IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 28 September 2023, accepted 12 October 2023, date of publication 16 October 2023, date of current version 26 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3325056

RESEARCH ARTICLE

A Decentralized Resource Allocation in Edge Computing for Secure IoT Environments

A. SASIKUMAR[1], LOGESH RAVI[2], MALATHI DEVARAJAN[3], SUBRAMANIYASWAMY VAIRAVASUNDARAM[4], A. SELVALAKSHMI[3], KETAN KOTECHA[5,6], AND AJITH ABRAHAM[7,8], (Senior Member, IEEE)

[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 Computer Science and Engineering, Vellore Institute of Technology, Chennai 600127, India
[4]School of Computing, SASTRA Deemed University, Thanjavur 613401, India
[5]Symbiosis Centre for Applied Artificial Intelligence, Symbiosis International (Deemed University), Pune 412115, India
[6]UCSI University, Kuala Lumpur 56000, Malaysia
[7]School of Computer Science Engineering and Technology, Bennett University, Greater Noida, Uttar Pradesh 201310, India
[8]Center for Artificial Intelligence, Innopolis University, Innopolis 420500, Russia

Corresponding authors: Subramaniyaswamy Vairavasundaram (vsubramaniyaswamy@gmail.com) and Ketan Kotecha (head@scaai.siu.edu.in)

This work was supported by the Analytical Center for the Government of the Russian Federation under Agreement 70-2021-00143 dd. 01.11.2021 and Agreement IGK 000000D730321P5Q0002.

ABSTRACT The expansion of Internet of Things (IoT) devices and their integration into a variety of vital sectors has created serious concerns regarding data protection, privacy, and resource management. As a promising model, edge computing has the ability to overcome these difficulties by putting the computing power closer to IoT devices. This article presents a novel approach for decentralized resource allocation in edge computing settings, with the goal of improving the security and efficiency of IoT systems. Edge nodes are critical in our proposed framework for managing and assigning computing resources to IoT devices, minimizing latency, and optimizing network traffic. The decentralization of resource distribution promotes resilience in the event of network outages or cyberattacks and provides robustness against single points of failure. We created a proof-of-importance (PoI) consensus mechanism for creating new blocks in the blockchain integrated edge-computing IoT devices. Therefore, the consensus mechanism will ensure the trust and security of IoT devices by authentication of each user in the network. We performed a series of experiments in a simulated edge-computing setting to assess the feasibility of our proposed method. We analyze the proposed system model based on the operation of three different file delivery and transactions. The simulation outcomes show that the blockchain system efficiently delivers the files and increases the transmission rate. We also compared our file delivery and transmission rate with existing techniques, and our proposed model provides a better result. Finally, we compared the power consumption of creating IoT nodes based on proof-of-work (PoW), proof-of-stake (PoS), and PoI. The proposed PoI consensus mechanism consumes less power than the other two methods.

INDEX TERMS Internet of Things, blockchain, edge computing, resource allocation, proof-of-importance (PoI).

I. INTRODUCTION

New innovative applications with increasingly demanding necessities of low end-to-end latency and data privacy have evolved due to the development of edge computing devices and network capabilities. IoT technology currently uses a

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

centralized infrastructure with server-based processing, data storage, and control. However, the server IoT connection is no longer practical because of its high latency, status as a network failure, and challenges in terms of privacy and other needs. Also, there is a greater chance of congestion and bandwidth waste because of the enormous volume of data created by end devices [1]. Critical infrastructure systems have been employed to support humanities and energy system operations. They span from strictly physical assets as they are historically described to a broader concept of digital assets defined in power, fuel, groundwater, farming, healthcare, logistics, security services, communications systems, etc. [2]. In IoTs, the important components for vital foundational systems in the era of digital twins are largely to blame for this transformation. IoTs have evolved into crucial components of smart infrastructure, generating innovative solutions like the smart city and providing several benefits for cost and efficiency reductions [3].

The term IoT describes how numerous electronic gadgets and sensors can communicate with one another and enhance our quality of life by transferring data online. The IoT uses smart web devices to find creative solutions to various issues and difficulties impacting various governmental, commercial, and medical systems worldwide. IoT devices can enhance many activities by collecting and analyzing enormous volumes of data to make them more measurable and visible. In several domains, including medicine, smart buildings, the construction sector, farming, watershed management, and the power sector, IoT can potentially enhance the quality of system [4].

Edge paradigms try to bring computing, control, or data resources from the server nearer to the network's edge to solve data storage problems. IoT applications become more responsive with low end-to-end latencies and quick reaction times as more processing power is enabled at the edge. The fact that most data collected from edge devices are processed at the node and then transmitted entirely to the server further increases scalability. Processing user data locally allows for privacy, an aim that is becoming more and more important [5]. Yet, new resource management strategies are required to effectively manage the distributed resources to benefit from these newly available hardware resources.

On-demand resource sharing has been accomplished using conventional cloud technology due to its significant capacity and flexibility. However, with the IoT expanding so quickly in recent decades, increasing real-time data needs for collection, computation, and interchange have emerged that far exceed the carrying capacity of conventional cloud computing. Particularly, latency and bandwidth constraints prevent conventional cloud technology in IoT due to massive data transfer among millions of devices and data centers in various IoT use cases, such as digital twins and intelligent transportation systems. The Telecom Industry estimates that by 2022, there will be 29 billion interconnected devices on the worldwide network, with about 18 billion of those being linked to the IoT [6]. The following section provides the basic description of edge computing technology in details.

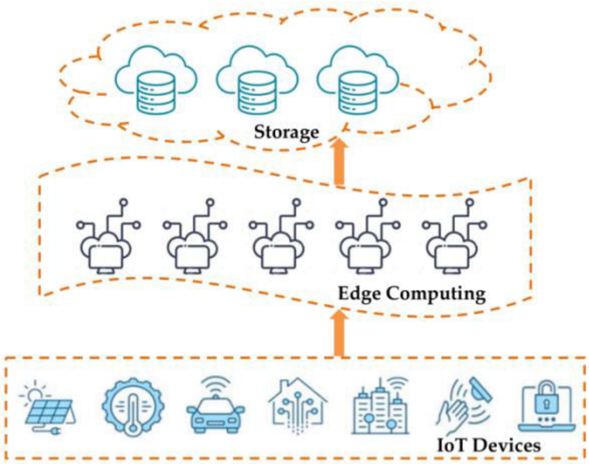

FIGURE 1. Edge computing architecture for IoT applications.

A. OVERVIEW OF EDGE COMPUTING

Edge computing is a category of a distributed system that puts computation and storage near the point of use instead of depending on a centralized, remote source. The data is digested and evaluated at the network's edge instead of being transported to a centralized location for assessment in edge computing. This method minimizes latency, boosts data processing speed, and improves system dependability and security. Edge computing is frequently utilized in IoT data processing situations, such as the digital twin, robotics, and automated vehicles [7]. Fig. 1 illustrates the conventional architecture of edge computing for IoT applications. In these situations, it is critical to have immediate access to data and the ability to process it, as delays might have catastrophic implications.

Edge computing includes numerous critical components, including:

1) EDGE DEVICES

These devices are positioned on the edge and accountable for collecting data, processing, and transmission. Sensors, webcams, and other connected devices are examples of edge devices.

2) GATEWAY

Edge gateways serve as a connection point between edge devices and centralized networks. They are in the position of gathering data from edge devices, analyzing it, and then delivering it to the centralized server or other edge devices.

3) EDGE SERVERS

These are servers that are positioned near the edge devices and are accountable for analysis complex data processing and large storage. Data processing, machine learning, and other computationally expensive processes can be performed on edge servers.

