IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 22 September 2023, accepted 30 November 2023, date of publication 5 December 2023,
date of current version 10 January 2024.

Digital Object Identifier 10.1109/ACCESS.2023.3339754

RESEARCH ARTICLE

Enhancing Logistics With the Internet of Things: A Secured and Efficient Distribution and Storage Model Utilizing Blockchain Innovations and Interplanetary File System

NWOSU ANTHONY UGOCHUKWU[1], S. B. GOYAL[1], (Senior Member, IEEE), ANAND SINGH RAJAWAT[2], CHAMAN VERMA[3], AND ZOLTÁN ILLÉS[3]

[1]Faculty of Information Technology, City University, Petaling Jaya 46100, Malaysia
[2]School of Computer Sciences and Engineering, Sandip University, Nashik 422213, India
[3]Department of Media and Educational Informatics, Faculty of Informatics, Eötvös Loránd University, 1053 Budapest, Hungary

Corresponding authors: Chaman Verma (chaman@inf.elte.hu) and S. B. Goyal (drsbgoyal@gmail.com)

The work of Chaman Verma and Zoltán Illés was supported by the Department of Media and Educational Informatics, Faculty of Informatics, Eötvös Loránd University, Budapest, Hungary.

ABSTRACT Logistics transports, stores, and delivers goods from the producer to the final user. Logistics have become increasingly complex in today's globalized world, making it imperative to address data integrity, transparency, and secure storage challenges. IoT devices in logistics allow for real-time monitoring of goods, vehicles, and environmental conditions. However, this generates vast amounts of data, necessitating a reliable and secure data storage and management system. These issues above can be addressed by deploying a blockchain-based solution. Blockchain is an innovative technology that operates on a decentralized database system, and it has different applications, which include finance, healthcare, and so on. This research proposed a blockchain- IoT-based Model for enhancing the logistics process. The proposed model utilized the Interplanetary file system to secure and efficiently store logistics data on a distributed and decentralized network and the SHA-256 hashing algorithm to ensure users' private information anonymity. The model also establishes rules by using smart contracts, which increases efficiency. The performance evaluation of the proposed model was done based on the security transactions, latency, cost, and throughput. The experimental results and performance evaluation show that the proposed model is more efficient and secure than the existing blockchain-based systems. Additionally, the proposed model offers the real-time monitoring of goods while in transit. The proposed model solves the IoT logistics system's Security, storage, and interoperability challenges. It also provides recommendations for logistics stakeholders to adopt blockchain technology. Despite the implications, the limitation of this study is that it was tested in a controlled environment.

INDEX TERMS Blockchain, efficiency, hashing algorithm, IoT, IPFS, logistics system, smart contract and security.

I. INTRODUCTION

A. GENERAL CONTEXT

The logistics industry is vital to the world economy as it moves and delivers goods and services from producers to consumers [1]. However, logistics operations involve complex procedures requiring efficient handling of numerous goods, vehicles, storage facilities, and stakeholders. It entails delivering the correct goods to the right customer in the proper condition at the right destination [2].

The logistics integration with the IoT has significantly improved the logistics domain. The IoT device aids in

The associate editor coordinating the review of this manuscript and approving it for publication was Alessandro Pozzebon.

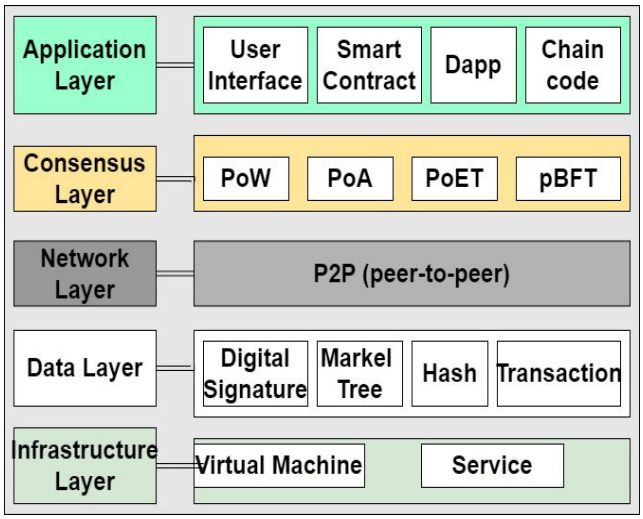

FIGURE 1. The blockchain-layered architecture.

efficiently acquiring logistics data using radio frequency identification (RFID), sensors, bar codes, [3] etc. In addition, the IoT tracking device helps in the real-time location of goods, which invariably increases the end-to-end visibility in logistics operations. IoT devices also help monitor logistics shipment conditions in transit using real-time sensing capability.

Despite the benefits of IoT in logistics, it poses some privacy, Security, and efficiency challenges in logistics systems. For example, the centralized database nature of IoT-enabled systems makes logistics systems more vulnerable to cyberattacks. Some vulnerable cyber-attacks in IoT-enabled logistics systems include DoS, DDoS, masquerading, insider attacks, and so on [4]. In addition, the vast amount of data collected with IoT devices creates efficiency issues that affect the logistics systems' data processing time and scalability. Finally, the inability of IoT devices to exchange data with other devices(interoperability) hinders the efficiency of information flow in logistics systems. However, the existing logistics system solution has yet to be able to address these challenges. Therefore, to address the issues above, we deploy a blockchain-based innovation with interplanetary file systems (IPFS) in the logistics system.

Blockchain is a distributed ledger system that provides a secure, decentralized network. It offers an environment where peer-to-peer networks validate transactions using cryptographic techniques to protect data [5]. Blockchain enables a transaction to be carried out in the network without the permission of a central authority. The decentralization features in blockchain reduce the risk of one-point failure attacks [6]. Blocks store transactions in the blockchain, and each block contains transaction data, timestamps, block hashes, Merkle toots, etc. These features offer better Security with anonymity, immutability, and transparency [7]. Fig 1 depicts the blockchain layer architecture.

Application Layer: This is the topmost layer of the blockchain, where smart contracts and decentralized applications interact with the users via scripts.

Consensus Layer: This layer is responsible for the authentication of transactions. It deploys nodes to validate transactions.

Network Layer: This layer is referred to as propagation or p2p layer. It helps nodes in the blockchain network to identify another node for internode communications.

Data Layer: This layer is responsible for storing data. When a transaction is validated through a consensus mechanism, the data is recorded in a block and linked in a chain.

Infrastructure Layer: This layer consists of a data server that securely stores data in the blockchain.

IPFS (interplanetary file system) is a decentralized [8] storage system used to store and distribute data in files with hashing identifiers that offers strong Security with low latency in data sharing and communication in the IoT network.

However, this research aims to develop a holistic logistics model that leverages the capabilities of IoT, blockchain, and IPFS to address the following key objectives:

Real-time Monitoring: Utilizing IoT sensors and devices to monitor the condition, location, and status of goods in transit, ensuring real-time traceability and transparency.

Data Integrity and Security: Implementing blockchain technology to create an immutable record of transactions, thereby ensuring the integrity and Security of logistics data, including the tracking of goods, contracts, and payments.

Efficient and Resilient Data Storage: Leveraging the IPFS to securely store and retrieve logistics data in a decentralized and efficient manner, reducing data redundancy and improving data availability.

Cost Reduction: Evaluating the proposed model by optimizing routes and reducing the cost of transportation and delivery.

Enhance Scalability and Interoperability: Develop smart contracts on the blockchain to automate IoT devices and streamline logistics processes, including goods monitoring, route optimization, and warehouse management.

B. THE CONTRIBUTION OF THE RESEARCH

The primary contributions of this study are presented as follows:

a) The research proposed a secured and efficient blockchain-based IoT logistics model on distributed and decentralized Ethereum networks.
b) A secured security mechanism that utilizes the SHA-256 hashing algorithm was deployed to improve users' private data anonymity. The model also used the Ethereum blockchain smart contract to enhance the system's efficiency
c) The proposed model deployed a secured, distributed, and decentralized storage mechanism using the IPFS system to store gathered logistics data.

d) The security evaluation of the proposed model is done based on DoS, DDoS, Sybil attacks, etc., while the performance evaluation is done based on latency, cost, and throughput of transactions. Experimental results show that the proposed model is more secure and efficient than the existing blockchain-based systems.

