IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 22 December 2023, accepted 10 January 2024, date of publication 16 January 2024, date of current version 26 January 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3354846

RESEARCH ARTICLE

Blockchain-Assisted Hierarchical Attribute-Based Encryption Scheme for Secure Information Sharing in Industrial Internet of Things

A. SASIKUMAR[1], LOGESH RAVI[2,3], MALATHI DEVARAJAN[4], A. SELVALAKSHMI[4], ABDULAZIZ TURKI ALMAKTOOM[5], ABDULAZIZ S. ALMAZYAD[6], GUOJIANG XIONG[7], AND ALI WAGDY MOHAMED[8,9]

[1]Department of Data Science and Business Systems, Faculty of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu 603203, India
[2]Centre for Advanced Data Science, Vellore Institute of Technology, Chennai 600127, India
[3]School of Electronics Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu 600127, India
[4]School of Computer Science and Engineering, Vellore Institute of Technology, Chennai 600127, India
[5]School of Business and Law, Dar Al-Hekma University, Jeddah 22246, Saudi Arabia
[6]Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[7]Guizhou Key Laboratory of Intelligent Technology in Power System, College of Electrical Engineering, Guizhou University, Guiyang 550025, China
[8]Operations Research Department, Faculty of Graduate Studies for Statistical Research, Cairo University, Giza 12613, Egypt
[9]Applied Science Research Center, Applied Science Private University, Amman 11937, Jordan

Corresponding authors: Ali Wagdy Mohamed (aliwagdy@staff.cu.edu.eg) and Logesh Ravi (LogeshPhD@gmail.com)

This work was supported by the Researchers Supporting Program through King Saud University, Riyadh, Saudi Arabia, under Grant RSPD2023R809.

ABSTRACT The edge devices will produce enormous quantities of data daily as the Industrial Internet of Things (IIoT) expands in scope. Still, most IIoT data is stored in data centers, making it challenging to transfer data between domains safely. Smart logistic products have dramatically changed due to the prevalence of decentralized edge computing and blockchain in the industry sector. To address the need to exchange data between logistics networks, we proposed a novel decentralized hierarchical attribute-based encryption (HABE) scheme combining edge computing and blockchain. To begin, we offer an IoT data encryption strategy in which edge devices can send data to a nearby cloud network for data processing while maintaining privacy. In addition, we developed a blockchain-integrated data-sharing scheme that makes it possible for users to share data via the use of edge and cloud storage. In particular, an IoT device incorporates an encryption-based authentication system to verify users' access rights at the network's periphery in a decentralized manner. Using HABE, we provide a blockchain-integrated architecture for the IoT that protects user privacy. The suggested design utilizes the edge and cloud network paradigms and HABE to maintain privacy and works well with smart logistics applications. The authentication time of the proposed model is reduced by 1.5 times compared with the centralized model. The analyses and experimental findings show that the proposed blockchain-integrated edge computing architecture is better than the existing schemes in terms of data sharing, data privacy, and security.

INDEX TERMS Blockchain, data encryption, edge devices, HABE, IIoT, user privacy.

I. INTRODUCTION

The present economic landscape poses challenges for new ventures in the form of creative trade practices, innovative rules, fierce rivalry, and the need for prompt delivery of goods. Because of this, a lot of businesses depend on the Industrial Internet of Things (IIoT) [1], a term that describes any steps taken by firms to duplicate, control, and enhance their business operations using data collected from thousands of connected machines, objects, and devices to increase their

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

revenue. As the name implies, an IIoT is a system that links and controls industrial objects, machines, and infrastructure via the Internet.

The IIoT has received significant attention from researchers and businesses, which may play a significant role in the impending conversion of commercial systems [2]. Industry 4.0 devotes much discussion to the industrial IoT, and IIoT is also widely debated in academic and governmental circles. The critical distinction between IoT and IIoT is that although IIoT is typically used in applications like smart factories and intelligent manufacturing, IoT environments typically contain a variety of automation gadgets and machinery. With the help of actuators, sensing devices, a pervasive network, and processing power, IIoT brings intelligence and connectivity to industrial systems. Implementing IIoT is intended to increase manufacturing efficiency and business productivity, lessen device downtime, and raise the caliber of the final output. Specifically, IIoT features the following traits: Decentralization of IIoT systems, a variety of IIoT applications and schemes, diversity of IIoT data, and networking strain are the first two.

The likelihood of addressing the cited IIoT difficulties increases with advancements in blockchain technology. Bitcoin's core technology is Blockchain [3]. Blockchain enables software programs to send and receive information or record transactions in a distributed and dependable (peer-to-peer) manner. Blockchain is being rapidly adopted and is mainly used for distributed storage, services involving intelligent contracts, and digital currencies. The Blockchain in IIoT capable applications include recording activities (such as moisture, temperatures, or geographical deviations) and generating block issue ledgers accessible only to specified participants, such as each participant across a supply chain.

The fourth industrial revolution merges the Internet of Things and the economic value chain. Since it can lower operational and capital expenses, assess and enhance financial processes—regardless of their difficulty—and promote creative companies, the IIoT is the most efficient catalyst for innovation [4]. IIoT has benefited from increased attention from academia and industry, which has resulted in exponential advancements in new methods utilized in the industry. For instance, big data techniques are employed to collect and transfer vast amounts of sensor data to the cloud to enable intelligent decision-making. Moreover, healthcare applications use lightweight authentication models for transferring medical data between peers [5].

The last few decades have seen rapid IIoT growth due to various scientific and economic advances. Catalyzed by the development of steam engines in the eighteenth century, this was the earliest significant technical achievement. Commercial construction saw a notable increase in output due to the mechanization of steam engines, which helped transition from the period of sanitized labor to the age of digitalization. In the 1870s, steam-powered machinery started to give way to electrically powered machinery. Simultaneously, the division

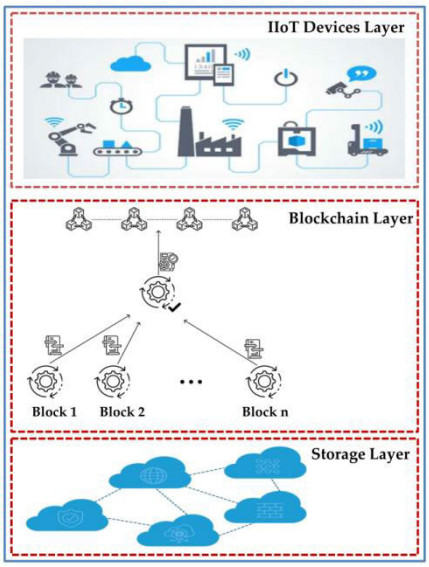

FIGURE 1. The basic blockchain integrated IIoT system.

of work into specialized industries brought about a boom in manufacturing, which was another economic achievement. It was around the 1960s that the third century of industrialization, also called "digitalization," began [6]. During this period, programmable logic controllers and enhanced electronics utilized to boost industrial productivity led to the creation of creative automation technologies.

Communication tactics and technologies underwent tremendous development between the turn of the twentieth century and the beginning of the twenty-first, opening up new technical possibilities. These tactics significantly increased the analytical abilities of the sensing, connecting, decision-making, and producing industries. In the industrial and educational domains, the IIoT—which seeks to incorporate cutting-edge data collection techniques within conventional industries—has lately taken on a normative role. Industry 4.0 was primarily used throughout the 2011 Hanover Exhibition to advance the fourth industrial revolution and increase European awareness [7].

Machines work together in the IIoT to complete tasks without human assistance. They are intelligent for a variety of application scenarios in the fields of medical care, production, logistics, and home automation. The IoT nodes can communicate data with one another individually via a Device to Device (D2D) connection [8]. The practical application of machine-created "Big data" technologies gives advantages to the data obtained to enhance the execution of the plan by creating functional domain expertise. By connecting the things and enabling mixed mechanization among things and manufacturing operations, the IIoT's ubiquitous sense, data interaction, collection of data, and data examination are promising solutions to modernize profitable services. The conventional architecture of IIoT integrated Blockchain is illustrated in Figure 1.

A. IIoT CHALLENGES

With the aid of various software frameworks, actuators, and sensors used to detect and collect information about the physical environment and produce activities using components, the IIoT ensures the connection of many different things. The unique properties of IIoT give birth to several research problems. Recent improvements in information and communication technology (ICT) have helped address several inherent constraints of the IIoT. For instance, exchanges with ambient backscatter can help IIoT devices and increase power. Furthermore, by shifting the process-intensive tasks to edge computers, mobile edge computing [9] can increase the functionality of the IoT device. Additionally, the current advancements in blockchain technology create issues, including insufficient interoperability, security flaws, and privacy issues.

B. BLOCKCHAIN FOR SUPPLY CHAIN MANAGEMENT

A supply chain usually aims to meet customer demand for goods while keeping the manufacturer's or retailer's stocks to a minimum. Since the 1980s, when the term ''supply chain management'' was first used, numerous supply chain leadership concepts have been developed to fulfill the demands of the various production networks. Some of these conditions include the following: the reduction of expenses from good transfer and supplies; the removal of obstacles (caused, for example, by postponed payments); the development of chains strong to shifts brought on by economic factors or a lack of essential substances; the safe and reliable traceability of an item's origins; the employment of nearby manufacturers and labor force; the reduction of transport. The blockchain data framework already satisfies many of these criteria for a successful supply chain system, making it a logical choice for companies and their monetary stakeholders to utilize it for supply chain management [10].

