Computer Information Systems and Security using Block chains and IoT for Traditional Industrial Sector

Mr. Sandeep Mishra
Ph.D. Research Scholar
Department of Computer Science
C.S.J.M. University, Kanpur, Uttar Pradesh, India

Dr. Rashi Agarwal
Faculty of Computer Science,
C.S.J.M. University, Kanpur, Uttar Pradesh, India

Dr. Renu Jain
Head of the Department
Computer Science
C.S.J.M. University, Kanpur, Uttar Pradesh, India

Abstract:

The integration of Computer Information Systems (CIS) and Security with Blockchain and IoT in traditional industries has the potential to revolutionize and secure these sectors. IoT sensors collect real-time data on machinery, production rates, and environmental conditions, enabling automation and remote management. Blockchain ensures data integrity and transparency, creating a secure record of assets and products. Smart contracts automate agreements within supply chains, reducing intermediaries and ensuring transparency. Data privacy is protected through encryption and other security measures. Blockchain allows for decentralized identity management and anomaly detection. IoT applications include real-time machine health monitoring, supply chain and logistics, and energy and utilities monitoring. Challenges include managing high data volumes, addressing complexity, and ensuring interoperability with legacy systems. Blockchain technology offers transaction security, transparency, and tamper resistance, potentially changing the global commercial landscape. The Internet of Things (IoT) and blockchain can create a safe and effective digital combination. However, challenges remain in each domain. This research paper aims to improve lightweight blockchain by adding three goals: improved hashing efficiency, enhanced encryption and decryption, and a novel signature system for non-repudiation. Hybrid encryption, decryption, and hashing mechanisms inspired by nature are proposed. The Edwards curve is also analyzed for potential curve replacement.

Keywords: Blockchain, Computer Inormation Systems, Industrial Sector,IoT, Security, Privacy, Non-repudiation.

Introduction:

Computer Information Systems (CIS) and Internet of Things (IoT) are crucial technologies in industrial applications, enabling the collection, processing, and management of large-scale data on operations, production, maintenance, and inventory[1-2]. CIS can optimize decision-making, improve resource allocation, streamline processes, and enhance operational efficiencies. IoT, also known as the Industrial Internet of Things (IIoT), provides real-time monitoring of key metrics, enabling better visibility and management of operations[3-5]. IoT can also predict equipment failures and schedule maintenance before breakdowns, leading to cost savings and reduced downtime. Blockchain, on the other hand, provides a decentralized and immutable ledger for securely storing data, ensuring tamper-proof records for compliance and audit purposes[6-8]. It also allows for smart contracts, automating tasks and enhancing security by decentralizing information storage across networks. Integrating IoT with blockchain for enhanced CIS and security can lead to secure data transmission, decentralized storage, improved incident response, and interoperability[9-10]. Challenges in integrating CIS, blockchain, and IoT integration include data management and storage, scalability, interoperability with legacy systems, and energy consumption. Potential industrial use cases include manufacturing, supply chain and logistics, energy and utilities, and healthcare manufacturing[11-13]. The convergence of CIS, blockchain, and IoT offers significant potential for improving efficiency, transparency, and security in traditional industrial sectors.

