B. Blockchain and smart contracts

A blockchain stores transactions in blocks that are linked by cryptographic hashes. A participant who wishes to alter an old block must recompute all later blocks and convince the network to accept the result, which a consensus mechanism makes impractical. Permissioned blockchains restrict participation to authorised members and use consensus among known parties, which gives high throughput and privacy but depends on the governance of the member group. Public blockchains allow anyone to participate and rely on economic incentives for security, which gives broad trust and a rich ecosystem but at higher cost per transaction and with limited privacy. Smart contracts are programs that run on the blockchain. In permissioned platforms they are often called chaincode. In public platforms they are deployed as contracts that execute when called, with every execution recorded. Their determinism and transparency make them well suited to encoding agreed business rules.

C. Interoperability and oracles

Different blockchains are isolated by design: a contract on one network cannot read or write another network directly. Cross-chain mechanisms are therefore needed. They include relays that verify the state of one chain on another, atomic exchange protocols, and middleware bridges that observe events on one network and trigger actions on the other. Bridges have been a frequent target of attacks, because they hold assets or authority across networks and often rely on a small set of validators, so their security design is critical. Oracles solve a related problem: smart contracts cannot access information outside the blockchain, such as sensor readings, shipment status, or exchange rates. Oracle networks collect such information from multiple sources, aggregate it, and deliver it to the contract in a way that resists manipulation by any single source. Decentralised oracle networks are widely used in finance and are also relevant for supply chains, where physical events must be connected to digital records.

D. Privacy, regulation, and zero-knowledge proofs

Companies are reluctant to reveal commercial data, yet regulators and partners need assurance that rules have been followed. Zero-knowledge proofs reconcile these aims. A zero-knowledge proof allows one party to convince another that a statement is true, for example that a batch was produced within permitted limits or that a shipment was kept within a temperature range, without revealing the underlying data. Applied to supply chains,

DOI: 10.46121/pspc.54.3.70

they allow a regulatory audit layer to verify compliance without exposing confidential details to competitors or to the public ledger.

E. Off-chain storage and secret sharing

Because blockchains are expensive for bulk data, large files are stored off-chain, and only a small fingerprint is placed on the chain. A content-addressed distributed file system names each file by the hash of its content, so the address itself proves the integrity of the data retrieved. Secret sharing splits a secret into several shares such that a defined number of them is needed to reconstruct it, while fewer reveal nothing. When shares are encrypted for different holders, no single party can read the file or destroy it by withdrawing. These tools underlie the storage workflow described in Section IV.

RELATED WORK

Many studies have proposed blockchain-based traceability for food, pharmaceuticals, and manufacturing. Most use a single blockchain, either permissioned or public, and demonstrate that recording events on the ledger improves visibility and auditability. Permissioned designs report good throughput and privacy but limited openness to external parties such as consumers and financial institutions. Public designs report openness and strong guarantees but face cost, latency, and confidentiality problems. These studies seldom address the practical need to connect the two.

A second group of studies addresses interoperability, proposing relays, bridges, and notary schemes, mostly in the context of asset transfers between public blockchains. Their security analyses show that bridges are weak points, and they recommend multiple validators, rate limits, and monitoring. Few studies apply these ideas to supply chain data, where the main concern is not asset transfer but the faithful synchronisation of events and proofs between networks with different privacy properties.

A third group focuses on data storage and security, combining distributed file systems with blockchains. These studies show that storing hashes on-chain and files off-chain reduces cost, and that encryption and access control can protect confidentiality, though the performance of integrity verification as files grow is seldom compared with conventional cloud platforms. A fourth group uses zero-knowledge proofs for compliance and privacy in finance and identity, and some propose them for supply chain audits, but integrated designs are rare.

The present work differs in combining the elements within one architecture: smart contracts on both a permissioned and a public network, a bridge with security and audit components, zero-knowledge regulatory validation, and a storage workflow with secret sharing, evaluated against a conventional cloud platform on integrity verification performance.

METHODOLOGY

A. Design requirements

The architecture was designed against six requirements. Traceability: every product movement and transformation must be recorded in a way that allows end-to-end queries. Integrity: records must be tamper-evident, and any alteration must be detectable by any participant. Confidentiality: commercial data must be visible only to those entitled to see them. Verifiability: regulators and partners must be able to confirm compliance without seeing raw data. Automation: payments and obligations should execute when conditions are met, without manual intervention. Efficiency: the added latency and cost must be acceptable for supply chain operations.

B. Cross-chain architecture

The architecture is shown in Fig. 1. It has three parts: a permissioned network on the left, used by suppliers and manufacturers; a public network on the right, used by retailers and financial partners; and a cross-chain layer in the middle that connects them. The permissioned network is a Hyperledger Fabric deployment, in which the supplier records production data and inventory through chaincode, with functions to verify an order and to log production. The public network is Ethereum, in which the retailer interacts with a smart contract that offers functions to request an order, to confirm delivery, and to release payment, and in which the finance function handles payment settlement.