1) TRACEABILITY

When managing the safety of delicate goods like food or medication, the ability to trace a product's origins is crucial. Tragically, there have been a few cases in recent times where contaminated or spoiled food was sold to consumers as fresh and resulted in illnesses [11]. The contaminated groceries and infections can spread to a more significant portion of the residents using the present supply chain management systems because it can take a while to identify the affected batches or the source of the issue. The ability to instantaneously identify the causes of such situations would be made possible by the time-stamped data of all details concerning the manufacturing, delivery, and sales of any specific product on a blockchain. Additionally, utilizing blockchain for their supply chain, it would be far more challenging to alter the quality of goods in any manner because the information system necessitates ongoing verification of the purchases enrolled on it by the entire network, not just the network's collaborations in charge of handling the specific stage of the supply chain. This ensures that there will be only one truth, eliminating the need for negotiations and settlement among all supply chain actors.

2) DISTRIBUTION

One aspect of blockchain technology that makes it appealing for supply chain deployments is its distributed environment, which carries many advantages. First off, since each node in the system keeps a record of the supply chain's operations and agreements and no central organization controls the transactions or stores them, a failure or exclusion of one or more network nodes (such as the bankruptcy of a supplier) would not result in the collapse of the entire system or the loss of operations. Next, while the reality that all network interactions and metadata are saved on all nodes results in some data replication, it also fosters security and confidence among cooperating parties because not only a select few have access to important information. Thirdly, using blockchain prevents expensive transactions because it eliminates the requirement for mediators in every contract and uses a single network for all of its operations [12].

3) IMMUTABILITY

The immutability attribute is arguably the most well-known because it shields blockchain participants from multiple fraud attempts and enemies. The inability to change information once registered on the chain directly leads to the traceability attribute. It is highlighted in the literature that perfect immutability is impossible because, in theory, a large portion of the network may synchronize to alter the data on the chain. But this is essentially impossible [13].

4) INTEROPERABILITY

It can exchange data with IIoT devices and communicate with physical devices [14]. Interoperability within the blockchain-composite layer can be achieved by building an overlay P2P connection on top with constant access across different IIoT systems.

5) AUTOMATIC EXECUTION

The potential for IIoT to cooperate without interruption from a trusted third party (TTP) is discussed in autonomous encounters. Blockchains allow smart contracts to attain this degree of independence. Notably, the smart contracts will be automatically executed every transaction [15].

6) RELIABILITY

The capacity of IIoT information to be trusted is referred to as reliability. Employing cryptographic techniques, which are all built into blockchains and include asymmetric cryptography and hash signature generation, ensures reliability [16].

C. MOTIVATIONS AND CONTRIBUTIONS

First, the study on smart logistics and data sharing is of considerable realistic value in enabling smart industry

applications. Second, the research on data privacy that has already been conducted [17] encourages us to concentrate on edge computing architecture for extremely effective data-sharing processing. Additionally, the research in [18] and the early findings from our most recent work [19] show that blockchain can offer potential options for sharing data with improved user privacy and increased security. Third, the extensive discussion in [20] emphasizes the pressing necessity for creating a thorough data-sharing architecture to raise the standard of IoT applications. The existing works reinforce our will to use blockchain, IoT devices, edge computing, and data encryption technologies to construct a holistic IIoT architecture. The significant contributions are listed as:

1. We propose a lightweight hierarchical attribute-based encryption algorithm based on blockchain technology for an intelligent logistic application that combines IoT devices and cloud storage with clients/users for secure transactions.
2. We developed a secure architecture for sharing goods delivery details across decentralized networks using the synergy of blockchain, IIoT, smart contracts, and edge devices. In particular, a decentralized authentication method is developed alongside distributed cloud storage to perform data transfer without requiring a third party, improving the security of information sharing and the speed with which it can be retrieved.
3. We perform simulation experiments to test the proposed blockchain architecture's efficacy. The implementation outcomes and subsequent discussions show that our proposed system outperforms the existing works.

The rest of the paper is structured as follows. Section II presented the related work that addresses security and exchanging data across IIoT networks. The network and the blockchain components are outlined in Section III, where we also describe our decentralized smart logistics scheme. Section IV discusses the security performances and discussions of our proposed scheme. In section V, we offer the proposed system implementation and experimental results. Finally, the paper wraps up in Section VIII, where potential future research directions are discussed.

II. RELATED WORK

Here, we provide context for this study and highlight previous research that has addressed similar questions. To simplify, think of blockchain as a distributed, immutable database in which information is broadcast as transactions to every node in the network. Data storage and organization methods in blockchains can vary widely. Block versions, hashes of previous blocks, timestamps, nonce values that begin at 0 and increase with each hash estimation. Each block in a blockchain network has a set of related communication and includes a reference to the block before it in the chain, called an inverted reference or hash value [21]. A hash generates a digital fingerprint of the data, which is then used to validate the original data.

The elements that make up a blockchain's structure can be thought of as belonging to one of four distinct ''layers'': the data layer, the network layer, the consensus layer, and the application layer. It is necessary to design the block arrangement, the efficiency of the communication, and the organization and storage of data while developing a data layer. The Network layer is a decentralized system often represented as a peer-to-peer (P2P) network. Any participant in a public Blockchain can join or leave at any moment. No controller node exerts authority over its subordinates. However, use cases like digital currencies are better suited to public blockchain. In combination with the IoT nodes, edge nodes and users are also part of the network layer in IoT applications. Convergence in the Consensus Layer is a core issue in cloud computing. Trust in blockchain-enabled systems is provided by the consensus process [22].

Highly computationally intensive consensus forms will not work well in an IoT setting. IoT will benefit more from stake consensus approaches like proof of stake (PoS) and its derivatives. A consensus of this sort, however, necessitates the participation of a central authority. There are now three main consensus algorithms: proof of work (PoW), PoS, and practical byzantine fault tolerance (PBFT). The PoW has been used successfully for many years in Bitcoin and has been demonstrated to be an efficient consensus technique [23]. However, it calls for intensive computations, which results in unnecessary energy use. While PoS does not necessitate intensive operations, it does centralize the blockchain as it relies on the nodes with the most significant stake [24]. Consensus in PBFT arrives based on the threshold value set by the network of the nodes deciding on the same block [25] through a voting process in which all nodes must take part. A decentralized storage model based on a graph called Tangle was proposed by Interest on Trust Account (IOTA) [26]. Blockchain enables decentralized consensus reaching across nodes in the application layer. The original inspiration behind consensus model was to stop anyone from spending the same cryptocurrency twice. As a result, its primary use nowadays is in digital currency. The addition of smart contracts to blockchain made it more than just a payment system, and it has since found use in areas as diverse as the IoTs, goods delivery, digital asset monitoring, and token administration [27]. Blockchain evolved to be better suited for use cases involving many parties. Ten years after the introduction of Bitcoin and the first blockchain, the technology's potential uses in fields beyond cryptocurrency still need to be explored.

Smart contracts are the perfect technological solution for safely archiving legal agreements. Chain codes are computer programmers who transmit and track digital money or other assets between participants by predefined criteria. It has the power to impose not only the rules or agreements but also the terms and penalties for which it has set the terms and penalties. When a financial transaction is scheduled to take place, the origin or destination of that transaction is identified by the smart contract. Data collection, storage, and processing

are the three main functions of every information system. The systematic integration of these parts guarantees the stability of the system.

Regarding the transfer of digital ownership, blockchain is one of the most groundbreaking technologies of recent years. To effectively manage its distributed technology, the company must adopt fresh company tactics and models. Integrating digital ownership into blockchain will help the company store its data securely using the decentralized model. Integrating blockchain technologies with information systems enables businesses to reap the benefits of blockchain's many applications. While many sectors are interested in the technology, only some are prepared to fully integrate it into their current methods for handling information.

A. BLOCKCHAIN INTEGRATED IIoT NETWORKS

IoT and blockchain innovation support one another, which is becoming increasingly apparent to both academics and practitioners. One illustration is the traceability approach Caro et al. [28] suggest for the agri-food industry by combining IoT devices with farmers in the chain. Similarly, Toyoda et al. [29] provide near-field communication (NFC) identification followed by blockchain enrollment, among many other goods. The idea that information on a chain is only as accurate as the data stored is recurrent in the literature. Waltonchain [30] aims to eliminate the widely criticized trust anchors, which are RFID tags and QR codes. They created a supposedly tamper-proof, secure two-way verification RFID with built-in encryption technology. IoT measurements (temperature, moisture, etc.) are much safer because the sensor device can function as a node and upload instantly to the chain. SKYFChain [31], which aims to build an infrastructure between uncrewed self-driving cars and enterprises, additionally focuses on machine-chain interaction. Finally, Malik et al. [32] contend that blockchain cannot ensure the dependability and integrity of data kept on the chain. The developed system offers a framework that automatically associates a trust value with each supply chain based on the participant's trustworthiness and the caliber of the good.

Building on top of an operational blockchain-based system is an increasingly common approach for integrating distributed ledger technology into the supply chain. The authorization rights of the employed blockchain system are frequently predetermined by design, depending on the platform's choice. In the way that only entities with authorization can access and inspect information on the chain, for instance, the network built on the distributed ledger is essentially private [33]. Despite such architectural decisions going against the grain of blockchain, they enable the many supply chain participants to adhere to established norms, create transparency in their transactions, and foster greater confidence among them for their respective businesses. On the other hand, public or permissionless systems allow anyone to communicate with the blockchain records, regardless of whether that business is a supply chain member. Specific applications use a hybrid system, which falls between these two design options and keeps the data entering portion private to the parties participating in the network exchanges while making the rest of the chain's data and information accessible for public auditing.