C. RESEARCH ORGANIZATION

The remaining parts of the research are organized as follows: Section II presents the background of the study, which comprises the overview of the IoT technology, the IoT in logistics, and the challenges of IoT logistics systems. In addition, this section also presents the blockchain smart contract with a hashing algorithm and IPFS mechanism with blockchain. Section III reviews the existing literature and works on two streams. They comprise blockchain-based logistics applications, IoT-enabled blockchain systems in different domains, and the limitations of related works. Section IV describes the proposed work, which consists of the proposed model, operational flow, the deployed smart contract algorithm, and the experiment environment setup. Section V presents the results and findings, which include security and performance analysis. Section VI offers the study's discussion, which addresses scalability and real-life deployment of the proposed model, and section VII concludes the research and recommends future research directions.

II. BACKGROUND OF RESEARCH

A. OVERVIEW OF IOT TECHNOLOGY

Internet of thing (IoT) may be defined as a network of physical objects, such as wearables, machines, etc., equipped with sensors, network connectivity, or other technologies that enable data exchange between devices [9]. The perspectives on the IoT paradigm for applications and developments are categorized as thing-based, internet-based, and semantic-based view [10].

Things-Based Perspective: This focuses on the research and development of physical and virtual things into smart things. Thus, IoT features itself as a technology responsible for this development. The embedded technologies in tracking and identification devices (RFID, barcode) facilitate smart objects to function effectively.

Internet-Based Perspective: This deals with developing Internet protocol-based networks, which facilitate smart objects to link and communicate with one another. All the things connected to the IoT network are recognized through their respective internet protocol addresses (IP addresses). The IPSO Alliance (IP for intelligent objects) developed an IP stack, a lightweight protocol to link a quiet number of IP-oriented bright things.

Semantic-Based Perspective: With the rising number of connecting devices in IoT systems, a vast amount of data is generated and transmitted with IoT devices. These data are diverse in terms of types, content, and shape. These data, which may originate from homogenous or heterogenous environments, create an interoperability problem in IoT networks. The Semantic IoT Perspective helps resolve this issue and allows IoT systems to recognize and extract raw data in homogenous or heterogeneous environments using semantic technologies. Semantic technology also aids in analysing and interpreting pre-processed data for a better understanding and fast decision-making [11].

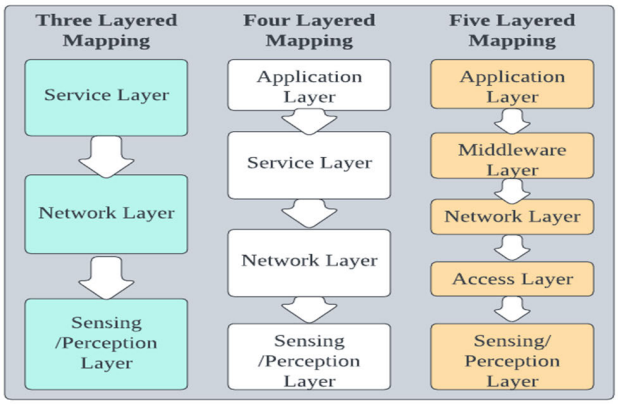

FIGURE 2. Architecture models of IoT-based systems with different mapping layers.

The concept of an IoT system can be compiled from all these perspectives and be construed as the interconnection and interoperation between intelligent objects connected to a network that facilitates ubiquitous data exchange. Thus, from an architectural view, IoT systems comprise numerous components with various characteristics that work in conjunction to achieve the functions of systems. It contains four layers: The sensing layer is used for data acquisition, the network layer is used for data communication, and the data processing layer is used for developing applications and services. The interface layer is used for end-user access to applications) [12]. IoT systems offer intelligent services like in-depth data analysis and prediction. Fig 2 depicts the three different architecture models of IoT-based systems with their mapping layers.

B. INTERNET OF THINGS IN LOGISTICS

The evolution of IoT technology in logistics has drastically transformed logistics operations. The data analytics generated from IoT-enabled logistics systems facilitate fast decision-making. IoT logistics (smart logistics) technology enablers comprise sensing and tracking devices such as GPRS, GPS, Bluetooth, 2G, 4G, WSN, etc. The machines facilitate the acquisition, transmission, and distribution of logistic data. Fig 3 shows the use cases of the Internet of Things in logistics.

Inventory Management: IoT sensors can monitor inventory levels in warehouses and distribution ports. Real-time stock-level data helps forecast demand better, reducing overstocking and understocking issues.

Asset Tracking: IoT sensors and GPS devices can be attached to trucks, containers, pallets, and individual

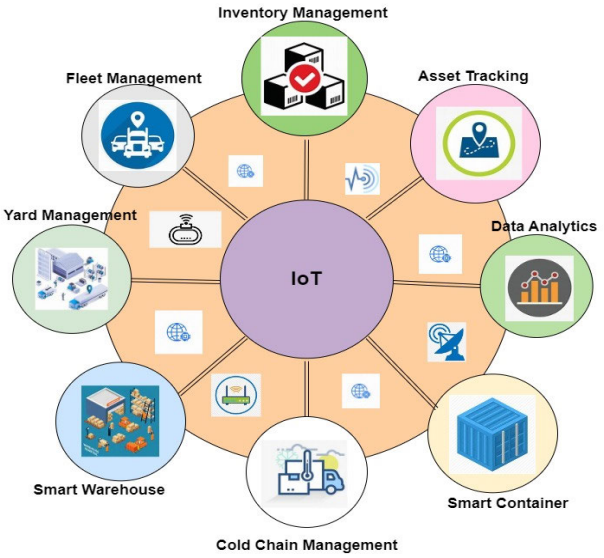

FIGURE 3. The use cases of IoT in logistic.

packages to track their real-time location. This enables logistics companies to monitor the movement of goods, optimize routes, and reduce theft and loss.

Fleet Management: IoT enables efficient fleet management through vehicle diagnostics, fuel monitoring, driver behavior tracking, and route optimization. This results in cost savings, improved safety, and reduced environmental impact.

Smart Containers: Containers equipped with IoT sensors can provide valuable data on cargo conditions, including humidity, temperature, shock, and tampering. This information is crucial for ensuring the integrity and quality of goods.

Smart Warehouse: The warehouse serves as a distribution or storage facility. Multiple logistics assets in warehouses are the core source of complexit **y.** Smart warehouse management implies using connected IoT devices that provide data about the availability of space or capacity in the warehouse to enhance the optimal usage of the warehouse for the storage of logistics goods.

Yard Management: IoT sensors and RFID technology can be used for efficient yard management, helping companies manage the flow of goods in and out of distribution ports.

Data Analytics: Analyzing IoT data to gain insights into operations, identify trends, and make data-driven decisions in logistics operations.

Cold Chain Management: For transporting temperature-sensitive goods such as pharmaceuticals and perishable foods, IoT sensors can monitor temperature, humidity, and other environmental conditions to ensure that products remain within specified ranges during transit.

C. CHALLENGES OF IOT LOGISTICS SYSTEMS

The significant challenges confronting IoT logistics systems are privacy, Security, scalability, and interoperability issues [13], [14].

- **Privacy Issue:** The privacy issues of IoT-enabled logistics result from the ubiquitous smart-integrated artifacts or sensors that allow information distribution in logistics operations. The pervasive connectivity provided by Internet access creates an avenue for privacy concerns by making the data of anonymous users more accessible.
- **Security Issue:** The IoT systems consist of traditional computers, computing devices, and sensors. The deployed sensors are often part of a collection of shared types of equipment with the same features and similar components. They also have a centralized database system. The quality makes them susceptible to the same pattern of attack.
- **Scalability Issue:** The vast amount of data collected from IoT sensors from a heterogeneous environment affects the data retrieval from the storage, affecting operation efficiency.
- **Interoperability:** This issue arises in IoT networks due to the vast data IoT devices generate. As more devices join the IoT system network in the heterogeneous environment, generating diverse data with different data sizes and contents creates interoperability issues. In addition, th inability of these sensing devices to communicate between themselves in heterogeneous environments hinders the adoption of IoT in logistics.

However, all these identified issues in IoT logistics will be addressed in this study by deploying blockchain smart contracts, hashing algorithms, and (IPFS).

D. BLOCKCHAIN SMART CONTRACT AND HASHING ALGORITHM

Smart contracts are non-hackable, self-executable computer programs stored in the blockchain server [15]. It can verify the accuracy of the rules, instructions, and conditions that are put into effect. Smart contracts are created using a high-level programming language, Solidity. Smart contracts can regulate interactions between parties to speed up decision-making, and when storing transaction data, intelligent contracts adhere to the blockchain consensus mechanism [16].

