Cureus Journal of Computer Science

Open Access Original Article

A Trustworthy IoT to Cloud Data Transmission Frameworks

Shatakshi Kokate [1] , Urmila Shrawankar [2]

1. Computer Science and Engineering, G. H. Raisoni College of Engineering, Nagpur, IND 2. Computer Science, Shri Ramdeobaba College of Engineering and Management (RCOEM) Nagpur (MS), Nagpur, IND

Corresponding author: Shatakshi Kokate, shatakshi.kokate@gmail.com

Review began 07/15/2024
Review ended 10/14/2024
Published 10/18/2024

DOI: 10.7759/11

Abstract

The IoT devices are growing rapidly, which has led to an exponential rise in the amount of data those devices are producing. There is a pressing need for effective and secure data transfer techniques from IoT devices to the cloud as the amount and complexity of IoT data keep growing. This paper introduces a revolutionary idea that combines fog computing, and blockchain technology and also uses a hybrid consensus mechanism to ensure secured data transmission between IoT and Cloud. Fog computing, a branch of the cloud provides local processing, storage, and communication capabilities. By leveraging fog computing, data transmission latency is reduced, and network congestion is minimized, resulting in improved performance and responsiveness. Blockchain technology is incorporated into the system to guarantee the security of IoT data while it is being transmitted. Blockchain, with its decentralized and immutable nature, provides a transparent and tamper-proof ledger for recording data transactions. Each data transaction from an IoT device is encrypted, timestamped, and appended to the blockchain, creating an auditable and trustworthy record of data transmission. Additionally, a hybrid consensus mechanism using Delegated Proof of Stake and Practical Byzantine Fault Tolerance is employed to validate the transaction. This concept addresses the challenges of data security, latency, and integrity in IoT applications, enabling the development of scalable and trustworthy IoT systems across various industries. The efficiency of the proposed system is validated by evaluating performance metrics such as latency, accuracy, precision, recall, F-score, and verification time, and comparing the results with those of existing approaches. The implemented systems, tailored for the healthcare domain, exhibit security measures and an impressive 18% reduction in latency, while enhancing the accuracy by 15% when compared to the conventional approach, as per the experimental results.

Categories: IoT Applications, IoT Integration with Emerging Technologies, Data Security
Keywords: data security, data integrity, data transmission, hybrid, smart contracts, blockchain, fog computing, cloud, pbft, dpos

Introduction

IoT devices have quickly taken over many industries, allowing cutting-edge applications and producing unprecedented data. Smart gadgets and IoT devices collect and send data to centralized cloud systems for archival, processing, and analysis [1]. However, the massive volume of IoT-generated data presents substantial security, integrity, and latency difficulties during transmission. Securing the transmission of IoT data is of paramount importance to protect sensitive information and ensure the trustworthiness of IoT applications [2]. Traditional methods of transmitting data from IoT devices to the cloud often rely on centralized servers, making them vulnerable to security breaches and single points of failure. Moreover, the latency introduced by long-distance data transmission can hinder real-time decision-making and responsiveness [3]. Relying only on the cloud creates network congestion and slows down response times. IoT systems that rely heavily on cloud infrastructure often struggle to scale efficiently, particularly when dealing with high data loads and frequent requests for real-time analytics. Existing systems often use encryption and access control mechanisms to secure IoT data. However, they still face challenges with ensuring end-to-end security and preventing unauthorized modifications during transmission. This paper offers a concept that addresses these issues by fusing fog computing and blockchain technology, and using a hybrid consensus mechanism to ensure secure and effective data transmission from IoT devices to the cloud. Fog computing is integrated into the system to enable localized data processing and storage at fog nodes near IoT devices. This reduces transmission time, minimizes network congestion, and improves system responsiveness [4]. In short, Fog computing is used for lowering latency and enabling localized processing and storage. The integration of blockchain technology into the concept adds a layer of transparency, immutability, and decentralization to the data transmission process. Blockchain, originally introduced as the underlying technology for cryptocurrencies, offers a distributed ledger where data transactions are securely recorded and verified [5]. By leveraging blockchain properties, such as transparency, data integrity, and tamper resistance, the concept ensures the secure and auditable transmission of IoT data [6]. In the proposes system, IoT devices collect the data and transmit it to the fog nodes. The fog nodes, equipped with computational and storage capabilities, process the data, create blocks, package it in the transaction, validate the transaction using a hybrid consensus mechanism, and append the block to the existing blockchain. The use of blockchain ensures tamper-resistant storage of

data, with every transaction being encrypted, timestamped, and added to the blockchain. Blockchain network ensures the integrity of data, providing an auditable trail of data transmission events and preventing unauthorized modifications [7]. This ensures that the transmitted data is immutable and can be audited at any time, guaranteeing data integrity. By distributing processing tasks between fog nodes and blockchain nodes, the proposed system achieves better load balancing and ensures that the network can handle a growing number of IoT devices without performance degradation. By combining fog computing and blockchain technology, and using a hybrid consensus mechanism, the proposed concept addresses the security, latency, and data integrity challenges associated with IoT data transmission.

Materials And Methods

Literature review

After examining various research papers, the following technologies are identified to improve the security of IoT data transmission to the Cloud.

Fog Computing

It is used to reduce latency and save bandwidth in IoT data transmission[1]. Fog computing enables localized data processing and reduces the dependency on cloud servers as they have their own computational and storage resources, which are distributed across boundaries of the network [2,3]. This approach improves the overall system performance by minimizing the latency introduced by long-distance data transmission [4,5]. Several studies have explored achieving efficient and timely data transmission by introducing fog computing in the IoT environment. Figure *1* shows the fog computing layer in the IoT-Cloud network.

