Journal of Scientific & Industrial Research
Vol. 82, January 2023, pp. 50-62
DOI: 10.56042/jsir.v82i1.69929

# An Integrated Secure Scalable Blockchain Framework for IoT Communications

G Chandra Sekhar[1]* & R Aruna[2]

[1]Vel Tech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Chennai 600 062, Tamil Nadu, India
[2]Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Chennai 600 062, Tamilnadu, India

*Received 10 June 2022; revised 24 September 2022; accepted 06 October 2022*

The Internet of Things (IoT) has shown great promise in the years since its invention and widespread acceptance by demonstrating its ability to adapt and improve manual processes while bringing them into the digital age. IoT's capacity to do so has elevated it to the ranks of the most promising technologies of our time. Despite the fact that IPv4 and IPv6 are being utilized to serve a growing number of devices in IoT connectivity, there are still issues with address space allocation and other security concerns, including scalability and poor access control methods. It is necessary to go through these difficulties and worries. Both of these organizations have spent a considerable amount of time in the vanguard of advancement in the study of IoT and Blockchain technology. Since IoT devices are capable of efficient two-way communication, integrating Blockchain technology is challenging. However, scalability is the biggest obstacle. The IoT Blockchain Framework discussed in the research article has the potential to be a game-changing solution to the issues that IoTs currently face, provided that it is used properly. Data access control and data interchange, transparency, and scalability without compromising privacy or dependability are all issues with the IoT paradigm that Blockchain technology may be able to efficiently address. Creating a local index that is scalable and does not interfere with either the local or global peer validation procedures is one way to limit the number of transactions that contact the global Blockchain. According to the findings, the blocks are significantly lighter and smaller than those seen in other parts of the world.

**Keywords:** Internet of things, Large scale IoT framework, Lpeer, Scalability

## Introduction

Depending on the circumstances, the Internet of Things (IoT) can serve a variety of functions in a variety of contexts. A few examples of items include medical equipment, nuclear power plants, and straightforward sensors for use around the house. The Internet of Things, often known as IoT, is an architecture for a dynamic global network that is built on open and interoperable communication protocols (IoT). According to Xu *et al.*[1] a straightforward internet-enabled communication architecture ought to be developed from a network of embedded sensors that are connected to the internet. Prior to the introduction of smart contracts, Blockchain technology was mostly seen as a tool for managing databases or transferring information.[2] However, this perception has been completely upended. Distributed systems get an additional boost from smart contracts, which are programmers that may run without human intervention and are stored on Blockchains. This topic has piqued the interest of a significant number of companies and developers working in the IoT sector.

Many IoT applications have been developed, including smart healthcare[3,4] smart agriculture [4,5], smart housing[5,6] wearables[6,7] augmented reality[8,9] and transportation[9,10]. The IoT is made up of Internet protocols and sensor networks, which make it possible for machines and other inanimate objects to talk to each other. Data protection is an essential component of any communication; centralized communication systems and client-server communication both carry the risk of exposing sensitive information to unauthorized parties. The disadvantageous tendency of the centralized computing model is that it tends to favor a large number of decentralized data centers, which causes a major demand on the processing, storage, and networking resources. Because of this, employing the conventional centralized communication models for activities like data-based communications, storage, and exploration that include billions of devices is practically unfeasible. With more embedded devices and networks that connect to the IoT, privacy and safety are now major concerns. Developing a secure

*Author for Correspondence
E-mail: sekhar.gillala@gmail.com

IoT framework includes various issues, summarized as follows:

**Scalability:** An Internet of Things system allows a large number of sensors, actuators, and other devices to be connected with one another for the purpose of sharing information and running a variety of applications through the web. It makes it hard to design and build a system that can adapt to people's changing needs and environments. This is also called scalability and adaptability.

Heterogeneity and Resource Limitedness: Traditional security methods, approaches, and services are not always appropriate for IoT devices and communications networks because of the variety of these environments and the limited resources available. Also, because IoT devices have limited resources, it would be hard to use modern security strategies to protect them.