Blockchain utilizes a hashing algorithm to improve the anonymity of data. In blockchain hashing algorithms, the input and output data can be alpha-numeric. The hash functions are mathematical operations that change input values with variable lengths or predetermined lengths. The hash value is used to describe the result of a hash function. SHA denotes a secured hashing algorithm, and Table 1 depicts the types of hashing algorithms used for the Security of data.

E. THE INTERPLANETARY FILE SYSTEM MECHANISM WITH BLOCKCHAIN

An interplanetary file system (IPFS) is a distributed and decentralized file storage system that offers an efficient storage system [17]. It defines how data in files moves over an IoT network. The IPFS network is very efficient since each file has a unique hash identifier, which helps in reducing the tendency of file redundancy. In IPFS, a file can only be updated on the IPFS network when several peer nodes publish

TABLE 1. Types of hashing algorithm.

Types of hashing algorithms	Description	Output size
MD5(Message digest)	This kind of algorithm is not cryptographically based, and it is measured in seconds	128 bits/16bytes
SHA-1	It consists of 1 hashing algorithm	160 bits/20 bytes
SHA-2	This hash consists of 2 algorithms (SHA-256 and SHA-512). The SHA-512 algorithm is more secure than SHA-256.	SHA-256(256 bits/32 bytes) SHA-512(512 bits/64 bytes)
SHA-3	It is a subset of the primitive family of Keccak with broader cryptography	SHA-(224) (256) (384) (512) bits

it. A file can be requested directly using its hash_ID rather than the actual file name.

A single IPFS object can store up to 256 kB in the size of files. Larger files are divided into 256 kB-sized units and dispersed throughout a network of nodes to be stored. IPFS uses the protocols of the Merkle tree to create a unique hash_ID. The hash_IDs assigned to each section of the original file are then added to create a single hash ID. Every file stored in the IPFS is identified by its unique hash ID, and the file will only be published and stored in the blockchain network after it passes the validation check.

III. RELATED WORKS

As a disruptive technology, blockchain has been deployed in the logistics supply chain domain to enhance visibility and improve efficiency. In this section, we present the applications of blockchain in logistics, IoT systems, and existing blockchain-based solutions in logistics.

A. BLOCKCHAIN APPLICATIONS IN LOGISTICS

Blockchain has been applied in different areas of logistics operation. For example, [18] proposed a food anti-counterfeiting traceability system utilizing smart contracts and the Ethereum blockchain platform. Blockchain is used to improve the Security of data records. The blockchain storage of the system ensured fast data retrieval. However, the plans were limited; they were dress trade party trust issues. [19] proposed a blockchain-based logistics solution on a peer-to-peer network. The authors used the Ethereum smart contracts and the RSA encryption method to improve the efficiency of the logistics system and the privacy of clients' private information. The proposed system's performance was evaluated in terms of throughput and latency. [20] presented an Ethereum blockchain-based solution for efficient tracking of healthcare materials. The author proposed a smart contract on decentralized off-chain storage. The smart contract was used to promote data provenance and improve the Security of transaction history. The security analysis of the proposed system, as well as its performance, was tested.

B. BLOCKCHAIN APPLICATIONS IN IOT SYSTEMS

Blockchain has been applied to IoT systems to solve different sector problems. For instance, using blockchain technology, [21] designed a novel authentication method for dispersed healthcare networks. Users are connected using the distributed identity. Public blockchain connected IoT devices with the distributed hospital network. Verification is unnecessary if participating individuals or devices move across hospitals. As a result, it cuts down on the time needed to authenticate genuine users or devices [22] blockchain to create a revolutionary rating-based data allocation technique for IoT. This approach uses the rating value to assign the data to the on-chain storage system. Additionally, it deploys a data controller that chooses how to distribute data across blockchain storage using fuzzy logic. The system's limitation is that it takes longer to complete the transactions [23] presented a blockchain-based, lightweight, and secure solution for healthcare systems. This model uses IoT devices for remote monitoring, and cryptographic techniques are used instead of a PoW algorithm. [24] presented an Ethereum innovative contract-based logistics management platform with IoT integration. The logistics data were collected using IoT Sensor devices. Blockchain storage acts as a central repository for all transactions. The author proposes the sequence diagram of the system, although the reliability of the framework was not tested. Table 2 compares related works on blockchain-based solutions in different domains.

C. EXISTING BLOCKCHAIN-BASED SOLUTIONS IN LOGISTICS

Blockchain technology has been increasingly explored and implemented in logistics systems due to its potential to enhance transparency, Security, and traceability. Table 3 summarizes the existing blockchain-based logistic solutions with their identified challenges.

The objective of this table is to present an informative and straightforward overview of the constraints identified by different writers and researchers in the blockchain solutions currently in use in the logistics industry. It will also act as a basis for demonstrating how the study's suggested model handles these particular difficulties.

Based on the identified limitations of the existing blockchain IoT solution, this research will implement a blockchain-based IoT logistics model deploying IPFS to address these issues.

IV. THE PROPOSED WORK

This part of the study presents the proposed model, the improved smart contract algorithms, and the materials used for the deployment of the Ethereum smart contract.

A. THE PROPOSED SYSTEM MODEL

The proposed blockchain-IoT-based model for an efficient and secured logistics operation is depicted in Fig 4.

TABLE 2. Comparison of blockchain-based solutions in different domain.

Author	Description	Technology Used	Domain	Limitations
[18]	Blockchain-based solution for tracking agricultural products	Ethereum Smart contract	Food-Agro Supply chain	Lack of proper authentication of the user
[19]	Blockchain-based solution for management of logistics goods, Security of client information	Ethereum smart contract, RSA encryption Method	Logistics/ Supply chain	Inadequate Security of user data
[20]	Blockchain-based solution for tracking medical product	A smart contract, decentralized storage	Pharmaceutical Logistics	Low efficiency
[21]	Blockchain-based solution for authentication of the healthcare network users	IoT devices, Blockchain Technology	Healthcare domain	Low efficiency
[22]	Blockchain-based system for rating-based data allocation	Blockchain, an On-chain storage system Fuzzy logic	Internet of Things Domain	Scalability Issues
[23]	Blockchain-based solution for monitoring and Security of healthcare system	Cryptographic techniques and IoT sensor	Healthcare Logistics	Lack of privacy of data
[24]	Blockchain-based solution for the management of logistics operation	IoT sensor, Ethereum smart contract	Logistics supply chain	Low Scalability
[25	Blockchain-based smart contract for logistics/supply chain	Smart Contract	Logistics Supply chain	High latency

The system model is made of the following components.

- The stakeholders: This comprises manufacturers, transporters, retailers, distributors, and customers. They are the users of the proposed system.
- IoT devices: sensors, RFID tags, GPS trackers, cameras, etc. These IoT devices collect and transmit data from different physical logistics assets.

TABLE 3. Existing blockchain-based solutions in logistics.

Authors /Citations	Blockchain Proposed Solutions	Limitations/Challenges Identified
[26]	Solution for Supply Chain Tracking	• Restricted scalability as transaction volumes rises • High data processing latency • Insufficient data privacy measures
[27]	Decentralized Logistics Management System	• Security flaws in the design of intelligent contracts • Interoperability problems with current logistics systems User interface complexity resulting in low adoption
[28]	Blockchain for Asset Tracking in Logistics	- Ineffective consensus process that raises transaction costs - Limited real-world applicability because of regulatory restrictions - Inadequate resilience against sophisticated cyberattacks
[29]	IoT-Blockchain Integration for Fleet Management	-Blockchain Integration in fleet management. - Difficulties with data synchronization throughout the blockchain network - -Excessive energy usage of the consensus algorithm
[30]	Blockchain Solution for Cold Chain Monitoring	• Low throughput hinders the ability to monitor data in real time. • Inadequate safeguards against loss of data integrity • Integration with conventional cold chain

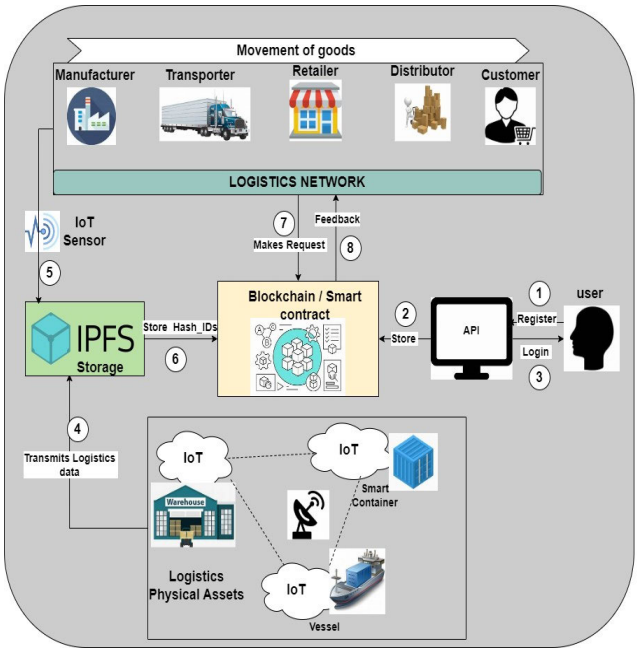

FIGURE 4. The proposed blockchain-based IoT logistics model.