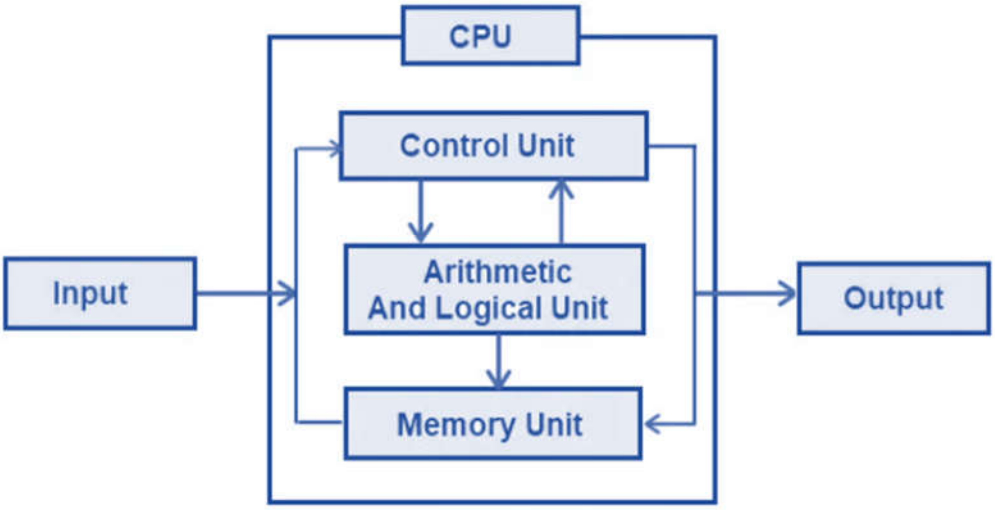

Fig.1 Art of Testing for a Computer System

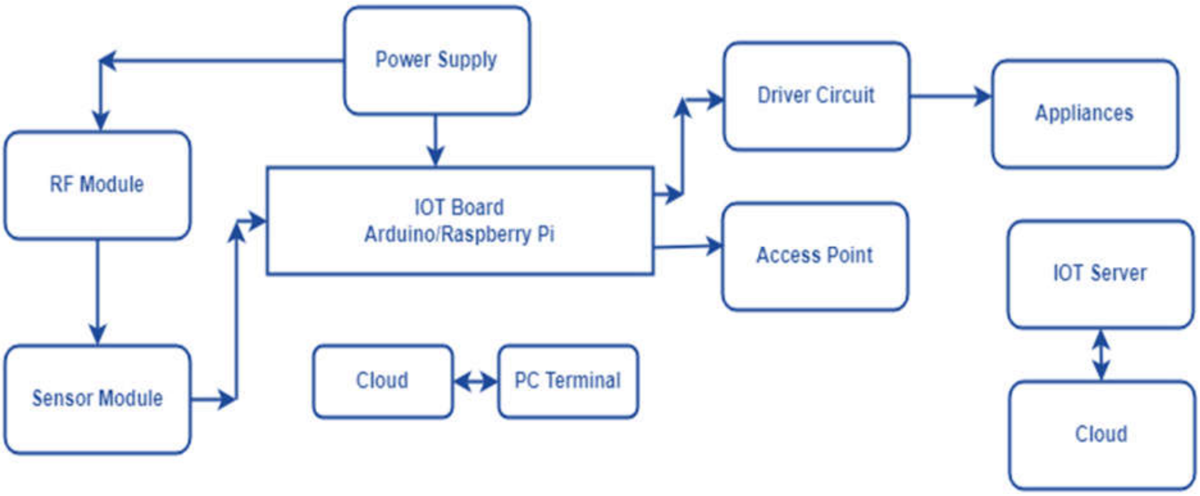

Fig.2 Block diagram of IOT

The rise of IoT and blockchain technology has raised security and privacy concerns in the digital age. Blockchain, a shared ledger, offers advantages such as immutability, decentralization, and transparency[14-15]. It allows for secure storage of data from sensors on devices, ensuring integrity and reliability. It also provides enhanced access control, preventing unauthorized data breaches and protecting user privacy. However, challenges include scalability and privacy. The Internet of Things (IoT) is a network of connected devices that collect and exchange data over the internet. Blockchain technology addresses these concerns by providing tamper-proof data, fostering decentralized trust, and allowing for granular access control[16]. However, challenges include scalability and privacy-preserving techniques.

Blockchain technology, first introduced in 2008, has gained popularity for its security, immutability, traceability, and transparency. It is composed of blocks linked together, providing a highly distributed ledger for transaction keeping, auditing, and recording. Blockchain simplifies transaction storage and asset tracking in business networks[17].

Fig.3 Generic flow of blockchain process

Blockchain technology offers numerous benefits for security and privacy use cases, including resilience, availability, decentralized infrastructure, transparency, traceability, identity protection, authentication, access management, and proof of ownership. It can be divided into four groups: consortium, private, hybrid, and public. The Internet of Things (IoT) is a rapidly growing field that connects billions of devices to the internet and streams data. However, security and privacy concerns remain due to increased attack surface and potential vulnerabilities in devices[18]. IoT devices can be exploited by hackers, posing threats to critical infrastructures like electricity, transportation, and financial services. Blockchain technology has evolved into various forms, each with unique characteristics and applications. The convergence of blockchain and IoT is essential for both industries, and the race to standardize is ongoing. As blockchain eventually takes over the internet, it might give rise to the Blockchain of Things (BoT). The growing use of blockchain in the Internet of Things raises questions about security, privacy, and scalability of performance. Sensor data is vulnerable to data hacking, data forging, and breaches during transmission, making it difficult for stakeholders to share IoT data. Centralized storage is susceptible to breaches, hacking, and intrusion, and digital data makes it difficult to confirm the accuracy and legitimacy of data. To address these challenges, it is crucial to evaluate and advance technologies that can resolve these issues.