**Transparency:** Users should not be made aware of the complex features that may be hidden by a secure framework. The deployment must be completely silent and must be able to "plug and play." Both the IoT and Blockchain technologies have dominated their respective research domains for a considerable amount of time. The IoT enables the employment of automated systems in a variety of different businesses, while Blockchain technology enables the processing of safe transactions for assets. Integrating IoT devices with Blockchain technology is the natural next step to enable IoT devices to create transactions. The scalability of the ledger and the speed at which trades can be carried out on the Blockchain are the two primary problems that are linked with this integration. Because there are so many of them, IoT devices can execute transactions far more quickly than traditional Blockchain technology. Because of limited resource availability, integrating IoT devices with Blockchain peers might be a difficult process. It is not possible to directly include either of these technologies at this time due to the way in which they are deployed. Our research suggests a solution to these issues, which entails the formation of a peer-to-peer network in the immediate area. While peer approval of transactions is maintained at both the local and global levels, the network makes use of a local ledger to limit the number of transactions that are added to the global Blockchain.

The primary focus of this paper is on a framework for IoT devices as well as a Blockchain-based system in which all IoT devices are linked to an organization and are certified by a local Certificate Authority (CA).

In addition, rather than utilizing a worldwide Blockchain network, it intends to link to an anchor peer in the global network by utilizing a local peer, also known as a Lpeer. This system has two primary objectives: the first is to assist the global Blockchain network in increasing the speed of transaction processing; the second is to reduce the amount of ledger storage that is required at each peer. The design limits the size of the ledger and splits it up between Lpeer and the anchor peer through the use of an intraorganizational transaction. This is done while maintaining the consistency of the peer validation. Blockchain technology, which has 100% peer validation from an international peer network, can be used to check transactions between organizations.[11] This paper's primary contribution is the development of a novel framework for enabling Blockchain scalability in terms of ledger size and transaction rate. This framework is the focus of the development of an Integrated Secure Scalable IoT Blockchain for IoT transactions, which is the main contribution of this paper.

### Background and Related Works

To begin, we provide some background information regarding the sorts of Blockchains, the uses they have, and the problems they cause in IoT. Additionally, it emphasizes the research that is pertinent to the topic.

#### *Blockchain Types*

Based on the several applications and their needs, Blockchain can be classified into four types as summarized in Table 1.[(8)]

#### *Blockchain for IoT*

Both the IoT and Blockchain technology have risen to popularity since their respective inventions.

Table 1 — Blockchain classifications

| Types of Blockchain | Network type | Features |
|---|---|---|
| Public Blockchain | Permissionless | Open network; Free access; No permission; Shared ledger; Full transparency |
| Private Blockchain | Permissioned | Closed network; DLT authority; On permission; Shared ledger; Full transparency |
| Federated Blockchain | Pre-selected nodes | Organization; Group access; On permission; Shared ledger; Transparency |
| Hybrid Blockchain | Public & private | Organization; Mixed access; Restrictions; Mixed ledgers; Semi-transparent |

The IoT will eventually have an impact on virtually everything that we use on a daily basis. There is a rising potential for abuse as more people make use of this technology. The currently available technology is incapable of managing it. Therefore, Blockchain has shown itself to be an ideal answer to the difficulties posed by the IoT. The use of Blockchain technology is currently becoming increasingly widespread. It has the potential to optimize and modernize the worldwide technological infrastructure that is connected through the internet. It will have an effect on both of the following areas:

- This system is entirely decentralized, as it eliminates the need for central servers and delivers a peer-to-peer experience.
- It generates a transparent and completely open database, which improves governance and elections by creating openness.

This technique comprises four components.