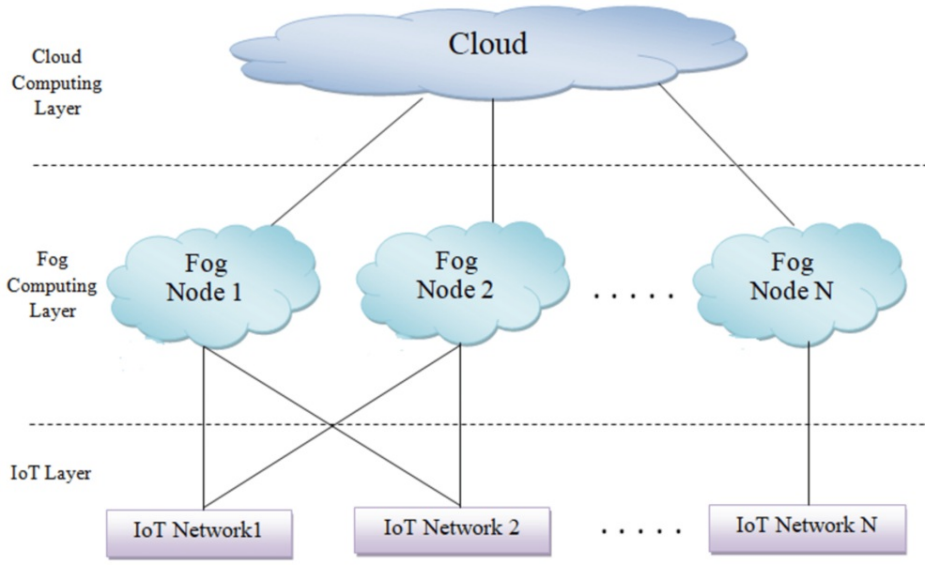

FIGURE 1: Fog computing layer in IoT-Cloud network

Table *1* provides a concise overview of characteristics that make fog computing suitable for IoT applications.

Characteristic	Description
Proximity to edge	- Fog computing is located closer to IoT devices, reducing latency and data transfer times.
	- Data processing occurs at or near the IoT device, improving real-time response.
Distributed compute	- Fog nodes distribute computation tasks across the network.
	- Decentralized processing reduces the burden on a centralized cloud.
Real-time analysis	- Enables real-time processing, analysis, and decision-making of the data
Scalability	- Scalable architecture allows for easy addition of fog nodes as IoT deployments grow.
	- Handles the increasing volume of IoT-generated data.
Resource efficiency	- Efficient utilization of computing resources on local fog nodes.
	- Reduces the need for continuous cloud connectivity and conserves bandwidth.
Data security	- Enhanced data security through local processing and reduced data transmission to the cloud.
	- Mitigates privacy concerns associated with transmitting sensitive data.
Interoperability	- Supports various IoT device types and communication protocols.
	- Ensures compatibility across heterogeneous IoT ecosystems.
Latency-sensitive	- Ideal for applications requiring low latency, like augmented reality and remote surgery.
Edge analytics	- Enables on-device analytics for immediate insights.

TABLE 1: Fog computing key characteristics

Blockchain Technology

Blockchain technology has gained significant attention for its potential to enhance data security and integrity in various domains, including IoT [6]. Because blockchain is decentralized and unchangeable, data transactions are transparently recorded and impenetrable [7]. Blockchain provides a robust mechanism for verifying the authenticity of data, preventing unauthorized modifications, and maintaining a trustworthy record of data transactions [8]. Many research studies have delved into the use of blockchain for securing data transmission and guaranteeing data integrity. Figure *2* illustrates the chain of blocks called a blockchain.

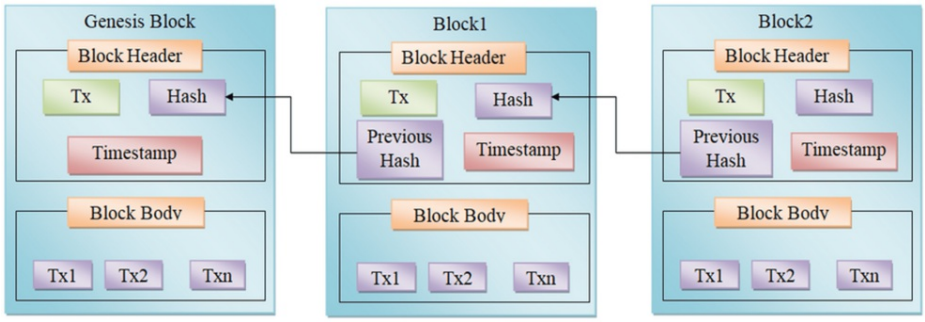

FIGURE 2: Blockchain

As Table *2* demonstrates, blockchain has evolved and improved over time to the point that it currently has four versions.

Version	Key Features	Use Cases	Examples
1st Generation	Decentralized ledger	Digital currency	Bitcoin
	Proof of Work (PoW) consensus		
	Limited smart contract support		
2nd Generation	Added smart contract	Decentralized applications	Ethereum
	Ethereum Virtual Machine	Initial Coin Offering	
	Proof of Stack (PoS) consensus	Assets tokenization	
3rd Generation	Enhance scalability	Supply chain management	Carano, Pokadot, Solana
	Interoperability	Cross-chain transaction	
	Advanced consensus mechanism	DeFi (Decentralized Finance)	
4th Generation	Quantum resistance	Healthcare data management	Hedera Hashgraph, IoTA
	Enhanced security	Identity verification	
	Increased transaction speed	Internet of Things (IoT)	
Future directions	Post-quantum cryptography	Governance and DAOs	Research projects (e.g., Algorand)
	Enhanced privacy	Cross-industry applications	

TABLE 2: Evaluation of blockchain

Advantages of Blockchain

Blockchain technology offers several advantages across various industries and applications. Here are some of the key advantages of blockchain:

1) Decentralization: Blockchain stands out for its decentralization. Unlike traditional systems that rely on a central authority (such as a bank or government) for transaction validation and recording, blockchain operates on a distributed ledger. Here, multiple nodes independently validate and record transactions. This eliminates the necessity for a central authority and mitigates the risk of a single point of failure [9].

2) Security: Once a transaction is documented on a blockchain, altering it becomes exceedingly difficult due to the application of cryptographic algorithms. This provides a robust defense against fraud and unauthorized activities [10].

3) Transparency and immutability: Transactions recorded on a blockchain are entirely transparent and accessible to all participants in the network [11]. This transparency fosters trust among participants. Additionally, once a transaction is recorded, it becomes unchangeable and cannot be deleted [12]. This immutability safeguards the integrity of the data.

4) Trust and accountability: Trust is established through transparency and immutability. Participants in a blockchain network can rely on the data recorded on the ledger because they are assured it cannot be tampered with [13]. This leads to heightened accountability, as every transaction can be traced back to its source.