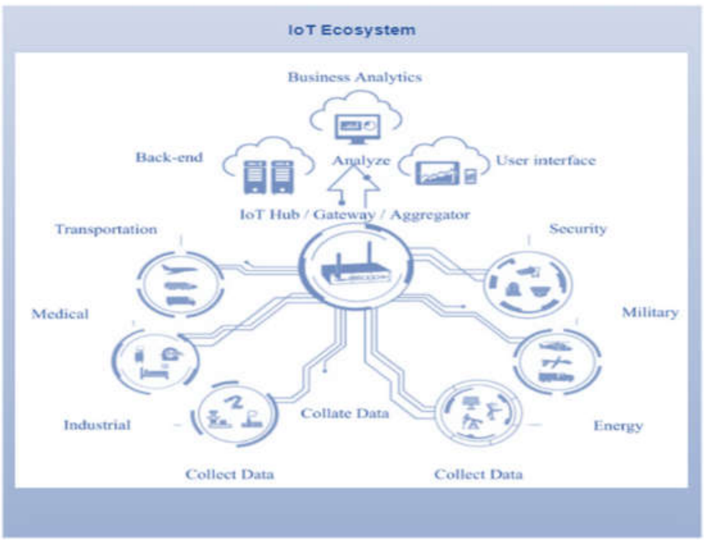

Fig.4 Concept of IOT Ecosystem

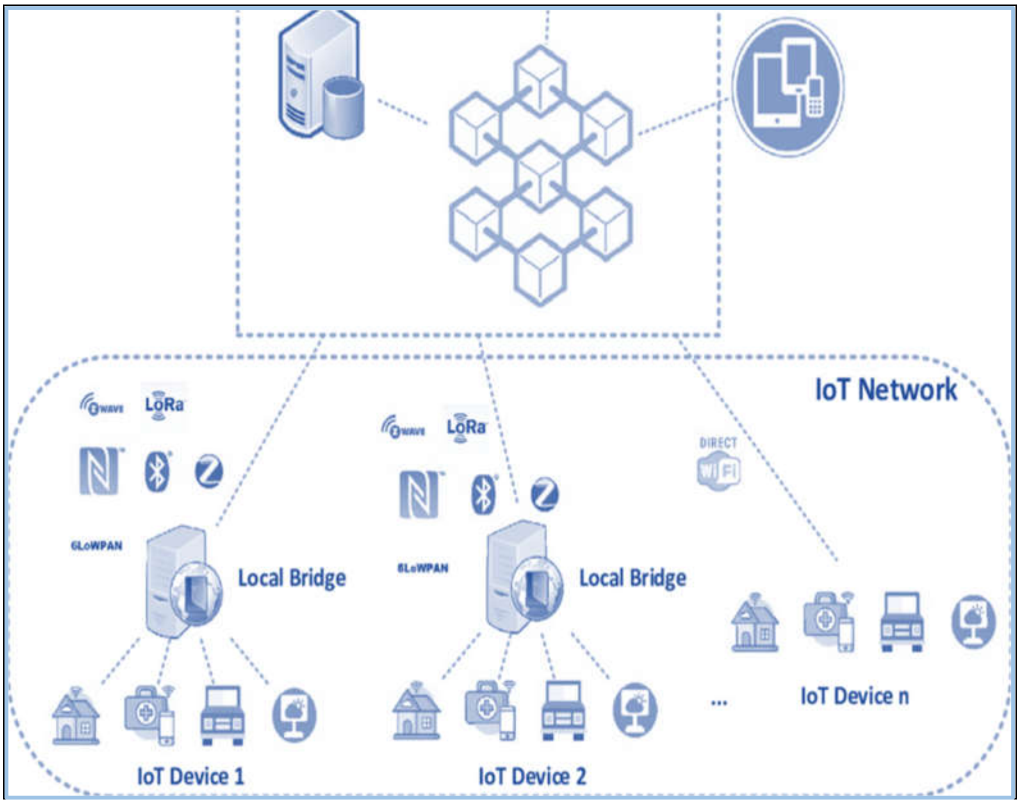

Fig.5 IoT blockchain platform conceptual scenario

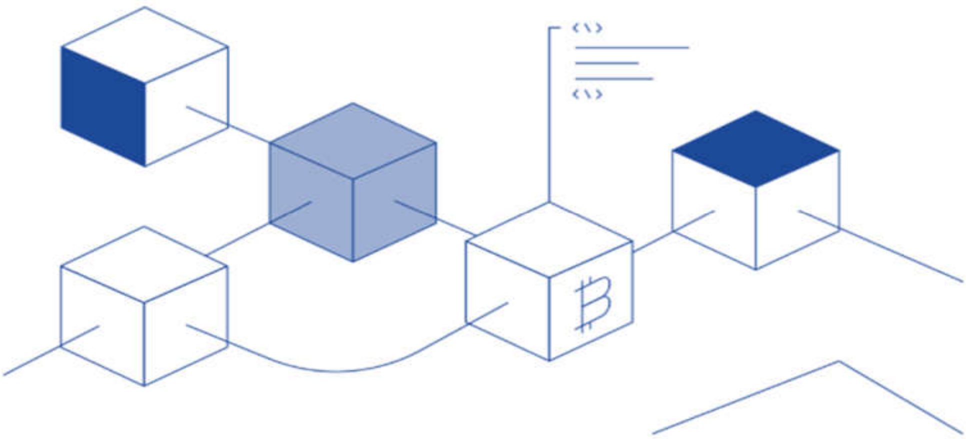

Fig.6 Concept of multiple blocks

Blockchain technology is a decentralized ledger of data validated by a network of users, supporting industries like cryptocurrency and finance. Its key features include constant, fast, secure, inexpensive, and tamper-proof transactions. Key applications include finance, supply chain, real estate, and gambling. Blockchain is gaining popularity in healthcare, IoT, and digital identity due to efficient data ownership and control mechanisms. However, challenges like hacks, centralized control, and decentralization remain. The Blockchain Trilemma aims to balance scalability, decentralization, and security.

Literature Review and Major Findings:

The literature review discusses various blockchain solutions for IoT applications, including lightweight blockchain systems, decentralized IoT systems, lightweight hashing, and smart home applications. However, these approaches have limitations such as performance lag, increased communication loops, and resource constraints. Some researchers have proposed lightweight hashing to improve transaction rates and reduce block latency, but lack a provable architecture for applications requiring provenance in the blockchain ecosystem. Shahid et al. (2019) proposed a solution based on a sensor chain, which includes three stages for transforming a conventional blockchain into a lightweight blockchain. PrivLiteChain, a privacy-preserving blockchain, employs temporal restrictions to ensure transaction privacy using local differential privacy. Dorri et al. (2017) employed LSB in a SMART home setup to ensure security and privacy. Various frameworks for decentralized privacy-preserving management have been developed, such