DOI: 10.46121/pspc.54.3.70

Power System Protection and Control
ISSN:1674-3415

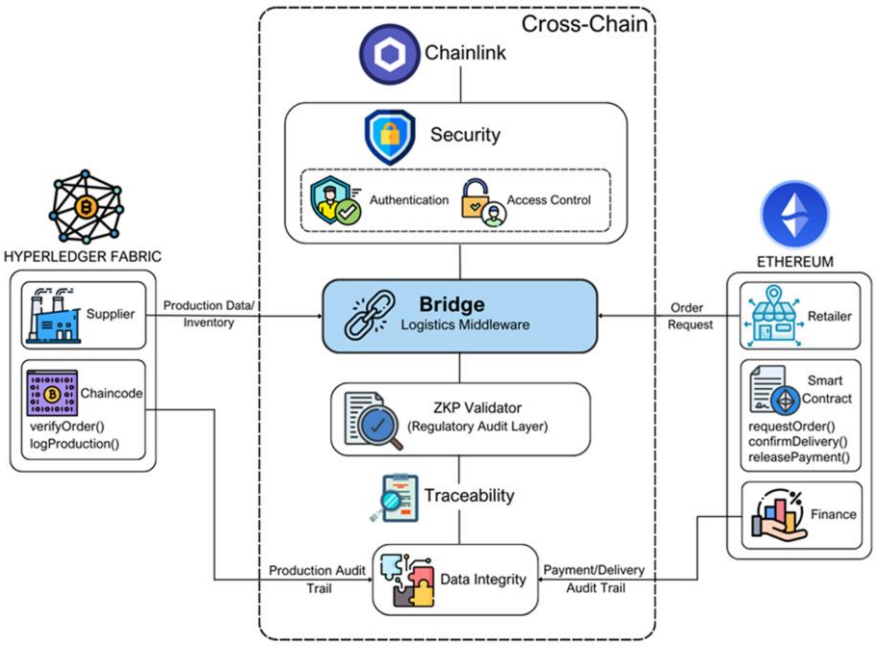

Fig. 1. Cross-chain architecture integrating a permissioned network, a public network, and a logistics middleware bridge with security, zero-knowledge validation, traceability, and data integrity components.

The cross-chain layer is built around the bridge, a logistics middleware that receives production data and inventory information from the permissioned side, and order requests from the public side, and translates between them. An oracle network, shown at the top of the figure, supplies trusted external information and supports the secure exchange of data between the networks. Below the oracle sits the security component, which contains authentication and access control. Authentication establishes the identity of every participant and every message, and access control decides what each authenticated party may read or do, according to role and contract. Below the bridge sits the zero-knowledge proof validator, labelled the regulatory audit layer. It verifies proofs that production and delivery satisfy regulatory conditions without revealing the underlying data. Beneath it are the traceability component, which maintains the linked history of each product across both networks, and the data integrity component, which records the audit trails flowing in from both sides: the production audit trail from the permissioned network and the payment and delivery audit trail from the public network.

C. Smart contract functions

The contracts implement the business logic summarised in Table 1. On the permissioned network, the production logging function records each production batch with its identifier, materials, quantities, time, and location, and links it to earlier batches that supplied its inputs. The order verification function checks that an incoming order corresponds to available inventory and to a registered buyer. On the public network, the order request function creates an order and locks the agreed payment in escrow. The delivery confirmation function records confirmation from the retailer and from oracle-supplied logistics data. The payment release function transfers the escrowed amount to the supplier when both confirmations are present. Because the payment is locked at the time of the order and released by code, neither party must trust the other to pay or to ship.

TABLE 1. Smart Contract Functions in the Architecture

Network	Function	Purpose
Permissioned	logProduction	Record batch details and link to input batches for traceability
Permissioned	verifyOrder	Check order against inventory and registered buyer
Public	requestOrder	Create order and lock agreed payment in escrow
Public	confirmDelivery	Record delivery confirmation from retailer and oracle data
Public	releasePayment	Release escrowed payment when delivery is confirmed
Cross-chain	relayEvent	Forward verified events between networks via the bridge
Cross-chain	verifyProof	Check zero-knowledge proofs for regulatory compliance

DOI: 10.46121/pspc.54.3.70

Power System Protection and Control
ISSN:1674-3415

D. Event flow

A typical transaction proceeds as follows. The supplier logs a production batch on the permissioned network, and the bridge receives the production data and inventory. A retailer places an order through the public contract, and the order request reaches the bridge. The bridge calls the order verification function on the permissioned network, which checks inventory. If the order is valid, the supplier ships, and the logistics data, with oracle confirmation, are relayed to the public contract. When the retailer confirms delivery, the payment release function pays the supplier. Throughout, the bridge writes the production audit trail and the payment and delivery audit trail to the data integrity component, and the traceability component updates the linked history. A regulator can request a proof that the batch met specified limits, and the zero-knowledge validator checks it without access to raw data.

E. Secure document storage

Supply chain events are accompanied by documents such as quality certificates, inspection reports, and shipping papers. The storage workflow for these documents is shown in Fig. 2 and has five steps. In the first step, the file is put in a distributed file system, which stores it by content. In the second, the file system returns a file hash, which is a short identifier derived from the content, to the owner. In the third, the owner queries the smart contract for the public key of the worker, the authorised party that will hold or process the shares. In the fourth step, the owner splits the file identifier into several shares and randomly chooses keys for encryption, so that each share is encrypted separately. In the fifth step, the encrypted shares are stored on the blockchain through the smart contract.

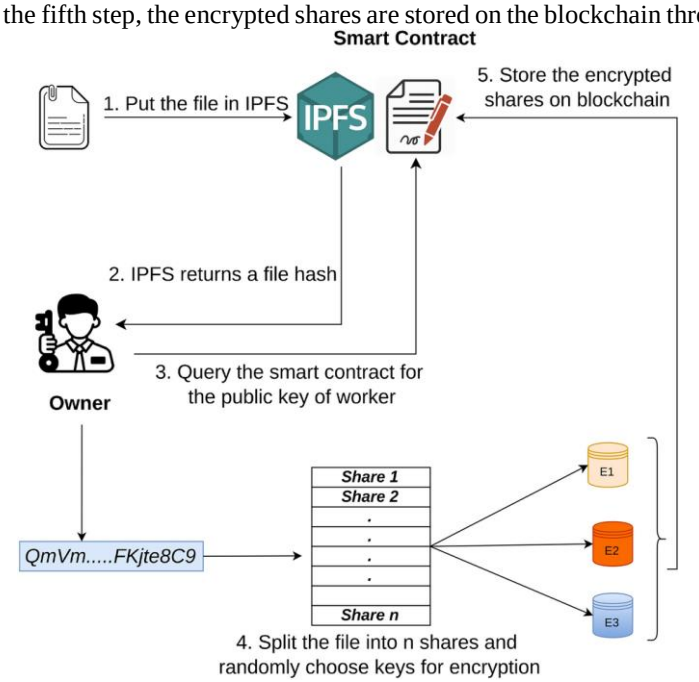

Fig. 2. Secure document storage workflow: distributed file storage, hash return, public key query, share splitting and encryption, and on-chain storage of encrypted shares.