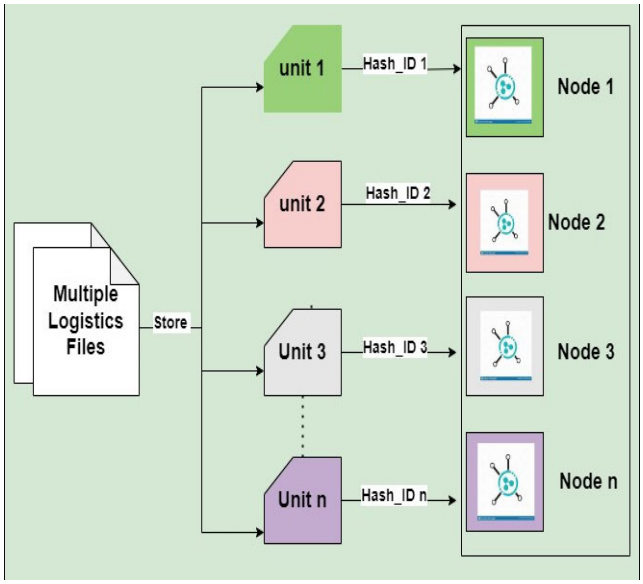

FIGURE 5. Logistics data/file distribution scheme with IPF.

- Blockchain: a distributed ledger that verifies transactions and occurrences.
- Smart contracts: The smart contract enforces agreements and automates operations
- IPFS: The IPFS stores data in a distributed decentralized format with unique hash_ID. Fig 5 depicts the IPFS distribution and decentralized storage scheme deployed by the model.

The proposed model operation is highlighted in the following steps below;

Step 1: The registration of (manufacturers, transporters, retailer' customers) and IoT devices through the application interfac

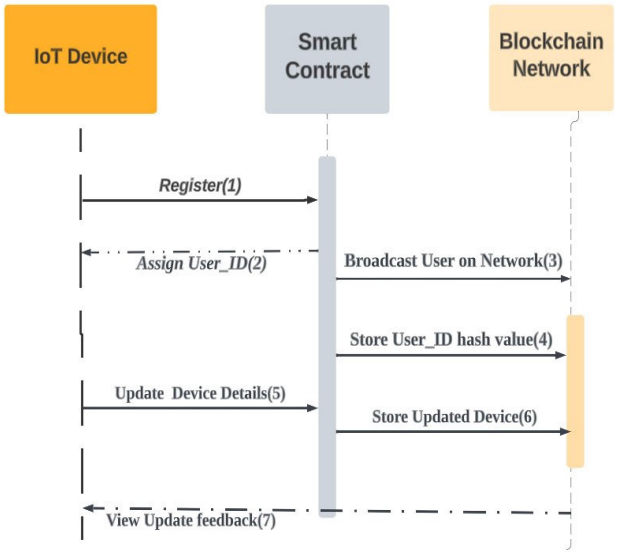

FIGURE 6. Sequence diagram of IoT device registration.

Step 2: The assigned user_IDs and device_IDs are automatically stored in the blockchain.

***Step 3*:** The registered users and devices can log in to the syste**m**

Step 4: The data gathered from the logistics physical assets are Stored in the IPFS, where they are assigned with unique hash_ID

Step 5: The data generated from logistics stakeholders are stored in the IPFS with a unique hash value.

***Step 6*:** The generated Hash_IDs are published in the blockchain.

Step 7: The registered users make some transactions such as customers, tracking goods, manufacturers checking the availability of the warehouse, etc.

Step 8: The feedback on the transactions will be sent to the initiator.

Fig 5 depicts the sequence diagram for registering IoT devices into the blockchain network utilizing smart contracts.

The device owner registers their device and is initiated by a smart contract, and they will be issued user_ID. The data is assigned with hash_ID and published in the blockchain network.

Fig 6 depicts the interaction between logistics stakeholders, IoT devices, IPFS, and blockchain.

The logistics stakeholders register through the application interface initiated by a smart contract. They can make inquiries through the application interface and receive feedback. The logistics data acquired or gathered by IoT devices is stored in the IPFS and assigned hash_ID. The hash_ID is broadcast on the blockchain network.

B. THE DEPLOYED SMART CONTRACTS ALGORITHMS IN THE PROPOSED SYSTEM MODEL

The core functions of the system consist of the following.

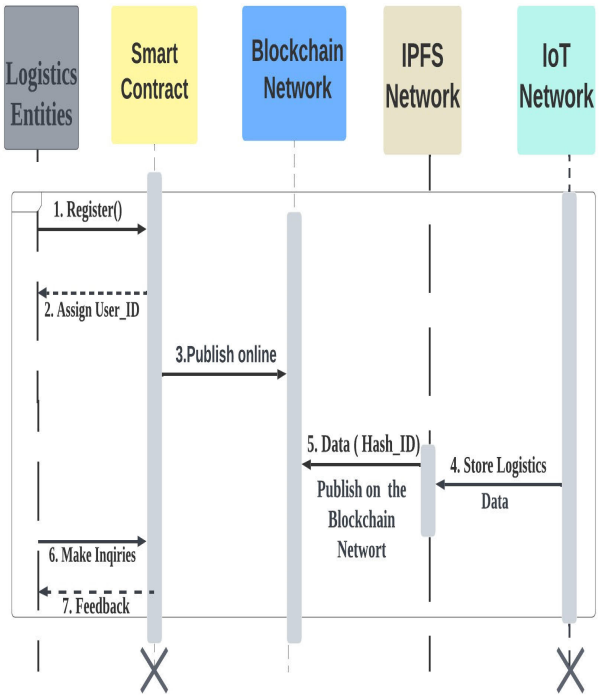

FIGURE 7. Sequence diagram for interaction between logistics entities devices, IPFS, and blockchain.

TABLE 4. Notations with meaning.

Notations	Meaning
User_AD	User address
User_ID	User unique identification
Asset_AD	Asset Address
Asset_ID	Asset unique identification
$\text{Asset}_{\text{CERT\_ID}}$	Asset Certification identification
Stakeholders	(Manufacturers, Suppliers, Distributors)

- Register _User: Register the User and assign the user_ID and public key.
- register_device: writes a new IoT device to the blockchain and gives it an ID and public key
- send_data: sends encrypted and signed data from an IoT device to the blockchain
- store_file: stores an image or document to the IPFS network and returns its hash
- retrieve_file: retrieves a file from the IPFS network using its hash
- create_contract: creates a blockchain smart contract that outlines the terms and conditions of a logistics operation
- execute_contract: executes a blockchain smart contract using IoT data and events.

All the notations used in the smart contract algorithms are depicted in Table 4.

Algorithm 1 describes the smart contract execution for registrations of logistics stakeholders (manufacturer, supplier, and distributor) and logistics physical assets (warehouse, ship, trucks, etc.). It uses the logistics stakeholders 'details, such as address and asset address. The smart contract verifies the address and issues a user_ID. The generated user_ID is assigned with hashing value, then stored and updated in the blockchain network. The same procedure is followed by the asset owners for registration.