as a four-layer framework for digital medical records, a modified ECC for identity-based access control, and a lightweight digital signature algorithm for electronic health records. ECC has also been used in cloud storage to prevent unauthorized access and has been used in energy trading, voting, and data and sociological mining. The Edwards curve cryptography has been widely used in IoT security, including public key generation algorithms and digital signatures. It offers fast grouping operation and resistance to side-channel attacks, making it ideal for resource and power-constrained IoT applications. However, more reliable security protocols are required due to insufficient transaction security mechanisms in existing studies. The literature survey indicates a growing demand for lightweight blockchains in IoT-based applications due to insecure transactions and lack of encryption. Key performance indicators include security, provability, high transaction throughput, block validation, less storage utilization, cost, and rapid sign and verification.

Research Methodology:

This research work aims to enhance data security and hashing performance in transit by proposing EC-ElGamal and SHA-384, powered by genetic algorithm-based key generation. The goal is to provide faster, stronger security and reduce block hashing time, inspired by evolutionary algorithms and evidence-based support from past literature. The following are the major goals:

- Strengthen the ecosystem's security for IoT data transmission.
- The IoT data saved on the blockchain is protected by encryption and privacy.
- Boost hash quality and performance.
- By cutting down on the processing times for encryption and decryption, transaction processing is enhanced.
- Enhance block validation by using better hashing to shorten the block processing time
- Cutting the size and length of the key to maximize storage utilization.