5) Efficiency and speed: Blockchain has the potential to process transactions more rapidly compared to traditional systems, especially for specific types of transactions, like cross-border payments. It can also diminish the need for intermediaries, resulting in faster and more streamlined processes [14].

6) Reduced costs: By removing intermediaries and automating processes, blockchain can substantially lower transaction costs. This is particularly advantageous for industries like finance, where fees for services such as remittances or cross-border payments can be exorbitant.

7) Smart contracts: They automatically execute and enforce the conditions of an agreement when predefined criteria are met [15]. This capability streamlines complex processes and diminishes reliance on intermediaries

Consensus Mechanism

In the dynamic landscape of blockchain technology, the careful crafting and thoughtful choice of consensus algorithms stand as the cornerstone for upholding the security, integrity, and decentralized nature of distributed ledgers. Numerous consensus mechanisms have emerged over the years, each addressing specific challenges and catering to various use cases. One of the earliest and most widely recognized consensus mechanisms is Proof of Work (PoW), which underpins cryptocurrencies like Bitcoin [16]. PoW depends on miners solving intricate mathematical puzzles to authenticate transactions and append blocks to the blockchain [17]. However, PoW's energy-intensive nature has prompted the development of more eco-friendly alternatives, such as Proof of Stake (PoS) [18]. PoS validators are selected based on the number of cryptocurrencies held by them as collateral, reducing energy consumption but raising questions about centralization [19]. Further innovation has resulted in Delegated Proof of Stake (DPoS), which leverages a select group of delegates to validate transactions, enhancing scalability and speed [20]. Additionally, consensus mechanisms like Practical Byzantine Fault Tolerance (PBFT) and HoneyBadgerBFT focus on achieving consensus in permissioned blockchains, ensuring efficiency and finality in transactions. Table *3* provides a simplified comparison of some key aspects of these consensus mechanisms.

Aspect	PoW	PoS	DPoS	PBFT
Consensus principle	Computational work (Mining)	Ownership stake (Validation)	Delegation of validation	Voting-based validation
Energy efficiency	High energy consumption	Low energy consumption	Moderate energy consumption	Low energy consumption
Security	Highly secure against attacks	Secure against attacks	Vulnerable to centralization	Secure against certain attacks
Scalability	Scalability challenges	Potential scalability issues	Good scalability	Good scalability
Speed	Moderate to slow	Moderate to fast	Fast	Fast
Decentralization	High decentralization	Decentralized but can vary	Moderate decentralization	Moderate decentralization
Use cases	Cryptocurrencies (e.g., Bitcoin)	Cryptocurrencies, Ethereum 2.0	Public Blockchains, EOS	Permissioned Blockchains, Hyperledger Fabric
Examples	Bitcoin, Litecoin	Ethereum 2.0, Cardano	EOS, Tron	Hyperledger Fabric, Ripple, Stellar

TABLE 3: Comparison of some key aspects of the consensus mechanism

Blockchain Platform

In the landscape of blockchain technology, various blockchain frameworks have been developed. These frameworks serve as the backbone of blockchain systems, providing the necessary architecture and infrastructure for the deployment of decentralized ledgers. One of the most prominent blockchain frameworks is Ethereum, renowned for its extensive smart contract capabilities, decentralized applications (DApps), and widespread adoption in the world of decentralized finance (DeFi) and initial coin offerings (ICOs) [21]. Hyperledger Fabric offers permissioned, modular, and scalable blockchain solutions designed for business consortia. Corda, another enterprise-focused framework, prioritizes privacy and interoperability among financial institutions, facilitating secure and confidential transactions. Further expanding the blockchain landscape, Binance Smart Chain offers a fast and low-cost alternative for developers and users, while Polkadot and Cosmos introduce interoperability by enabling different blockchains to communicate and share data seamlessly [22]. These diverse blockchain frameworks underscore the adaptability of blockchain technology, accommodating a wide spectrum of applications, from public cryptocurrencies to private consortium networks, and from decentralized finance to supply chain management, thus showcasing the versatility and potential of blockchain technology in today's digital landscape [23]. Understanding these frameworks is pivotal for selecting the appropriate one that aligns with the specific needs and objectives of a blockchain project. Table *4* provides a simplified overview of some critical aspects of these blockchain frameworks.

Aspect	Ethereum	Hyperledger Fabric	Corda	Binance Smart Chain	Polkadot	Cosmos
Consensus mechanism	PoS	PBFT	PBFT	DPoS	Nominated PoS	Tendermint BFT
Smart contracts	Yes (Solidity)	Yes (Chaincode)	Yes (Corda Contracts)	Yes (Solidity-compatible)	Yes (Parachains)	Yes (Cosmos SDK)
Privacy features	Limited	Private channels	Confidential transactions	Limited	Customizable	Confidential transactions
Interoperability	Limited	Limited (via adapters)	Limited (by design)	Limited	High (with bridges)	High (with IBC)
Scalability	Issues with scalability	Scalable	Scalable	Scalable	Scalable	Scalable
Use cases	DeFi, DApps, ICOs	Enterprise, Consortiums	Financial Institutions, Trade	DApps, DeFi	Cross-Chain, DApps	Interoperable Chains
Community support	Very strong	Strong	Strong	Growing	Strong	Growing
Permissioning	Private and public	Private	Private	Private and public	Private and public	Private and public

TABLE 4: Critical aspects of blockchain frameworks

Fog Computing and Blockchain Integration

Combining fog computing and blockchain technology offers a synergistic solution for secure and efficient IoT data transmission. Fog computing addresses the challenges of latency and bandwidth [24]. Blockchain improves the security. With the use of blockchain, fog nodes can securely transmit IoT data to the cloud while maintaining data integrity and preventing unauthorized modifications [25]. Several studies have proposed hybrid approaches that integrate fog computing and blockchain to achieve secured data transmission in IoT applications.

Use Cases and Implementation Challenges

Numerous real-world applications benefit from the integration of fog computing, and blockchain for secured IoT data transmission to the cloud [26]. These applications include smart cities, healthcare systems, industrial automation, and supply chain management, among others. Consensus procedures in blockchain networks, scalability, interoperability, and energy efficiency are a few implementation issues that still need to be resolved. Researchers have been actively investigating these challenges and proposing solutions to enable the practical implementation of secured IoT data transmission through fog computing with blockchain.