Blockchain 3.0 broadens the spectrum of industries it might use, moving beyond just financial transactions [34] to include electricity, education, governance, medical care, and more. A direct IIoT energy exchange based on blockchain that uses a credit-based settlement technique to cut down on transaction verification latency was proposed by Hu and Li [35]. In order to realize safe energy exchanges between the energy system and the smart home, Aggarwal et al.'s EnergyChain blockchain concept is proposed. The network was presented with miner production; block production, authentication, and data transfer. By utilizing blockchain technology, multiple signatures, and anonymous encryption communication flow, Aitzhan and Svetinovic [37] established the idea of validating the distributed energy trade structure, allowing peers to confidently reach agreements on energy pricing and carry out transactions securely. In [38], authors discussed the various decentralized authentication models based on attribute encryption schemes. The encryption method is suitable since the IoT application requires a lightweight authentication model for that attribute. In order to accomplish efficient billing administration, Baza et al. [39] presented a grid management model based on blockchain that employs an unspecified signature to convey the power data demanded in the transaction. It also incorporates smart contracts for setting priorities.

However, as mentioned earlier, most techniques rely on workload proof, which has adverse effects such as duplicated storage, a lengthy transaction time, and inefficient consensus. The consortium algorithm boosts the effectiveness of the network. Typically, non-POW algorithms form the foundation of the consortium chain. BFT methods can address Byzantine issues, such as PBFT, and methods that cannot, like Raft. These two algorithms have been improved in the following ways: The PBFT algorithm and a trust-based network of nodes can further improve the head of the group's resilience via signature sharing and mutual monitoring. Tong et al. [40] suggested a Trust-PBFT that integrates the P2P node with the PBFT consensus mechanism to improve the network's capacity and flexibility. By utilizing the K-Bucket node association formed by the Kademlia protocol, Wang et al. Raft-like smart contract Kraft [41] improves the leader selection and agreement procedure of the Raft method. It increases the quickness and efficiency of the leadership selection.

A proof of voting (POV) approach based on vote evidence was proposed by Li et al. [42]. The majority is consortium partners' coordinating nodes, which will use voting to undertake decentralized arbitration. In order to cut down on the involvement of abnormal nodes, the scheme bases itself on a voting incentive and penalty scheme and performs an

appropriate credit evaluation. Although each of the studies, as mentioned earlier, makes a different contribution to the consortium chain's consensus algorithm, they hardly ever concentrate on the unique needs of the smart grid. There are various power transaction studies in the smart grid. A peer-to-peer energy trading model using a consortium chain was put forth by Li et al. [43] that maximize cost earnings from a security standpoint while realizing the incremental double competing system through consensus mechanism, electronic signature on the internet, and asymmetric encryption technology. In order to organize interruption operations, the privacy-enabled blockchain model was introduced. The technique employs an account mapping method to finish node tasks, preventing attacks and guaranteeing correct fault records of transactions. A consensus algorithm with a reward and punishment mechanism was created by Wang et al. [44] for the smart grid's private key generator (PKG) choice. They created a blockchain-based entry management system employing an integrated encryption system at the same time. A smart grid data gathering and regulatory blockchain system was proposed by Zhong et al. [45]. The consortium blockchain's encryption method can be used for multimodal data collecting and many receivers. Each receiver analyses multidimensional data for a single user and develops corresponding control algorithms. Operators of electric grids execute user power control by giving smart contracts feedback.

B. SECURE DATA TRANSFER IN BLOCKCHAIN INTEGRATED IoT ARCHITECTURE

For the IoT, blockchain has numerous uses. For the IoT devices to operate correctly, numerous security and trust-related problems are resolved thanks to its decentralized nature. In particular, smart contracts provide numerous IoT services such as device registration and authorization, communication of data security, administration of user agreements, and more. We next review a few uses for the blockchain in edge-based IoT. Numerous security and confidence problems relating to interconnected automobiles on the internet are resolved by blockchain. It is necessary to have a successful, dependable system that can guarantee fundamental security and trust criteria, such as vehicle identification management, among others [46].

Auditing and access data can also be shared with blockchain and smart contracts. Over edge-based IoT connections, blockchain-based approaches may effectively manage security and access control [47]. Each interconnected component in edge-based IoT networks increases the risk of interrupting device updates, and the flow of code performance can be altered for fraud. Furthermore, pushing out appropriate firmware updates is difficult due to the IoT equipment's restricted abilities. Most asymmetric encryption methods used in firmware update procedures are complicated and powerful. Blockchain can solve the issue of the single point of failure because it is distributed by design. Blockchain uses consensus methods and smart contracts to ensure the efficiency of software upgrades.

These features offer exceptional opportunities for information exchange and real-time synchronization in supply chain administration since blockchain and attribute-based encryption can be utilized to address storage and communications issues [48]. Off-chain archives and on-chain files can work together in a clearly defined arrangement to supplement conventional databases. By doing this, pertinent data are distributed to interested parties, preventing the emergence of ''data silos'' and the storage issues caused by ''data explosion'' [49]. The accessibility of trustworthy, accurate information emphasizes blockchain to achieve traceability and end-to-end openness throughout the supply chain [50]. This method eliminates one-step-back and one-step-ahead practices. In a transparent and persistent system, the information supplied can facilitate continuous tracking of container motions, recall activities, and goods traceability. Blockchain registers can be used to assess a supplier's credibility. When paired with additional intelligent techniques like the IoT, big data, and cloud services, it offers an efficient, evolving, flexible, and scientific approach that works with practices in producing, distributing, and recovering goods.

Additionally, short-term relationships among buyers and sellers take place in a virtual setting referred to as a ''network of trust'' [51], which is based on a single version of reality that is gradually developed through communication between potentially unknown parties, altering the way that the supply chain team views trust. A blockchain additionally supports combining diverse traceability information collected by the various participating parties. A blockchain is categorized as ''public'' or ''private'' in terms of access for involvement, while the words ''permissionless'' and ''permissioned'' refer to the actions each member can carry out. A hybrid mixture is additionally categorized as a consortium blockchain [52]. A rising number of primary and even additional study papers on blockchain have been published due to the potential to enhance supply chain management, going beyond cryptocurrencies and smart contracts for financial transactions. The strategies have steadily changed from theoretical application efforts to actual implementation initiatives.

As a result, many existing works are now available in the literature, which could make the integration of IoT with blockchain possible. Moreover, the security and privacy of IoT network data is still challenging. We proposed blockchain integration with IoT for secure data transfer using a lightweight authentication mechanism to overcome these challenges. Thus, this article provides the present state of the art regarding blockchain in supply chain management and enhances the trust among the IoT nodes.

III. THE PROPOSED BLOCKCHAIN INTEGRATED HABE BASED EDGE COMPUTING ARCHITECTURE

The following section, we present the proposed blockchain integrated HABE based edge computing architecture and its system model in detail.

A. SYSTEM ARCHITECTURE

We establish the security framework in this part by identifying the key elements and their corresponding capacity. When IoT devices communicate with mobile edge devices inside a radio network, an event-driven approach topology is suitable for efficient data transfer. These Mobile Edge devices have the computing ability to generate and authenticate blockchain transactions because they are not resource-constrained. The cloud server nodes are linked. Assume that the cloud server node $CN = CN_1, CN_2, .., CN_n$ make up the Upper-tier that is nearer to the users. The upper-tier nodes can be thought of as a portable data centre. Assume further that the middle tier is made up of a collection of IoT sensors, each of which is part of an IoT device network and is situated inside a base station or a gateway. Let's imagine that the users on the lower layer collect information from the network surroundings.

B. SMART LOGISTICS: SUPPLY CHAIN TRACKING & MONITORING

Logistics chain, home automation, medical care, and manufacturing machinery are a few of the IoT blockchain application cases that are frequently cited. To illustrate this point, we give the example of smart logistics, which are placed in various geographic regions to catch over-goods delivery information. Within a nation, the governing body has control over the goods. Its structure and capabilities are distinct from the typical IoT blockchain use-case examples. The data produced by the users is now transferred to a decentralized cloud system using a database. The user ID is generated, and the delivery of a good is initialized.

1. Integrity: Those who obtain access to the goods delivery data can alter it. Therefore, it is necessary to set up suitable integrity controls.

2. Availability: Cloud storage of data creates a potential weak spot. The constant threat is the attack on centralized databases. Therefore, it is important to guarantee data accessibility.

3. Confidentiality: Those with access to the database can view the user information. The IoT device records, including the good's current location and time, should be kept secret if it detects speeding.

C. THE PROPOSED SMART LOGISTICS ARCHITECTURE

The primary aim of this work is to present a private ledger that is impenetrable even to an insider, making sensor data completely unalterable. To this end, it is proposed to back the functioning of IoT nodes with a blockchain-based system. As the enterprise authority puts the planned system into place, it will be developed as a permissioned distributed ledger. Blockchain still ensures that the data received from the IoT devices cannot be tampered with by the government. This will aid in building trust with its clientele by making the system more open and accessible. As illustrated in Fig. 2, edge nodes in the proposed system will carry out the blockchain process. It is built on edge devices and a cloud server for its edge-based architecture. It is assumed that edge devices exist within an enterprise network and are the nodes nearest to the IoT devices. The cloud server is located near the end users and can be considered a decentralized cloud service. The edge nodes store and copy the data into the cloud while they verify and validate the transactions. In the edge, nodes are organized into clusters according to their locations, and nearby nodes receive event transactions from IoT devices and forward them to all edge nodes in the cluster. A copy of the validated and added transactions is saved in the edge node, and another copy is copied to the cloud server via the Miner-selection mechanism. By excluding the cloud server from the edge, an abstraction layer is created. Users access the transaction by connecting to the cloud from wherever they happen to be. The Private Key Generator (PKG) in the cloud server (CS) is responsible for creating the users' private key.

D. SYSTEM COMPONENTS

The components of the proposed architecture are the IoT devices, Edge Node, cloud server node, user, PKG, and authority Node.

1. IoT: These limited-capacity components communicate with one another using internet connections. They are capable of carrying out elementary cryptographic operations. The device's private key is kept as embedded hardware; hence it needs to be protected using hardware security models.

