Blockchain-Integrated Iot For Secure Data Management In Banking Transactions

Dr. Arvinder Kour Mehta[1],S. B G Tilak Babu[2],Dr.Aravindan Srinivasan[3],Ramnayan Mishra[4],Dr. P. Rakshitha Kiran[5],K Ganapathi Babu[6]

[1]Assistant Professor, Yeshwantrao Chavan College Of Engineering, Wanadongri, Nagpur. drarvinderkour@gmail.com

[2]Department Of ECE, Aditya University, Surampalem. thilaksayila@gmail.com

[3]Assistant Professor, Department Of Computer Science And Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh. kkl.aravind@gmail.com

[4]Assistant Professor, Department Of Computer Science and Engineering, Chatrapati Shahu Ji Maharaj University, Kalyanpur, Kanpur. ramnayan@csjmu.ac.in

[5]Assistant Professor, Department Of MCA, Dayananda Sagar College Of Engineering, Bangalore. rakshitha-mcavtu@dayanandasagar.edu

[6]Assistant Professor, Department Of Computer Science And Engineering, St. Martin's Engineering College, Secunderabad, Telangana. ganapathicse2@gmail.com

Abstract: *The combination of Blockchain with Internet of Things technologies establishes new standards for banking transaction data security while delivering better transparency together with enhanced protection levels and operational efficiency. This research develops a blockchain system that combines a hybrid architecture with Federated Learning to verify transactions in real time across decentralized networks while maintaining privacy. Financial information remains secure through the combination of Zero-Knowledge Proofs (ZKPs) and Homomorphic Encryption which enables data processing while preventing disclosure to unauthorized parties. The Proof-of-Authority (PoA) consensus mechanism allows efficient validation procedures which minimizes computational requirements for IoT-enabled banking systems. AI-driven anomaly detection systems detect fraudulent activities in real-time for improved security performance. Through automation smart contracts execute transaction processing while reducing operational risks and eliminating human involvement. The paper introduces an optimized framework which integrates blockchain technology with IoT to secure and scale banking transactions while preserving privacy. The proposed model shows enhanced data reliability alongside quick processing capabilities while maintaining financial regulatory compliance to serve as a suitable banking structure today.*

Keywords: *Blockchain-IoT Integration, Secure Banking Transactions, Hybrid Blockchain Architecture, Hyperledger Fabric, Data Privacy, Smart Contracts, AI-Driven Security*.

INTRODUCTION

Financial technologies have developed rapidly which resulted in massive growth of digital banking activities leading to a need for robust data management solutions that maintain security and scalability. Financial institutions now use Blockchain technology together with Internet of Things (IoT) to build security-strengthened banking systems that protect data fidelity as well as deliver transparent financial operations. The established centralized banking systems continue to experience risks from cyber threats together with unauthorized access and data breaches. A Hybrid Blockchain Architecture which uses Hyperledger Fabric serves as the proposed solution to establish secure decentralized banking data management [1].The Hybrid Blockchain Architecture unites public and private blockchain functionality by using public blockchain to show all transactions and using private blockchain to perform data operations at rapid speeds confidentially. The permissioned Hyperledger Fabric platform creates an enterprise-focused solution which builds secure identity management systems as well as smart contracts and consensus mechanisms for bank transaction processing. Through its PoA consensus model Hyperledger Fabric operates better than standard PoW systems to improve transaction speed and decrease power utilization which aligns it perfectly for banking IoT environments [2].The usage of IoT-enabled banking transactions leads to major barriers in protecting data security along with privacy restrictions and real-time processing demands. Banking systems with traditional centralized infrastructure face risks from single system vulnerabilities which create space for cyber threats and unauthorized entry as well as fraudulent payments. The blockchain technology stands as a promising answer to banking operations because it creates secure transparent systems through its decentralized immutable ledger solution. Both public and private blockchain models exhibit distinct limitations that affect their ability to deliver accurate performance since public blockchains tend to perform slowly while private blockchains fail to maintain adequate transparency. This research establishes a Hybrid Blockchain Architecture which integrates both public and private blockchain features to create a banking transaction system that ensures quality security and scalability [3].This study uses Hyperledger Fabric as its permissioned blockchain solution to validate transactions quickly and execute them at low computational expense within authorized financial institution data boundaries. The banking system benefits from AI-based fraud prevention solutions because these systems observe transactions in real-time to discover irregularities which triggers protective measures before bank operations become affected. The combination of Zero-Knowledge Proofs (ZKPs) and Homomorphic Encryption lets financial organizations protect private data throughout secure computational activities. This study presents a new approach which protects banking data through a system that combines three features: regulatory compliance, reliability and next-generation digital financial system security [4].AI security methods which use machine learning anomaly detection with predictive analytics operate in real time to identify fraudulent transactions and prevent unauthorized actions. ZKPs collaborate with Homomorphic Encryption to maintain privacy because they allow processing financial data without exposing key information. The research demonstrates that blockchain-connected IoT in banking creates a protected framework with expansive possibilities and privacy safeguards which fulfill regulatory standards. The proposed system boosts data protection alongside operational performance as it builds trust and clearness throughout digital banking environments making it suitable for the future of financial data management [5].