In conclusion, the literature review underscores the latest technologies such as fog computing, blockchain, and consensus mechanism, which offer a robust and efficient solution for addressing security concerns, ensuring the integrity of IoT data, and reducing latency.

Implementation

System Architecture

The proposed framework integrates fog computing with blockchain, incorporating multiple components that work together to enhance security, data integrity, and performance during IoT data transmission. As illustrated in Figure *3*, the architecture includes IoT devices, MQTT (Message Queuing Telemetry Transport) servers, fog computing with blockchain, cloud infrastructure, and end users accessing the system via the Internet.

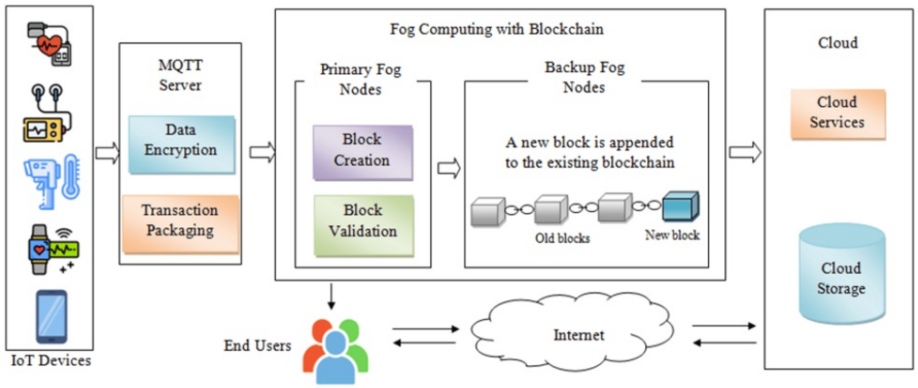

FIGURE 3: Proposed system architecture

IoT devices collect data and transmit it to the MQTT server, which acts as an intermediary between IoT devices and the fog nodes. The MQTT server receives data from IoT devices, encrypts it, packages it into transactions, and sends it to the fog nodes without storing the data. The fog nodes are divided into primary and backup groups to ensure data redundancy and integrity.

The primary fog node creates, broadcasts, and verifies data blocks by using the proposed hybrid consensus algorithm to ensure their authenticity and integrity. Once verified, the backup nodes append the new block to the existing blockchain and transfer it to the cloud. Data are stored in the cloud in its encrypted form using blockchain mechanisms to maintain security and prevent unauthorized access. This process ensures secure and efficient data handling from IoT devices to cloud storage. End users decrypt the data using private keys associated with their identities, which are granted through a secure authentication process. When a user requests access, the system verifies their authorization and provides the necessary decryption key. The decryption process follows the blockchain's encryption standards, ensuring that only authorized users with valid keys can access the original data. This ensures both data security and controlled access.

Smart Contract

The proposed model incorporates the utilization of two smart contracts.

• Block creation

Algorithm 1 shows how to generate a block, such as a genesis block or an additional next block. In the function of Algorithm 1, the genesis block is only ever created once (Table *5*). This block is the first block in the blockchain, and the prevHash of such blocks, which hold the hash value of the previous block, is set to zero. For the remaining blocks, prevHash field is set with the value of its parent's hash.

Algorithm 1: Creating block
Procedure Block (Block parent, long time, int nonce)
this.id ← latest_Id
this.time ← time
this.nonce ← nonce
this.hash_Data = Call HashProcess();
if (latest_ID = 0)
this.prevHash ← 0
this.parent ← 0
else
this.parent ← parent
this.prev_Hash ← parent.getHash();
end-if
Procedure end

TABLE 5: Algorithm to create a new block

• Hash Process:

SHA-256 algorithm is used to generate hash by merging nonce, prevHash, and field-id which is shown in Algorithm 2 (Table *6*).

Algorithm 2: Process hash function using SHA-256
Procedure HashProcess()
HashProcess ← SHA-256(this.id+this.prv_Hash+this.nonce)
Return HashProcess
Procedure end

TABLE 6: Algorithm for Hash Process

Consensus Mechanism

The proposed system integrates the features of DPoS and PBFT algorithms for transaction verification and validation, offering a secure and efficient consensus mechanism. DPoS operates on the concept of validators, which are a known set of entities with public keys, and use cryptographic keys for signing and verification. Validators participate in DPoS for leader election, while PBFT utilizes a reputation system to prevent malicious actors from participating.

The hybrid consensus algorithm is designed to handle Byzantine failures; ensuring consensus can be achieved even with a few malicious nodes. In the proposed framework, the primary fog node functions as the leader and backup nodes act as validators. Thus the time required to elect the leader is reduced. The steps of the proposed DPoS-PBFT algorithm are as follows:

1. Block creation: The leader aggregates a set of transactions into a block and signs it with its private key.

2. PBFT phase:

· Pre-Prepare phase: The primary validator creates a proposal containing the signed block and broadcasts it to all other validators. Validators verify the proposal's authenticity and contents.

· Prepare phase: Validators broadcast their "prepare" votes for the received proposal. Validators verify that they have received 2/3 of prepared votes from other validators.

3. Commit phase: If 2/3 of prepared votes are received, validators broadcast their "commit" votes. Validators verify that they have received 2/3 of commit votes from other validators.

4. Consensus check: Validators verify that they have received 2/3 of the commit votes. If successful, consensus is achieved.

5. Block addition to the blockchain: Once consensus is reached, the blockchain, accessible at the backup nodes, is expanded with a new block.

This algorithm combines the advantages of DPoS and PBFT to ensure secure and reliable transaction verification and validation.

Process Flow

Figure *4* depicts the process flow of the proposed system that combines IoT devices, MQTT server, and fog computing with blockchain to ensure secure data transmission and storage. Here is an explanation of each step in the diagram:

1. The IoT devices collect data and send it to the MQTT server for processing.

2. The MQTT server encrypts the data to ensure its security. After encryption, the data are packaged into transactions.

3. The packaged transactions are sent to the primary fog node. The primary fog node aggregates a set of transactions into a block and signs it with its private key. It broadcasts the new block to all fog nodes. The new block is then validated to ensure its authenticity and integrity by using a hybrid consensus algorithm.