2. Edge Node: These nodes are unlimited-resource devices. They are expected to have sufficient computing resources for cryptographic computations and sufficient memory to record all the block chain's transactions. IoT access is provided through this.

Enterprise: This is a transaction-validating peer node on the edge node network. The edge nodes reject invalid transactions before they can make it through the network. A proposal for a transaction is forwarded to an endorser. There is no difference between an endorsing peer and a committing peer since both can update the ledger.

4. Cloud servers Node (CS): Every node in the CN receives a copy of all the transactions simultaneously. But they have nothing to do with checking and validating the transactions themselves. These hubs may be databases or storage networks keeping a record of all the deals. Users are able to communicate with one another using these. At the outset, every user joins a specific CS. The CS where a user has been added is where the user's photographs and videos captured by their IoT devices will be kept.

5. Client: A client is a piece of equipment that initiates contact by sending a request to the edge nodes to retrieve the transactions related to a specific user ID. At first, a customer registers their ownership and personal information with the authority nodes. Once the client's identity has been confirmed, the authority node (AN) node will send the client's private key to them through PKG. The client decrypts the transaction to view the information associated with that vehicle identifier.

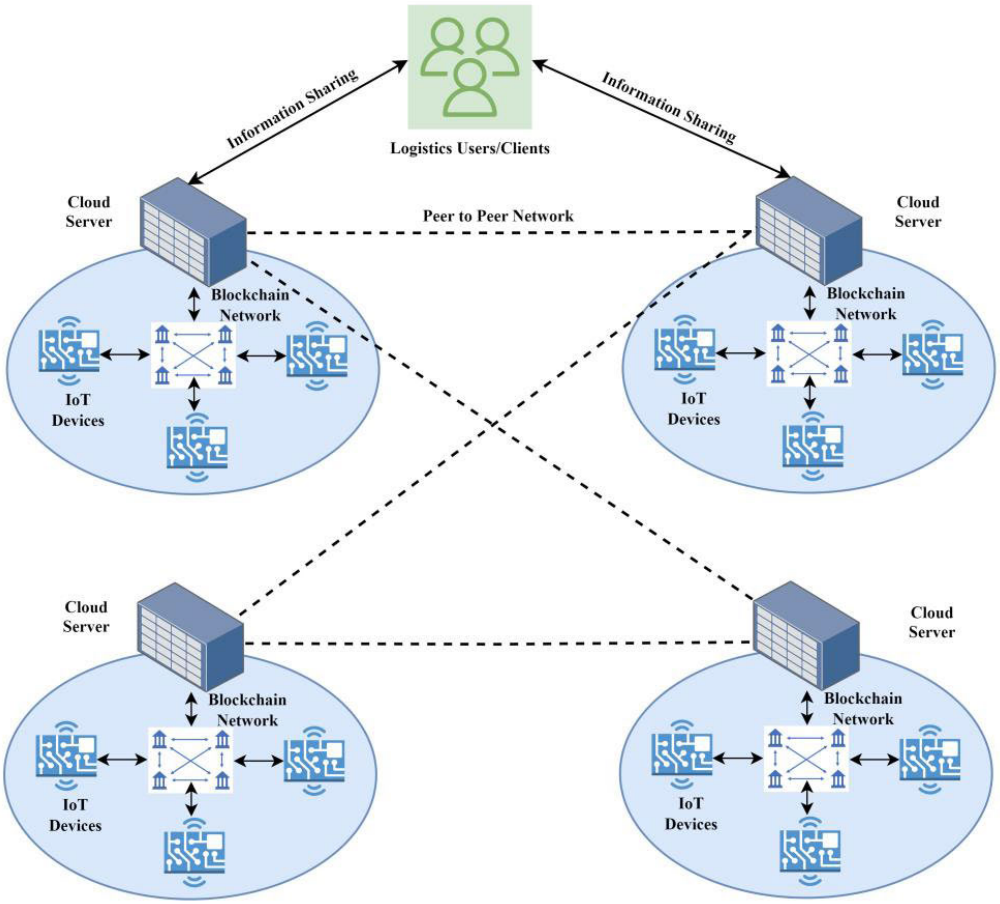

FIGURE 2. The Blockchain integrated edge computing architecture for smart logistics.

6. PKG: When a public key is input into the PKG server, the secret key is generated. It is situated inside of the CS. Additionally, PKG provides the details of the public key that generates the secret key.

7. Authority Registration (AR): The client completes initial user registration with an AR. It verifies the client's identification and then establishes a connection to the PKG in order to request the secret key.

E. THE BLOCKCHAIN INTEGRATED GOODS DELIVERY SYSTEM

In this section, we explain the proposed supply chain enterprise for tracking and monitoring the records of goods delivery systems. When an enterprise sells goods to a client, it records the client's details and accepts money from them.

The operational processes of different components are given in Fig. 3. Assume that the Identity of the User as UID, the time of delivery is t. The location of the user denoted as loc, the amount for delivering the goods be amt. Finally, the public key is denoted by PK, the secret key is MSK and edge Node Id as EID.

The goods in the IoT device detect a user with the programmed delivery details. It monitors the User ID location and calculates the amount. It encrypts the data using the proposed encryption algorithm and creates Tr. The Tr is an encrypted transaction and is sent to its nearest edge devices.

$$Tr = Encrypt[UID, loc, amt]$$

Once receiving the good delivery invitation from IoT devices linked to the blockchain network, the edge device authenticates the user details and adds a timestamp to the block. The data transaction will updated in the block as follows as

$$Tr_1 = [EID \parallel tr \parallel Timestamp]$$

The edge node contains the list of users in the cloud network. Therefore, the transactions of tr1 of each user are predetermined. Once the total number of transactions exceeds the threshold values, the leader node will be selected based on the endorser algorithm. Selected users can be authenticated using the tr1 equation and validate the timestamp. Finally, the leader node will be updated in the cloud network, and all the nodes in the blockchain network will be updated. The

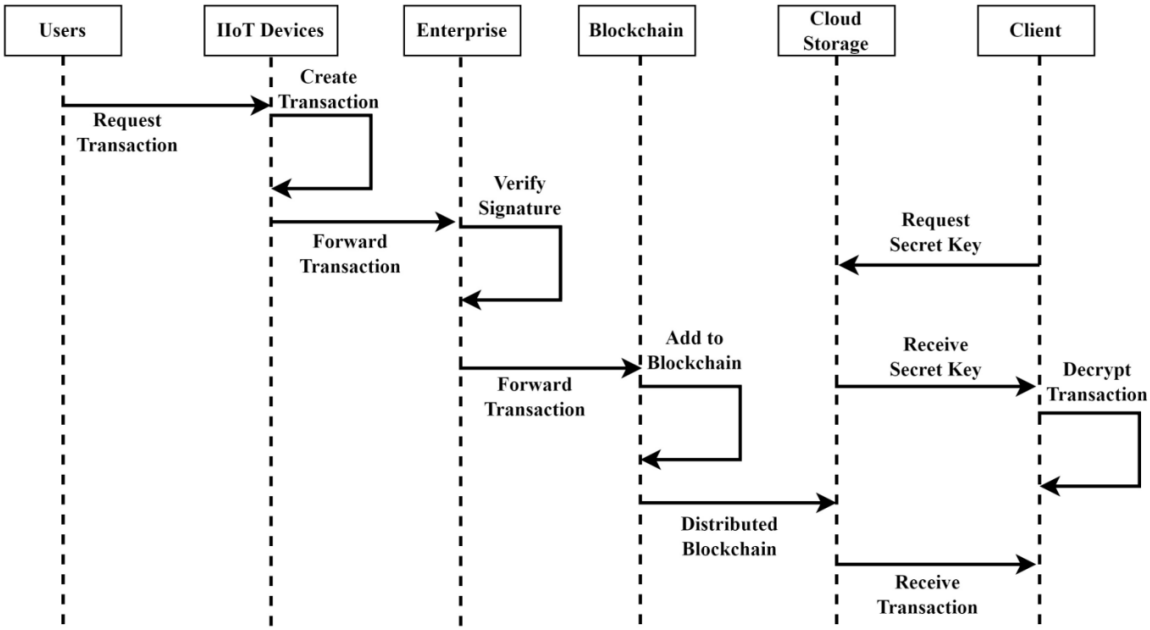

FIGURE 3. The transaction process using proposed system architecture.

users are connected to the nearby cloud node to maintain their transactions. The users need PKG for its secret key and decrypt the message.

When the user receives a good for their purpose, it produces an encrypted transaction with the user's identity. The user's communications include the user ID and other transaction parameters. The encrypted transactions are distributed to its edge node with the required transaction parameters. The miner user node has been validated with the proposed encryption algorithm. The user goods are connected to PKG in the cloud node to decrypt the secret key. For this application, we have proposed a hierarchical attribute-based encryption algorithm for authentication and data encryption at the IoT network. HABE allows encryption and deception processes dependent on user attributes and a lightweight model since we have adopted HABE for our proposed blockchain-based IoT architecture. We have adapted a HABE based privacy-aware data encryption technique that allows IoT devices to send data to the closest cloud server, subject to system constraints. In order to achieve access management, we have developed a HABE that permits data encryption at the network edge without requiring an authoritative source, guaranteeing data reliability and reducing network latency.