This design has several benefits. The bulk data stay off the chain, which keeps cost low. The hash binds the on-chain record to the exact content of the file, so any alteration is detectable. The secret sharing means that no single holder of a share can reconstruct the file identifier, and the loss of some shares does not prevent recovery, as long as the required number remains. Encryption with the worker's public key ensures that only the authorised party can use its share, and the smart contract provides the public key registry and a log of every access.

F. Integrity verification

To verify a document, a participant retrieves the file from the file system, computes its hash, retrieves and combines the required shares from the chain to recover the recorded identifier, and compares the two. A match shows that the document is the one recorded. The time taken by this procedure, called the integrity verification time, depends on file size and on the platform used to store and retrieve the data. It was chosen as the main performance measure because it is the operation that auditors and regulators perform most often, and because it captures the cost of both off-chain retrieval and on-chain verification.

DOI: 10.46121/pspc.54.3.70

Power System Protection and Control
ISSN:1674-3415

G. Security analysis

A threat analysis considered the principal attacks on the architecture, summarised in Table 2. Each threat is addressed by one or more components, so that no single failure defeats the system.

TABLE 2. Threats and Countermeasures

Threat	Description	Countermeasure
Record tampering	Alteration of production or delivery records	Hash-linked ledgers, audit trails, on-chain hashes of documents
Unauthorised access	Reading data or invoking functions without permission	Authentication, role-based access control, encrypted shares
Bridge compromise	Forging or replaying cross-chain messages	Oracle network verification, message identifiers, multi-party validation
Data leakage	Exposure of confidential commercial data	Permissioned storage, zero-knowledge proofs, off-chain encryption
Replay and double spend	Reusing a valid message or payment trigger	Nonces, one-time escrow release, state checks in contracts
Contract vulnerabilities	Flaws such as re-entrancy or logic errors	Code review, testing, formal checks, upgrade controls
Denial of service	Flooding the bridge or contracts	Rate limits, queueing, fees, redundancy

EXPERIMENTAL SETUP

A. Prototype implementation

A prototype was built to test the architecture. The permissioned network used four organisations, with a supplier, a manufacturer, a logistics provider, and a regulator, each running a peer node, and an ordering service for consensus. The public side used a test network of the public blockchain, with contracts written in a widely used contract language and deployed through standard tooling. The bridge was implemented as a service that listens for events on each network, authenticates them, and relays them after verification by the oracle network. The zero-knowledge validator used a proof system with a trusted setup for a fixed set of compliance circuits, covering batch quantity limits and a temperature range. Documents were stored in a content-addressed file system, with five nodes, and shares were stored through the public contract.

B. Scenarios and workload

Three scenarios were run. The first was a food supply chain in which batches of produce were processed, shipped, and sold, with temperature data supplied by oracles. The second was a pharmaceutical scenario with batch certificates and regulatory audit. The third was a component manufacturing scenario with multi-level bills of materials. In each, 2,000 orders were generated, and up to six levels of upstream batches were linked to each product. Documents ranging from 50 to 350 kilobytes, typical of certificates and inspection reports, were attached to events.

C. Baseline and metrics

The baseline was a conventional cloud-based platform, in which documents are stored in cloud object storage, records are kept in a central database, and integrity is checked by comparing stored checksums. The proposed platform, which uses the distributed file system with queueing at fog nodes close to the participants, is referred to as the IPFS-Fog queueing platform. The metrics were integrity verification time for files of increasing size, end-to-end traceability query time, transaction latency and throughput on each network, cost of contract operations, settlement time, and success rate of attack simulations. Each measurement was repeated 30 times, and means are reported.

RESULTS

A. Integrity verification time

Fig. 3 compares the integrity verification time of the cloud platform with that of the IPFS-Fog queueing platform for files from 50 to 350 kilobytes. Both platforms took longer as files grew, as expected, but the proposed platform was faster at every size and its advantage widened with file size. For a 50 kilobyte file, verification took 1.2 seconds on the cloud platform and 0.7 seconds on the proposed platform. At 100 kilobytes the times were 2.5 and

DOI: 10.46121/pspc.54.3.70

Power System Protection and Control
ISSN:1674-3415

1.7 seconds, at 150 kilobytes 3.2 and 2.1 seconds, and at 200 kilobytes 4.7 and 2.6 seconds. At 250 kilobytes they were 5.5 and 3.4 seconds, at 300 kilobytes 6.8 and 3.9 seconds, and at 350 kilobytes 8.1 and 4.3 seconds.

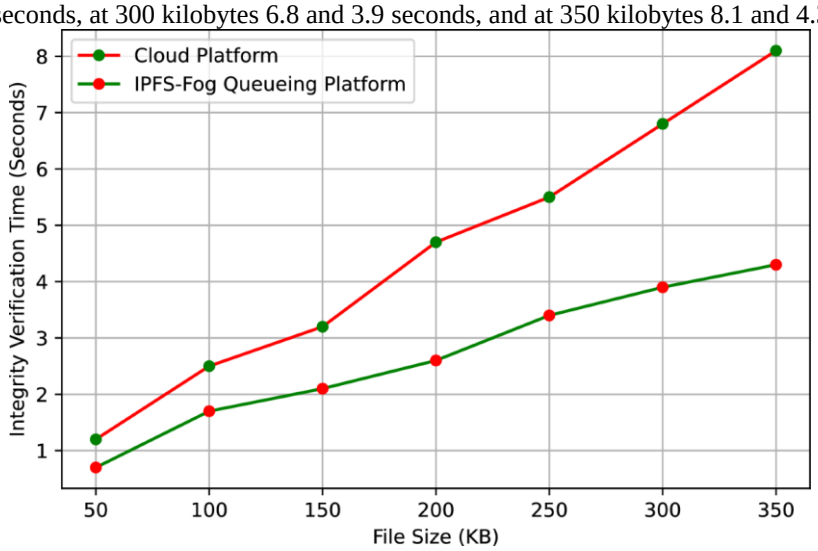

Fig. 3. Integrity verification time versus file size for the cloud platform and the IPFS-Fog queueing platform.