The proposed work, illustrated in Fig., aims to enhance security and performance by utilizing EC-ElGamal and Genetic algorithm-based key generation for SHA-384. The proposed blockchain method, EC-ElGamal, enhances security and performance for IoT devices by reducing transaction overhead and increasing transaction flow. It can handle IoT device transactions without a queue and achieve high performance and security with a high hash rate and quality. The experiment design involves temperature sensor data as transaction data, which is encrypted during transmission and decrypted upon arrival at the gateway. The method adds an extra layer of security to transactions, and block hashing is performed using a hybrid approach using the Genetic Algorithm and SHA-384. The experiment simulates an environment for storing environmental phenomena for audit by governing agencies and policymakers, using a temperature dataset as a data feed.

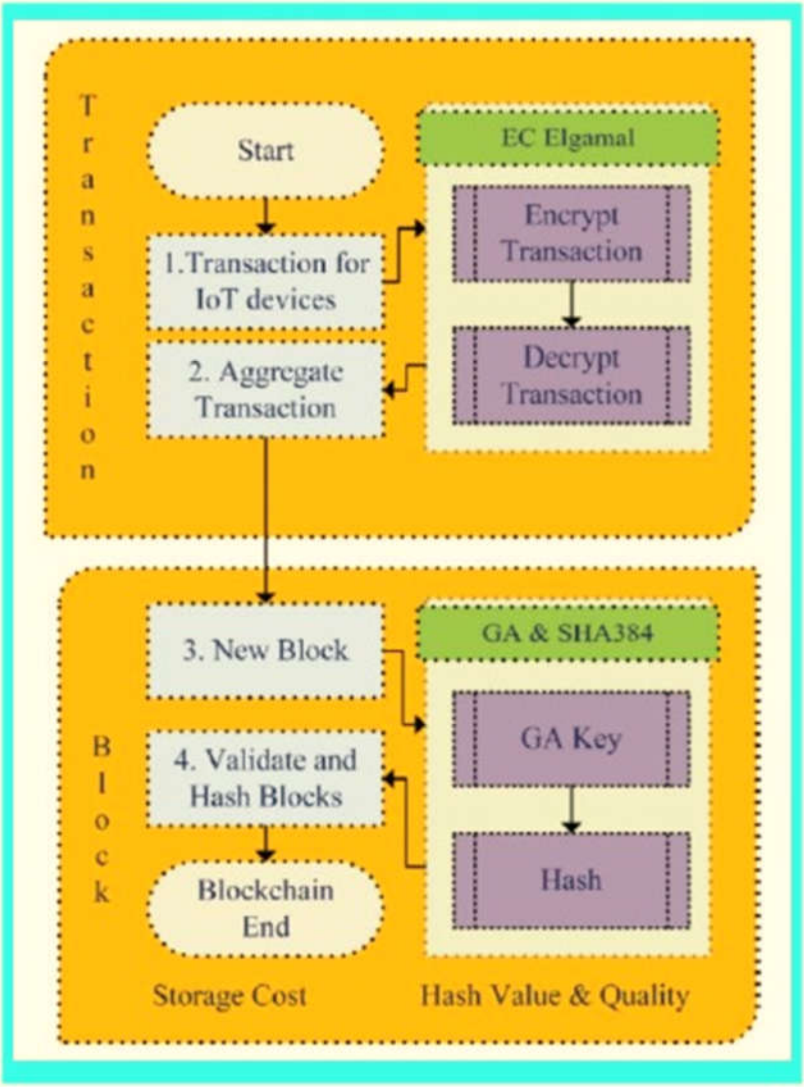

Fig.7 Proposed workflow for security, privacy and hashing enhancement

Result and Analysis:

Experimental evaluations show the proposed methodology in the IoT domain improves performance by 20%, 22%, 53%, and 7%, with enhanced transaction security and an extra layer of transaction encryption, surpassing existing methods.