F. HIERARCHICAL ATTRIBUTE-BASED ENCRYPTION SETUP AT VARIOUS LAYERS

PKG first creates a master public key and a private key. The master public key can be used as a starting point to derive user public keys. The identity holder should get in touch with the PKG to have a private key generated. PKG uses the master private key to create a unique private key for each user. With the use of the proposed Hierarchical Attribute-Based Encryption (HABE), a root PKG can delegate tasks like private key creation and identity authentication to other, more specialized PKGs. All that's needed for the IoT device to encrypt the message is the vehicle ID and the Public parameters from the root PKG. In contrast, if the domain PKG secret is revealed, the higher level PKG secret is safe with the HABE presented by Wang et al. [53]. Using this method, we have Root PKG at Level 1, Cloud server node at Level 2, and Users at Level 3.

$$ID_{Root} = ID_R$$
$$ID_{CSN} = ID_C \parallel ID_R$$
$$ID_{User} = ID_U \parallel ID_C \parallel ID_R$$

1) ROOT NODE SETUP

Let G_0, G_T are the elements in the bilinear map of prime set p with random number generator g. Assume e is the admissible pair and calculated from the map of $e : G_0 \times G_1 \rightarrow G_T$. The proposed bilinear map follows the properties of attribute based encryption model.

The root node selects random numbers generator

$$PK_1 \in G_0$$

and chooses the random numbers for master secret key

$$MSK_1 \in Z_p$$

and sets

$$S_R = \{S_1, S_2, \ldots, S_m \in Z_p\}$$

Two hash operation namely $H_1 : \{0,1\}^* \rightarrow G_0$ and $H_2 : \{0,1\}^* \rightarrow G_T$ are utilized to produce public keys for the different users.

2) CLOUD SERVER NODE SETUP PERFORMED BY ROOT NODE

We selected all cloud nodes at level 1, to compute a random secret key s_1. This key will be shared with cloud node and root nodes. These random secret key generation setups ensure the details of the private key for user transparency.

$$s_1 \in Z_q^*$$

The public key of cloud node is calculated as

$$PK_2 = H_1(ID_C \parallel ID_R) \in G_T$$

Produce the master secret key for cloud node

$$MSK_2 = MSK_1.PK_2$$

Calculate

$$S_{CN} = S_R.PK_1$$

In cloud node the master secret keys are firmly preserved, while the public key and other random sets are made public. Our proposed system uses the HABE encryption model to ensure the user's data privacy.

3) VEHICLE KEY CREATION BY CLOUD SERVER NODE

Calculate the public key of vehicle

$$PK_3 = H_1(ID_V \parallel ID_C \parallel ID_R)$$

Produce the secret key for Vehicle

$$MSK_3 = MSK_2 + s_1.PK_3$$

Produce secret set s_2 should be available for cloud node and Vehicle user,

$$s_2 \in Z_p^*$$

Then calculate public variable

$$S_V = S_R.PK_2$$

In Users the master secret keys are firmly preserved, while the public key and other random sets are made public.

4) ENCRYPTION BY USERS

For encryption, the cipher text is generated from the random variable as follows

$$r \in Z_p^*$$

Assume that a user share messages, $M = \{m_1, \ldots, m_k\}$ be the Message to be encrypted.

Encrypt (PK, ck, T), where ck is the content keys of $ck = \{ck_1, \ldots, ck_k\}$, and T is the hierarchical access tree. The Cipher text is calculated as follow as

$$CT = \{T, \overline{C_i}, C_i', C_{(x,y)}, C'_{(x,y)}, \overrightarrow{C}_{(x,y),j}\}$$

5) DECRYPTION BY USERS

Decrypt (PK, CT, SK), where user needs their public and secret key to decrypt cipher text.

To decrypt cipher text, the users calculates

$$DecryptNode(CT, SK, (x,y)) = \frac{e(D_i, C_{(x,y)})}{e(D_i', C'_{(x,y)})}$$

The proposed encryption based blockchain architecture will ensure the data privacy in the IoT systems. This lightweight encryption algorithm integrated with blockchain for secure data transmission. Hence all the sensors data are signed and hashed.

IV. THE SECURITY MEASURE OF PROPOSED SYSTEM

Here, we detail the attack scenario and theorize on the efficacy of the various security measures included in our blockchain-integrated user data encryption scheme.

1) Attack Model: In security attack model, both internal and external attacks are taken into account.

Internal attack: The cloud servers and goods consumers in this work are treated as semi-trusted entities in the data sharing. In contrast, the users are treated as wholly trusted entities in the private network, as described in the preceding sections. Using the semi-trusted model, cloud servers can infer specific confidential details from blockchain interactions because they are trustworthy but curious about the data.

External attack: External attackers may acquire ownership of information during the sharing in order to obtain delivery-related data. In order to get client information that users have delegated, for instance, a rival may attack the cloud server. Data attacks on communications between the server and users may also make data exchange insecure. The primary security features of our proposed scheme are then presented, together with an explanation of how these features make our proposal resistant to security threats using an encryption algorithm.

2) Security Analysis: Four crucial security features data privacy, authentication, traceability, and confidentiality can be provided by our system.

2.1) Data privacy: The information data-sharing strategies can maintain data privacy using our proposed encryption method. The information transferred from users is encrypted using the private key. Without the private key for the cloud server, a third-party adversary could not decrypt the data. So, the confidentiality of user data is maintained. In order to secure private user information from dangers, the data request is additionally encrypted during data exchange. Additionally, the blockchain's data transactions are unchangeable and cannot be altered through irreversible ledgers. Our design offers tight data control in the cloud network under the control of blockchain without a third party. In order to better control data privacy, single-point failures would be eliminated, and unauthorized data usage would be avoided.

2.2) Authentication: With the aid of the distributed smart contract, data sharing in our system is authenticated and decentralized by the user encryption model. Because the smart contract in our architecture functions independently

of the cloud server, the global blockchain network can set the authentication rules instead of the malfunctioning server. All MEC servers track and reflect any contract modifications on the blockchain network. This would eliminate the possibility of internal attacks leading to contract revisions, ensuring trustworthy contract operations. Data retrieval in a data-sharing scenario is only done if the smart contract verifies the user information.

2.3) Traceability: Our proposed architecture guarantees this operates on a blockchain network, enabling all entities to track information access occurrences and user behaviors. The cloud server records a user request to our proposed system and distributes it to all other users on the blockchain networks. So, if a data transfer request happens, all edge nodes and users have accepted it. Additionally, transaction logs simplify determining where data is updated or modified. In order to achieve accountability over data utilization, we also store data on the cloud linked to smart contracts rather than on the hard disc of the edge devices. The hash value of the data is preserved in the smart contract, while the raw data is kept in the edge node blocks. As a result, any alteration or change in behavior on a data record will change its hash value, which the smart contract can recognize for prevention.

2.4) Confidentiality: By utilizing the simple cryptographic model, the proposed architecture guarantees the privacy of user interactions. Our sharing scheme uses digital certificates in conjunction with key-based encryption models at different stages. Due to the lack of entity private keys, an external attack cannot access the user information. The blockchain's digest of messages would catch any malicious attempts to alter or update the method of transactions, even if they came from an external attacker. An attack must have substantial computation capabilities to take control of all edge devices and edit the data stored on the blockchain network. As a result, user confidentiality can be maintained.

2.5) Data Tampering: In our proposed IoT, data is transmitted through the HABE algorithm since the sensor's data are hashed and signed.

2.6) Sybil Attack: The multiple fake IDs can be prevented using blockchain-integrated IoT architecture. Since the entire user ID is connected through the blockchain network. The addition of new users required verification before entering the network. Also, the new user needs to get permission from enterprise authorities.

V. IMPLEMENTATION AND PERFORMANCE ANALYSIS

The outcomes of the investigations we ran to show the viability of our suggested architecture are shown in this section. Our tests mainly target on assessing the system's efficiency in relation to the case study of good delivery systems. To evaluate the blockchain system for supply chain, we developed and executed smart contracts in Ethereum. Smart contracts are computerized, self-executing agreements having precise instructions specified in their code that are carried out when particular criteria are met. Solidity was utilized to create the smart contract. We used Ubuntu 16.04 LTS to establish a

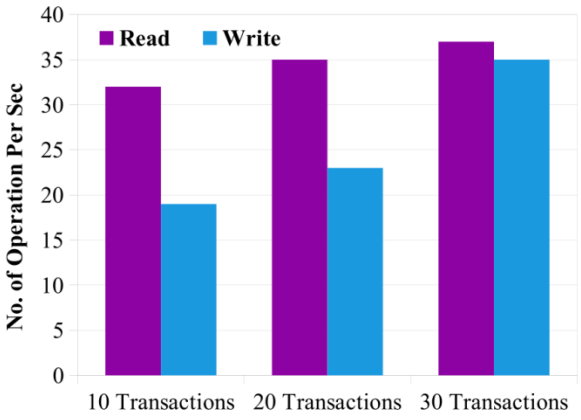

FIGURE 4. The average read and write time requirement of proposed system.

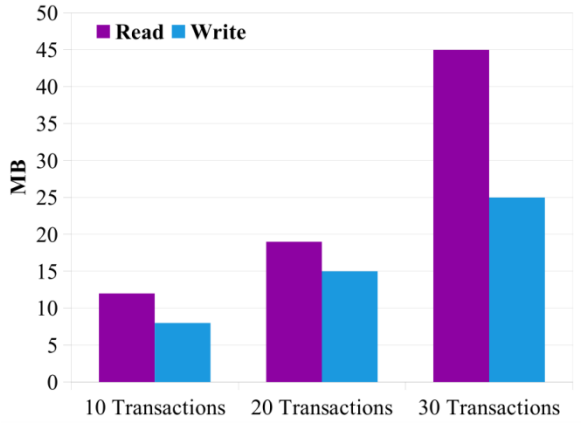

FIGURE 5. Memory utilization of read and write operation.

four-node network in a virtualized setup with 2GB RAM for every virtual machine in order to assess the system efficiency. It was an Intel® CoreTM i5-4300M CPU running at 2.60GHz. The Ethereum blockchain is used to transmit the encrypted data that comes from the Internet of Things together with the other characteristics. We consider the network to the test by producing 10, 20, and 30 transactions at three distinct time intervals. Five times, the test was run, and an average (15 minutes) disc and memory activations were recorded. We used the Ethereum Geth version, and the efficiency data was calculated using Geth measurements. The disc and memory activity were measured. Figures 4 and 5 show the average read-and-write count and read-and-write data, respectively. The random read/write access that was unrelated to the test was removed using several tests. With a surge in transactions, read/write rates rise.