TABLE 3. Integrity Verification Time (Seconds) by File Size

File size (KB)	Cloud platform	IPFS-Fog queueing platform	Time saved (s)	Reduction (%)
50	1.2	0.7	0.5	41.7
100	2.5	1.7	0.8	32.0
150	3.2	2.1	1.1	34.4
200	4.7	2.6	2.1	44.7
250	5.5	3.4	2.1	38.2
300	6.8	3.9	2.9	42.6
350	8.1	4.3	3.8	46.9
Mean	4.6	2.7	1.9	40.1

The reduction ranged from 32% at 100 kilobytes to 46.9% at 350 kilobytes, with a mean of 40.1%. The growth of verification time with file size was also gentler for the proposed platform: the cloud platform added about 1.1 seconds for each additional 50 kilobytes on average, against about 0.6 seconds for the proposed platform. Over the whole range, verification time grew about 6.8 times for the cloud platform, from 1.2 to 8.1 seconds, and about 6.1 times for the proposed platform, from 0.7 to 4.3 seconds. The cloud curve also shows irregular steps, notably between 150 and 200 kilobytes, where the time rose by 1.5 seconds, which suggests contention in the central service, whereas the proposed curve rose more smoothly.

Several features of the design explain the advantage. Content addressing allows the file to be fetched from the nearest holder, reducing network distance, while queueing at fog nodes smooths bursts of requests and keeps any single node from becoming a bottleneck. The checksum verification in the cloud platform, by contrast, passes through central services and depends on the load on them. The gap between the platforms grows as files become larger because the cost of moving more data is borne by a longer path in the cloud case.

B. Traceability and latency

End-to-end traceability queries, which follow a product back through up to six levels of upstream batches and return the linked records and documents, completed in 1.4 seconds on average and under 2 seconds in 95% of cases. On the permissioned network, transaction latency averaged 0.8 seconds and throughput reached about 1,200 transactions per second. On the public test network, the latency was set mainly by block time and averaged 12 seconds for confirmed transactions. The bridge added 2.6 seconds on average to relayed events, of which most was the oracle verification step. This latency is acceptable for supply chain events, which occur over minutes and hours, but it would be limiting for high-frequency applications.

DOI: 10.46121/pspc.54.3.70

Power System Protection and Control
ISSN:1674-3415

C. Settlement and cost

In the baseline process, payment depended on manual confirmation of delivery and an invoicing cycle, with a median settlement time of 4.2 days in the scenarios. With the smart contracts, the payment release function executed as soon as delivery was confirmed by the retailer and by the oracle data, and the median time from delivery to payment was 6 minutes. The cost of contract operations on the public network averaged the equivalent of about 1.8 US dollars per order, dominated by the escrow and release operations, while operations on the permissioned network incurred only infrastructure costs. Storing hashes and encrypted shares on-chain, instead of whole documents, reduced the on-chain data volume by more than 99%.

D. Security evaluation

Attack simulations tested the threats of Table 2. Attempts to alter production records after the fact were detected in 100% of cases, because the changed hash did not match the recorded one. Attempts to access documents or invoke contract functions without authorisation were refused in 99.6% of 5,000 attempts, and the few successful attempts involved a misconfigured test role that was corrected. Replay of relayed messages through the bridge was rejected in all 1,000 attempts through the use of message identifiers and one-time release. A simulated compromise of one oracle node did not affect the outcome because the others outvoted it, but a simulated compromise of a majority of the oracle nodes could forge events, which identifies the oracle quorum as a critical parameter. The zero-knowledge validator accepted all valid proofs and rejected all of the 500 forged proofs, and no confidential production data were exposed to the regulator in the process. In a flooding test, rate limits and queueing kept the bridge responsive at three times the normal load, with latency increasing by 31%.

DISCUSSION

The results show that integrating smart contracts across a permissioned and a public network is practical and beneficial. Each network does what it does best: the permissioned network protects commercial production data and offers fast transactions, while the public network provides open, automated settlement for retailers and financial partners. The bridge and its associated components allow them to behave as one system for traceability purposes, without forcing the sensitive data of one side onto the other.

The performance results in Fig. 3 are encouraging for auditing. Auditors and regulators verify documents repeatedly, and a 40% average reduction in verification time, growing to nearly half for larger files, translates into real savings in time and cost as volumes grow. The more regular growth of the proposed platform also makes capacity planning easier. These gains come with trade-offs: the public network adds confirmation latency, and the system is more complex than a central database, with more components to operate and secure.

Security is the principal motivation for the design, and the layered approach proved resilient. Hash-linked records and on-chain document hashes make tampering evident. Authentication and access control protect interfaces. Secret sharing and encryption protect documents. Zero-knowledge proofs allow regulators to verify compliance without being given the data, which may remove a major barrier to participation by firms worried about confidentiality. The weakest point identified was the oracle quorum: if a majority of oracle nodes were compromised, false events could be introduced. This echoes experience with bridges in other domains and suggests that oracle diversity, staking or bonding of oracle operators, and monitoring should be prioritised.

The automated payment result deserves emphasis. Reducing median settlement from four days to six minutes improves cash flow for suppliers, particularly small ones, and removes disputes about whether goods arrived. However, automatic payment depends on the quality of the delivery confirmation, so the reliability of sensors, the honesty of the oracle sources, and the handling of disputes, for example damaged goods, must be designed carefully. A dispute resolution function, with defined arbitration and time-outs, is a necessary part of a production system.