**Consensus**: The consensus method ensures the networks are safeguarded with the verification of the transactions.

**Ledger**: Track every activity in the network.

**Cryptography**: Network and ledger data is encoded, and only authorized users can decrypt it.

**Smart-contract***:* This verifies and validates network participants, is employed.

The Blockchain-based IoT has three communication models i.e.,

- Peer-to-peer messaging
- Distributed data sharing
- Autonomous device coordination

***Constraints:*** Slow Processing and Limited Storage

In this paradigm, the nodes on a Blockchain function as members of the network. They might be home computers, servers used in businesses, or nodes located in the cloud. Clients are devices that are connected to the IoT. Through the use of Blockchain APIs, clients and nodes are able to connect with one another. Transactions are started by clients, and when they have been routed to nodes, they are processed, and the results are stored in the distributed ledger.

When it came to the privacy of IoT devices, the Sahinoglu *et al.*[10] came to the conclusion that decentralization and cryptography were the best solutions, provided that there were no problems with implementation or design. It has been determined that the most significant benefits of integrating Blockchain technology with the IoT are the maintenance of security and privacy, the management of information, data, and assets, and the use of lightweight cryptographic authentication. Some of the problems with putting Blockchain into the IoT are interoperability, different network topologies, compatibility, developments in quantum computing, user identity tracking, scalability, and communication overhead.

There is a projection that the IoT will connect more than 30 billion devices by the year 2020.[(11,12)] This number will dwarf the population of the world. Because there are so many gadgets, modern academics are under increasing pressure to develop management strategies that take into account all aspects of the IoT. In general, the IoT comprises three fundamental architectural levels, which may be broken down as follows: perception (the realm of sensing devices), networking (the domain of networking), and application (the domain of application) (Application domain). Depending on the layer of the IoT ecosystem they are targeting, threats and assaults might take either an aggressive or passive form. These assaults might have been launched from either an external source or the internal network. The creation of secure and scalable frameworks for IoT applications stood out as one of the most significant areas in which to concentrate efforts.

The concept of cryptocurrencies was central to the development of Blockchain technology, and that focus has not changed (e.g., Bitcoin, Ethereum, etc.). The goal of the Hyperledger[9] project is to add Blockchain technology to business networks that are already in place.

In the decentralized IoT access management system proposed in[13] information pertaining to access control is kept on the Blockchain (BC) and dispersed across the network in a decentralized method. A management hub gateway is used to establish a connection between the IoT and BC. If the IoT node doesn't have endorsement or a clear way to identify the system, it will get in touch with the BC node to ask for help. Use scenarios like this might make a permission system an absolute necessity for a query technique like this. Since the management node is not part of the Bitcoin Core network, it also has to collect transaction fees for millions of transactions every day. Accessible through the internet, a Lightweight and Scalable Blockchain (LSB) platform that functions as a hub and controls all incoming and outgoing transaction requests is provided by a centralized management known as a Block Manager (BM).[14] In addition to this, it saves a record of every transaction on the local computer. It does not clarify how local business management and overlay business management would collaborate in the process of transfers. Although the answers to the challenges with storage and scalability at a higher level have not yet been implemented, the text does not cover reducing the overhead size, storage, or management of the block's scalability. It shows how important it is to develop TPS as one of the things that need to be done.

However, there are just a handful of research studies that investigate the potential applications of Blockchain technology to the IoT.[15] This work provides a distributed Blockchain SDN architecture that has high performance availability flow-rule tables. The goal of the design is to provide support for the IoT.

The report suggests that smart contracts might be one method in which the application of Blockchain technology could assist with IoT connectivity. To increase the number of transactions per second satellite chains can be employed.[16] Mishra *et al.*[16] slock conducts an analysis of how to address problems of protection, identification, collaboration, and privacy without the need for a middleman by empowering millions of devices to act on their own. The B2ITS intelligent transportation system is not an IoT solution, despite the fact that it makes use of Blockchain technology.[17] Instead, it addresses a seven-layer computational architecture for large-scale vehicle networks. According to Zeng *et al.*[18] BC may also be used in transactions involving smart grids in order to maintain stability.[19] It has been proposed that Blockchain technology be used to ensure the safety of smart devices. An open technology stack known as Filament makes it possible for dispersed and autonomous devices to discover one another, communicate with one another, and interact with one another. Using Blockchain technology, which is made possible by Provenance, gives proof of existence and responsibility for things like supply chain management.[20,21]