Algorithm 1 Registration of User and Asset

```
1:Input: User details, Asset details
2: Output: Registered and Assigned User_ID
3:  if (user_AD == True)then
4:        Register and assign User_ID
5:        Assign a hash of user_ID = (SHA-256)
6:        Store the hash of user_ID in the blockchain
7:    else
8:        Return to None
9: if (Asset address == True) then
10:           Register and assign Asset_ID
11:           Assign a hash of Asset_ID =(SHA-256)
12:           Store hash of Asset_ID in Blockchain
13:    else
14:     Return to None
15 : end if
```

Algorithm 2 Smart Contract for Validation Check on Stakeholders and Assets

```
1:Input: User detail, Asset details
2: Output: Log in to the system and generate certification of
operation
3:   if (user_ID == True) then
4: Login user to the Blockchain network
5:        else
6:           Declare that the user does not exist and create an account
7:   end if
8: if (Asset_ID == True) then
9:           login an asset to the blockchain network
10:           Generate a certificate of operation
11:        else
12:           Declare that the Asset does not exist and register an
account
13:        end if
14: if (Asset CERT_ID == Pass) then
15:           Declare Asset fit for use
16:           Transmit collected data in and save as (Hash_ID)
17:        else
18:           Reschedule for Inspection of Asset and apply for certi-
fication
19: end if
```

Algorithm 2 describes the validation checks of all the logistics stakeholders and assets with their unique User_ID. The smart contract generates a certificate of operation for the logistics physical assets and checks the Asset's functionality. The smart contract fastens the transmission of collected data from a specific asset and saves it as a file with a unique IPFS_ID. This algorithm utilized the stakeholder details and the asset details.

Algorithm 3 Smart Contract to Check Warehouse Availability and Goods Condition

```
1: Input: Asset details
2: Output: Confirm Asset availability and monitor goods condition
3: if (Asset CERT_ID =Pass) then
4:         Check for available space
5:     else
7:         Reschedule for Inspection of Asset and apply for certification
8: If(goods stored in Asset_ID >1000 Units), then
9:           Declare Asset not available for booking
10:        else
11:          Return to none 12 if (goods stored in Asset_ID < 10 units), then
11:          Mark Asset_ID open for booking
12:        else
13:          Return to none
12: If (the temperature of goods stored in Asset_ID <25 degrees), then
13:        Mark goods safe
14:        else
15:          Alert the management
16: end if
```

In algorithm 3, the intelligent contract checks the availability of assets for bookings and monitors the condition of goods with regulated temperatures. It makes use of the asset details to validate transactions.

C. EXPERIMENT ENVIRONMENT SETTINGS AND TOOLS

The experiment environment setting for the proposed model consists of the Remix IDE (Remix Integrated Development Environment). Remix IDE is utilized to deploy smart contracts using solidity language. The proposed model is implemented on an Ethereum blockchain platform, and Ethereum provides an open-sourced public blockchain network. The test net is used to check the deployment of smart contracts. The Ganache tool was utilized to set up the blockchain network. The application interface front end was created using React Native. In addition, NodeJS 10.16.0 offered a communication channel between the application interface and the Ethereum framework.

Etherscan, an analytics platform for decentralized Ethereum intelligent contracts, was utilized to record the transaction's duration in seconds and the cost of gas (fees associated with the successful execution of commerce on the Ethereum blockchain) deployed in the transaction. Table 5 shows the used tools with their specifications.

TABLE 5. Tools used with specifications.

S/NO	Tools	Specifications
1	Windows 10 personal computer	i5-10210 processor, 2.10 GHz, and 16 GB RAM
2	Remix IDE	(Intel (R) Core (TM), i5 8250U) (0.7.0)
3	IoT device	CC2530
4	Solidity Version	0.7-0.9

V. RESULTS AND FINDINGS

A. SECURITY ANALYSIS OF THE PROPOSED MODEL

The security evaluation of the proposed model is evaluated based on theorems. The security threats prevalent in IoT logistics consist of masquerade attacks, DoS, DDoS, and phishing attacks [31], [32]. The Proposed Model is secured against the following attacks with the specified mechanism:

a) Masquerade Attack: A masquerade attack enables an unauthorized user to enter a system using fictitious information or credentials. To stop a masquerade attack, the proposed model offers a registration service for users, and unauthorized users are prevented from utilizing a false identity to access the suggested application services. In the worst-case scenario, the proposed model verifies the user identification using the requested logistics certificate of operation before giving access to the transaction.

b) Denial of Service (DoS) Attack: This attack occurs when an adversary sends several bogus messages to the communication network, slowing it down and allowing it to exploit network traffic. Attacks can also be used to block or ruin communication channels. However, using IPFS with high latency will protect the Internet of logistics systems from this kind of attack.

c) Distributed Denial of Service (DDoS) Attack: This attack is similar to a traditional DoS attack. The main difference between DoS and DDoS is the attack size that an enemy could launch. In a distributed denial of service attack, an adversary jams or floods the communication channels with substantial traffic, thereby hijacking the communication network. The proposed model prevents this attack using IPFS with more decentralized nodes.

d) Phishing Attack: In this attack, the adversary has access to a user's login details, such as their user_ID, and uses it to gain access to the sensitive information, but in the proposed model, the blockchain network will store all user information as hash values. Since all user ID hash values are stored in the blockchain, it will be hard for the attacker to access this information.

e) Man-in-the-Middle Attack: In this attack, the adversary takes over the communication channel to find the identities of the real nodes participating in network exchange. Since the attacker does not need to know the alleged victim's identity, the adversary forces the server to identify the transaction as a legitimate event. However, the proposed model uses blockchain smart contracts to secure the system against this attack.

f) Sybil Attack: In this attack, the adversary initiates the attack by providing a node with multiple identities and taking over several other nodes in the network. The proposed model offers Security against this attack by using an identifying mechanism. Each user in the proposed model

TABLE 6. The security comparison between blockchain-related work and the proposed model.

Authors	Masquerading	Man, in middle	Phishing	Sybil	DoS	DDoS
[33]	✗	✓	✗	✗	✓	✓
[34]	✗	✓	✓	✗	✗	✗
[35]	✗	✓	✗	✓	✓	✓
Proposed Model	✓	✓	✓	✓	✓	✓

is validated using a different user_ID and stored as a hash, preventing the process of giving the same identity to many users.

Table 6 depicts the security comparison of existing blockchain-related works with our proposed model.

B. THE PERFORMANCE EVALUATION OF THE PROPOSED MODEL

The performance evaluation of the proposed model was done by utilizing two blockchain-based systems, the test blockchain system (Test-BS) and the proposed model. The Test-BS is a blockchain-based system on a distributed network without IPFS, while the proposed model is a blockchain-based model on a distributed, decentralized network with IPFS. The smart contract transactions consist of registration of the logistics user, generation of hashing after validation, issuing of the certificate, verification, and querying of logistics file with unique hash_ID. To evaluate the network overhead of the systems, 20 transactions were carried out; the experiment's outcome shows that the Test BS system can only handle 15 transactions, and the proposed model can handle more.

The three metrics parameters utilized in the proposed model performance analysis consist of transaction latency, cost of transactions, and throughput.

1) TRANSACTION LATENCY

Transaction Latency is the duration from the transaction submission time to the transaction completion time. Table 7 shows the transaction time on the test blockchain-based system and the proposed blockchain model with different smart contract transactions and corresponding results.

From the above table, the proposed model latency is lower than the test blockchain system. Fig 8 shows the latency comparison between the proposed model and the test blockchain system for retrieving logistics data.

From the diagram above, the latency of the proposed model is lower than that of the test blockchain syste; it is also deduced that as the amount of retrieved data increases, the transaction execution time rises, too.

TABLE 7. Comparison of transaction latency between the test system and the proposed model.

Initiators	Smart Contract functions	Test-BS Transaction Time (Sec)	Proposed model Transaction Time (Sec)
Logistics User	Registration ()	11.54	10.55
Logistic User	Generate Hash ()	10.34	9.57
Asset Owner	Issue Certifications ()	12.04	11.44
Asset Owner	Verify Certificate ()	8.58	7.47
Logistics User	Query file ()	10.11	9.45

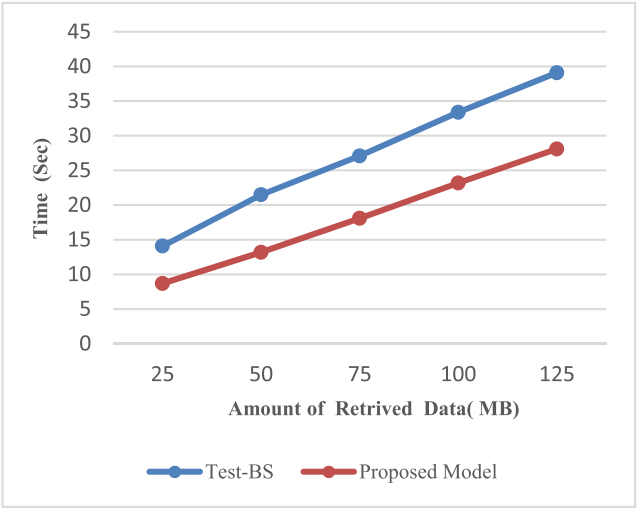

FIGURE 8. Latency comparison in data retrieval.