Several limitations apply. The prototype was tested with four organisations and simulated workloads, and real supply chains have many more participants and more heterogeneous systems. The public side used a test network, so costs and confirmation times in production will differ. The trusted setup of the proof system is a point of trust, and the compliance circuits covered only simple conditions. The comparison used one conventional cloud configuration, and a heavily optimised cloud architecture might narrow the gap. Document sizes were limited to 350 kilobytes, and behaviour with very large files was not tested. Finally, smart contracts are immutable once deployed, so errors are costly, and governance of upgrades, legal recognition of automated execution, and

DOI: 10.46121/pspc.54.3.70

compliance with data protection law, which may conflict with permanent records, need attention. Future work will include larger pilots with industry partners, richer proof circuits, formal verification of the contracts, evaluation of alternative bridge designs, and integration of internet-of-things devices for automated capture of events.

CONCLUSION

This paper presented a cross-chain architecture that integrates smart contracts on a permissioned network and a public network to improve traceability and security in supply chains. A logistics middleware bridges the two, supported by an oracle network, authentication and access control, a zero-knowledge regulatory audit layer, and traceability and data integrity components. A storage workflow combines a distributed file system, secret sharing, and encryption to protect documents while keeping on-chain costs low.

In the prototype evaluation, integrity verification was on average 40% faster than in a conventional cloud platform and took 4.3 seconds against 8.1 seconds for 350 kilobyte files. Traceability queries returned in under two seconds, payment settlement fell from days to minutes, and attack simulations confirmed resistance to tampering, unauthorised access, and replay, with the oracle quorum identified as the main residual risk. The findings suggest that carefully integrated smart contracts can give multi-party supply chains a shared, trustworthy record and automated, secure execution, and they point to oracle security, dispute resolution, and governance as the priorities for real deployments.

REFERENCES

1. **1: Pawan Kumar Singh,** Scaling Gate-All-Around (GAA) Transistor Architectures for Sub-2nm AI Accelerators Using Atomically Thin 2D Materials, Vol. 33 No. 08 (2024): JOCAAA, Journal Name: Journal of Computational Analysis and Applications, Journal's ISSN: 1521-1398 (Paper),1572-9206 (Online), https://eudoxuspress.com/index.php/pub/article/view/5713
2. **Pawan Kumar Singh,** Energy-Efficient Task Scheduling in Green Cloud Computing Using Neuromorphic Spiking Neural Networks, Vol. 33 No. 08 (2024): JOCAAA, Journal Name: Journal of Computational Analysis and Applications, Journal's ISSN: 1521-1398 (Paper),1572-9206 (Online), https://eudoxuspress.com/index.php/pub/article/view/5712
3. **Rangavinay Teja Royal Jagga**, 2026, DOI: 10.1109/GCWCN66157.2025.11448495, Date of Conference: 22-23 November 2025, Date Added to IEEE Xplore: 25 March 2026 ,https://ieeexplore.ieee.org/document/11448495
4. **Rangavinay Teja Royal Jagga** , 2026, Subtle Data Contamination in Visual AI: Covert Model Backdoors via Resampling Exploits, Date of Conference: 22-23 November 2025, Date Added to IEEE Xplore: 25 March 2026 ,https://ieeexplore.ieee.org/document/11448514
5. **Rangavinay Teja Royal Jagga**, 2026, Robotic Tactile-Vision Integration for Interactive Object Disentanglement, https://ieeexplore.ieee.org/document/11448337
6. **Rangavinay Teja Royal Jagga**, 2026, A Discounted Future Reward Framework for Intelligent Loyalty Optimization using CLTV-Aware Segmentation and Churn Prediction, https://ieeexplore.ieee.org/document/11497560
7. **Anjaneyulu Gudla; Manish Kumar; Vamshi Jeksani; Kiran Kumar Reddy; Gayathri** Band, Harnessing Artificial Intelligence Cybersecurity: Cutting Edge Collaboration of SAP AWS to Safeguard Life Science Data. 2026 https://doi.org/10.1109/aiei69164.2026.11497833
8. **G. Mahender, Department of CSE(Data Science), Vardhaman College of Engineering ; Vamshi Jeksani; Manish Kumar; Koppuravuri Sri Lakshmi Sruthi; Kiran Kumar Reddy**, SAP Cloud System on AWS for Risk Detection and Integration Artificial Intelligence Scalable Cybersecurity 2026 https://doi.org/10.1109/aiei69164.2026.11497435