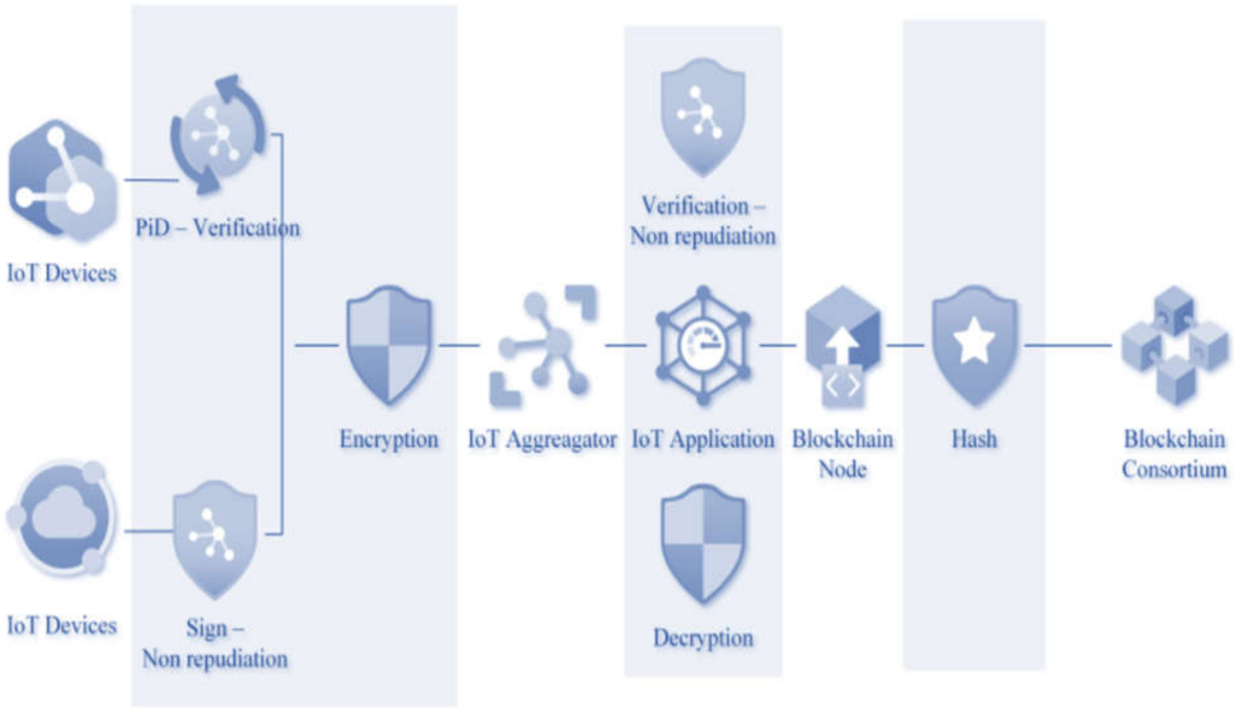

Fig.8 Research outcomes

Table 1: Advantage of the proposed work compared with existing works

Features	Earlier Research	Proposed Research
Application Specific	YES	NO
Transaction Security	NO	Yes
Blockchain agnostic	NO	YES
Multichain provenance	NO	Yes
Security	BASIC	ENHANCED
Hashing	BASIC	ENHANCED
DSA	RSA/EC	ED
Curve	EC	ENHANCED EC and ED
Hash	SHA 256	SHA 384/BLAKES

Table 2: Goals proposed and goals attained

Goals – Proposed	Goals – Attained
Improve Security and Privacy with enhanced encryption methods.	Enhanced security and privacy.
Design a non-repudiation process with a high-performance digital signature.	Novel HECAS.
Platform agnostic application with superior security, privacy, and provenance	Blockchain agnostic Insurance application.