2) COST OF TRANSACTION

The transaction cost is the gas used to carry out smart contract transactions (where gas price $= 1Gwei$ and one ether $= 176.62USD$). Table 8 shows the cost of transactions between the test blockchain-based system and the proposed blockchain model with the corresponding results.

The above table shows that the proposed model uses a lower gas price to execute the smart contract transaction. Fig 9 compares the cost of gas for registering users between the proposed model and the test blockchain system.

The proposed model consumes less gas compared to the test blockchain system while registering users, and there is an increase in the cost of gas as the number of registered logistics users increases.

3) TRANSACTION THROUGHPUT

The transaction throughput is the number of transactions a system can process at a given time. It is measured in TPS (Transaction per second). Table 9 shows the transaction

TABLE 8. Comparison of transaction cost between the test system and proposed mode.

Initiators	Smart Contract functions	Test-BS Gas Cost (USD)	Proposed model Gas Cost (USD)
Logistics User	Registration ()	0.95	0.19
Logistics User	Generate Hash ()	1.21	0.21
Asset Owner	Issue Certifications ()	1.05	0.25
Asset Owner	Verify Certificate ()	1.15	0.31
Logistics User	Query Logistics file ()	1.10	0.45

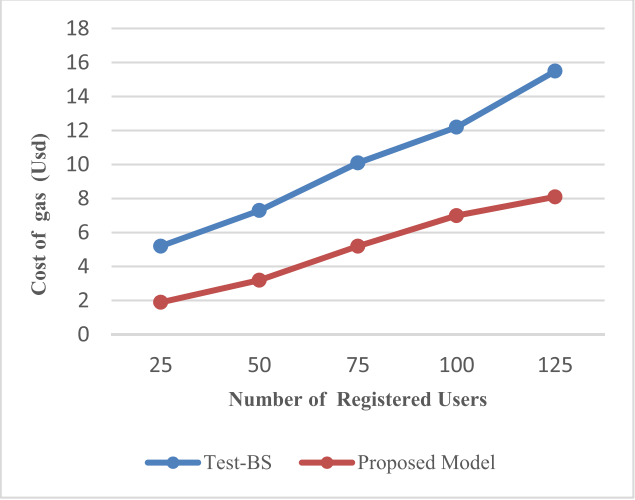

FIGURE 9. Comparison of gas cost for user registration.

TABLE 9. Comparison of transaction throughput between the test system and the proposed mode.

Initiators	Smart Contract functions	Test-BS Transaction Throughput (TPS)	Proposed model Transaction Throughput (TPS)
Logistics User	Registration ()	330	310
Logistics User	Generate Hash ()	430	475
Asset Owner	Issue Certifications ()	440	605
Asset Owner	Verify Certificate ()	431	625
Logistics User	Query Logistics file ()	552	701

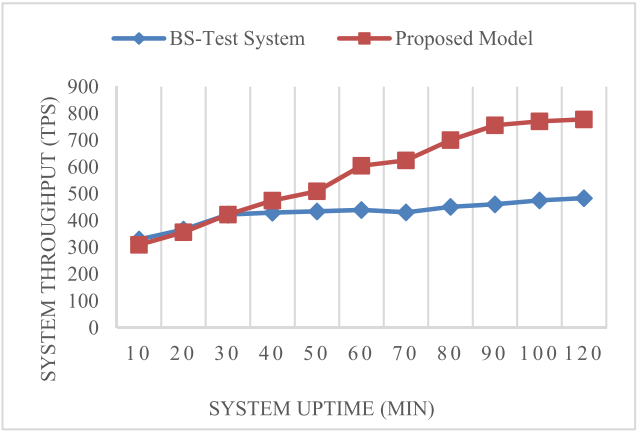

FIGURE 10. Comparison of system uptime and throughput.

TABLE 10. The comparison of blockchain-based related work and the proposed model.

Author	Access control	Data Integrity	Efficiency	Scalability	Interoperability
[36]	✓	✗	✓	✓	✗
[37]	✓	✓	✗	✓	✗
[38]	✓	✓	✓	✗	✗
[39]	✓	✓	✗	✓	✗
[40	✓	✗	✗	✗	✗
Propose System	✓	✓	✓	✓	✓

throughput between the test blockchain-based system and the proposed blockchain model with the corresponding results.

The above table shows that the proposed model has higher throughput than the test system in performing intelligent contract transactions. Fig 10 shows the comparison between the system uptime and the throughput.

From the above diagram, the proposed model system throughput is higher than the test system, and as the system uptime increases, the system throughput rises, too.

C. COMPARATIVE ANALYSIS OF THE PROPOSED MODEL AND EXISTING BLOCKCHAIN-BASED SYSTEM

The proposed model is compared with blockchain-related works. Table 10 compares the proposed model and related results on blockchain-based logistics supply chain systems.

Access Control: Th e access control of the proposed model is defined by the smart contract. The smart contract will trigger the validation of an authenticated user. But when an illegitimate user wants to access the system, the predefined smart contract will deny him access.

Data Integrity: The immutability of logistics data stored in the blockchain repository ensures that the data stored in them are tamper-proof.

Efficiency: Theefficiency is measured in terms of latency, cost of gas deployed to perform an innovative contract transaction and throughput. The model is more efficient with the use of smart contracts and IPFS.

Scalability: The use of blockchain smart contracts and IPFS Improved the scalability of the proposed system.

Interoperability: The use of intelligent contracts automated the communication between logistics sensing devices and improved interoperability.

VI. DISCUSSION

In this section, we discuss the proposed model's limitations in terms of scalability and future work for real-world deployment.

A. ADDRESSING SCALABILITY

In the present study, scalability was examined regarding the capacity of IPFS and the blockchain to withstand growing loads; however, a more comprehensive investigation is necessary. For example, the network's efficiency and Security must be maintained as the number of IoT devices and transaction volume rise. Blockchain systems are prone to this scalability issue, especially regarding transaction throughput and block size restrictions.

To overcome this, subsequent versions of our model might investigate blockchain sharding techniques, in which the network is split up into more manageable, smaller sections (shards) that can process transactions concurrently, thus boosting the total transaction throughput. Scalability may also be increased by introducing more effective consensus techniques, like Proof of Stake (PoS) or Directed Acyclic Graphs (DAGs).

B. REAL-WORLD DEPLOYMENT CONSIDERATION

Several factors beyond technological capabilities need to be considered for real-world deployment. These include cost ramifications, user adoption obstacles, regulatory compliance, and interoperability with current logistics systems.

- Regulatory Compliance: It's critical to comprehend and abide by the legal frameworks in various jurisdictions, particularly regarding data privacy (such as GDPR) and the application of blockchain technology.
- Interoperability: Our Model must integrate with current logistics systems and Internet of Things devices to facilitate seamless communication between various platforms and technologies. This may involve the need for standardization protocols or APIs.
- User Adoption: The Model should be easy to use to promote broad adoption. This entails developing user-friendly interfaces and ensuring all relevant parties know the advantages and workings of the blockchain and Internet of Things systems.
- Cost Implications: A cost-benefit analysis is necessary for real-world deployment, considering the expenditures associated with system updates, maintenance, and infrastructure.

VII. CONCLUSION AND FUTURE WORK

The originality of this research is that it identified and presented the security, privacy, and efficiency challenges of IoT logistics systems. This study mitigated all these challenges by proposing a blockchain-IoT-based logistics model for secured and efficient logistics management. This model enhances the privacy of logistics users and IoT devices by utilizing the SHA-256 hashing algorithm to enforce the anonymity of user-private information. In addition, a secure storage scheme using an interplanetary file system for storing logistics data was proposed and integrated into the IoT logistics system. The smart contracts, automated transactions, and interoperability of IoT devices enhance logistics operations' efficiency.

The findings show that the proposed model is secured against cyber threats such as insider attacks, masquerade attacks, DoS, DDoS, phishing, etc. The model is efficient in registering logistics users, registering IoT devices, issuing a certificate of operation for the Asset, checking the availability of the logistics warehouse, and monitoring the condition of goods.