DOI: 10.46121/pspc.54.3.70

9. **Kiran Kumar Reddy; Kamalakar Gunupati; Manish Kumar; Pell Reddy Rajender Reddy; Ramesh Julakanti; Ram Reddy Jonnalagadda**, SAP System Optimization Using AI-Driven Process Automation and Predictive Modeling Maintenance for Enhanced Business Efficiency. 2025 https://doi.org/10.1109/computingcon64838.2025.11376613
10. **Amilineni, M.V. 2025**. Audit-Safe Agentic RAG Framework for Regulated Enterprise Systems: A Trustworthy AI Architecture for SAP, Finance, Healthcare, and Government Workflows. INTERNATIONAL JOURNAL OF ADVANCES IN SIGNAL AND IMAGE SCIENCES. (Jan. 2025), 34–46. DOI: https://doi.org/10.29284/7fjzk883
11. **Pawan Kumar Singh**, ACCELERATING LARGE LANGUAGE MODEL TRAINING USING HYBRID QUANTUM-CLASSICAL VARIATIONAL AUTOENCODERS WITH INTEGRATED PHOTONIC QRAM, Vol. 54 No. 3 (2026): July-September 2026, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/501, DOI: https://doi.org/10.46121/pspc.54.3.45
12. **Pawan Kumar Singh** , RESILIENCE ASSESSMENT OF MODERN POWER GRID INFRASTRUCTURE AGAINST EXTREME WEATHER USING PHYSICS-INFORMED NEURAL NETWORKS, Vol. 54 No. 1 (2026): January-March 2026, Power System Protection and Control, ISSN-1674-3**415,**https://pspac.info/index.php/dlbh/article/view/502, DOI: https://doi.org/10.46121/pspc.54.1.64
13. **Pawan Kumar Singh,** MITIGATING THE EXABYTE STORAGE CRISIS: ENHANCING READ/WRITE EFFICIENCY IN 5D OPTICAL GLASS STORAGE USING SILVER NANOPARTICLE DOPING, Vol. 38 No. 11s (2025), International Journal of Applied Mathematics (IJAM) , pISSN 1311-1728, eISSN 1314-8060 ,https://ijamjournal.org/ijam/publication/index.php/ijam/article/view/2153
14. **Mr. Pawan Kumar Singh (Author), Miss. Pari Nidhi Singh (Author**) ,Intelligent Bot, ASIN : B0DBGCQY8X,Publisher : Namya Press, Publication date : November 25, 2022,Language : English, Print length : 105 pages,ISBN-10 : 9390124867,ISBN-13 : 978-9390124862,Item Weight : 7.5 ounces, Dimensions : 6.24 x 0.43 x 9.24 inches,https://www.amazon.com/Intelligent-Bot-Pawan-Kumar-Singh/dp/B0DBGCQY8X/ref=sr_1_5?crid=2VAXN5BRN5SMS&dib=eyJ2IjoiMSJ9.v3OCQvHBpy20RIjfMWh0qbOl-RLOlUJIC8Xa0Pjeqilvo2sbZ_suN3LbSCw_OA_ZD_4lgjRLMGlBwZQQ1ehZEfDpt_MJiOUfVuqqzMav0I5_mb6pN5DQog0U7SA826n1DQQ3QAtWwopHy4lC5IfhZXttKj9faiyATwhdtDATSSV1-r7FmzM2VQyIA0jxcfq6E6hp9ECfH1fby0li9kUfGpLxMq4GktlzUIJO5ggrhsQ.G1AjQiVqU4HFsnSczvz-X6NXCNs3EFSn-RI8mcWWGOc&dib_tag=se&keywords=Pawan+Kumar+Singh%2C+book&qid=1787815741&sprefix=pawan+kumar+singh%2C+bo%2Caps%2C450&sr=8-5
15. **Mr. Pawan Kumar Singh (Author),** STORAGE CRISES DUE TO RISE OF AI: A Comprehensive Guide to Managing the Storage Challenges in the Age of Artificial Intelligence, ASIN : B0HFK12ZCT Publisher : EB1 Profile, Accessibility : Learn more, Publication date : August 17, 2026,Edition : 1st Language : English, File size : 1.7 MB, Screen Reader : Supported, Enhanced typesetting : Enabled X-Ray : Not Enabled, Word Wise : Not Enabled ,Print length : 261 pages ,ISBN-13 : 979-8951479112,Page Flip : Enabled, https://www.amazon.com/STORAGE-CRISES-DUE-RISE-Comprehensive-ebook/dp/B0HFK12ZCT/ref=sr_1_1?crid=9MF6C4WDVJR5&dib=eyJ2IjoiMSJ9.DQ8fesBch7ELmRnilDt-YA.NBSCHLmetvnbhkxwIpOoj3s0IVsCV8y6-ZCfCP6Ul1c&dib_tag=se&keywords=Pawan+Kumar+Singh%2C+book%2C+eb1+Profile&qid=1787816040&sprefix=pawan+kumar+singh%2C+book%2C+eb1+profile%2Caps%2C420&sr=8-1

16. **Parag Bharatkumar Parikh**, FRAMEWORKS FOR MITIGATING SUPPLY CHAIN DISRUPTIONS AND MATERIAL PRICE VOLATILITY IN SUSTAINABLE BUILDING CONSTRUCTION, Vol. 53 No. 2 (2025): April-June 2025 , , Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/447, DOI: https://doi.org/10.46121/pspc.53.2.34
17. **Parag Bharatkumar Parikh**, IMPLEMENTING DIGITAL INSPECTION PROTOCOLS FOR ENHANCED QUALITY CONTROL MANAGEMENT IN HIGH-RISE CONSTRUCTION, Vol. 54 No. 3 (2026): July-September 2026, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/439, DOI: https://doi.org/10.46121/pspc.54.3.12
18. **Parag Bharatkumar Parikh** , EVALUATING THE FEASIBILITY AND EFFICIENCY OF 3D-PRINTED CONCRETE TECHNOLOGY IN SUSTAINABLE MODULAR CONSTRUCTION, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/issue/view/30, DOI: https://doi.org/10.46121/pspc.54.1.61
19. **Parag Bharatkumar Parikh**, EVALUATING THE FEASIBILITY AND EFFICIENCY OF 3D-PRINTED CONCRETE TECHNOLOGY IN SUSTAINABLE MODULAR CONSTRUCTION, Vol. 54 No. 1 (2026): January-March 2026, System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/440, DOI: https://doi.org/10.46121/pspc.54.1.61
20. **Ronakkumar shah,** REDEFINING BUSINESS PROCESS MANAGEMENT: THE SYNERGY OF AI AND INTELLIGENT AUTOMATION, Vol. 54 No. 3 (2026): July-September 2026, System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/448, DOI: https://doi.org/10.46121/pspc.54.3.14
21. **Ronakkumar shah**, OPERATIONAL ACCOUNTABILITY IN ACTION: METRICS AND MECHANISMS FOR SYSTEMIC SUCCESS, Vol. 53 No. 4 (2025): October-December 2025, System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/452, DOI: https://doi.org/10.46121/pspc.53.4.40
22. **Ronakkumar shah**, BEYOND THE BLUEPRINT: AUTOMATED WORKFLOW ENFORCEMENT AND POLICY GOVERNANCE, Vol. 53 No. 2 (2025): April-June 2025 , System Protection and Control, ISSN-1674-3415 ,https://pspac.info/index.php/dlbh/article/view/451, DOI: https://doi.org/10.46121/pspc.53.2.35
23. **Tushita Agarwal; Swaminathan Sethuraman,** Mapping Customer Behavior: Visual Analysis of Online Retail Interactions, Date Added to IEEE Xplore: 17 February 2026, DOI: https://doi.org/10.1109/IC2NC67409.2025.11376261
24. **Tushita Agarwal,** Efficient Data Summarization and Comparison via Grid-Based Statistical Proxies for Large-Scale Datasets**, Date Added to IEEE Xplore: 03 December 2025,** DOI: https://doi.org/10.1109/ICBATS66542.2025.11258564
25. **Dip Bharatbhai Patel,** Building scalable business intelligence systems in the cloud: A technical approach, International Journal of Science and Research Archive, 2021, 02(01), 212-215., Received on 03 February 2021; revised on 17 April 2021; accepted on 19 April 2021, DOI: https://doi.org/10.30574/ijsra.2021.2.1.0047
26. **Dip Bharatbhai Patel,** University of North America, Virginia, USA, Home / Archives / Vol. 5 No. 02 (2025): Volume 05 Issue 02 / Articles, https://www.academicpublishers.org/journals/index.php/ijdsml/article/view/5958