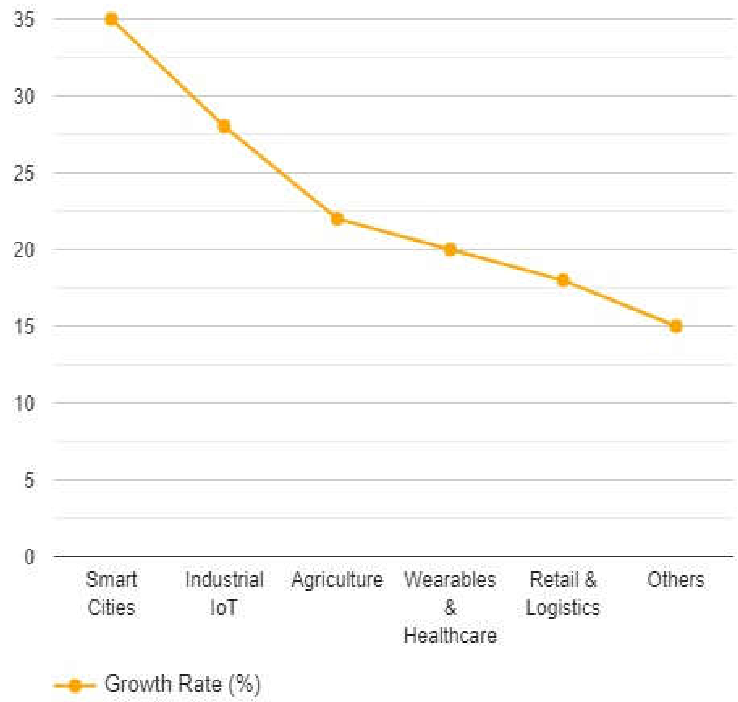

Fig.9 Analysis of Growth Rate (%)

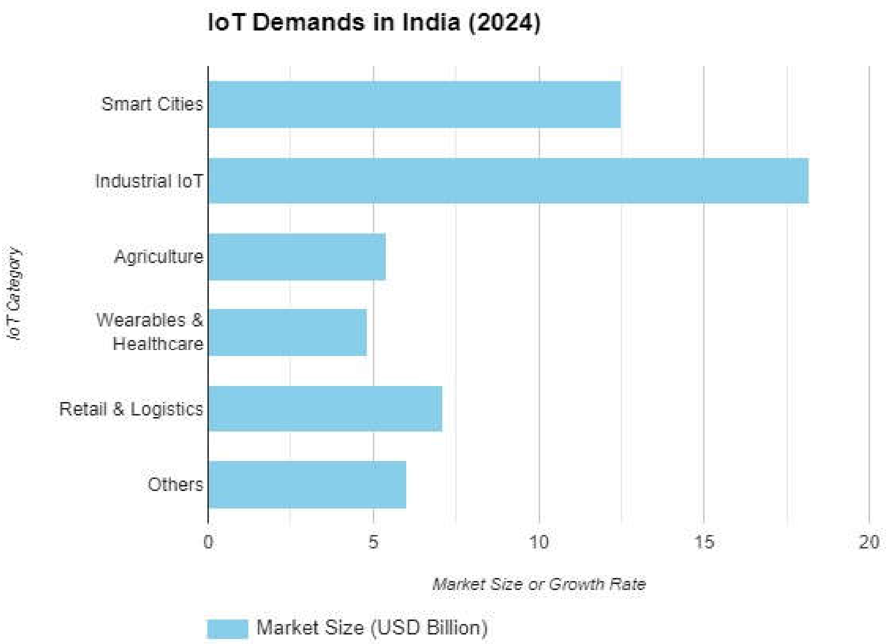

Fig.10 Analysis of Market Size (USD Billion)

Government initiatives, rising smartphone adoption, and an emphasis on digital transformation are anticipated to fuel India's IoT demands in 2024. Concerns about security and privacy, 5G technology for bandwidth-intensive applications, and AIoT integration for real-time automation and decision-making are among the high-demand sectors. It is anticipated that edge computing will result in less network congestion and quicker reaction times. The "Digital India" and "Smart Cities Mission" initiatives of the Indian government seek to use IoT to advance infrastructure, enhance citizen services, and spur economic expansion. The nation's increasing smartphone usage provides a solid basis for the implementation of IoT.

Conclusion:

Efficiency, transparency, and security in traditional industrial sectors could be greatly enhanced by the confluence of CIS, blockchain, and IoT. By enabling automated procedures, secure data exchange, tamper-proof record-keeping, and real-time data collection, these technologies promote a strong, forward-thinking industrial environment. Blockchain technology, often associated with Bitcoin, offers transaction security, tamper resistance, and transparency for IoT applications. However, combining IoT and blockchain requires addressing challenges. This research focuses on lightweight blockchain techniques, improved hashing efficiency, enhanced encryption and decryption, and a novel signature system for non-repudiation. It also presents a platform-neutral IoT blockchain technology, strengthening the ecosystem's security for IoT data transmission, protecting data, boosting hash quality, enhancing transaction processing, block validation, and minimizing key size and length. Future developments in lightweight blockchain may include eliminating aggregators, incorporating incentive systems, creating co-processors, and supporting quantum cryptography.