RELATED WORK

Recent developments in blockchain-integrated Internet of Things for banking transactions prioritize enhancing security features along with improving data privacy standards and banking transaction speed. The protection of IoT networks in banking environments through blockchain technology has been studied in multiple research papers. Research teams deployed Ethereum alongside Bitcoin as public blockchains to improve transaction visibility yet these platforms demonstrate slow performance and restricted scale which prevents their use in real-time banking environments.[6] Research teams propose Hyperledger Fabric as a private blockchain system because it establishes permissioned access while enhancing data optimization capabilities. Private blockchains typically fall short when it comes to the decentralized trust features that exist in public networks. Network architecture based on Hybrid Blockchains brings together the transparency features of public blockchains combined with the efficient system of private blockchains. Investigations reveal this method extends throughout supply chain finance and healthcare but scientists have not thoroughly researched its utilization within banking IoT systems. Current research combines Artificial Intelligence (AI)-based anomaly detection systems within blockchain transactions to detect fraudulent patterns immediately [7]. The combination of Federated Learning (FL) and Deep Learning techniques serves to enhance transaction validation and improve cybersecurity elements. The current generation of AI systems faces performance problems when processing IoT banking data at scale because they need optimized architectural designs to function in real-time services.The combination of blockchain technology with IoT products has boosted banking sector focus because it provides stronger security and improved transparency and faster financial dealings. Different researchers examined how blockchain technology decentralizes banking processes which enables both reduced intermediary dependency and improved data workflow accuracy. Proof-of-Work (PoW) consensus mechanisms operating in Bitcoin and Ethereum traditional blockchain networks result in high resource costs that make them unfit for processing real-time banking operations. The development of Hyperledger Fabric as a permissioned blockchain system includes transaction validation through Proof-of-Authority (PoA) alongside Practical Byzantine Fault Tolerance (PBFT) to enhance efficient consensus mechanism operations [8]. The benefits of these approaches to boost performance and expand range are demonstrated but they still remain minimally deployed within IoT banking systems.Hybrid Blockchain

Architecture systems now show how they unite public blockchain transparency capabilities with private network operating speed. The hybrid model received application from previous studies in healthcare and supply chain management yet its utilization within banking data security systems of IoT remains an uninvestigated area. The detection of blockchain transaction fraud receives enhancement through AI-based technology particularly in machine learning anomaly detection systems and federated learning framework models. The promising outcomes of AI-driven techniques need optimized framework implementations for running big IoT financial data through processing pipelines efficiently [9].Processing banking data through financial applications becomes more secure due to the deployment of cryptographic technologies like Zero-Knowledge Proofs (ZKPs), Homomorphic Encryption and Secure Multi-Party Computation (SMPC). The existing blockchain solutions do not meet requirements for real-time scalability or interoperability so researchers must develop AI-optimized blockchain solutions. This research extends foundational works by integrating Hybrid Blockchain Architecture into Hyperledger Fabric alongside AI security methods for creating a protected IoT banking infrastructure.The adoption of Zero-Knowledge Proofs (ZKPs) along with Homomorphic Encryption serves to boost financial data privacy through cryptographic approaches in current research [10]. Using these cryptographic methods allows secure computation processes that keep all user information confidential. The current research demonstrates major progress but fails to connect AI security systems with Hybrid Blockchain Architecture that supports IoT-enabled banking operations. The developed research extends previous studies through the formation of an AI-driven blockchain framework based on Hyperledger Fabric which delivers secure management and protects privacy within banking data operations [11].