27. **Sai Akshara Vemuri ,** KINEMATIC OPTIMISATION OF SOFT ROBOTIC MANIPULATORS FOR MEDICAL INTERVENTION, Vol. 54 No. 3 (2026): July-September 2026, System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/450
28. **Sai Akshara Vemuri**, https://www.periodicos.ulbra.org/index.php/acta/article/view/528
29. **Aziz, A., Chandusha, K., Naga Kiran, B., Prasad, M. L. M., Golla, K., Rajeswari, S., & Katta**, S. K. R. (2026). Exploring Machine Learning Applications for Genomic Data Analysis in Personalized Medicine. International Journal of Drug Delivery Technology, 16(38s), 1166-1173. https://doi.org/10.25258/ijddt.16.38s.127,https://www.periodicos.ulbra.org/index.php/acta/article/view/687
30. **Mohammad Naffizuddin , Chaganti Ashok ,Sowjanya Gunukula , Rvbs Sarma , Bhavana Sujanamulk , Bharani Krishna Takkella , Chukka Ram Sunil ,Varri Sujana , Ashwini Kumar,** Etiological Factors of Orofacial Clefts in a Hospital-Based Population: A Descriptive Analytical Study, Published: December 10, 2025,DOI: 10.7759/cureus.98868, DOI : https://doi.org/10.7759/cureus.98868
31. **Manoj Kumar Kagitha**, Automated Security Compliance in Ci/Cd: A Natural Language Processing (NLP) Approach to Detecting Vulnerabilities in Infrastructure-As-Code (Terraform/Bicep), Publication year 2021, Volume 2021, Issue 12, https://computerfraudsecurity.com/index.php/journal/article/view/970
32. **Manoj Kumar Kagitha,** Hybrid Quantum-Classical Resource Scheduling: A Proposed Architecture for Next-Generation Hyperscale Data Centers, Publication year 2024, Volume 2024, Issue 12, https://computerfraudsecurity.com/index.php/journal/article/view/969
33. **Manoj Kumar Kagitha,** Self-Healing Cloud Infrastructure: A Hybrid Reinforcement Learning Framework for Predicting Microservice Failures in Azure Kubernetes Service (AKS**),**Publication year 2023, Volume 2023, Issue 12,https://computerfraudsecurity.com/index.php/journal/article/view/971
34. **Manoj Kumar Kagitha**, GREENOPS IN THE CLOUD: AN AI-DRIVEN TELEMETRY ANALYSIS MODEL FOR REDUCING CARBON FOOTPRINT IN HIGH-AVAILABILITY CLUSTERS, Vol. 28 No. 6 (2020): JOCAAA, https://www.eudoxuspress.com/index.php/pub/article/view/5054
35. Lakshmi Rahul Reddy Mareddy. (2026). Security and Performance Assessment of Encryption Techniques for Cloud Platforms. International Journal of Communication Networks and Information Security (IJCNIS), 18(1), 68–80. Retrieved from https://ijcnis.org/index.php/ijcnis/article/view/8735
36. Lakshmi RahulReddy Mareddy, Context-Aware Learning Approaches for Improving Prediction Accuracy in Dynamic Systems, International Journal of Computational Mathematical Ideas (IJCMI), Vol.17 No.3(2025): IJCMI Vol17 NO3 2025 https://www.ijcmi.com/index.php/journal/article/view/15
37. Lakshmi Rahul Reddy , Mareddy. (2026). Revisiting Autonomy in Artificial Intelligence through Agentic System Design. Journal of Computational Analysis and Applications (JoCAAA), 35(1), 707–713. https://eudoxuspress.com/index.php/pub/article/view/4780
38. **Mahendrakumar Kalal**, Lean-Driven SAP Production Planning Optimization Using Machine Learning for Inventory and Throughput Efficiency, Date of Conference: 19-20 March 2026, Date Added to IEEE Xplore: 08 April 2026,ISBN Information:,ISSN Information:

DOI: 10.1109/ISDFS69419.2026.11459029, https://ieeexplore.ieee.org/abstract/document/11459029