Overall, edge computing can improve a system's performance, dependability, and security by putting computation and storage systems closer to the point of use. Congestion and instability have become key issues due to the active nature of consumer demands due to the advancement of pervasive network solutions [8]. User networks have developed between data consumers and owners. The demand for big data processing systems such as data collecting, pattern matching, and data mining is important for user networks [9]. Because of these changing customer needs and the limits of edge devices and dynamic environments, network speed is critical for IoT applications. Time-sensitive services such as location tracking, machine vision, text analysis, real-time deep learning, smart healthcare systems, automotive networks, and so on make it nearly difficult to accept any latency in the network-integrated architecture.

Hence, the constraints of conventional edge computing using central control paradigms are as follows [10]:

I. The linear rise of edge computational capacity needs to be improved at the network's periphery, where the need for processing data from several sources is greatest.

II. A huge number of users are putting damage on the network bandwidth and transmission speed. Sending data from the user's location to the cloud data center may create service delays and a waste of computer power.

III. Third, outsourcing increases the risk that sensitive data stored in IoT devices may be compromised.

In addition to the limitations mentioned above, the physical separation between mobile nodes and the cloud hub also prohibits the cloud from gaining access to sensitive information about users' movements or local network conditions. Data from several IoT devices can quickly accumulate in IoT systems. Data can be more easily scaled and reacted to locally before being transferred to the cloud if it is processed at the network's edge. By utilizing the cloud's network along with additional resources like storage and complex systems, data can be moved from the border of the network. Excellent throughput and low latency at the network's periphery are two requirements of IoT systems that can be met with these capabilities [11].

Mobile and wireless networks are only two examples of edge computing systems. These variants include multi-access edge computing and ad-hoc vehicle systems. Originally known as Mobile Edge Computing (MEC) enables a cloud capabilities ecosystem at the edge of the telecommunication network, facilitating Digital Twin (DT) [12]. In a similar vein, automobile ad hoc networks permit ad hoc communication between disparate nodes.

A core implication of blockchain technology is that it offers a viable method for creating positive interactions between unreliable and unknown parties, enabling the distributed system of IoT, and doing away with the requirement for centralized power as in cloud computing [13]. A cryptographic hash key is used to connect the data blocks that make up the ledger, and this verifying process is called PoW. However, complete PoW puzzles using resource-constrained IoT devices require extensive computing power, making adopting blockchain technology in the IoT environment difficult. For real-time IoT applications, the mining process's delay could be better, in contrast to the blockchain's scalability problems and additional complexity brought on by its consensus methods.

The decentralized feature of blockchain technology and its cryptographic protocols can improve the privacy and reliability of data collected and handled at the edge. In the edge computing setting, it can offer a permanent record of activities or data trades, fostering trust. With blockchain's consensus algorithms, several edge nodes or devices can interact, verify data, and achieve consensus without a centralized authority. In an edge computing setting, the transparency of blockchain can offer an auditable record of data transfers and interactions, enhancing responsibility and facilitating legislative conformance. This developing strategy has basic security issues, notwithstanding the advancements provided by various edge devices in offering effective alternatives to the restrictions and inefficiencies of conventional cloud systems. This work explores a typical security issue when privacy preservation and data security are considered paradigms. Edge devices' computing, storage, and energy resources are frequently constrained.

B. CONTRIBUTIONS

We use blockchain technology to overcome edge-computing security issues and reduce the demanding nature of edge servers. The following are the rationales for using blockchain: The advantages of using blockchain include: (1) eliminating the requirement for a centralized administrator, which would increase costs and reduce the reliability of edge computing; (2) ensuring the smooth operation of resource allocation at the edge; and (3) enhancing security without the necessity for a private entity.

To that purpose, the following is a summary of the article's key contributions:

- For end-to-end supported edge computing, we proposed decentralized blockchain-based resource allocation architecture for IoT environments.
- We present a secure block mining mechanism for edge resource management system. Instead of solving a mathematical challenge to fight for block creation, we introduced proof of importance (PoI) consensus mechanism. The PoI metrics is calculated based on the proposed model for access control.
- To assess edge's resource allocation performance, simulated experiments are carried out. The experiment's findings show that Edge outperforms other benchmark schemes regarding file transfer and network resource usage.

The rest of the article follows: Section II provides a general idea of on-edge computing and decentralized blockchain. Section III describes the proposed blockchain-based edge computing framework. Section IV discusses the simulation results of the proposed framework. Finally, Section V summarizes our work and discusses plans.

II. RELATED WORK

The following section introduces the basic principles and underlying technologies related to standard blockchains and edge computing. In edge computing, we apply these ideas to create a novel blockchain system that addresses challenges, including security and resource utilization in a distributed environment like the IoTs.

A. BLOCKCHAIN

Blockchain technology was developed by Satoshi and put into practice with Bitcoin [14]. Blockchain networks naturally necessitate prevention measures since, unlike physical cash; virtual money has the danger of being used twice by the same stakeholder. Double spending can be avoided with the use of blockchains and decentralized authority. Blockchain technologies are peer-to-peer, distributed ledgers that hold records of network transactions. These logs are arranged into blocks, forming a series of blocks connected by their hash.

Blockchain are distributed among all network peers, and the mathematical consensus preserves a shared state. Blockchain networks do not support transactions (hence rooting out double-spending). Blockchain technologies are incremental backup data structures that cannot change their contents because of their replicated shared ledger. Blockchain technology has found use in various fields, including but not limited to transportation, accounting, healthcare, and electronic governance systems, in addition to the exchange of virtual currency. Blockchains offer a possible paradigm change through the provision of distributed services without the requirement to "trust" any centralized parties. Blockchain applications to decentralize distinct edge IoT services are the subject of active research [15]. Research is gaining momentum toward blockchain-based edge computing because of the following possible advantages:

- Single points of failure are eliminated, and fault tolerance is improved via decentralized blockchain-based edge computing [16].
- Distributed peer-to-peer system architectures promote edge device independence with decentralized identity verification, registration, and verification capabilities.
- Blockchain-based logging is guaranteed to be auditable and immutable. Blockchain enable "trustless" data sharing in edge computing. Public blockchain users can check the accuracy of data or code they obtain through ledger transactions.
- By utilizing smart contracts, blockchains can enforce terms and conditions during IoT interactions and gain the capabilities of digital logic. Blockchain networks' decentralized services are built on top of smart contracts. Without centralized banks or regulatory bodies, blockchains make it possible to monetize data and devices in a truly democratic way, whether through the rental of gadget utility, data monetization, or even micro transactions.

Despite these advantages, study into design compromises is becoming increasingly important to address the scalability and performance problems that blockchains may experience. Our efforts to create a blockchain-based edge computing architecture are intended to show how crucial blockchains play in decentralizing and providing secure IoT services. The demands of blockchain-assisted edge computing are following as:

Various requisites must be met to combine blockchain with edge computing [17], [18].

1) AUTHENTICATION

In IoT device contexts with many interconnected nodes, platforms, and activities, it is crucial to verify the identity of network organizations before they collaborate via their interfaces to reach a deal by executing smart contracts. Blockchains keep track of entities' rights and needs as the contract is established. Even if they are from various security sectors, this is important for creating secure channels of communication between the components of edge environments.

2) ADAPTABILITY

Over the period, more devices and more complex applications are available, especially when blockchain technology is used on devices with limited resources. To allow objects or nodes to link to or leave the network easily, the secure solution of blockchain with edge devices should accommodate a changing number of end viewers and jobs with varied levels of complexity.

3) NETWORK SECURITY

Because of its diversity and attacker sensitivity, network security is an important issue for edge computing networks. Edge computing systems must incorporate blockchain to eliminate some transmission protocols' cumbersome access control and make massively dispersed edge servers easier to maintain. This integrated architecture will improve control layer surveillance to stop malicious behavior.