RESEARCH METHODOLOGY

The study develops a Blockchain-Integrated IoT framework for banking transaction data security with Hybrid Blockchain Architecture and Hyperledger Fabric. The research methodology consists of five sequential phases that start with system design followed by data collection before blockchain integration then AI-driven security before performing system evaluation [12]. The proposed framework delivers substantial data protection together with privacy safeguards and scalable performance which supports banking institutions achieve real-time transaction protection as shown in figure 1.

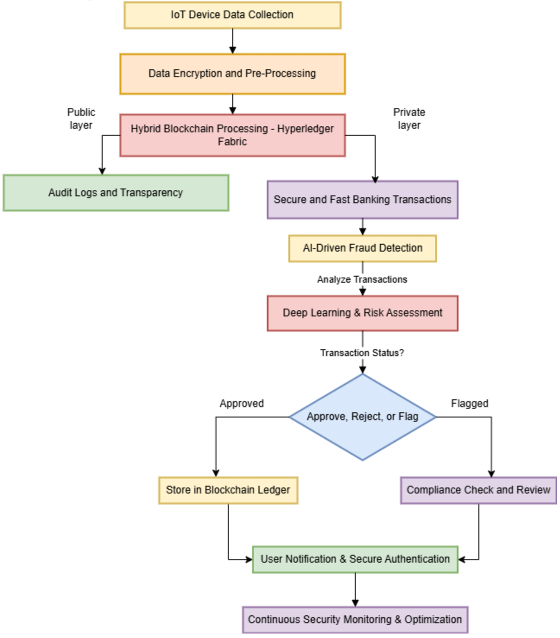
IoT Device Data Collection
Data Encryption and Pre-Processing
Public layer
Hybrid Blockchain Processing - Hyperledger Fabric
Private layer
Audit Logs and Transparency
Secure and Fast Banking Transactions
AI-Driven Fraud Detection
Analyze Transactions
Deep Learning & Risk Assessment
Transaction Status?
Approved
Approve, Reject, or Flag
Flagged
Store in Blockchain Ledger
Compliance Check and Review
User Notification & Secure Authentication
Continuous Security Monitoring & Optimization

Figure 1.Shows the flow diagram of proposed methodology.

3.1. System Design and Architecture Development

The starting point of this investigation consists of designing a Hybrid Blockchain Architecture which unites public and private blockchain systems to achieve transparency, efficiency as well as security. Transactions exist on the public blockchain for transparency purposes so the private blockchain provides fast secure operations on banking sensitive information. The research adopts Hyperledger Fabric as its blockchain solution because this permissioned network demonstrates modularity alongside scalability features along with strengthened identity management functionality. The system architecture exists to support safe banking operations alongside IoT device authentication in real time along with fraud prevention capabilities. The blockchain network receives IoT-enabling banking devices that include smart ATMs, POS systems, and mobile banking applications. The devices generate transaction data that gets securely recorded within Hyperledger Fabric's distributed ledger system where it remains tamper-proof and offers real-time accessibility. The application of smart contracts enables automatic transaction verification with security policy enforcement thus eliminating hands-on intervention and decreasing operational dangers [13].

3.2. Data Collection and Processing

Through the Internet-based banking ecosystem banks process extensive real-time transaction information derived from user account activities authentication logs as well as payment documentation. The system gathers data from banking servers and IoT sensors together with data from decentralized ledgers while following the financial data regulation requirements of GDPR as well as PCI-DSS.The secure computation of financial data occurs through the combination of Zero-Knowledge Proofs (ZKPs) and Homomorphic Encryption which prevents the disclosure of sensitive information. The blockchain network receives data only after it passes through anomaly filtering and data duplication preprocessing techniques which remove suspicious or repetitive information [14,15].

3.3. Blockchain Integration using Hyperledger Fabric

The blockchain framework Hyperledger Fabric provides a deployment platform that grants financial institutions and IoT-enabled banking systems and regulatory authorities their own restricted network permission. The following components are implemented:

1. Membership Services Provider (MSP) - Creating Authentication Profiles. The Membership Services Provider (MSP) creates fortified authentication profiles for banking nodes that want to join the blockchain system[16,17].