The performance evaluation of the proposed model shows that the transaction latency is very low, the cost of gas used for transactions is lower compared to the (Test-BS) test blockchain system, and the throughput is higher compared to the test system. The comparative analysis shows that the proposed model is more efficient and secure than the existing logistics blockchain-based systems.

The study implies that global logistics companies with lower and higher computer configurations can use the proposed model. Smart contract automation optimizes transportation, which will help reduce transportation costs and increase the fast delivery of goods.

Despite the contributions of this study, this research is limited since the simulation was carried out in a controlled environment, and the system may encounter some challenges in a real-life scenario.

Based on the limitation of existing literature and technology deployed in this study, this research will recommend the application of machine learning and Blockchain in IoT logistics to predict data breaches and improve the Security of IoT logistics systems.

REFERENCES

[1] *Council of Supply Chain Management Professionals (CSCMP)*, Lombard, IL, USA, 2020, doi: 10.1057/978-1-349-95988-4_291.

[2] K. Wang, "Logistics 4.0 solution-new challenges and opportunities," in *Proc. 6th Int. Workshop Adv. Manuf. Autom.*, 2016, pp. 68–74, doi: 10.2991/iwama-16.2016.13.

[3] R. M. Gomathi, G. H. S. Krishna, E. Brumancia, and Y. M. Dhas, "A survey on IoT technologies, evolution and architecture," in *Proc. Int. Conf. Comput., Commun., Signal Process. (ICCCSP)*, Chennai, India, Feb. 2018, pp. 1–5, doi: 10.1109/ICCCSP.2018.8452820.

[4] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, Aug. 2018, doi: 10.3390/s18082575.

[5] I. Önder and H. Treiblmaier, "Blockchain and tourism: Three research propositions," *Ann. Tourism Res.*, vol. 72, pp. 180–182, Sep. 2018, doi: 10.1016/j.annals.2018.03.005.

[6] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019, doi: 10.1109/ACCESS.2019.2936094.

[7] N. Hackius and M. Petersen, "Blockchain in logistics and supply chain: Trick or treat?" in *Proc. Hamburg Int. Conf. Logistics (HICL)*, 2017, pp. 3–18, doi: 10.15480/882.1444.

[8] V. Tabora. (2020). *Using IPFS for Distributed File Storage Systems*. [Online]. Available: https://medium.com/0xcode/using-ipfs-for-distributed-file-storage-systems-61226e07a6f

[9] S. Dhar et al., "The advanced security model for multimedia data sharing in the Internet of Things," *Trans. Emerging Telecommun. Technol.*, vol. 34, no. 11, 2022, doi: 10.1002/ett.4621.

[10] H. Tran-Dang, N. Krommenacker, P. Charpentier, and D.-S. Kim, "The Internet of Things for logistics: Perspectives, application review, and challenges," *IETE Tech. Rev.*, vol. 39, no. 1, pp. 93–121, Jan. 2022, doi: 10.1080/02564602.2020.1827308.

[11] Z. Song, A. A. Cárdenas, and R. Masuoka, "Semantic middleware for the Internet of Things," in *Proc. Internet Things (IoT)*, Nov. 2010, pp. 1–8, doi: 10.1109/iot.2010.5678448.

[12] A. Colakovic and M. Hadžialic, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," *Comput. Netw.*, vol. 144, pp. 17–39, Oct. 2018, doi: 10.1016/j.comnet.2018.07.017.

[13] K. Shaukat, T. M. Alam, I. A. Hameed, W. A. Khan, N. Abbas, and S. Luo, "A review on security challenges in Internet of Things (IoT)," in *Proc. 26th Int. Conf. Autom. Comput. (ICAC)*, Portsmouth, U.K., Sep. 2021, pp. 1–6, doi: 10.23919/ICAC50006.2021.9594183.

[14] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, Jun. 2017, doi: 10.1016/j.jnca.2017.04.002.

[15] M. Banerjee, J. Lee, and K.-K.-R. Choo, "A blockchain future for Internet of Things security: A position paper," *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 149–160, Aug. 2018, doi: 10.1016/j.dcan.2017.10.006.

[16] S. B. Rane and S. V. Thakker, "Green procurement process model based on blockchain–IoT integrated architecture for a sustainable business," *Manag. Environ. Quality, Int. J.*, vol. 31, no. 3, pp. 741–763, Dec. 2019, doi: 10.1108/MEQ-06-2019-0136.

[17] S. Dhar, A. Khare, and R. Singh, "Advanced security model for multimedia data sharing in Internet of Things," *Trans. Emerg. Telecommun. Technol.*, vol. 34, no. 11, Nov. 2023.

[18] Y. Lu, P. Li, and H. Xu, "A food anti-counterfeiting traceability system based on blockchain and Internet of Things," *Proc. Comput. Sci.*, vol. 199, pp. 629–636, Jan. 2022, doi: 10.1016/j.procs.2022.01.077.

[19] N. A. Ugochukwu, S. B. Goyal, A. S. Rajawat, S. M. N. Islam, J. He, and M. Aslam, "An innovative blockchain-based secured logistics management architecture: Utilizing an RSA asymmetric encryption method," *Mathematics*, vol. 10, no. 24, p. 4670, Dec. 2022, doi: 10.3390/math10244670.

[20] A. Musamih, K. Salah, R. Jayaraman, J. Arshad, M. Debe, Y. Al-Hammadi, and S. Ellahham, "A blockchain-based approach for drug traceability in healthcare supply chain," *IEEE Access*, vol. 9, pp. 9728–9743, 2021, doi: 10.1109/ACCESS.2021.3049920.

[21] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K. R. Choo, and M. Aledhari, "Decentralized authentication of distributed patients in hospital networks using blockchain," *IEEE J. Biomed. Health Informat.*, vol. 24, no. 8, pp. 2146–2156, Aug. 2020, doi: 10.1109/JBHI.2020.2969648.

[22] W. Yánez, R. Mahmud, R. Bahsoon, Y. Zhang, and R. Buyya, "Data allocation mechanism for Internet-of-Things systems with blockchain," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3509–3522, Apr. 2020, doi: 10.1109/JIOT.2020.2972776.

[23] G. Srivastava, J. Crichigno, and S. Dhar, "A light and secure healthcare blockchain for IoT medical devices," in *Proc. IEEE Can. Conf. Electr. Comput. Eng. (CCECE)*, May 2019, pp. 1–5, doi: 10.1109/CCECE.2019.8861593.

[24] N. A. Ugochukwu, S. B. Goyal, and S. Arumugam, "Blockchain-based IoT-enabled system for secure and efficient logistics management in the era of IR 4.0," *J. Nanomaterials*, vol. 2022, pp. 1–10, Jun. 2022, doi: 10.1155/2022/7295395.

[25] M. A. Alqarni, M. S. Alkatheiri, S. H. Chauhdary, and S. Saleem, "Use of blockchain-based smart contracts in logistics and supply chains," *Electronics*, vol. 12, no. 6, p. 1340, Mar. 2023, doi: 10.3390/electronics12061340.

[26] J. Sunny, N. Undralla, and V. M. Pillai, "Supply chain transparency through blockchain-based traceability: An overview with demonstration," *Comput. Ind. Eng.*, vol. 150, Dec. 2020, Art. no. 106895, doi: 10.1016/j.cie.2020.106895.

[27] M. Müller, S. R. Garzon, M. Westerkamp, and Z. A. Lux, "HIDALS: A hybrid IoT-based decentralized application for logistics and supply chain management," in *Proc. IEEE 10th Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON)*, Oct. 2019, pp. 0802–0808, doi: 10.1109/IEMCON.2019.8936305.

[28] Y. Issaoui, A. Khiat, A. Bahnasse, and H. Ouajji, "Smart logistics: Blockchain trends and applications," *J. Ubiquitous Syst. Pervasive Netw.*, vol. 12, no. 2, pp. 9–15, Mar. 2020, doi: 10.5383/JUSPN.12.02.002.

[29] M. Humayun, N. Jhanjhi, B. Hamid, and G. Ahmed, "Emerging smart logistics and transportation using IoT and blockchain," *IEEE Internet Things Mag.*, vol. 3, no. 2, pp. 58–62, Jun. 2020, doi: 10.1109/IOTM.0001.1900097.

[30] S. M. H. Bamakan, S. G. Moghaddam, and S. D. Manshadi, "Blockchain-enabled pharmaceutical cold chain: Applications, key challenges, and future trends," *J. Cleaner Prod.*, vol. 302, Jun. 2021, Art. no. 127021, doi: 10.1016/j.jclepro.2021.127021.