The typical memory utilized for 10, 20, and 30 transactions is shown in Fig. 6. The average amount of RAM needed rose sharply after 30 transactions were carried out, much like in the instance of read/write data. This is due to the fact that all transactions must be transmitted to all peer nodes, and as the

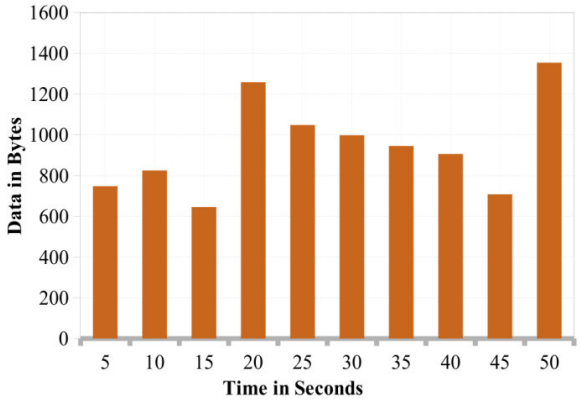

FIGURE 6. Memory requirement for different number of transactions.

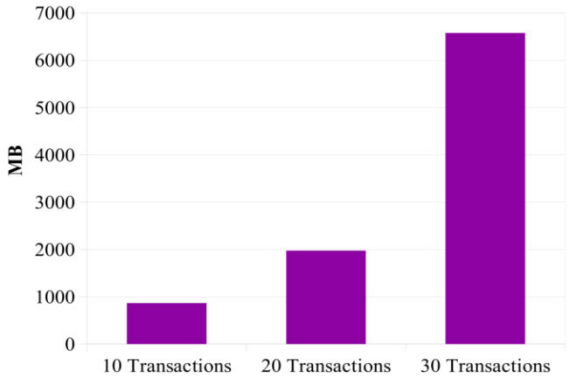

FIGURE 7. The average throughput of the proposed system.

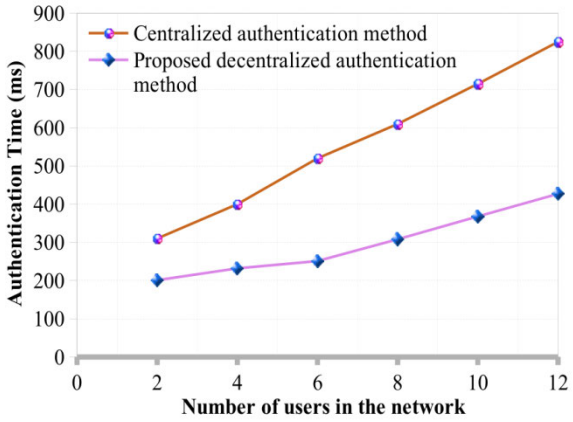

FIGURE 8. The evaluation of authentication time.

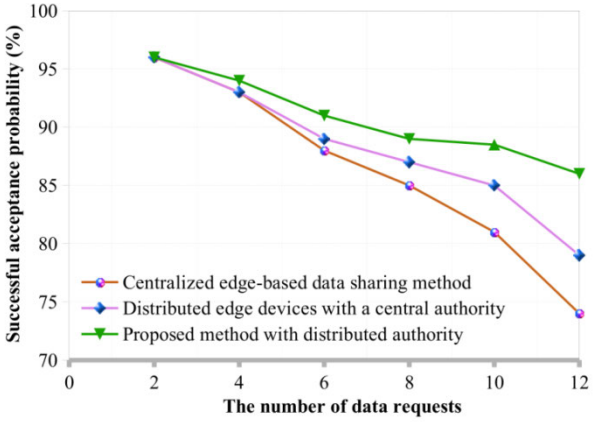

FIGURE 9. Data retrieval latency of the proposed system.

quantity of transactions rises, so does the amount of computing needed. According to the results of our investigation, the best range for the maximum number of transactions per block is between 10 and 30 transactions.

Figure 7 displays the average throughput. The simulation ran for a full minute. The size of the smart contract that we performed determines how much data will be transmitted. To peer nodes, this data is transmitted. The packets' transmitting nodes are chosen at random. 100ms latency, on average, was what we saw. The test to gauge system and network efficiency was carried out separately.

We looked into the cost of authentication, retrieval of information delay, likelihood that a request would be accepted, and blockchain efficiency for information exchange.

A. AUTHENTICATION COST

We determine the cost of computing resource for the authentication process. On this case, a user uses his smart device to send a demand to the edge server for data recovery on the distributed network with a 160-bit request size. For user verification, the edge server executes some operations as encryption, decryption, and transaction decoding. The compute costs for consensus are low, and the tolerable latency makes it suited for time-sensitive applications. In addition, we contrast the computing delay of our suggested approach with a centralized scheme [54] using a variety of architecture. In the suggested method, access authentication is organized at the edge node, where each edge devices authenticates its users using a distributed digital contract. In the meanwhile, the existing approach implements its user authentication through a central authority. Our method demonstrates a decreased delay compared to the baseline, as seen in Fig. 8. This is due to the fact that using decentralized smart contracts allows for quick authentication at the network edge without requiring the passage of a remote authority, which lowers transmission costs associated with the authentication procedure.

B. DATA RETRIEVAL LATENCY

According to Fig. 9, we looked at the network architecture and blockchain design aspects of our suggested algorithm's retrieval of data delay. To record the outcomes, we regularly sent data requests from smartphones to the edge databases. We compare two existing works in terms of blockchain architecture.

The first is a centralized edge-based data-sharing scheme without storage [55] that made use of a centralized MEC

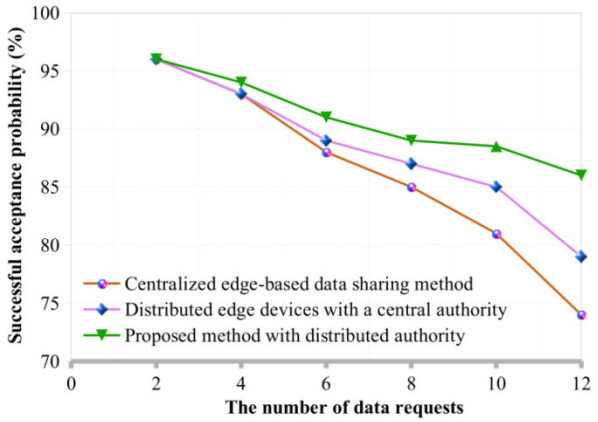

FIGURE 10. The probability of request acceptance.

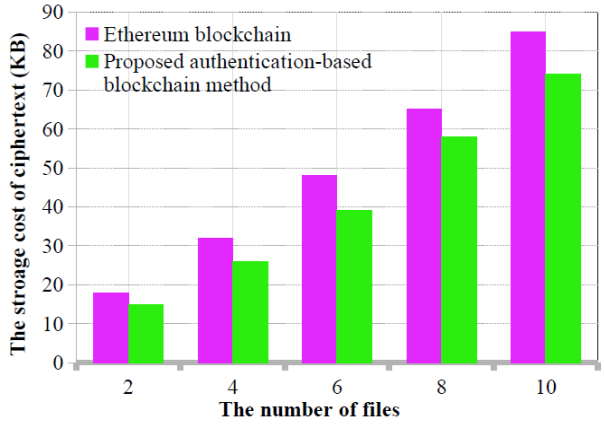

FIGURE 11. Blockchain network performance of proposed architecture.

server to support a sizable network and stored health information in a traditional database. The second one combines blockchain and edge computing without making any changes to IPFS's design and uses a conventional file system [56]. According to Fig. 9, the baseline [55] has the largest data retrieval delay when the number of queries rises because of the centralized MEC server's queuing latency. The basic [56] employed an outdated global DHT look-up approach with a traditional IPFS store, which adds extra communication overhead. Our system, in contrast, offers a completely decentralized solution with distributed MEC and smart contracts. Also our system enables request validation and data look-up to be implemented at the network edge without the need for a global DHT. The data retrieval latency of our proposed system has less time delay compared with existing systems.

C. REQUEST ACCEPTANCE PROBABILITY

To create an additional transaction, including the latency circumstance, we appended a time limit to the requested transaction in the blockchain network. The acceptance rate is the maximum amount of time that must pass before an inquiry is considered successful and the requested data is returned to the requester within the specified deadline. The amount of accepted inquiries divided by the overall amount of inquiries is the definition of the approval likelihood function that we introduce in the network. As seen in Fig. 10, our scheme has a greater request approval rate than the existing work [57].

Our decentralized system still produces the best results despite the fact that the probability decreases as the number of requests rises due to the longer wait time. This can be understood by the sizable processing time savings gained in our system as a result of an edge computing strategy that is optimized and decentralized architecture.

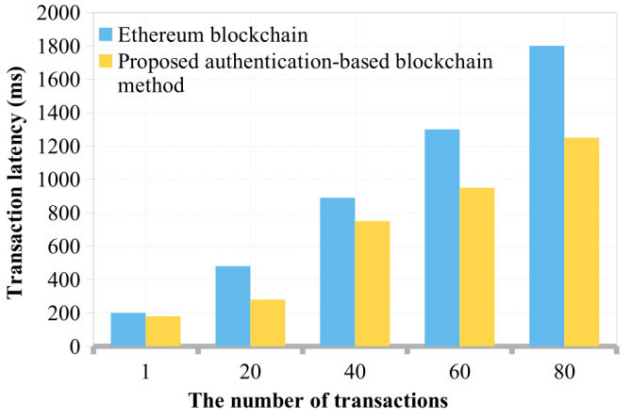

FIGURE 12. The cipher text storage cost of proposed model.