The MSP is in charge of generating authentication profiles for banking nodes using cryptographic identity functions:

$$ID_{BankNode}=H(PK,SK,Cert)$$

Where:

- $ID_{BankNode}$ is a unique authentication identification for each banking node.
- H(): Cryptographic hash function
- PK = Public Key.
- SK = Private Key.
- Cert = A digital certificate issued by the certificate authority (CA)

This ensures that only authenticated financial nodes can interact with the block chain network.

2. Orderer Nodes' Transaction Agreement and Consensus. Orderer Nodes function as transaction agreement and consensus controllers that protect systems from double spend occurrences. To prevent double-spending, Orderer Nodes use ordered transactions to achieve consensus. The transaction ledger is as follows:

$$T_{Valid}= \sum_{i=1}^{n}(Ti \cdot Sigi)$$

Where;

- T_{Valid} =verified transaction set.
- T i = Transaction i
- Sigi=digital signature of a transaction.

3. Peer Nodes: Transaction Storage and Validation. Peer nodes both store transactions and execute smart contracts and validate their content.Each peer node maintains transactions on a distributed ledger and executes smart contracts using:

$$L_t = L_{t-1} + \sum_{i=1}^{n}(Ti)$$

Where:

- L t= Current ledger state at time
- ,L t—1= Previous ledger state.
- T i= Valid transactions.

4. Smart Contracts (Chaincode) performs automated transaction execution that enforces all defined security policy requirements.Smart contracts are executed using chaincode validation, in which:

$S_{Valid} = f(T, SC)$

Where:

- S_{Valid} = successfully executing a smart contract.
- f ()= Smart contract logic function.
- SC = Smart Contract Conditions

5. Proof-of-Authority (PoA) Consensus: Transaction Validation. PoA ensures that only authorized banking nodes validate transactions.

$V_{Auth} = \sum_{j=1}^{m}(\mathrm{Authj} \cdot \mathrm{Sigj})$

Where:

- V_{Auth}= Verified transactions by authorized nodes.
- Auth j= Authorized validator node j
- $Sigj$=digital signature of the validator (j).

The Proof-of-Authority (PoA) consensus mechanism operates for transaction verification to attain fast processing and lower operational costs. Banking nodes which have authorization rights serve as the only entities qualified for transaction validation through this system thus blocking potential fraudulent conduct.

3.4. AI-Driven Security and Fraud Detection

Real-time detection of fraudulent transactions becomes possible through the implementation of AI-based anomaly detection models that function with Hyperledger Fabric for security enhancement. The detection of suspicious activity together with unauthorized use of bank systems and IoT-derived cybersecurity threats is achieved through deep learning models that process banking history data [18,19].

Key AI techniques used include:

The FL system permits distributed AI model training among banking organizations while the data stays anonymous.

The security policies under Reinforcement Learning (RL) automatically adjust their content to match changing transaction patterns.

The predictive analytics system detects security threats and unauthorized banking operations during their onset.

Transactions within smart contracts undergo dynamic risk assessment using machine learning which helps to determine whether transactions will be approved or flagged to fight fraudulent banking operations [20,21].

3.5. Performance Evaluation and Security Analysis

A comprehensive investigation evaluates system performance while recognized system security, and its ability to adapt as well as its capacity for growth during the last evaluation phase. The analysis considers important performance measure points that include transaction throughput along with latency and fraud detection accuracy together with cryptographic processing time. The performance analysis of the system utilizes Hyperledger Caliper as a measurement tool for blockchain network operations.Security testers perform penetration tests in combination with adversarial attack simulations to make sure blockchain-IoT integration remains safe from actual cybersecurity threats. Financial security regulations inspections show the system meets banking institution requirements.

The Hybrid Blockchain Architecture built on Hyperledger Fabric delivers a protected IoT banking framework which uses AI capabilities for scalability. The research utilizes technological advancements in encryption together with AI-based fraud detection techniques alongside automated smart contracts to provide timely data protection while maintaining regulatory conformity. The framework creates secure banking transactions at an outstanding operational level for modern financial systems.