[31] G. Coulouris. (2021). *Distributed Systems: Concepts and Design*. [Online]. Available: https://www.pearson.com/en-us/subject-catalog/p/distributed-systems-concepts-and-dsign/P200000003160/9780137521081

[32] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2027–2051, 3rd Quart., 2016, doi: 10.1109/COMST.2016.2548426.

[33] D. Bhowmik and T. Feng, "The multimedia blockchain: A distributed and tamper-proof media transaction framework," in *Proc. 22nd Int. Conf. Digit. Signal Process. (DSP)*, Aug. 2017, pp. 1–5, doi: 10.1109/ICDSP.2017.8096051.

[34] M. A. Jan, J. Cai, X.-C. Gao, F. Khan, S. Mastorakis, M. Usman, M. Alazab, and P. Watters, "Security and blockchain convergence with Internet of Multimedia Things: Current trends, research challenges and future directions," *J. Netw. Comput. Appl.*, vol. 175, Feb. 2021, Art. no. 102918, doi: 10.1016/j.jnca.2020.102918.

[35] F. Li, X. Yu, R. Ge, Y. Wang, Y. Cui, and H. Zhou, "BCSE: Blockchain-based trusted service evaluation model over big data," *Big Data Mining Analytics*, vol. 5, no. 1, pp. 1–14, Mar. 2022, doi: 10.26599/BDMA.2020.9020028.

[36] C. Xie, Y. Sun, and H. Luo, "Secured data storage scheme based on block chain for agricultural products tracking," in *Proc. 3rd Int. Conf. Big Data Comput. Commun. (BIGCOM)*, Aug. 2017, pp. 45–50, doi: 10.1109/BIGCOM.2017.43.

[37] S. Wang, X. Tang, Y. Zhang, and J. Chen, "Auditable protocols for fair payment and physical asset delivery based on smart contracts," *IEEE Access*, vol. 7, pp. 109439–109453, 2019, doi: 10.1109/ACCESS.2019.2933860.

[38] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. 6, pp. 38437–38450, 2018, doi: 10.1109/ACCESS.2018.2851611.

[39] K. Behnke and M. F. W. H. A. Janssen, "Boundary conditions for traceability in food supply chains using blockchain technology," *Int. J. Inf. Manag.*, vol. 52, Jun. 2020, Art. no. 101969, doi: 10.1016/j.ijinfomgt.2019.05.025.

[40] A. Shahid, A. Almogren, N. Javaid, F. A. Al-Zahrani, M. Zuair, and M. Alam, "Blockchain-based agri-food supply chain: A complete solution," *IEEE Access*, vol. 8, pp. 69230–69243, 2020, doi: 10.1109/ACCESS.2020.2986257.

NWOSU ANTHONY UGOCHUKWU received the Diploma, bachelor's, master's, and Ph.D. degrees in information technology from City University, Malaysia. He has participated in international conferences. He has published several WoS/Scopus-indexed journal articles. His research interests include blockchain technology, logistics management, cloud computing, the Internet of Things, cybersecurity, machine learning, and AI automation. He was a recipient of the Award Excellency as the Best Graduating IT Student from City University Malaysia, in 2020, and the Best Paper Presenter Award from the Doctoral Symposium on Computational Intelligence, in 2022. He received the Higher Achiever Award from City University, in 2023. He also received a scholarship for the Ph.D. degree. He is a Reviewer of IEEE Access.

S. B. GOYAL (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from Banasthali University, Rajasthan, India, in 2012. He is currently the Director of the Faculty of Information Technology, City University, Malaysia. He served many institutions in many different academic and administrative positions. He holds more than 20 years of work experience at national and international levels. He has peerless inquisitiveness and enthusiasm to get abreast with the latest developments in the IT field. He has good command over Industry Revolution (IR) 4.0 technologies, such as big data, data science, artificial intelligence and blockchain, and cloud computing. He is the first one to introduce IR 4.0, including blockchain technology in the academic curriculum in Malaysian universities. He had participated in many panel discussions on IR 4.0 technologies at academia as well as industry platforms. He has contributed to many Scopus/SCI journals/conferences. He holds more than ten international patents/copyrights from Australia, Germany, and India. His current research interests include blockchain, artificial intelligence, cloud computing, cyber security, the Internet of Things, data mining and warehousing, and method engineering. He had received many academic excellence awards at national and international levels. He is contributing as an editor and a co-editor in many Scopus books. He is serving as a reviewer or guest editor in many international journals published by IEEE, Inderscience, IGI Global, and Springer. He participated as a Speaker at the Bloconomic 2019 Event on Blockchain and World AI Show 2021 Event on AI.

ANAND SINGH RAJAWAT is currently a Computer Science and Engineering Professor with the School of Computer Science and Engineering, Sandip University, Nashik, India. He has published more than 100 research publications in various reputed peer-reviewed international journals, book chapters, and conferences. He has been associated with several research journals and reviewer committee members. His research interests include developing healthcare data security, privacy, and processing algorithms for the multidisciplinary field of computer science; and patient data (image, video, and text) has become the most potent tool in bioinformatics.

CHAMAN VERMA received the Ph.D. degree in informatics from the Doctoral School of Informatics, Eötvös Loránd University, Budapest, Hungary. He is currently an Assistant Professor with the Department of Media and Educational Informatics, Faculty of Informatics, Eötvös Loránd University. He is also a Postdoctoral Researcher in statistical and machine learning financed under the ÚNKP Scholarship by the Ministry of Innovation and Technology and the National Research, Development and Innovation Office (NRDIO) Fund, Government of Hungary. He has around ten years of experience in teaching and industry. He reviews many scientific journals, including IEEE, Springer, Elsevier, Wiley, and MDPI. He has Scopus citations of 820 with an H-index of 16. He has Web of Science citations 91 with an H-index of 9. He has more than 100 scientific publications in IEEE, Elsevier, Springer, IOP Science, MDPI, and Walter de Gruyter. His research interests include data analytics, the IoT, feature engineering, real-time systems, and educational informatics. He is a Life Member of ISTE, New Delhi, India; a member of the editorial board; and a reviewer of various international journals and scientific conferences. He was a recipient of the Best Scientific Publication Awards from the Faculty of Informatics, Eötvös Loránd University, Budapest, Hungary, from 2021 to 2023. He has been awarded two times the ÚNKP Scholarship for research by the Ministry of Innovation and Technology and NRDIO Fund, from 2021 to 2023. During the Ph.D. degree, he won the EFOP Scholarship, Co-Founded by the European Union Social Fund and the Government of Hungary, as a Professional Research Assistant in a real-time system, from 2018 to 2021, and the Stipendium Hunagricum Scholarship funded by the Tempus Public Foundation, Government of Hungary. He also received the Stipendium Hungaricum Dissertation Scholarship of Tempus Public Foundation, Government of Hungary, from 2021 to 2022. He has been awarded several Erasmus Scholarships for conducting international research and academic collaboration with European and non-European universities. He was the leading Guest Editor of the Special Issue *Advancement in Machine Learning and Applications in Mathematics*, IF-2.25, MDPI, Basel, Switzerland, in 2022. He is a co-editor in the series of conference proceedings of ICRIC-2021-23 published by Springer, Singapore.

ZOLTÁN ILLÉS received the Ph.D. and Habilitation degrees in mathematics and physics from Eötvös Loránd University. Later, he took up the computer science supplementary course, which was started at that time. His Ph.D. dissertation was titled "Implementation of Real-Time Measurements for High-Energy Ion Radiations," in 2001. After graduating in 1985, he joined the Department of Computer Science, Eötvös Loránd University. In 2004, at the request of Jedlik Publisher, he also wrote a textbook on the C programming language. This book has a second, expanded edition in 2008. In 2007, he was awarded a scholarship by the Slovak Academy of Sciences, where he spent six months researching and teaching with Constantine the Philosopher University, Nitra. The NJSZT awarded the Rezső Tarján Prize, in 2016, for the success of the joint work that has been going on ever since. He and his colleagues also researched the issue of mobile devices and applications in the framework of a tender won, in 2014. Based on their research findings, he launched a pilot project to support real-time, innovative performance management. The first results of this research are an integral part of the habilitation dissertation. He got a Hungarian Republic Scholarship based on the outstanding academic achievements during university studies. Since 2020, he has been an invited speaker at several international conferences and an Amity University Advisory Board Member.