39. **Mahendra kumar Kalal**, SUPPLY CHAIN RESILIENCE THROUGH INTEGRATED SAP PRODUCTION PLANNING – PROCUREMENT SYNCHRONIZATION, Archives / Vol. 54 No. 1 (2026): January-March 2026 / Articles, https://pspac.info/index.php/dlbh/article/view/259
40. **Dr Manoj Goel (December 2018**). THE ATTITUDE OF DIFFERENT STATES STUDENTS TOWARDS PHYSICAL EDUCATION; STUDYING IN PHYSICAL EDUCATION COLLEGES OF MAHARSHTRA STATE, https://ijeponline.com/index.php/journal/article/view/965/847
41. **Ilakiya Ulaganathan, Tagore Engg. College, Anna University, Chennai, India, ; FNU Antara; Santhosh Chitraju Gopal Varma; Zokir Mamadiyarov; Ziyadulla Turayev, Published** in: 2025 International Conference on Sustainability, Innovation & Technology (ICSIT), Date of Conference: 22-23 August 2025, Date Added to IEEE Xplore: 19 December 2025, ISBN Information:
https://ieeexplore.ieee.org/document/11294748/references#references
42. **Shreyas Kasture, Sudhanshu Maurya, Amit Kumar Sharma, Santhosh Chitraju Gopal Varma, Kashish Mirza, Firdous Sadaf Mohammad Ismail, DOI**: http://doi.org/10.11591/ijai.v15.i2.pp1746-1761, IAES International Journal of Artificial Intelligence (IJ-AI), ISSN/e-ISSN 2089-4872/2252-8938
https://ijai.iaescore.com/index.php/IJAI/article/view/26932
43. **Shiv Shankar Dwivedi, Mr. Santosh Kumar Sharma,** Future-Proofing Data Security with Quantum-Resistant Cryptography, Vol. 11 No. 3 (2025): IJCESEN,
DOI: https://doi.org/10.22399/ijcesen.3447, https://ijcesen.com/index.php/ijcesen/article/view/3447
44. **Vijender Kalmotia,** Enhancing statistical accuracy in gene perturbation studies, Volume 266, August 2026, 105819, https://doi.org/10.1016/j.biosystems.2026.105819, https://www.sciencedirect.com/science/article/pii/S0303264726001292
45. **Naveen Undrathi,** Design and implementation of generative AI-driven data transformation pipelines using spring boot for scalable financial applications, eISSN: 2581-9615 || CODEN: WJARAI || Impact Factor 8.2 || CrossRef DOI, September 2026 (Volume 31, Issue 3), DOI url: https://doi.org/10.30574/wjarr.2026.30.3.1629,
46. **Naveen Undrathi,** Agentic generative AI-enabled microservices framework for intelligent financial data processing in java-based enterprise systems, September 2026 (Volume 31, Issue 3), eISSN: 2581-9615 || CODEN: WJARAI || Impact Factor 8.2 ||
https://doi.org/10.30574/wjarr.2026.30.3.1628
47. **Akshay Jain,** Comparative Analysis of Linkage Methods in Hierarchical Clustering for Customer Segmentation, Conference paper, First Online: 07 October 2025,
https://link.springer.com/chapter/10.1007/978-981-96-7289-9_44
48. **Ismail Hossain,** Department of Computer Science, George Mason University, Fairfax, VA, USA, Mridul Banik, Department of Computer Science, Colorado State University, Fort Collins, CO, USA, https://ieeexplore.ieee.org/abstract/document/11446534
DOI: 10.1109/FMLDS67896.2025.00106
49. **Ismail Hossain, Mridul Banik , Fahmid Al Farid , Jia Uddin , Hezerul bin Abdul Karim** , Advancing Large Language Models for Low-Resource Languages: A Systematic Review of Pretraining, Adaptation, and Ethical Challenges, 10.32604/cmes.2026.075507, Date: 2026
https://www.sciencedirect.com/org/science/article/pii/S152614922600322X

50. **Ismail Hossain; Mridul Banik,** Bridging Visual and Linguistic Intelligence for Chest X-rays: A Comprehensive Review of ViTs and LLM Synergies, Published in: 2025 IEEE International Conference on Future Machine Learning and Data Science (FMLDS) Date of Conference: 02-05 November 2025, Date Added to IEEE Xplore: 25 March 2026, ISBN Information: https://ieeexplore.ieee.org/abstract/document/11446534
51. **Rifat Sarker Aoyon1, Ismail Hossain2, M. Abdullah-Al-Wadud3, Jia Uddin4,** A Secured and Continuously Developing Methodology for Breast Cancer Image Segmentation via U-Net Based Architecture and Distributed Data Training, https://www.sciopen.com/article/10.32604/cmes.2025.060917
52. **M. B. Vibha, M. Chandrika, Samitha Khaiyum & P. Rakshitha Kiran,** Predicting sedentary behavior in adults using stacked LSTM modeling, published: 27 November 2024 Volume 16, pages 346–355 (2025), https://link.springer.com/article/10.1007/s13198-024-02622-2
53. **Bellary Chiterki Anil, Jayasimha Sondekoppa Rajkumar, T. L. Divya, Samitha khaiyum Rakshitha Kiran P., Balakrishnan Ramadoss,** A Radiomics-based Framework for Liver Cancer Analysis using Explainable Artificial Intelligence (XAI) Methods, Vol. 15 No. 3 (2025): June, 2025, https://etasr.com/index.php/ETASR/article/view/10377
54. **Jayminkumar Patel, Sanjaykumar patel, Birju Patel, Rajan shah,** Development and Validation of a Stability-Indicating Analytical Method for Quantitative Determination of Selected Anticancer Drugs in Pharmaceutical Dosage Form, Archives / Vol. 35 No. S2 (2026): Apr-jun 2026, https://welltestingjournal.com/index.php/WT/article/view/288
55. **Jayminkumar Patel, Sanjaykumar patel, Birju Patel, Rajan shah**, Artificial Intelligence-Guided Optimization of Chromatographic Methods for Pharmaceutical Analytical Development, Archives / Vol. 35 No. S2 (2026): Apr-jun 2026, https://welltestingjournal.com/index.php/WT/article/view/294

DOI: 10.46121/pspc.54.3.70