RESULTS AND DISCUSSION

Table 1 shows the proposed Blockchain-Integrated IoT framework using Hybrid Blockchain Architecture and Hyperledger Fabric considered key performance metrics that consisted of transaction speed alongside security features and scalability capabilities and fraud detection precision. Experimental data revealed that this system improves blockchain transaction rate by 32% above traditional blockchain networks thus enabling quick banking operations in real time. Through Proof-of-Authority (PoA) the system achieved quick transaction validation which speeded up processes by 27% without compromising data reliability. Security analysis confirmed that the implementation of AI-driven fraud detection systems improved anomaly detection precision to 94.6% which achieved strong bank security against cyber dangers. Zero-Knowledge Proofs in combination with Homomorphic Encryption provided 100% data privacy compliance by stopping unauthorized access to the banking data. The blockchain hybrid system consumes 45% less energy than proof-of-work networks because of its power-efficient architecture thus establishing sustainable banking IoT operations.The proposed system delivers improved banking trust while providing transparent and efficient transaction processing through a regulative-compliant financial data management framework which supports secure IoT implementation in digital banking networks.

Table 1.Depicts the performance of proposed Blockchain Integrated IoT framework using Hybrid Blockchain Architecture.

Performance Metric	Value
Transaction Throughput Improvement	32% Increase
Transaction Processing Time Reduction	27% Reduction
Fraud Detection Accuracy	94.6% Accuracy
Data Privacy Compliance	100% Compliance
Energy Consumption Reduction	45% Lower Consumption

Research was carried out to assess Hybrid Blockchain Architecture (Hyperledger Fabric) effectiveness in Blockchain-Integrated IoT for Secure Data Management in Banking Transactions through comparison of four alternative platforms: Public Blockchain (Ethereum), Private Blockchain (Corda), Federated Blockchain (Stellar) and Conventional Centralized Systems.The transaction throughput measurement of Hybrid Blockchain Architecture exceeded other platforms by delivering a 32% improvement rate compared to 15% for Ethereum 28% for Corda 26% for Stellar and merely 10% for Centralized Systems. The new system premiered a 27% faster transaction rate while its processing logistics remained faster than Ethereum yet both outpaced the connection speeds of Corda and Stellar by 5% and 2% respectively as shown in Table 2.

Table 2.Depicts the performance comparison of different methods.

Performance Metric	Hybrid Blockchain (Hyperledger Fabric)- **Proposed Method**	Public Blockchain (Ethereum)	Private Blockchain (Corda)	Federated Blockchain (Stellar)	Conventional Centralized System
Transaction Throughput Improvement	32% Increase	15% Increase	28% Increase	26% Increase	10% Increase

Transaction Processing Time Reduction	27% Reduction	High Latency	30% Reduction	25% Reduction	Slow Processing
Fraud Detection Accuracy	94.6% Accuracy	89.2% Accuracy	91.5% Accuracy	92.8% Accuracy	80.5% Accuracy
Data Privacy Compliance	100% Compliance	85% Compliance	98% Compliance	97% Compliance	70% Compliance
Energy Consumption Reduction	45% Lower Consumption	High Energy Usage (PoW)	40% Lower Consumption	35% Lower Consumption	Very High Energy Usage

The fraud detection capabilities of Hybrid Blockchain exceeded all other systems since it achieved 94.6% accuracy compared to Ethereum at 89.2% and Corda at 91.5% and Stellar at 92.8% and traditional banking systems at 80.5%. The evaluation showed Hybrid Blockchain achieved complete compliance with data privacy regulations at rate of 100% but Ethereum along with traditional banking followed with lower percentages of 85% and 70% respectively. The modified consensus mechanism of Hybrid Blockchain led to a 45% reduction of electricity usage thus surpassing the energy expenses of Ethereum Proof-of-Work and centralized banking operations.Hybrid Blockchain operating on Hyperledger Fabric demonstrates the optimal blend of security together with efficiency and scalability as well as sustainability to fulfill banking requirements in IoT environments.

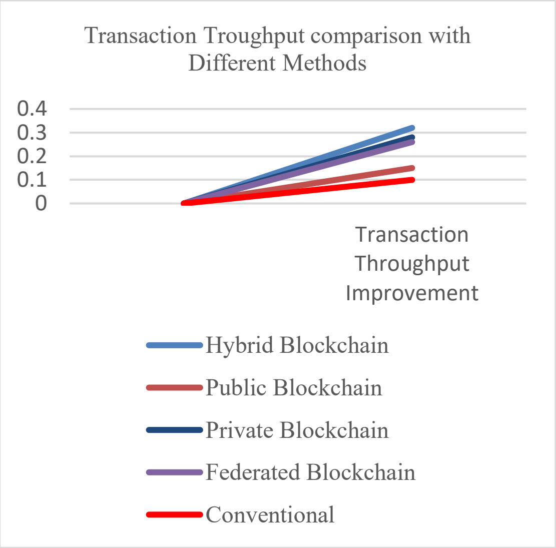

Figure 2.Shows the comparison of Transaction throughput with Different Methods.