It is recommended that the International Telecommunications Union take into consideration a proposal for a decentralized Blockchain of stuff system (ITU). Scalability, interoperability, and the use of a distributed ledger are just a few of the important needs that are being considered as part of this ongoing project. It is anticipated that many consensus mechanisms will be functional on the IoT network that Blockchain will power. The majority of the present research on the integration of IoT with Blockchain does not concentrate on improving the scalability or transaction rate of the ledger's speed. The development of an IoT network infrastructure that is scalable to support a high number of IoT devices is the primary objective of this project. This objective applies independently of the application situation.

## Methodology

### Scalable Blockchain for IoT: System Design

An IoT network with Blockchain integration is presented in Fig. 1. Notably, Blockchain is a novel technology with few real-world applications. The IoT Blockchain process comprises three phases: 1)

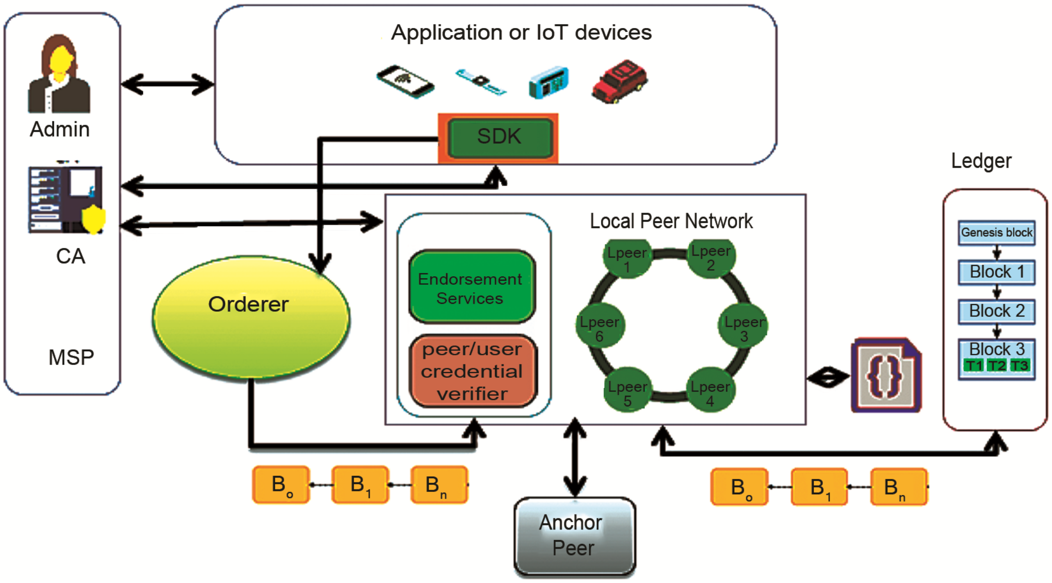

Fig. 1 — Proposed block diagram of the model

Application, 2) Local Peer network and 3) Blockchain network.

### Network Model

### Working Principle

The goal of the framework that has been developed is not to openly link IoT devices to one another. It is possible to place limitations on transactions between devices and BC peers by utilizing a third party as an intermediate agent. Additionally, it is vital for all IoT devices to be connected to a certain business. The organization that builds local networks keeps the transactions that take place in their networks distinct from those that the global Blockchain is obligated to carry out. Initialization, configuration, and deployment are the three stages of the Blockchain implementation in the IoT. The first is the phase of trade origination. Next comes the phase of verification and validation, and finally, there is the phase of commitment. The first connectivity of IoT devices to Blockchain nodes is depicted in diagram 2(b). These nodes serve the purposes of prospective endorsers. In addition, the system has a trustworthy Certification Authority (CA) that is also a major Membership Service Provider (MSP).