4) DATA INTEGRITY

Maintaining and ensuring the correctness and reliability of information over its full life cycle is referred to as data dignity. Data integrity contraventions are much less likely when using the abundant shared storage spaces of edge computing. The replicating data over the network of servers at the edge, and using the use of blockchain technology for data security service in a fully distributed setting. As a result, there has to be a more accountable means of confirming data integrity for both data owners and users.

5) VERIFIABLE COMPUTATION

The calculation can be delegated to a few unreliable clients while keeping accurate results. Edge computing allows for outsourcing computing without even being limited by blockchain scaling. Efficient processing timing and precise responses should be guaranteed by the incentive and autonomy of smart contracts that operate on the Ethereum network.

6) LOW LATENCY

The transmission and processing delay are the two components that make up a platform's delay. Data processing and blockchain mining take time, are measured by computation delay, and depend on the system's computing power. The ability to provide quick computing expands from cloud storage to end-user but also significantly increases transmission delay. We need to use a combination of edge computing and blockchain technology to get the optimal balance between transfer and computation latency. Understanding the relationship between the calculation type and the execution site is crucial for the system's efficiency.

B. BLOCKCHAIN -BASED DECENTRALIZED EDGE COMPUTING

Using blockchain technology to establish a decentralized ecosystem of edge devices that can work independently of a central authority is what is meant by "decentralizing edge devices." to control this, blockchain technology can keep track of and verify the behaviors of all edge devices and govern their interaction and data transfer with one another. The IoTs is one area where blockchain technology could decentralize devices at the network's edge.

Distributed computing platforms are another future use case for decentralized edge devices made possible by blockchain [19]. In these systems, a network of edge devices is employed to perform computational tasks in a decentralized fashion. The edge device can pave the way for more scalable and robust distributed services that don't require a single point of failure. Decentralizing edge devices with blockchain could lead to more adaptable and safe distributed networks and the development of decentralized applications. In [20], authors proposed a power allocation platform using a decentralized edge computing model. They have implemented deep reinforcement learning-based model for vehicular edge computing with the help of decentralized network architecture.

Many recent studies have looked at blockchain innovation as a possible solution to the problems with edge computing that have been discussed thus far. For instance, "EdgeMediChain" is a blockchain and edge computing system created by Akkaoui et al. [21]. To establish the scalability and security of medical data, its framework was created using an Ethereum-based permissionless blockchain. The created framework makes use of a permissionless blockchain, which means that privacy is not guaranteed and no one entity can be reliably identified within the system.

Edge computing and blockchain were integrated by Bonnah et al. [22] to create distributed security by implementing a publicly trustworthy network. The proposed architecture utilized the main permissioned blockchain ideas within the network. Additionally, distributed networks succeeded in authenticating users within the system that aims to access resources or services. Decentralized data storage in the distributed ledger system mitigated the threat of a single point of failure, although privacy concerns were not adequately addressed. A trust-aware IoT data processing unit called "TIDES" was unveiled by Chuang et al. [23] and is based on blockchain and a centralized edge computing ecosystem. Their economically sound method enables IoT devices to exchange data and decrease transaction latency. The focus of this study was on something other than IoT device security. Furthermore, the multi-access edge computing system's central role in data storage has remained unchanged.

Cui et al. developed and created a blockchain-based secure edge computing IoT system [24]. Their work focused on using a heuristic approach to solve task allocation issues in IoT systems. Xiong et al. [25] combined edge framework with blockchain to establish a peer to peer mining network for edge devices and distributed trustworthy authentication architecture. The edge computing security framework includes machine learning [26], reinforcement learning [27], and surveillance devices [28] principles. These experiments mostly employed permissionless blockchain, which does not offer sufficient anonymity. To enhance security, privacy, data traceability, and sharing, designing, developing, and deploying an infrastructure that exclusively uses permissioned blockchain systems and entrepreneurship is necessary.

In [29] implemented a decentralized cloud environment with edge devices made possible by Software-Defined Networking (SDN) architecture. The developed architectures are divided into three layers: endpoint, fog, and cloud. Blockchain technology is being used to connect all SDN devices distributed. When there aren't enough local processing resources, a fog node can send its application service deployment request to the cloud and share its data analysis results with the distributed cloud and system layers. Finally, a fog device sends the computational workloads to the cloud network. This design addresses many problems plaguing traditional cloud computing, such as sluggish data transfer, lack of scalability, insufficient security, and a lack of accessibility.

In [30] proposes a multi-layer blockchain-enabled IoT system model. The edge layers and the high-level layers make up the IoT model. The edge layer is a small, private network where a single controlling node oversees a small set of nodes. There is no centralized node; therefore all of the nodes can function independently when it comes to data. Data maintenance is handled autonomously within each node. However, the data exchanged between nodes are recorded in a distributed consensus ledger modified by all nodes. The multi-layer network concept supported by blockchain paves the way for the creation of a globally secure IoT network. In [31], the authors presented a block-chain-integrated edge computing and InterPlanetary File System (IPFS)-enabled convolution neural network-based video surveillance system. Blockchain technologies improve the system's sturdiness and dependability. Data from a large number of wireless sensor nodes can be collected, analyzed, and evaluated with the help of edge computing. To accomplish massive graphical storage and continuous surveillance, IPFS and Convolutional Neural Networks (CNNs) are used.

The authors of [32] create a system centered on blockchain identification and access control to address the issue of edge nodes in industrial IoT. The self-certified credential technique is used for network entity creation and identification. Based on public keys, they proposed a protocol for a lightweight key establishment that offers IIoT identification, traceability, and secrecy. In [33], authors proposed two different consensus mechanisms for energy trading in the internet of edge vehicles. The authors of [34] utilized wireless services leading to a greater variety of requirements for mobile devices' communications, computation, and caching (3C) capabilities. This work developed an integrated structure to characterize the various services, and it optimizes the 3C resources of the base station (BS) and mobile devices together to provide a distinguished Quality of service (QoS) for various services, in contrast to previous work that only considered a single type of service. In the proposed framework, we model the job needed by the mobile device to be produced at the BS, the mobile device itself, or both of them. This means the demanded tasks are provided via different channels, requiring varying bandwidth, computation, and caching capabilities.

In [35], the authors proposed a blockchain infrastructure based on IoT virtual supply on an edge host. As a result, the fog node can be used as an extension of cloud computing. The authors also think about how the edge network in a system configures the Machine to Machine (M2M) applications that connect via peer-to-peer. It's meant to virtualize software-defined IoT modules to control the settings of a large and varied collection of gadgets. The blockchain must be used to securely store any code or metadata that configures digital assets. Tenants can readily recognize and install digital systems, as well as access and write to blocks, with a blockchain that requires no special permissions. As a result, multi-tenant accessibility and virtualized distribution of resources are safely under the authorized blockchain's authority. The paper implies that the proposed work addresses resource allocation difficulties in the context of edge computing, emphasizing the solution's decentralized nature. Furthermore, it emphasizes the crucial need for security in IoT setups, which is a major worry in today's interconnected society.

III. THE PROPOSED BLOCKCHAIN-ASSISTED DECENTRALIZED EDGE COMPUTING FRAMEWORK

The proposed architecture for integrating blockchain with edge devices for IoT environments is presented in this section. The plan is organized in layers to move the complex activities of blockchain to a different layer. This layer is outside of the application that contains IoT nodes with limited resources. We then continued by explaining the tasks performed by each architecture layer. Computing loading, offshore storage systems, control and administration of networking transactions, and their implementation in the framework were proposed as core IoT necessities. The proposed system shows the framework's solutions for privacy, authenticity, and flexibility and has deployed an explanation of the facility's implementation. The following sections describe the system integration of proposed architecture.