4. If the block is validated, then the backup fog nodes append the new block to the existing blockchain otherwise the block is discarded.

5. Finally blockchain is submitted to the cloud for storage and further processing.

This process ensures that the data collected from IoT devices are securely transmitted, validated, and stored in the cloud through a combination of fog computing and blockchain technology.

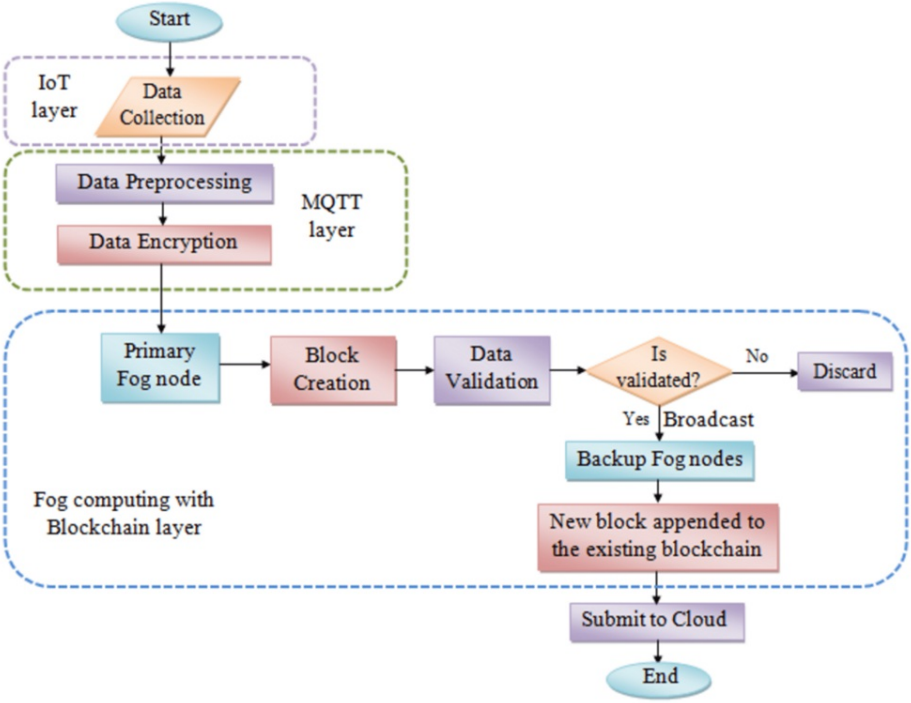

FIGURE 4: Data flow diagram of the proposed system

Experimental Setup

The experimental evaluation took place within a real-time healthcare IoT environment. Proposed Fog computing with Blockchain paradigm is evaluated through modeling and experimentation. All communication channels are secured using TLS/SSL encryption. Additionally, IoT devices are pre-registered on the blockchain to ensure secure authentication and authorization.

1. IoT devices and data types

A variety of healthcare IoT sensors are used, including:

Heart Rate Monitor - Transmitting heartbeats per minute (BPM).

Blood Pressure Sensor - Recording systolic and diastolic blood pressure readings.

Temperature Sensor - Measuring body temperature in Celsius/Fahrenheit.

Pulse Oximeter - Reporting SpO_2 levels (blood oxygen saturation).

A total of 25 IoT devices are deployed, each generating data streams at different intervals based on the sensor type (e.g., heart rate every second, blood pressure every minute). The size of each transaction ranged between 200 and 300 KB, depending on the sensor and the type of data transmitted.

2. Communication protocol and blockchain setup

MQTT is used to facilitate lightweight, reliable communication between the IoT devices and the fog nodes.

The Ethereum blockchain is employed for the implementation of the proposed system, providing decentralized and tamper-proof storage. Smart contracts are developed in Solidity to automate transaction handling and ensure the execution of predefined rules.

The blockchain component utilized a hybrid DPoS-PBFT consensus mechanism to validate transactions efficiently. A block size of 1 MB is considered to optimize storage and processing.

3. Simulation environment

The simulation is carried out using NS-3 (Network Simulator-3), which provides extensive features for modeling and simulating diverse network protocols and scenarios. This tool is selected for its ability to replicate intricate network behaviors, making it especially suitable for IoT and Fog computing environments.

4. Software environment

Operating system: Ubuntu 20.04 LTS (for fog nodes and cloud server).

Blockchain platform: Ethereum (Geth client).

Simulation tool: NS-3 for network modeling and simulation.

Programming language for smart contracts: Solidity.

Development tools: Visual Studio Code and Remix IDE for smart contract development.

This experimental setup ensures a realistic healthcare IoT environment, with secure communication, distributed processing, and decentralized data storage. The combination of fog computing and blockchain addresses latency, security, and scalability challenges, facilitating real-time healthcare monitoring and decision-making.

Evaluation Metrics

The following parameters are used to evaluate the proposed framework

a. Latency (ms): Total time required to transfer the data packet from one end to another end.

b. Accuracy: Represents correctly predicted observation to the total observation.

c. Precision: How often is the prediction correct when a positive value is predicted?

d. Recall (Sensitivity): Indicating the percentage of positive instances in the test dataset that the classifier correctly identified as positive.

e. F-Score: This is the weighted average of Precision and Recall. It is generally more informative than accuracy.

f. Verification time: Refers to the duration required to validate and confirm a block of transactions within a blockchain. This period encompasses all the processes needed to ensure that the transactions within the block are legitimate, properly formatted, and adhere to the network's consensus rules. Key aspects of verification time include:

- Transaction validation: Checking each transaction within the block for correctness and compliance with protocol rules.

- Consensus mechanism: Engaging in the protocol-specific process to reach an agreement among network participants that the block is valid.

- Block propagation: Propagating the new block through the network for consensus approval.

- Consensus finalization: Achieving a state where the majority (or required threshold) of network participants agree on the validity of the block.

Results

The result obtained after the implementation of the proposed system is compared with the conventional cloud system. Initially, the latency for 100 transactions is recorded for analysis, and then these data are extrapolated to 500 transactions for both the proposed system and the conventional cloud with the blockchain system. As shown in Figure *5*, the proposed system exhibits an 18% reduction in latency.