References:

[1] G. Sagirlar, B. Carminati, E. Ferrari, J. D. Sheehan, and E. Ragnoli, “Hybrid-IoT: Hybrid Blockchain Architecture for Internet of Things - PoW Sub-blockchains,” pp. 1–10.

[2] B. Cao *et al.*, “When Internet of Things Meets Blockchain : Challenges in Distributed Consensus,” vol. XX, pp. 1–8, 2019.

[3] T. Alam, “Blockchain and its Role in the Internet of Things (IoT),” vol. 5, no. 1, pp. 151–157, 2019, doi: 10.32628/CSEIT195137.

[4] A. Dorri, “Towards an Optimized BlockChain for IoT,” pp. 227–232, 2017, doi: 10.1145/3054977.3055003.

[5] G. Rathee, A. Sharma, and R. Iqbal, “A Secure Communicating Things Network Framework for Industrial IoT using Blockchain Technology,” no. June, 2019, doi: 10.1016/j.adhoc.2019.101933.

[6] S. I. N. K. Lo *et al.*, “Analysis of Blockchain Solutions for IoT : A Systematic Literature Review,” *IEEE Access*, vol. 7, pp. 58822–58835, 2019, doi: 10.1109/ACCESS.2019.2914675.

[7] S. Aich, S. Chakraborty, M. Sain, H. Lee, and H. Kim, “A Review on Benefits of IoT Integrated Blockchain based Supply Chain Management Implementations across Different Sectors with Case Study,” *2019 21st Int. Conf. Adv. Commun. Technol.*, no. February, pp. 138–141, 2019, doi: 10.23919/ICACT.2019.8701910.

[8] S. A. Kondaveeti and S. Shekhar, “CONTINUOUS SECURITY IN IOT USING BLOCKCHAIN Rahul Agrawal , Pratik Verma , Rahul Sonanis , Umang Goel , Dr . Aloknath De , Samsung Research Institute Bangalore,” pp. 6423–6427, 2018.

[9] A. F. Zorzo, H. C. Nunes, R. C. Lunardi, R. A. Michelin, and S. S. Kanhere, “Dependable IoT using blockchain-based technology,” pp. 1–9, 2018, doi: 10.1109/LADC.2018.00010.

[10] X. Wang *et al.*, “Survey on Blockchain for Internet of Things Survey on Blockchain for Internet of Things,” no. January, 2019, doi: 10.1016/j.comcom.2019.01.006.

[11] O. Novo, “Scalable Access Management in IoT using Blockchain : a Performance Evaluation,” no. June, 2019, doi: 10.1109/JIOT.2018.2879679.

[12] O. Novo, “Blockchain Meets IoT : an Architecture for Scalable Access Management in IoT,” no. December, 2018, doi: 10.1109/JIOT.2018.2812239.

[13] G. Sladic, “A Case Study IoT and Blockchain powered Healthcare,” no. June, 2017.

[14] A. Rejeb, J. G. Keogh, and H. Treiblmaier, “Leveraging the Internet of Things and Blockchain Technology in Supply Chain Management,” pp. 1–22, 2019.

[15] T. Dey, S. Jaiswal, S. Sunderkrishnan, and N. Katre, “A Medical Use Case of Internet of Things and Blockchain,” *2017 Int. Conf. Intell. Sustain. Syst.*, no. Iciss, pp. 486–491, 2017.

[16] A. P. Id and N. Tapas, *Blockchain and IoT Integration : A Systematic Survey*. 2018. doi: 10.3390/s18082575.

[17] U. Blockchain, “Management and Monitoring of IoT Devices Using Blockchain †,” 2019, doi: 10.3390/s19040856.

[18] X. Liang, J. Zhao, S. Shetty, and D. Li, “Towards Data Assurance and Resilience in IoT Using Blockchain,” no. October, 2017, doi: 10.1109/MILCOM.2017.8170858.