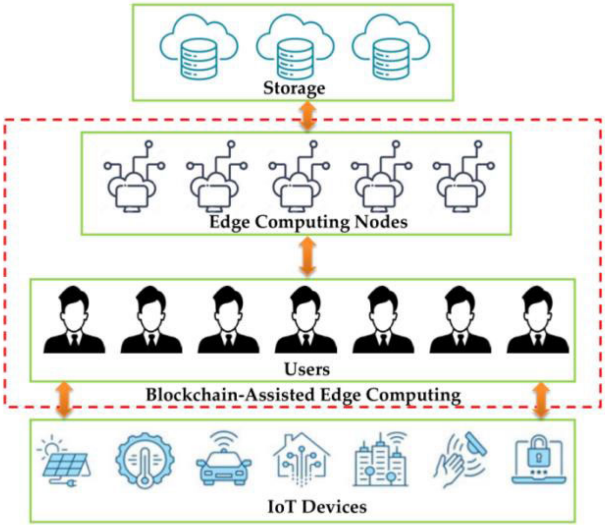

FIGURE 2. The proposed Blockchain-assisted edge computing architecture for IoT Environments.

A. SYSTEM ARCHITECTURE

Fig. 2 depicts the four-tiered IoT device layer, User layer, edge computer node layer, and storage layer that make up the presented blockchain-assisted resource distribution framework. The raw data is monitored and acquired from the nearest server on the bottom layer by the IoT devices, which include various sensor devices like mobile, smart devices, notebooks, etc. Several IoT devices are owned and managed by each data layer user. The cleaned raw data is then sent to the edge computing layer for further processing, allowing for rapid data analysis or processing. For further data evaluation or long-term archiving, the cloud or data layer can receive the output data from edge computing processing. In this case, we assume that the data layers employ real-time dynamic solutions, which necessitates the timely delivery of analysis findings to Decision Support Systems (DSSs). Each Computing Node (CN) is distributed along the network's edge and contains a collection of low-power computers that can provide data cloud services.

Any IoT device with more processing capabilities can explicitly integrate this Edge Computing Node (ECN). Every distributed processing system needs scheduling because the software's efficiency defines how well they work. Therefore, when a data layer requires a data service, the best ECN should be selected to fulfill the request based on the system's current state (such as the workloads each ECN is presently managing) and the DSS's QoS specifications. Consequently, ECNs can shift the analysis of the receiving data to the server network at the rate of a quick response time and increased network resource utilization.

1) IOT DEVICE LAYER

Peer to Peer (P2P) networks of user devices that may exchange information and act as consumers and producers of IoT data within a blockchain system make up this layer. Among these are smart gadgets equipped with sensors and actuators for data collection, sharing, and transmission to higher levels. Edge gateways or a P2P network can be used for decentralized information sharing between smart devices and the storage system. In the decentralized interface, a public ledger is constructed to handle peer-to-peer transactions, including the installation of new peers, mining of blocks, and the cancellation of an existing peer. In this configuration, peer devices can only establish a connection with one another via a shared secret key that is distributed by the server.

P2P connections, on the other hand, allow devices and servers to join the blockchain network together. Because end devices in this situation have limited resources, their involvement in blockchain was made possible by stronger servers that could be found at higher levels, at the edge, and on the cloud storage. Thus, servers handle the more demanding activities, leaving end devices to handle simpler ones like exchanging transaction summaries with peer nodes or receiving firmware updates.

Safely providing vast quantities of remote storage and high computational capabilities on demand to IoT devices with limited resources is the specialty of edge devices, which may be used in both centralized and decentralized connection techniques. As a bonus, edge servers' proximity to end users allows for faster response times in IoT applications. Devices can flexibly outsource their expensive tasks, such as processing or storage, to a neighboring, more capable peer or an edge server for even faster response times, all thanks to the decentralization made possible by our proposed model. By loading, only the essential part of the chain is stored on the devices, saving them from having to conduct unnecessary calculations. The lack of interoperability between smart devices from different manufacturers prevents them from working together in a single network, but blockchain makes it possible for them to do so nevertheless.

2) BLOCKCHAIN-ASSISTED DECENTRALIZED EDGE NODE

To improve throughput and lower latencies, the edge layer takes advantage of cloud computing to bring services closer to end devices. Edge servers can relay messages amongst one another to produce redundant data storage, synchronized data processing, and supply for smart IoT devices. Distributed ledger technology, or blockchain, is installed on edge servers to create a system that guarantees secure data movement across the network. Edge nodes in the network do light monitoring for themselves and other peers to achieve identity during the dynamic addition and deletion of edge nodes. In addition, they dynamically process the data and send it to a distributed cloud, either for long-term storage or use by back-end devices. This layer's end-to-end architecture coordinates a distributed set of resources for in-memory analytics, near-real-time processing, and other tasks that can't wait.

The servers can load their workloads and make cloud service demands if the compute demands exceed the edge servers' handle. The novelty of this work is to offer consensus mechanism to verify assertions made by devices regarding their capacity for computing and storage. Using smart contracts with basic consensus methods on a blockchain network like Ethereum is the best solution to provide lower latency and improved bandwidth for a larger range of end-to-end edge servers and distributed resources in the cloud.

3) DISTRIBUTED STORAGE NETWORK

Providing the ability to process and store the term service is the primary goal of the storage layer. In our view, it also qualifies as a public blockchain node that can take part in mining. Since the cloud layer houses immense storage and processing capabilities, the consensus method in the distributed blockchain is crucial for providing secure, inexpensive, and rapid access to greater than the finest-grade computing resources. Devices deployed as blockchain nodes can receive proportionate rewards for good and penalties for bad behavior using the built-in integrity of data service. As opposed to the data-dependent edge nodes, the cloud nodes can use blockchain to ensure that all similarly recorded insights are replicated across all of them.

B. DISTRIBUTED DATA TRANSFER PROCESS

The proposed architecture involves the following data exchange operations.

- Data exchange transaction. Smart contracts are utilized in edge device to compensate and honor facility owners for donating computing resources. The facility owner and the associated mobile user will swap tokens when a task is finished. The facility's productivity concerning token swaps should influence future facility decisions. A facility owner will be fined if they fail to offer the specified resource-giving service.
- Data submission transaction. Request submission transactions are transmitted to the network whenever an average user requires computational resources for data processing. The transaction outlines the conditions needed to complete a task, including the resources needed and the anticipated time frame. The transaction includes the CPU need, memory usage, and drive the necessity for data transmission. The sign is then produced using the private key. The public key and sign are then placed on the contract's head.
- Data request-response transaction. The network receives a request-response transaction when a facility owner decides to accept a request. A consensus protocol is suggested to choose the best owner because multiple owners may approve the same request over time. According to the smart contract, it is checked to see if the transaction's content has changed. If nothing changes, it is determined whether the available resource is greater than or equal to the needed resource based

on PoI metrics. A response transaction is generated once there are sufficient resources available. The facility's information is included in the transaction.

- Ability node selection transaction. A facility decision transaction is communicated to the network when a facility owner is chosen using the PoI consensus protocol. In the section that follows, the PoI consensus mechanism is covered. According to PoI, the best device was chosen based on performance. A selection transaction is subsequently generated. The created transaction includes the information of the sender, which corresponds to the response transaction.

In our system, there are three different sorts of contracts.

- Registrar agreement: Identity keys are generated for a user by this global contract.
- Contract for Selection: Several facility owners may respond to a request for computing resources. This global contract uses a proof-of-importance consensus methodology to choose the best facility. This contract also generates a set of data-sharing keys.
- Payment contract: After a demand has been executed, this global contract gene-rates a token exchange transaction.