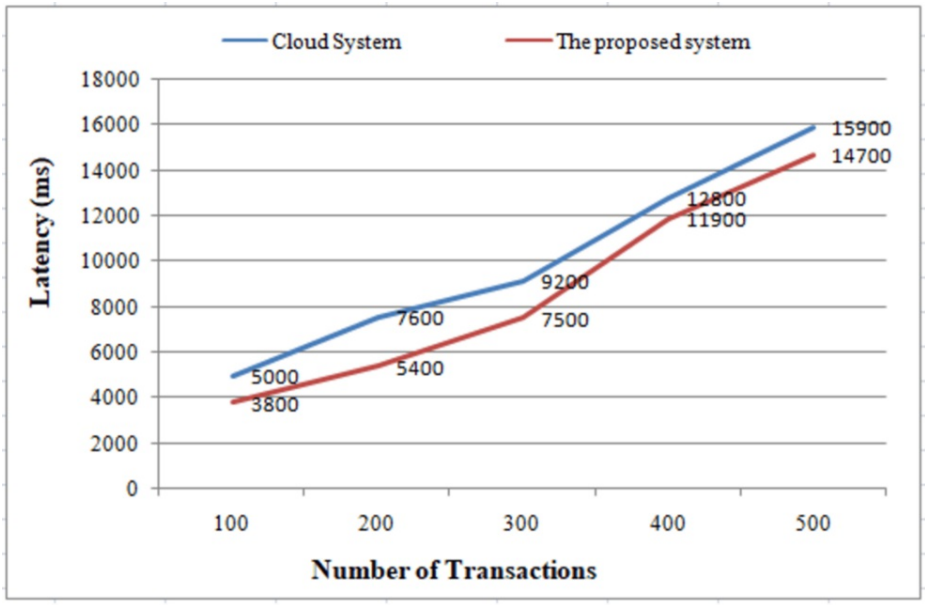

FIGURE 5: Latency comparison of the proposed system with the cloud system

Figure 6. illustrates the comparison between the suggested system and the conventional cloud system using various parameters, clearly demonstrating that the proposed technique yields superior results than the alternative.

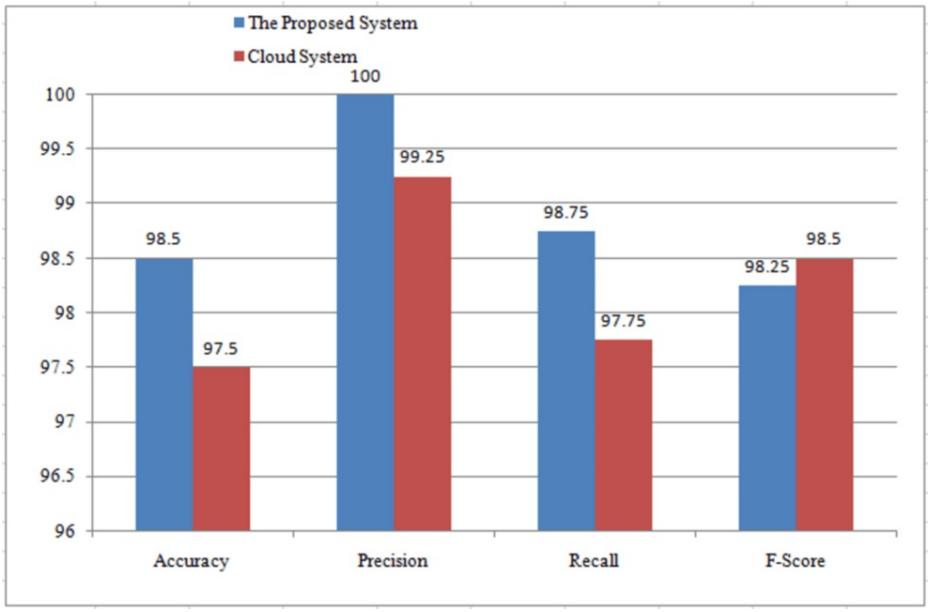

FIGURE 6: Comparison using various parameters

The observed 18% reduction in latency is attributed to the use of fog computing, which enables localized data processing and reduces the dependency on cloud infrastructure, minimizing transmission delays. The 15% improvement in accuracy stems from blockchain-based data integrity and secure authentication mechanisms, which ensure that only authorized and accurate data is transmitted and processed. These improvements highlight the effectiveness of the proposed system in enhancing responsiveness and reliability for IoT applications, especially in real-time scenarios like healthcare.

The block verification time required by different consensus algorithms is evaluated and compared with the proposed hybrid DPoS and PBFT algorithm. Figure 7 illustrates the block verification times for various consensus algorithms, revealing significant differences in their efficiency.