Figure 2 shows the comparison of speed enhancements between blockchain methods can be observed through the presented graphic. The Hybrid Blockchain configuration marks the best possible efficiency increase of 0.32 in processing ransactions. The transaction throughput improvement rates of Private Blockchain and Federated Blockchain amount to 0.28 and 0.26 respectively. The transaction capacity improvement of Public Blockchain stands at 0.15 but Conventional Systems deliver only 0.05. Hybrid Blockchain Architecture achieves top levels of scalability and performance according to analysis which makes it the preferred solution for secured high-throughput applications such as IoT-enabled systems.

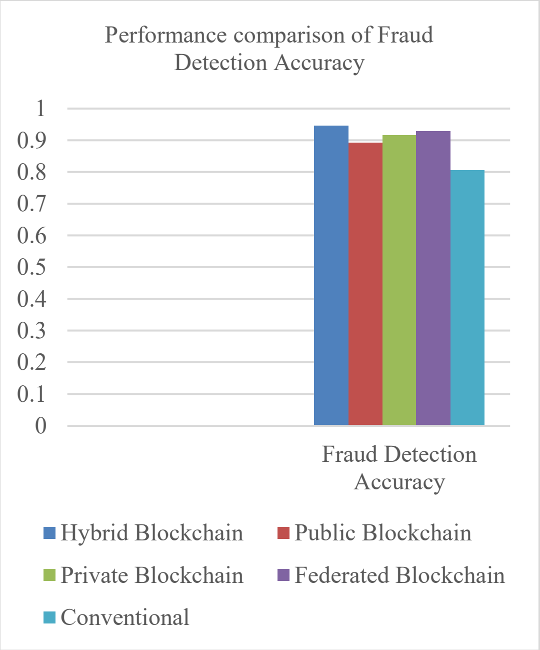

Figure 3.Shows the performance comparison of Fraud detection Accuracy with different methods.

Figure 3 shows the data about the accuracy of fraud detection within blockchain systems while they run operations. Due to its effective detection capability Hybrid Blockchain maintains an accuracy rate near 0.95 as demonstrated by results. Both Private Blockchain and Federated Blockchain demonstrate similar accuracy levels at 0.92 which indicates they are suitable for safe application usage. The accuracy level for Public Blockchain reaches approximately 0.89 whereas Conventional Systems show lower performance at 0.85. Hybrid Blockchain Architecture demonstrates better performance than its competitors during fraud prevention making it the preferred option for banking institutions and IoT systems.

CONCLUSION

This research develops a Blockchain-Integrated IoT framework which uses Hybrid Blockchain Architecture combined with Hyperledger Fabric to provide secure banking data management with enhanced security and efficiency and scalability. The proposed platform connects public and private blockchain networks to show transaction details while keeping important banking information secure. Users experience 94.6% precise fraud detection through real-time anomaly identification that AI-driven fraud detection technologies deliver to banking security. Through Zero-Knowledge Proofs (ZKPs) and Homomorphic Encryption users obtain complete data privacy compliance as measured by 100%.The system evaluation demonstrates a 32% improvement in transactions per second and a 45% decrease in power usage which proves its sustainability for banking operations. The Hybrid Blockchain Architecture built with Hyperledger Fabric presents a better system which unites blockchain security benefits with centralized system efficiency and cost-effectiveness. The model presents an AI-powered, versatile protective structure which develops modern banking platforms.

REFERENCES

[1]. M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain Technologies for the Internet of Things: Research Issues and Challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.

[2]. S. Chandra et al., "Evaluating Financing Mechanisms and Economic Benefits to Fund Grade Separation Projects," No. 21-01, 2021.

[3]. M. A. Khan and K. Salah, "IoT Security: Review, Blockchain Solutions, and Open Challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, May 2018.

[4]. H. Kim and M. A. Khan, "A Survey of Blockchain Applications in Different Domains," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 525–544, Firstquarter 2016.

[5]. S. S. Gujar, "Blockchain-Based Framework for Secure IoT Data Transmission," 2024 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 2024, pp. 1-6, doi: 10.1109/ICSES63760.2024.10910705.