C. PROOF OF IMPORTANCE

The New Economy Movement (NEM) first developed the consensus procedure known as Proof of Importance (PoI). PoI and Proof of Stake (PoS) are generally similar in that nodes are needed to lock up a specific number of coins. To incentivize network activity and determine a wallet's importance, PoI has additional requirements besides simply having a node operational, as shown in Fig. 3. Each wallet must have a minimum of 10,000 coins invested for a specific time to be considered for the importance estimation. Additionally, using the NEM network and submitting transactions might raise an important score. Security restrictions have been implemented to increase its significance to prevent loop attacks, which entail moving coins between wallets managed by a single individual. A technique has been developed by NEM that gives a lot of weight to accounts that transmit NEM and less weight to accounts that transfer many coins but get most or all of their NEM back. Even if an account used the loop approach, it would only see a small (10%) increase in its importance score and very little financial advantage because the extra money it would have made from its greater importance would have been wasted on transaction fees. Tokens created on the NEM blockchain are called XEM. The same way we are utilizing PoI consensus mechanism for resource allocation. The node having more number of resources will be considered based on PoI metrics. The proposed PoI metrics are discussed in the following section.

1) DETERMINING POI SCORES

The device resource importance score is denoted by Ψ, which is measured as given;

$$\Psi = (normalize_1(\max(0, v + \sigma c_0)) + rc_i)\chi$$

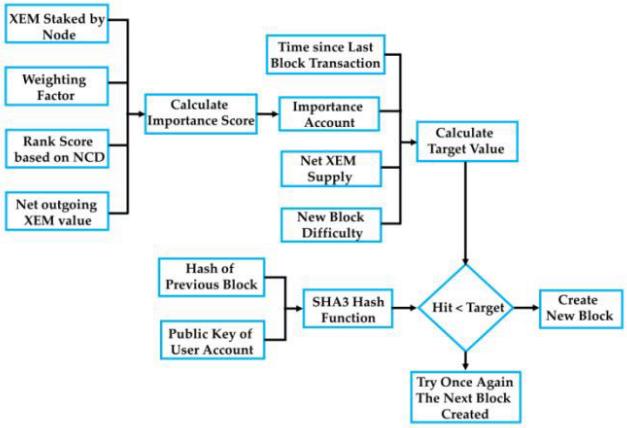

FIGURE 3. The PoI consensus mechanism blocks creation process.

where the normalized vested score is calculated as follows;

$$normalize_1(v) = \frac{v}{\|v\|}$$

where v denotes the vested amount of XEM in terms of computing resources. σ represent the weighted net score of XEM, r is the weighted net score of XEM. Finally χ is a weighting vector in the network topology and c_0, c_1 are the weighting constants. The weighting vector χ considers the network topology and allocates a higher weight to blocks that are parts of the blockchain network, rather than outliers or hubs. Outliers and hubs are generally fixed at 0.9 of their weighted score. In the case of blocks in the networks are weighted at 1.0. In NEM wallets, c_0 *and* c_1 weighting constants fixed are at 1.25 and 0.1337, respectively.

Based on the importance scores, the value of vested wallets sent XEM and exchange network transactions are considered to evaluate new block creation. The main feature of PoI is the importance score cannot be randomly manipulated or changed since the importance scores are calculated using the PoI model. For example, the scores are considered a form of reputation. Therefore all weighted scores sum to unity; they denote the proof of importance, which can be utilized for voting or eliminating scams. The PoI allows the maximum number of users to communicate with each other because a single user does not have control over manipulating the weighting scores and other identities.

With the help of security credentials, security operations were separated into several modules and distributed on edge devices. These decentralized security services function as a service cluster for the edge computing platform to provide a scalable, adaptable, and inexpensive data exchange and access control mechanism. Following is an introduction to the main service processes and modules:

a: REGISTRATION SERVICE

Before utilizing the open source edge platform Edgex Foundry capabilities, each proposed edge network endpoint entity must send a request message to the enrolment service.

The Secure Hash Algorithm (SHA)-256 method is utilized by the process of registering service to generate the user's information, known as InfoHash. A new peer node is created by the Hyperledger Fabric blockchain. The interface and a peer node exchange a public-private key pair if the node is bound to it. The peer node initiates a smart contract to record the terminal's In-foHash in the blockchain, and then generates and transmits the user ID. The User ID and associated public-private key pair are stored locally on the terminal.

b: IDENTITY AUTHENTICATION

The interface relays the personal data proof of identity, the reliability of the data as text, and the securely verified private key to the authentication of identity service. The correct InfoHash data is sent to the account authenticator from the Virtual ID-based smart contract. Verify that the interface's provided data is correct and agrees with the identity information on file. Whether or not the Hash and InfoHash are the same is checked by the identity authentication service. The identity authentication service verifies the terminal's digital signature to guarantee it owns the corresponding private key. After verifying the terminal's identifiers, the authorization service writes the verification steps into the smart contract for posterity. Once the aforementioned steps have been completed, the authentication service will return the authentication result.

c: ACCESS CONTROL

To obtain a permission token, the gateway must first submit a user request for access to the authentication service. The access control service will use the visitor's identification data in conjunction with an authorization policy to determine whether or not to provide access. If the request for admission is approved, the access control service will return a query token and create a smart contract to record the outcome of the investigation on the blockchain. The token is checked by the service providers when a request is received from an endpoint to determine whether or not to proceed with the request. The token then consults the blockchain's permission data to see if the service is available to the interfaces.

d: SECURITY MANAGEMENT

The system security gateway acts as an information and safety site supervisor. The security authentication modules provide registration data and access control policy. These security policies are kept current and maintained by the smart contract service. When an endpoint is recognized, the smart contract service applies an authorization policy tailored to its needs. The edge server operator can modify registered device credentials through the smart contract service, while regular users have access to this functionality only for their registered interfaces. Access permissions can be made by the operator and the terminal's registered members, while the operator can only change access privileges. Hence the proposed decentralized edge computing architecture provides the better user access control for resource management.

TABLE 1. System specifications of decentralized edge computing architecture.

System Details	Specifications	Descriptions
Personal Computer	OS CPU RAM External Memory	Ubuntu 20.04 Intel Core i5 8 GB 500 GB
Edge Device (Raspberry Pi 4)	OS CPU RAM External Memory	Ubuntu 20.04 BCM2711 2 GB 128 GB
Software	Library Application	Python SDK, Docker, Docker Compose

IV. EXPERIMENTS

In this section, we run simulation tests and assess how well the proposed dynamic resource allocation strategy performs. We first describe the simulation environment and particular experimental setup. Next, the number of file transfer rates is examined to determine the best ways IoT devices can manage resource requirements. The best approach for an Edge Computing Server (ECS) to manage the usage of the allotted edge resources is highlighted with help of Raspberry Pi 4.

A. SIMULATION SETTING

This section considers an edge network with a single ECS and several IoT devices. The simulation environment settings are listed in the Table 1. In the proposed model, IoT devices depend on the edge computing capabilities of the ECS to deliver satisfying services to users. To make money, the ECS distributes edge computing resources to IoT devices. The ECS should pay for the mining reward for exchanges between the ECS and IoT devices. The best resource request techniques for IoT devices will be provided for various metrics, such as delivery rate, transmission overhead, and power consumption, mostly influenced by user service requests. In line with the Stackelberg game, the base price of edge computing resources released by the ECS will be used to examine the best methods for requesting resources for IoT devices. In this analysis, the resource delivery and transmission rates are considered for all IoT nodes. The probability that resource interactions between the ECS and IoT devices can be recorded into a valid block is 100%. After the IoT devices decide on the necessary resources, the ECS will regulate the resource pricing to optimize its data rate.