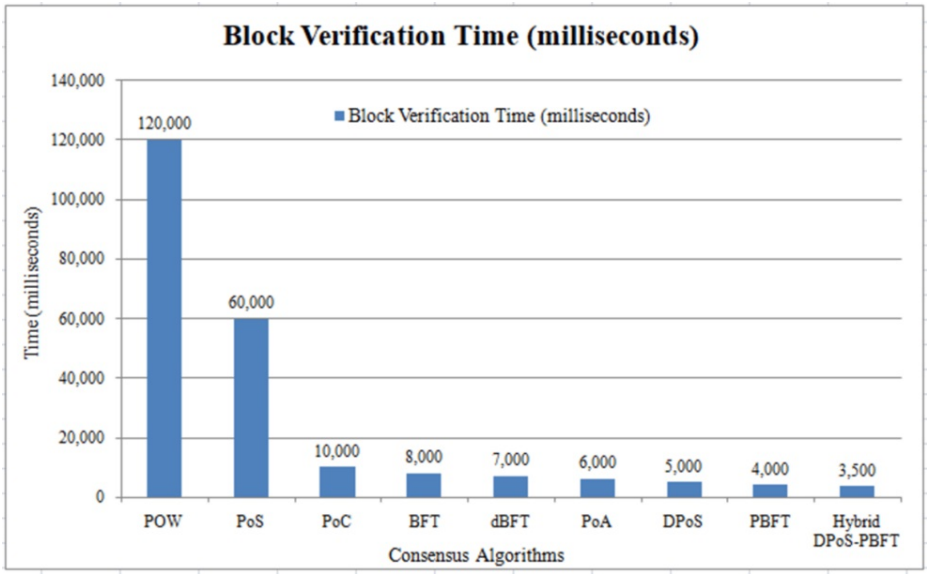

FIGURE 7: Block verification times for various consensus algorithms

PoW has the longest verification time at 120,000 milliseconds (2 minutes) due to the computationally intensive process of solving cryptographic puzzles, making it secure but slow and energy-intensive. PoS reduces this time to 60,000 milliseconds (1 minute) by selecting validators based on their stake in the network, requiring less computational effort. PoC decreases the verification time to 10,000 milliseconds (10 seconds) by utilizing unused disk space for mining, which balances efficiency and resource usage. Byzantine Fault Tolerance (BFT) achieves consensus in 8,000 milliseconds (8 seconds) through multiple rounds of voting, ensuring security and fault tolerance despite potential malicious nodes. Delegated Byzantine Fault Tolerance (dBFT) improves upon this with a verification time of 7,000 milliseconds (7 seconds), combining aspects of DPoS and BFT to elect validators and achieve consensus through phased voting. Proof of Authority (PoA) offers a verification time of 6,000 milliseconds (6 seconds) by relying on a small number of pre-approved validators, ensuring fast and efficient block creation. DPoS further enhances efficiency with a block verification time of 5,000 milliseconds (5 seconds) through elected validators. PBFT achieves one of the fastest times at 4,000 milliseconds (4 seconds) by optimizing the Byzantine fault tolerance process. Our proposed hybrid DPoS-PBFT algorithm combines the strengths of DPoS and PBFT, resulting in the shortest verification time of 3,500 milliseconds (3.5 seconds), providing a secure and efficient consensus mechanism suitable for fast and reliable transaction processing.

Discussion

The proposed system addresses critical concerns regarding data security, integrity, and latency in IoT applications by integrating fog computing with blockchain technology. By leveraging blockchain, the system ensures the confidentiality and authenticity of IoT data. Blockchain technology plays a vital role in maintaining data integrity by creating immutable records, thus preventing data tampering. The hybrid DPoS-PBFT consensus mechanism employed in the proposed system enhances security by efficiently achieving agreement among distributed nodes regarding the state of the blockchain ledger. This ensures the reliability and functionality of the blockchain network.

In contrast to traditional cloud-based IoT systems, which rely on centralized servers and are prone to single points of failure, the proposed system enhances security by distributing trust among multiple nodes. Additionally, existing studies such as Rani and Bhambay [18] and Hu et al. [20] focused on securing the data using conventional consensus algorithms like PoW and PoS, respectively. However, these algorithms either consume excessive energy (in the case of PoW) or exhibit slower transaction validation (in PoS). Our proposed hybrid consensus mechanism, combining DPoS and PBFT, significantly reduces the transaction time while maintaining high levels of security.

The integration of fog computing enables the system to reduce latency by providing localized storage and processing closer to IoT devices. Unlike purely cloud-based approaches, which introduce delays due to long-distance data transmission, the proposed system allows real-time actions and decisions to be made at the fog layer. This capability is crucial for time-sensitive applications like real-time health monitoring or emergency response systems, where every second matters.

Experimental results in a healthcare IoT environment demonstrate the proposed system's efficacy, showing an 18% reduction in latency and a 15% increase in accuracy compared to conventional approaches. The proposed framework addresses the critical challenges of data security, latency, and integrity.

While earlier research has addressed either latency reduction (through fog computing) or data security (through blockchain), very few studies have successfully integrated both technologies. The proposed system bridges this gap by offering a comprehensive framework that simultaneously addresses security, latency, and data integrity challenges. The system also ensures scalability by maintaining distributed processing across multiple fog nodes, making it applicable to large-scale IoT environments.

In conclusion, the proposed system effectively improves data security, reduces latency, and enhances performance compared to existing solutions. It offers a scalable and reliable approach for IoT applications, ensuring secure real-time data transmission and processing while maintaining a high degree of fault tolerance through the distributed fog nodes and blockchain ledger.

Conclusions

The concept of secure data transmission from IoT to the Cloud through fog computing integrated with blockchain presents a robust and promising solution for addressing the challenges of data security, integrity, and efficiency in IoT applications. The proposed system leverages blockchain technology and hybrid consensus mechanisms to establish data integrity through immutable and transparent records. It offers scalability, resource efficiency, trust, and transparency, fostering a secure and reliable IoT ecosystem.

The system provides multiple advantages. It enhances data security by encrypting data during transmission and storing it on an immutable blockchain ledger, thus protecting sensitive information from unauthorized access and tampering. The reduced latency and improved responsiveness enable timely actions and decisions, leading to enhanced operational efficiency and user experience. Scalability and resource efficiency are achieved through distributed data processing and storage across fog nodes. Trust and transparency are established by the decentralized nature of blockchain, instilling confidence in the integrity of transmitted data.

The system incorporates authentication mechanisms through the pre-registration of IoT devices and access control policies embedded in the blockchain via smart contracts. Only authorized users with valid credentials and decryption keys can access the encrypted data, preventing unauthorized access.

The experimentally tested model demonstrates a 15% improvement in accuracy and an 18% reduction in latency compared to the conventional methods. The system shows potential for various use cases across industries, such as smart cities, healthcare, industrial automation, agriculture, supply chain, and environmental monitoring. By securing data transmission and enabling real-time analytics, the proposed framework drives innovation and offers transformative benefits for IoT applications.

Ensuring seamless interoperability between different blockchain platforms and IoT protocols presents a challenge that requires further exploration.

Additional Information

Author Contributions

All authors have reviewed the final version to be published and agreed to be accountable for all aspects of the work.

Concept and design: Shatakshi Kokate, Urmila Shrawankar

Acquisition, analysis, or interpretation of data: Shatakshi Kokate, Urmila Shrawankar

Drafting of the manuscript: Shatakshi Kokate, Urmila Shrawankar

Critical review of the manuscript for important intellectual content: Shatakshi Kokate, Urmila Shrawankar

Supervision: Shatakshi Kokate, Urmila Shrawankar

Disclosures

Human subjects: All authors have confirmed that this study did not involve human participants or tissue. **Animal subjects:** All authors have confirmed that this study did not involve animal subjects or tissue. **Conflicts of interest:** In compliance with the ICMJE uniform disclosure form, all authors declare the following: **Payment/services info:** All authors have declared that no financial support was received from any organization for the submitted work. **Financial relationships:** All authors have declared that they have no financial relationships at present or within the previous three years with any organizations that might have an interest in the submitted work. **Other relationships:** All authors have declared that there are no

other relationships or activities that could appear to have influenced the submitted work.