D. BLOCKCHAIN PERFORMANCE

Following that, we assess the functionality of our proposed encryption model-based blockchain and contrast it with the well-known permissionless blockchain utilized in [58]. To assess the typical transaction latency in the neighbourhood blockchain, we execute the smart contract on three computers and send transactions continually to the computers using edge devices. As seen in Fig. 11, when compared to the Ethereum blockchain, our proposed decentralized user authentication-based blockchain demonstrates significantly shorter transaction latency.

As seen in figure 12, we have compared the cipher text cost of proposed encryption based blockchain with existing well-known Ethereum blockchain model. Compared with existing blockchain the cost of cipher text is reduced using proposed encryption mechanism. This experiment's findings demonstrate how well the proposed blockchain works for time-sensitive logistics applications like the one we're considering.

VI. CONCLUSION

The paper proposes a decentralized system that shares data among distributed logistics networks using blockchain and encryption based on edge computing. First, we have introduced a privacy-aware data encryption technique that allows IoT devices to send data to the closest cloud server, subject to system constraints. Later, an innovative data-sharing

method utilizing encryption and blockchain technology was developed to enable safe data exchange between devices in IoT networks. In order to achieve access management, we have developed a HABE that permits data encryption at the network edge without requiring an authoritative source, guaranteeing data reliability and reducing network latency. By using HABE, the proposed architecture ensures secrecy without requiring nodes to share secret keys. We have conducted several experimental tests to assess the suggested architecture's efficacy. The implementation results demonstrate the advantages of the proposed encryption scheme at different layers over the baseline methods in terms of reduced energy consumption, time latency, and better memory management. Furthermore, the data-sharing approach performs better on the blockchain and allows faster data retrieval than previous research. The evaluations show the high degree of system security in our design and the practicality of the proposed paradigm for applications in smart logistics. Future work is being done to incorporate secure real-time transport monitoring systems, data management, and other industry components into our blockchain-integrated edge computing paradigm.

REFERENCES

[1] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, "Challenges and opportunities in securing the industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 17, no. 5, pp. 2985–2996, May 2021.

[2] Q. Qi, Z. Xu, and P. Rani, "Big data analytics challenges to implementing the intelligent industrial Internet of Things (IIoT) systems in sustainable manufacturing operations," *Technol. Forecasting Social Change*, vol. 190, May 2023, Art. no. 122401.

[3] K. John, M. O'Hara, and F. Saleh, "Bitcoin and beyond," *Annu. Rev. Financial Econ.*, vol. 14, pp. 95–115, Jan. 2022.

[4] A. A. Khan, A. A. Laghari, P. Li, M. A. Dootio, and S. Karim, "The collaborative role of blockchain, artificial intelligence, and industrial Internet of Things in digitalization of small and medium-size enterprises," *Sci. Rep.*, vol. 13, no. 1, p. 1656, Jan. 2023.

[5] M. Al-Zubaidie, Z. Zhang, and J. Zhang, "RAMHU: A new robust lightweight scheme for mutual users authentication in healthcare applications," *Secur. Commun. Netw.*, vol. 2019, pp. 1–26, Mar. 2019.

[6] G. Bressanelli, M. Perona, and N. Saccani, "Challenges in supply chain redesign for the circular economy: A literature review and a multiple case study," *Int. J. Prod. Res.*, vol. 57, no. 23, pp. 7395–7422, Dec. 2019.

[7] R. Drath and A. Horch, "Industrie 4.0: Hit or hype? [Industry forum]," *IEEE Ind. Electron. Mag.*, vol. 8, no. 2, pp. 56–58, Jun. 2014.

[8] A. Rana, S. Sharma, K. Nisar, A. A. A. Ibrahim, S. Dhawan, B. Chowdhry, S. Hussain, and N. Goyal, "The rise of blockchain Internet of Things (BIoT): Secured, device-to-device architecture and simulation scenarios," *Appl. Sci.*, vol. 12, no. 15, p. 7694, Jul. 2022.

[9] X. Dai, Z. Xiao, H. Jiang, M. Alazab, J. C. S. Lui, S. Dustdar, and J. Liu, "Task co-offloading for D2D-assisted mobile edge computing in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 480–490, Jan. 2023.

[10] J. Li, A. Maiti, M. Springer, and T. Gray, "Blockchain for supply chain quality management: Challenges and opportunities in context of open manufacturing and industrial Internet of Things," *Int. J. Comput. Integr. Manuf.*, vol. 33, no. 12, pp. 1321–1355, Dec. 2020.

[11] M. Palazzo and A. Vollero, "A systematic literature review of food sustainable supply chain management (FSSCM): Building blocks and research trends," *TQM J.*, vol. 34, no. 7, pp. 54–72, Dec. 2022.

[12] S. A. Bhat, N.-F. Huang, I. B. Sofi, and M. Sultan, "Agriculture-food supply chain management based on blockchain and IoT: A narrative on enterprise blockchain interoperability," *Agriculture*, vol. 12, no. 1, p. 40, Dec. 2021.

[13] P. Helo and Y. Hao, "Blockchains in operations and supply chains: A model and reference implementation," *Comput. Ind. Eng.*, vol. 136, pp. 242–251, Oct. 2019.

[14] M. Al-Rakhami and M. Al-Mashari, "Interoperability approaches of blockchain technology for supply chain systems," *Bus. Process Manage. J.*, vol. 28, no. 5/6, pp. 1251–1276, Oct. 2022.

[15] S. E. Chang, Y.-C. Chen, and M.-F. Lu, "Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process," *Technol. Forecasting Social Change*, vol. 144, pp. 1–11, Jul. 2019.

[16] A. Park and H. Li, "The effect of blockchain technology on supply chain sustainability performances," *Sustainability*, vol. 13, no. 4, p. 1726, Feb. 2021.

[17] S. K. Dwivedi, R. Amin, and S. Vollala, "Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism," *J. Inf. Secur. Appl.*, vol. 54, Oct. 2020, Art. no. 102554.

[18] Z. Wang, T. Wang, H. Hu, J. Gong, X. Ren, and Q. Xiao, "Blockchain-based framework for improving supply chain traceability and information sharing in precast construction," *Autom. Construct.*, vol. 111, Mar. 2020, Art. no. 103063.

[19] M. Hader, D. Tchoffa, A. E. Mhamedi, P. Ghodous, A. Dolgui, and A. Abouabdellah, "Applying integrated blockchain and big data technologies to improve supply chain traceability and information sharing in the textile sector," *J. Ind. Inf. Integr.*, vol. 28, Jul. 2022, Art. no. 100345.

[20] Z. Wang, Z. Zheng, W. Jiang, and S. Tang, "Blockchain-enabled data sharing in supply chains: Model, operationalization, and tutorial," *Prod. Oper. Manage.*, vol. 30, no. 7, pp. 1965–1985, Jul. 2021.

[21] M. Shah, M. Shaikh, V. Mishra, and G. Tuscano, "Decentralized cloud storage using blockchain," in *Proc. 4th Int. Conf. Trends Electron. Informat. (ICOEI)(4)*, Jun. 2020, pp. 384–389.

[22] Y. Lee, S. Rathore, J. H. Park, and J. H. Park, "A blockchain-based smart home gateway architecture for preventing data forgery," *Hum.-Centric Comput. Inf. Sci.*, vol. 10, no. 1, pp. 1–14, Dec. 2020.

[23] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 3–16.

[24] M. Saad, Z. Qin, K. Ren, D. Nyang, and D. Mohaisen, "E-PoS: Making proof-of-stake decentralized and fair," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 8, pp. 1961–1973, Aug. 2021.

[25] H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi, and A. Rindos, "Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric)," in *Proc. IEEE 36th Symp. Reliable Distrib. Syst. (SRDS)*, Sep. 2017, pp. 253–255.

[26] M. Conti, G. Kumar, P. Nerurkar, R. Saha, and L. Vigneri, "A survey on security challenges and solutions in the IOTA," *J. Netw. Comput. Appl.*, vol. 203, Jul. 2022, Art. no. 103383.

[27] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends," *Peer-Peer Netw. Appl.*, vol. 14, no. 5, pp. 2901–2925, Sep. 2021.

[28] M. Caro, P. Ali, M. Vecchio, and R. Giaffreda, R, "Blockchain-based traceability in agri-food supply chain management: A practical implementation," in *Proc. IoT Vertical Topical Summit Agricult.*, 2018, pp. 1–4.

[29] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, "A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain," *IEEE Access*, vol. 5, pp. 17465–17477, 2017.

[30] W. Team, "Waltonchain white paper," Tech. Rep., 2017.

[31] K. M. Aboul-Dahab, "The readiness of the maritime education for the autonomous shipping operations," Arab Acad. Sci., Technol. Maritime Transp., 2021.

[32] R. Malik, H. Raza, and M. Saleem, "Towards a blockchain enabled integrated library managment system using hyperledger fabric: Using hyperledger fabric," *Int. J. Comput. Innov. Sci.*, vol. 1, no. 3, pp. 17–24, 2022.

[33] Q. Nasir, I. A. Qasse, M. A. Talib, and A. B. Nassif, "Performance analysis of hyperledger fabric platforms," *Secur. Commun. Netw.*, vol. 2018, pp. 1–14, Sep. 2018.

[34] D. D. F. Maesa and P. Mori, "Blockchain 3.0 applications survey," *J. Parallel Distrib. Comput.*, vol. 138, pp. 99–114, Jan. 2020.

[35] W. Hu and H. Li, "A blockchain-based secure transaction model for distributed energy in industrial Internet of Things," *Alexandria Eng. J.*, vol. 60, no. 1, pp. 491–500, Feb. 2021.