With the help of Python-based SDK, we put the modelling into practice. We create additional transaction types using the blockchain as the private network in simulation environment. Using HTTP facilities, the official private network transmits data between nodes. By adding capabilities for requesting, forwarding, and file delivery provided by HTTP providers, we increase the capability of the client in private network. The client can listen on a number of ports that are used by

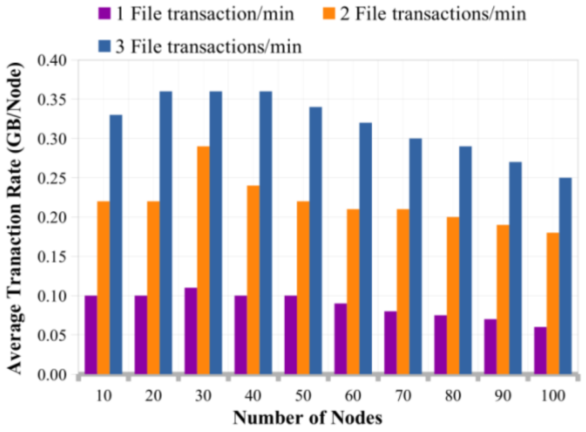

FIGURE 4. The average file transfer rate of the proposed framework.

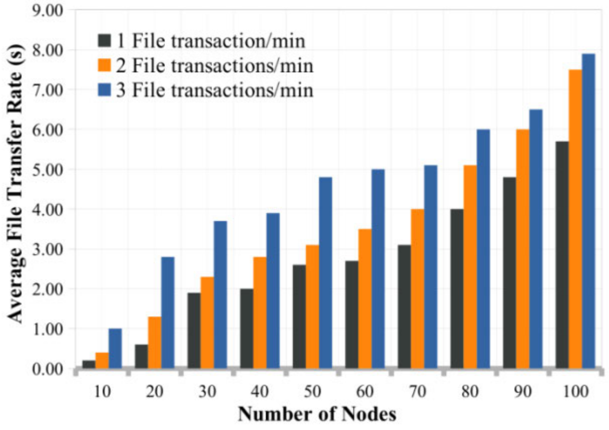

FIGURE 5. The average transaction rate of the proposed framework.

the blockchain system's file transfer, relay, and blockchain services. Next, we model data movement utilizing various advanced mobility patterns. We set a node's maximum range to 7 meters. A node is considered to have moved if it went outside of this range. We do not test the data migration due to node mobility using the private network because it is challenging to change the connection actively over multiple containers. Instead, we use Python to develop the method and tested the data movement using certain established movement patterns. Therefore, we just model movement and storage. The system specifications are described in the Table 1.

B. PERFORMANCE DISCUSSION

First, we examine the differences in user service requirements under two different types of settings: delivery file rate and transmission file rate. Fig. 4 shows the data delivery service requirements concerning the number of nodes, while Fig. 5 show the transmission service requirements for the IoT nodes in the network. The delivery and transmission rate required by the developed blockchain-assisted network with IoT nodes is illustrated in Fig. 4 and 5.

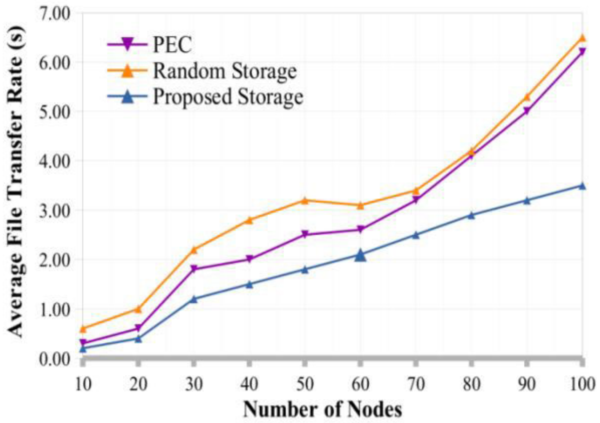

FIGURE 6. The proposed file transfer rate is compared with the existing framework.

At the start of the process, we may observe that users have higher service expectations to get the necessary services from IoT devices. Services demand declines and converge to an equilibrium position as more consumers meet their needs. When the demand for delivery rate services rises and then slowly increases based on the IoT nodes. We increase the IoT devices in Fig. 4 to get the transmission rate service requirements in three different scenarios, namely, 1 file/min, 2 files/min, and 3 files/min.

From figure 4 and 5, we conclude that the proposed system's transmission service requirements are unaffected by IoT devices because those IoT devices file 1, 2, and 3 are consistent with the earlier results.

The ways IoT devices access the necessary edge computing resources are next examined. The effect of delivery rate on the resource allocation of IoT nodes is momentarily disregarded because the unit file rate for the assigned edge computing resources is believed to be a fixed value. The IoT devices would need edge computing resources from the ECS based on the service requirements to satisfy edge consumers. Fig. 6 and 7 shows the file delivery rate requirements for IoT nodes. Fig. 6 depicts the delivery rate of edge computing resources that IoT devices need for several nodes, whereas Fig. 7 depicts the transmission rate of the IoT nodes in the network.

Each IoT device needs a significant quantity of edge computing resources from the ECS to satisfy the potential service requirements. At the start of the process, the IoT devices need to know how many resources are required to meet users' service needs. The amount of edge computing resources needed by each IoT device would decrease throughout the process to a stable equilibrium position based on the real needs of users. Different edge computing resources are needed depending on the user's service requirements. IoT devices need greater edge computing resources as more consumers want more services.

Once we double the number of IoT devices in the proposed scheme, we can find that the number of IoT devices will not impact the amount of edge computing resources needed, as shown in Fig. 6 and 7, since we assume sufficient edge computing resources in the blockchain for

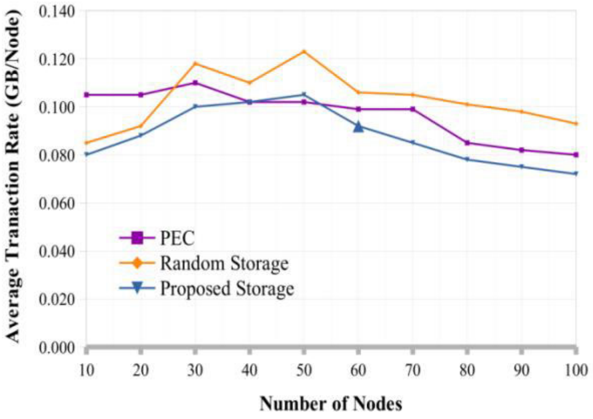

FIGURE 7. The proposed transaction rate is compared with the existing framework.