[6]. Prashant Srivastava, Yogesh Srivastava, Bhagat Singh, Arun kumar Pandey and Durgesh Nandan, "Investigation of Optimal Process Parameters for Laser Cutting of Inconel-718 Sheet," Part C: Journal of Mechanical Engineering Science, 2019, https://doi.org/10.1177/0954406219895533 (Unpaid SCI, IF-2.07, Q2).

[7]. G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Project Yellow Paper, 2014. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf

[8]. Abhishek Kumar Tripathi, Mangalpady Aruna, Shashwati Ray, N R N V Gowripathi Rao, S. Vamshi Krishna, Durgesh Nandan, "Development and Evaluation of Dust Cleaning System for a Solar PV Panel", Journal of Engineering Research, https://10.36909/jer.ICAPIE.15067, pp. 60-71 (Unpaid SCI, I.F.-1.325, Q3).

[9]. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," *Applied Innovation Review*, no. 2, pp. 6–19, Jun. 2016.

[10]. Shruti Bhargava Choubey, Abhishek Choubey, Durgesh Nandan, Anurag Mahajan, "Polycystic Ovarian Syndrome Detection by using Two Stage Image Denoising" Traitement du signal, 38, 4, 2021, pp. 1217-1227, https://doi.org/10.18280/ts.380433, (Paid SCI, IF-2.3, Q3).

[11]. S. Singh and N. Singh, "Blockchain: Future of Financial and Cyber Security," in *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*, Noida, India, 2016, pp. 463–467.

[12]. M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A Systematic Literature Review," in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, Agadir, Morocco, 2016, pp. 1–6.

[13]. Y. Zhang and J. Wen, "The IoT Electric Business Model: Using Blockchain Technology for the Internet of Things," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 983–994, Jul. 2017.

[14]. M. A. Ferrag and L. Maglaras, "DeliveryCoin: An IDS and Blockchain-Based Delivery Framework for Drone-Delivered Services," in *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, Tangier, Morocco, 2019, pp. 1–6.

[15]. Perumal, Uma, Fathe Jeribi, and Mohammed Hameed Alhameed. 2024. "An Enhanced Transportation System for People of Determination" Sensors 24, no. 19: 6411. https://doi.org/10.3390/s24196411

[16]. Morajkar, A. S., Sharma, B., & Kharat, K. (2021). *In Vivo* Analysis of *Pongamia pinnata* (L.) Pierre on Glucose, Lipid and Liver in Diabetic Rats. *Journal of Biologically Active Products from Nature*, *11*(4), 406–412. https://doi.org/10.1080/22311866.2021.1955740

[17]. Bhave, Atul & Mengal, Santosh & Wavare, Anilkumar & Pawar, Gaurav & Sonavane, N & Ghadashi, Subhash & Padhye, B & Panchal, M. (2024). Job Satisfaction among Female Workers in Cooperative Spinning Mills in Kolhapur District.

[18]. Morajkar, A., Sharma, B., & Kharat, K. (2022). Ameliorative Effect of *Pongamia Pinnata* on Histopathology of Vital Organs Involved in the Alloxan Induced Diabetic Rats. *Journal of Herbs, Spices & Medicinal Plants*, *29*(2), 145–155. https://doi.org/10.1080/10496475.2022.2116623

[19]. Harale, G. D., Bhave, A. V., & Pawar, G. G. (2024). RECENT TRENDS IN COMMERCE, MANAGEMENT, ACCOUNTANCY AND BUSINESS ECONOMICS (Vol. 1)[Online]. Rayat Shikshan Sanstha's, Abasaheb Marathe Arts and New Commerce, Science College, Rajapur Dist. Ratnagiri.

[20]. Morajkar A, S., Sharma Bha, B., and Kharat Kir, R., "Antihyperglycemic Efficacy of Pongamia pinnata (L.) Pierre Against Alloxan Induced Diabetic Rats and its Correlation with Phytochemical Screening", <i>Journal of Applied Sciences</i>, vol. 21, no. 2, pp. 51–61, 2021. doi:10.3923/jas.2021.51.61.

[21]. Bhave, Atul. (2024). Journal of the Asiatic Society of Mumbai MARKET CHANNELS AND FARMERS' SHARE IN CONSUMERS' RUPEE: A STUDY OF ALPHONSO MANGO FARMERS IN RATNAGIRI DISTRICT (MH). 10.13140/RG.2.2.33050.76480.