References

1. Fersi G: Fog computing and Internet of Things in one building block: a survey and an overview of interacting technologies. Cluster Computing. 2021, 24:2757-87. 10.1007/s10586-021-03286-4.
2. Neware R, Shrawankar U: Fog computing architecture, applications and security issues. International Journal of Fog Computing (IJFC). 2020, 3:75-105,. 10.4018/IJFC.2020010105.
3. Naeem RZ, Bashir S, Amjad MF, Abbas H, Afzal H: Fog computing in internet of things: practical applications and future directions. Peer-to-Peer Networking and Applications. 2019, 12:1236-62. 10.1007/s12083-019-00728-0
4. Shukla S, Hassan MF, Khan MK, Jung LT, Awang A: An analytical model to minimize the latency in healthcare internet-of-things in fog computing environment. PLoS ONE. 2019, 14:e0224934-e0224934. 10.1371/journal.pone.0224934
5. Kokate S, Shrawankar U: An efficient approach for secured data transmission between IoT and Cloud. Research Reports on Computer Science. 2023, 35-44. 10.37256/rrcs.2320232628.
6. Guo H, Yu X: A survey on blockchain technology and its security. Blockchain: Research and Applications. 2022, 3:100067. 10.1016/j.bcra.2022.100067.
7. Rajasekaran AS, Azees M, Fadi Al-Turjman: A comprehensive survey on blockchain technology. Sustainable Energy Technologies and Assessments. 2022, 52:102039. 10.1016/j.seta.2022.102039.
8. Jena AK, Panda SK, Swain SK, Satapathy S: Blockchain Technology: Introduction, Applications, Challenges. Springer International Publishing, Cham; 2021. 1-11. 10.1007/978-3-030-69395-4_1.
9. Velliangiri S, Karthikeyan P: Blockchain Technology: Challenges and Security Issues in Consensus Algorithm. 2020 International Conference on Computer Communication and Informatics (ICCCI). IEEE, Coimbatore, India; 2020. 1-8. 10.1109/ICCCI48352.2020.9104132.
10. Khan FA, Asif M, Ahmad A, Alharbi M, Aljuaid H: Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. Sustainable Cities and Society. 2020, 55:102018.
11. Memon M, Hussain SS, Bajwa UA, Ikhlas A: Blockchain Beyond Bitcoin: Blockchain Technology Challenges and Real-World Applications. 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE). Southend, UK; 2018. 29-34. 10.1109/iCCECOME.2018.8658518
12. Attaran M: Blockchain technology in healthcare: challenges and opportunities. International Journal of Healthcare Management. 2020, 15:70-83. 10.1080/20479700.2020.1843887
13. Malik L, Arora S, Shrawankar U, Deshpande V: BlockCloud: Blockchain as a Cloud service. Blockchain for Smart Systems: Computing Technologies and Applications. Chapman and Hall/CRC, New York; 2022. 214.
14. Samanta S, Sarkar A, Sharma A, Geman O: Security and challenges for blockchain integrated fog-enabled IoT applications. Advances in Distributed Computing and Machine Learning: Proceedings of ICADCML. Springer Nature, Singapore; 2022. 13-24. 10.1007/978-981-19-1018-0_2
15. Shrawankar U, Malik L, Arora S: Virtualization technology for Cloud-based services. Cloud Computing Technologies for Smart Agriculture and Healthcare. Chapman and Hall/CRC, New York; 2020. 336.
16. Chaudhry N, Yousaf MM: Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities. 12th International Conference on Open Source Systems and Technologies (ICOSST). Lahore, Pakistan; 2018. 54-63. 10.1109/ICOSST.2018.8632190
17. Bhardwaj R, Datta D: Consensus algorithm. Decentralised Internet of Things: A Blockchain Perspective. Springer, 2020. 91-107. 10.1007/978-3-030-38677-1_5.
18. Rani P, Bhambay R: A Comparative Survey of Consensus Algorithms Based on Proof of Work Emerging Technologies in Data Mining and Information Security, Proceedings of IEMIS 2022. Springer Nature, Singapore; 2022. 1:261-68. 10.1007/978-981-19-4193-1_25.
19. Li Y, Wang Z, Fan J, Zheng Y, Luo Y, Deng C, Ding J : An Extensible Consensus Algorithm Based on PBFT. 2019 International Conference on Cyber-enabled Distributed Computing and Knowledge Discovery (CyberC). 2019. 10.1109/CyberC.2019.00013.
20. Hu Q, Yan B, Han Y, Yu J: An improved delegated proof of stake consensus algorithm Procedia Computer Science . 2021, 187:341-46,. 10.1016/j.procs.2021.04.109.
21. Ramadoss R: Blockchain technology: an overview. IEEE Potentials. 2022, 41:6-12. 10.1109/mpot.2022.3208395
22. Zhao Z: Comparison of Hyperledger Fabric and Ethereum Blockchain. 2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC). IEEE, Dalian, China; 2022. 584-87. 10.1109/IPEC54454.2022.9777292
23. Mohammed AH, Abdulateef AA, Abdulateef IA: Hyperledger, Ethereum and Blockchain Technology: A Short Overview. 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). Ankara, Turkey; 2021. 1-6. 10.1109/HORA52670.2021.9461294
24. Sinha S, Bhatnagar V, Agrawal P, Bali V: Integration of the Cloud with fog computing to secure data transmission between IoT and Cloud. Integration of Cloud Computing with Emerging Technologies. Issues, Challenges, and Practices. CRC Press, Boca Raton; 2023. 270. 10.1201/9781003341437.
25. Shukla S, Thakur S, Hussain S, Breslin JG, Jameel SM: Identification and authentication in healthcare Internet-of-Things using integrated fog computing based blockchain model. Internet of Things. 2021, 15:100422. 10.1016/j.iot.2021.100422
26. Ahmad I, Abdullah S, Ahmed A: IoT-fog-based healthcare 4.0 system using blockchain technology. Journal of Supercomputing. 2023, 79:3999-4020. 10.1007/s11227-022-04788-7.