[36] S. Aggarwal, R. Chaudhary, G. S. Aujla, A. Jindal, A. Dua, and N. Kumar, "EnergyChain: Enabling energy trading for smart homes using blockchains in smart grid ecosystem," in *Proc. 1st ACM MobiHoc Workshop Netw. Cybersecur. Smart Cities*, Jun. 2018, pp. 1–6.
[37] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep. 2018.
[38] P. S. K. Oberko, V.-H.-K. S. Obeng, and H. Xiong, "A survey on multi-authority and decentralized attribute-based encryption," *J. Ambient Intell. Humanized Comput.*, vol. 13, no. 1, pp. 515–533, Jan. 2022.
[39] M. Baza, M. Nabil, M. Ismail, M. Mahmoud, E. Serpedin, and M. A. Rahman, "Blockchain-based charging coordination mechanism for smart grid energy storage units," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 504–509.
[40] W. Tong, X. Dong, and J. Zheng, "Trust-PBFT: A PeerTrust-based practical Byzantine consensus algorithm," in *Proc. Int. Conf. Netw. Netw. Appl. (NaNA)*, Oct. 2019, pp. 344–349.
[41] R. Wang, L. Zhang, Q. Xu, and H. Zhou, "K-bucket based raft-like consensus algorithm for permissioned blockchain," in *Proc. IEEE 25th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2019, pp. 996–999.
[42] K. Li, H. Li, H. Hou, K. Li, and Y. Chen, "Proof of vote: A high-performance consensus protocol based on vote mechanism & consortium blockchain," in *Proc. IEEE 19th Int. Conf. High Perform. Comput. Commun.; IEEE 15th Int. Conf. Smart City; IEEE 3rd Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Dec. 2017, pp. 466–473.
[43] Z. Li, S. Chen, and B. Zhou, "Electric vehicle peer-to-peer energy trading model based on SMES and blockchain," *IEEE Trans. Appl. Supercond.*, vol. 31, no. 8, pp. 1–4, Nov. 2021.
[44] Y. Wang, Z. Su, N. Zhang, J. Chen, X. Sun, Z. Ye, and Z. Zhou, "SPDS: A secure and auditable private data sharing scheme for smart grid based on blockchain," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7688–7699, Nov. 2021.
[45] Y. Zhong, M. Zhou, J. Li, J. Chen, Y. Liu, Y. Zhao, and M. Hu, "Distributed blockchain-based authentication and authorization protocol for smart grid," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–15, Apr. 2021.
[46] M. Labrador and W. Hou, "Implementing blockchain technology in the Internet of Vehicle (IoV)," in *Proc. Int. Conf. Intell. Comput. Emerg. Appl. (ICEA)*, Aug. 2019, pp. 5–10.
[47] S. Rouhani and R. Deters, "Blockchain based access control systems: State of the art and challenges," in *Proc. IEEE/WIC/ACM Int. Conf. Web Intell. (WI)*, Oct. 2019, pp. 423–428.
[48] L. Vishwakarma, A. Nahar, and D. Das, "LBSV: Lightweight blockchain security protocol for secure storage and communication in SDN-enabled IoV," *IEEE Trans. Veh. Technol.*, vol. 71, no. 6, pp. 5983–5994, Jun. 2022.
[49] M. Ali, M.-R. Sadeghi, and X. Liu, "Lightweight revocable hierarchical attribute-based encryption for Internet of Things," *IEEE Access*, vol. 8, pp. 23951–23964, 2020.
[50] A. Dolgui and D. Ivanov, "5G in digital supply chain and operations management: Fostering flexibility, end-to-end connectivity and real-time visibility through Internet-of-Everything," *Int. J. Prod. Res.*, vol. 60, no. 2, pp. 442–451, Jan. 2022.
[51] R. Kumar and R. Sharma, "Leveraging blockchain for ensuring trust in IoT: A survey," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 10, pp. 8599–8622, Nov. 2022.
[52] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-Health systems via consortium blockchain," *J. Med. Syst.*, vol. 42, no. 8, p. 140, Aug. 2018.
[53] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1265–1277, Jun. 2016.
[54] W. Zhan, C.-L. Chen, W. Weng, W.-J. Tsaur, Z.-Y. Lim, and Y.-Y. Deng, "Incentive EMR sharing system based on consortium blockchain and IPFS," *Healthcare*, vol. 10, no. 10, p. 1840, Sep. 2022.
[55] X. Li, X. Huang, C. Li, R. Yu, and L. Shu, "EdgeCare: Leveraging edge computing for collaborative data management in mobile healthcare systems," *IEEE Access*, vol. 7, pp. 22011–22025, 2019.
[56] P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, and M. Atiquzzaman, "A trustworthy privacy preserving framework for machine learning in industrial IoT systems," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 6092–6102, Sep. 2020.
[57] S. Song, "An effective big data sharing prototype based on Ethereum blockchain," *Sci. Program.*, vol. 2022, pp. 1–14, Mar. 2022.
[58] Z. Ullah, B. Raza, H. Shah, S. Khan, and A. Waheed, "Towards blockchain-based secure storage and trusted data sharing scheme for IoT environment," *IEEE Access*, vol. 10, pp. 36978–36994, 2022.

A. SASIKUMAR received the B.E. and M.E. degrees from Anna University, in 2011 and 2013, respectively, and the Ph.D. degree from SASTRA Deemed University, in 2020. He is currently an Assistant Professor with the Department of Data Science and Business Systems, School of Computing, SRM Institute of Science and Technology, Chennai, India. He has published more than 25 journal articles. His research interests include blockchain, analog VLSI, digital VLSI, and swarm intelligence.

LOGESH RAVI is currently associated with the Centre for Advanced Data Science, Vellore Institute of Technology, Chennai, India. He has published more than 100 papers in reputed international journals and conferences. His research interests include artificial intelligence, recommender systems, big data, information retrieval, fintech, and social computing. He is listed and ranked in the Prestigious Top 2% Scientists Worldwide by Stanford University and Elsevier B.V.

MALATHI DEVARAJAN received the B.Tech. degree in information technology and the M.Tech. degree in computational biology from Pondicherry University, India, and the Ph.D. degree in computer science and engineering (cybersecurity) from SASTRA Deemed University, India. Currently, she is associated with the School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India. Her research interests include cybersecurity, blockchain, network security, and the IoT.

A. SELVALAKSHMI received the B.Tech. degree from SASTRA Deemed University, Thanjavur, India, in 2012, and the M.Tech. degree from PMIST, Thanjavur, in 2014. She is currently associated with the School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India. Her research interests include blockchain, the IoT, quantum computing, and swarm intelligence.

ABDULAZIZ TURKI ALMAKTOOM received the Ph.D. degree in industrial engineering from Wichita State University. He is currently an Associate Professor. He has published many journal and conference papers. His research interests include optimization under uncertainty, energy systems, supply chain management and logistics, inventory management, operations management health care management, safety, sustainability, decision making, and risk and lean management. Besides, he is a member of IEOM, IISE, ASQ, PMI, INFORMS, CSCMP, and ISCEA. He is a fellow of the Higher Education Academy (FHEA), U.K., and Advance HE, certified supply chain analysis, and a Lean Six Sigma Trainer.

ABDULAZIZ S. ALMAZYAD received the Ph.D. degree in computer engineering from Syracuse University, Syracuse, NY, USA. He is currently a Professor with the College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. His research interests include the Internet of Things, cloud computing, artificial intelligence, mobile and wireless networks, and information security.

GUOJIANG XIONG received the B.Sc. degree in automation from Zhejiang University, Hangzhou, China, in 2009, and the M.Sc. and Ph.D. degrees in power system and its automation from the Huazhong University of Science and Technology (HUST), Wuhan, China, in 2011 and 2014, respectively. From August 2014 to August 2017, he was an Engineer with the Guizhou Electric Power Grid Dispatching and Control Center, Guiyang, China. After that, he joined the College of Electrical Engineering, Guizhou University (GZU), as an Associate Professor. Since January 2019, he has been a Distinguished Professor with GZU. He has published more than 70 research articles in journals. His main research interests include renewable energy, power system operation, fault diagnosis of power systems, and application of artificial intelligence in power systems. He has been a reviewer for more than 30 journals and conferences.

ALI WAGDY MOHAMED received the B.Sc., M.Sc., and Ph.D. degrees from Cairo University, Egypt, in 2000, 2004, and 2010, respectively. He was an Associate Professor of statistics with the Wireless Intelligent Networks Center (WINC), Faculty of Engineering and Applied Sciences, Nile University, from 2019 to 2021. He is currently a Professor and the Chair of the Operations Research Department, Faculty of Graduate Studies for Statistical Research, Cairo University. He is a Professor with the Mathematics and Actuarial Science Department, School of Sciences and Engineering, The American University in Cairo, Cairo, Egypt. He published more than 140 articles in reputed and high-impact journals. Recently, he was appointed as a member of the Education and Scientific Research Policy Council, Academy of Scientific Research, from 2021 to 2024. Recently, he has been recognized among the top 2% scientists according to Stanford University reports 2020, 2021, and 2022. He serves as a reviewer of more than 100 international accredited top-tier journals and has been awarded the Publons Peer-Review Awards 2018, for placing in the top 1% of reviewers worldwide in assorted fields. He is the Chair of the Egyptian Chapter of the African Federation of Operations Research Societies (AFROS). He is an Editor of more than ten journals of *Information Sciences*, *Applied Mathematics*, *Engineering*, *System Science*, and *Operations Research*. He is an Associate Editor of *Swarm and Evolutionary Computation* (Elsevier). He has presented and participated in more than ten international conferences. He participated as a member of the reviewer committee for 35 different conferences sponsored by Springer and IEEE.