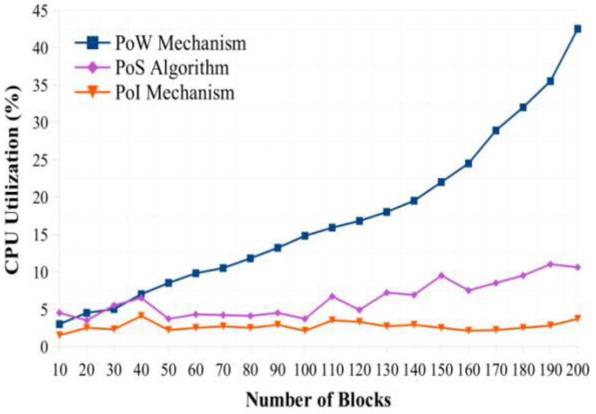

FIGURE 8. The CPU utilization of the proposed consensus compared with the existing model.

resource allocation. The blockchain-assisted network would re-allocate the delivery rate of the assigned edge computing resources to optimize its performance based on the judgments made by the IoT devices on the needs for edge computing resources. The random methods and pervasive edge computing (PEC) [36] in the delivery and transmission rates, respectively, are depicted in Fig. 6 and 7, which are the better solution for the proposed model. The delivery rate decreases initially for ECS's best technique for the blockchain-assisted network. As demonstrated in Fig. 7, the quantity of IoT devices may have an impact on the transmission rate since it may affect the delivery rate from the assigned edge computing resources and the payments to miners

Fig. 8 shows the CPU utilization of IoT nodes in proof-of-work, proof-of-stake, and proposed proof-of-importance, respectively, with 200 IoT nodes. It is demonstrated that IoT device power consumption can fast converge to a stable value in the proposed PoI model. In the case of PoW and PoS, the power consumption may initially remain constant before increasing swiftly to their maximum value. Fig. 8 shows how the CPU utilization of IoT devices diminishes as the number of IoT devices increases from 10 to 80. IoT devices would cost more for a similar amount of edge computing resources. The power consumption would be scaled back as the number of IoT devices expanded due to the blockchain setting an importance score value for the resources assigned to edge computing. However, in a PoIconsensus mechanism, the power consumption would be the same because IoT devices would have minimal resource consumption in the initial stages. The value of the importance score given to the nodes will also impact CPU utilization. Additionally, the CPU utilization is less in the proposed PoI-based model than in the existing PoW and PoS. The proposed blockchain-assisted edge computing platform can reduce the power consumption of IoT nodes as the number of devices increases.

V. CONCLUSION

The goal of our work was to combine the two widely popular innovations of edge devices and blockchain for resource allocation. We proposed IoT environments based on a decentralized architecture to allow edge devices and blockchain to support a secure data processing system at the edge. Using the decentralized framework, we presented a PoI-based consensus model in a smart contract for data integrity service to validate stored transactions and strengthen data security. We used a layered architecture to improve scalability in our design, separating the blockchain from the application layer and extending the smart contract with quick and scalable transactions through the distributed network. Thanks to the division, IoT devices with limited resources can now only store the sections of the blockchain they require for their transactions. In terms of anonymity, we implemented an authentication mechanism linkable to hash signatures, timestamps, and smart contracts to be suitable methods for disguising transaction information and user identities. Therefore, to increase anonymity, we used authentication based on hash signatures and timestamps in our architecture's registered node. Experimental analyses of the proposed blockchain-assisted edge computing framework show viability in successfully adequately allocating resources among various IoT devices. In future work, we are planning to integrate Internet of Vehicle with the proposed blockchain architecture for vehicle maintenance at the edge.

REFERENCES

[1] S. Zhang and J.-H. Lee, "A group signature and authentication scheme for blockchain-based mobile-edge computing," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4557–4565, May 2020.

[2] K. Yu, L. Tan, S. Mumtaz, S. Al-Rubaye, A. Al-Dulaimi, A. K. Bashir, and F. A. Khan, "Securing critical infrastructures: Deep-learning-based threat detection in IIoT," *IEEE Commun. Mag.*, vol. 59, no. 10, pp. 76–82, Oct. 2021.

[3] A. Sasikumar, L. Ravi, K. Kotecha, J. R. Saini, V. Varadarajan, and V. Subramaniyaswamy, "Sustainable smart industry: A secure and energy efficient consensus mechanism for artificial intelligence enabled industrial Internet of Things," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–12, Jun. 2022.

[4] A. Sasikumar, L. Ravi, K. Kotecha, A. Abraham, M. Devarajan, and S. Vairavasundaram, "A secure big data storage framework based on blockchain consensus mechanism with flexible finality," *IEEE Access*, vol. 11, pp. 56712–56725, 2023.

[5] X. Lu, Y. Liao, P. Lio, and P. Hui, "Privacy-preserving asynchronous federated learning mechanism for edge network computing," *IEEE Access*, vol. 8, pp. 48970–48981, 2020.

[6] A. Nistor and E. Zadobrischi, "Analysis and estimation of economic influence of IoT and telecommunication in regional media based on evolution and electronic markets in Romania," *Telecom*, vol. 3, no. 1, pp. 195–217, Mar. 2022.

[7] M. Cui, S. Zhong, B. Li, X. Chen, and K. Huang, "Offloading autonomous driving services via edge computing," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10535–10547, Oct. 2020.

[8] A. Husen, M. H. Chaudary, and F. Ahmad, "A survey on requirements of future intelligent networks: Solutions and future research directions," *ACM Comput. Surv.*, vol. 55, no. 4, pp. 1–61, Apr. 2023.

[9] J. Wang, Y. Yang, T. Wang, R. S. Sherratt, and J. Zhang, "Big data service architecture: A survey," *J. Internet Technol.*, vol. 21, no. 2, pp. 393–405, 2020.

[10] W. Li, J. Wu, J. Cao, N. Chen, Q. Zhang, and R. Buyya, "Blockchain-based trust management in cloud computing systems: A taxonomy, review and future directions," *J. Cloud Comput.*, vol. 10, no. 1, pp. 1–34, Jun. 2021.

[11] T. Mai, H. Yao, S. Guo, and Y. Liu, "In-network computing powered mobile edge: Toward high performance industrial IoT," *IEEE Netw.*, vol. 35, no. 1, pp. 289–295, Jan. 2021.

[12] C.-M. Huang and C.-F. Lai, "The delay-constrained and network-situation-aware V2 V2I VANET data offloading based on the multi-access edge computing (MEC) architecture," *IEEE Open J. Veh. Technol.*, vol. 1, pp. 331–347, 2020.

[13] D. V. Medhane, A. K. Sangaiah, M. S. Hossain, G. Muhammad, and J. Wang, "Blockchain-enabled distributed security framework for next-generation IoT: An edge cloud and software-defined network-integrated approach," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6143–6149, Jul. 2020.

[14] N. Satoshi, "A peer-to-peer electronic cash system," *Decentralized Bus. Rev.*, to be published.

[15] A. Sasikumar, S. Vairavasundaram, K. Kotecha, V. Indragandhi, and L. Ravi, "Blockchain-based trust mechanism for digital twin empowered industrial Internet of Things," *Future Gener. Comput. Syst.*, vol. 141, pp. 16–27, Apr. 2023.

[16] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues, and K. Ko, "Decentralized consensus for edge-centric Internet of Things: A review, taxonomy, and research issues," *IEEE Access*, vol. 6, pp. 1513–1524, 2018.

[17] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 33–39, Aug. 2018.

[18] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: A distributed and trusted authentication system," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 1972–1983, Mar. 2020.

[19] A. Stanciu, "Blockchain based distributed control system for edge computing," in *Proc. 21st Int. Conf. Control Syst. Comput. Sci. (CSCS)*, May 2017, pp. 667–671.

[20] D. Long, Q. Wu, Q. Fan, P. Fan, Z. Li, and J. Fan, "A power allocation scheme for MIMO-NOMA and D2D vehicular edge computing based on decentralized DRL," *Sensors*, vol. 23, no. 7, p. 3449, Mar. 2023.

[21] R. Akkaoui, X. Hei, and W. Cheng, "EdgeMediChain: A hybrid edge blockchain-based framework for health data exchange," *IEEE Access*, vol. 8, pp. 113467–113486, 2020.

[22] E. Bonnah and J. Shiguang, "DecChain: A decentralized security approach in edge computing based on blockchain," *Future Gener. Comput. Syst.*, vol. 113, pp. 363–379, Dec. 2020.

[23] I.-H. Chuang, S.-H. Huang, W.-C. Chao, J.-S. Tsai, and Y.-H. Kuo, "TIDES: A trust-aware IoT data economic system with blockchain-enabled multi-access edge computing," *IEEE Access*, vol. 8, pp. 85839–85855, 2020.

[24] L. Cui, Z. Chen, S. Yang, Z. Ming, Q. Li, Y. Zhou, S. Chen, and Q. Lu, "A blockchain-based containerized edge computing platform for the Internet of Vehicles," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2395–2408, Feb. 2021.

[25] X. Wang, C. Qiu, X. Ren, Z. Xiong, and V. Leung, *Overview of Edge Intelligence and Blockchain. In Integrating Edge Intelligence and Blockchain: What, Why, and How*. Cham, Switzerland: Springer, 2020, pp. 9–31.

[26] Z. Shahbazi and Y.-C. Byun, "Improving transactional data system based on an edge computing–blockchain–machine learning integrated framework," *Processes*, vol. 9, no. 1, p. 92, Jan. 2021.

[27] X. Qiu, L. Liu, W. Chen, Z. Hong, and Z. Zheng, "Online deep reinforcement learning for computation offloading in blockchain-empowered mobile edge computing," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 8050–8062, Aug. 2019.

[28] R. Wang, W.-T. Tsai, J. He, C. Liu, Q. Li, and E. Deng, "A video surveillance system based on permissioned blockchains and edge computing," in *Proc. IEEE Int. Conf. Big Data Smart Comput. (BigComp)*, Feb. 2019, pp. 1–6.

[29] S. Asaithambi, L. Ravi, H. Kotb, A. H. Milyani, A. A. Azhari, S. Nallusamy, V. Varadarajan, and S. Vairavasundaram, "An energy-efficient and blockchain-integrated software defined network for the industrial Internet of Things," *Sensors*, vol. 22, no. 20, p. 7917, Oct. 2022.

[30] H. H. Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Multi-layer blockchain-based security architecture for Internet of Things," *Sensors*, vol. 21, no. 3, p. 772, Jan. 2021.

[31] J. C. Ú. Ortega, J. Rodríguez-Molina, M. Martínez-Núñez, and J. Garbajosa, "A proposal for decentralized and secured data collection from unmanned aerial vehicles in livestock monitoring with blockchain and IPFS," *Appl. Sci.*, vol. 13, no. 1, p. 471, Dec. 2022.

[32] Y. Ren, F. Zhu, J. Qi, J. Wang, and A. K. Sangaiah, "Identity management and access control based on blockchain under edge computing for the industrial Internet of Things," *Appl. Sci.*, vol. 9, no. 10, p. 2058, May 2019.

[33] H. N. Abishu, A. M. Seid, Y. H. Yacob, T. Ayall, G. Sun, and G. Liu, "Consensus mechanism for blockchain-enabled vehicle-to-vehicle energy trading in the Internet of electric vehicles," *IEEE Trans. Veh. Technol.*, vol. 71, no. 1, pp. 946–960, Jan. 2022.

[34] M. Tang, L. Gao, and J. Huang, "Communication, computation, and caching resource sharing for the Internet of Things," *IEEE Commun. Mag.*, vol. 58, no. 4, pp. 75–80, Apr. 2020.

[35] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city," *IEEE Access*, vol. 7, pp. 18611–18621, 2019.

[36] Y. Huang, J. Zhang, J. Duan, B. Xiao, F. Ye, and Y. Yang, "Resource allocation and consensus of blockchains in pervasive edge computing environments," *IEEE Trans. Mobile Comput.*, vol. 21, no. 9, pp. 3298–3311, Sep. 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 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. She is currently associated with the School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India. Her research interests include cybersecurity, blockchain, network security, the IoT, and cloud computing.

SUBRAMANIYASWAMY VAIRAVASUNDARAM received the Ph.D. degree from Anna University, in 2013, and continued the extension work with the Department of Science and Technology Support, as a Young Scientist award holder. He is currently a Professor with the School of Computing, SASTRA Deemed University, Thanjavur, India. With the experience of more than 18 years, as an Academician and a Researcher, he has contributed more than 200 articles and chapters for many high-quality technology journals and books that are being edited by internationally acclaimed professors and professionals. He is a Research Supervisor and successfully guided five research scholars, and he is also a Visiting Expert to various universities in India and Abroad. His technical competencies lie in recommender systems, the Internet of Things, artificial intelligence, machine learning, and big data analytics. He has received government funded and consultancy projects from DST-SERB, ICSSR–IMPRESS, MHRD, TVS MOTORS, MHI, and SERB–MATRICS. He is on the reviewer board of several international journals and has been a program committee member for several international/national conferences and workshops. He serves as the guest editor for various special issues of reputed international journals.

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.

KETAN KOTECHA is currently an Administrator and a Teacher with the Symbiosis Centre for Applied Artificial Intelligence, Symbiosis International (Deemed University), Pune, India. He has expertise and experience in cutting-edge research and projects in A.I. and deep learning for the last 25 years. He has published more than 200 articles widely in several excellent peer-reviewed journals on various topics ranging from cutting edge A.I., education policies, teaching-learning practices, and A.I. for all. He has published three patents and delivered keynote speeches at various national and international forums, including the Machine Intelligence Laboratory, USA; IIT Bombay under the World Bank Project; the International Indian Science Festival organized by the Department of Science and Technology, Government of India, and many more. His research interests include artificial intelligence, computer algorithms, machine learning, and deep learning. He was a recipient of the two SPARC projects worth INR 166 lakhs from MHRD Government of India in A.I. in collaboration with Arizona State University, USA, and The University of Queensland, Australia. He was a recipient of numerous prestigious awards, such as the Erasmus+ Faculty Mobility Grant to Poland, the DUO-India Professors Fellowship for research in responsible A.I. in collaboration with Brunel University, U.K., the LEAP Grant at Cambridge University, U.K., the UKIERI Grant with Aston University, U.K., and the Grant from the Royal Academy of Engineering, U.K., under Newton Bhabha Fund. He is an Associate Editor of IEEE Access.

AJITH ABRAHAM (Senior Member, IEEE) received the B.Tech. degree in electrical and electronic engineering from University of Calicut, in 1990, the M.Sc. degree from Nanyang Technological University, Singapore, in 1998, and the Ph.D. degree in computer science from Monash University, Melbourne, Australia, in 2001. He is currently the Pro-Vice Chancellor of Bennett University, New Delhi, responsible for the University's Research and International Academic Affairs. Prior to this, he was the Dean of the Faculty of Computing and Mathematical Sciences, FLAME University, Pune, and the Founding Director of Machine Intelligence Research Labs (MIR Labs), USA, a not-for-profit scientific network for innovation and research excellence connecting industry and academia. He held two International University Professorial appointments: a Professor of artificial intelligence with Innopolis University, Russia, and was the Yayasan Tun Ismail Mohamed Ali Professorial Chair of the Artificial Intelligence, UCSI, Malaysia. He works in a multi-disciplinary environment, and he has authored/coauthored more than 1,400 research publications out of which there are more than 100 books covering various aspects of computer science. One of his books was translated to Japanese and a few other articles were translated to Russian and Chinese. He has more than 53,000 academic citations (H-index of 108+ as per Google scholar). He has given more than 150 plenary lectures and conference tutorials (in more than 20 countries). He was the Chair of the IEEE Systems Man and Cybernetics Society Technical Committee on Soft Computing (which has over 200 members), from 2008 to 2021, and served as a Distinguished Lecturer for the IEEE Computer Society Representing Europe, from 2011 to 2013. He was the Editor-in-Chief of *Engineering Applications of Artificial Intelligence* (EAAI), from 2016 to 2021, and serves/served on the editorial board of over 15 international journals indexed by Thomson ISI.