### Terminologies to Understand

***Device***: The proposed system uses the term "device" to refer to any IoT equipment that can generate or receive Blockchain trades (transactions). The internet is utilized by various devices, such as sensors and other gadgets, in this portion. The machines are controlled by either firmware or gateway programs. We think that any application will be built with a uniform Blockchain Software Development Kit (SDK) for communications also smart contracts.

***Peer or Node***: One of the core network's nodes is called a node. It's a machine that can process the consensus algorithm and keep a ledger.

All IoT devices have a Node to which they are connected, and this Node executes the transactions initiated by the device. To employ Blockchain, a company must have a peer somewhere in the global Blockchain network. Thus, this paper recommends implementing a Local Peer Network that incorporates a Certification Authority (CA) and a Local Peer (Lpeer). When applied at the enterprise level, the Lpeer network raises the Blockchain scalability of anchor peers and the transaction rate of peers.

***User***: A user in the proposed architecture is a person that is not human, and hence all users are, in fact, admins. In contrast to trading platforms that include human contact, IoT is entirely controlled by the machine and is not open to manipulation by a user. Because the administrator is a component of the architecture, as illustrated in Fig. 1, it's possible to initialize and manage the MSP.

***Blockchain Network***: Each peer administers its ledger and smart contracts in the global network of interconnected peers. Anchor peers serve as intermediaries in the communication between Lpeer and Peer.

### Local peer network: Design details

The Local Peer Network generates transactions and provides each device with a separate instance of itself. The anchor pier is a global member of the Blockchain network. The other portion of the image displays the entire local peernetwork. Network implementation of Lpeer occurs at the organisational level. Although specific gadgets can engage in D2D communication, they cannot do so unless they are attached to some company.

### CA server

The CA Server is a comprehensive certification authority that gives users a wide variety of choices regarding certification architecture. The design element is crucial since other users on the network are unable to offer certificates, signatures, or keys. Additionally, it is able to give registration certificates for both administrators and users. Every application has to establish a connection to the CA in order to get the necessary keys and signatures for encryption. In addition to this, it provides TLS-secured connections between all of the components of the Blockchain, as well as credential validation, signature creation, and verification.

### Local peer (Lpeer)

A peer network is the foundation upon which a Blockchain network is constructed (or, simply, peers). Peer nodes' ability to store ledgers and smart contracts is essential to the functioning of the network. Keep in mind that a ledger stores all of the transactions related to smart contracts indefinitely. In a network, it is easier to keep track of shared information and operations with the use of ledgers and smart contracts. Fabric networks require a variety of different components, including, but not limited to, ledgers, smart contracts, ordering services, policies, channels, applications, organisations, and memberships. Each of these parts focuses on the connections between peers that are part of the Fabric network.

As may be seen From Fig. 2(a), A Blockchain network has three types of participants:

- Peers (peers 1, 2, and 3 in the diagram).
- Ledger (who maintain their copy of the Blockchain).
- Smart Contract (which support the complete Blockchain and disseminate it to the other nodes).

P1, P2, and P3 all have the same copy of S1, and they all use it to access their own individual copies of the distributed ledger. It is possible to create peers, start them, end them, reconfigure them, or delete them. They provide a collection of application programming interfaces (APIs) that enable administrators and apps to interact with the services that they provide. A ledger and its accompanying chain code are both hosted on a peer. The LP1 instance has a ledger named L1 and a chain code named S1 shows in above Fig. 2(a). A number of different ledgers and Blockchains can be hosted by local peers.

### Multiple Ledgers

As shown in Fig. 2(b), a peer is able to retain more than one ledger, which helps to ease the development of a system architecture that is very adaptable. A peer is able to keep track of a single ledger, but if required, they should also be prepared to deal with two or more ledgers.

A peer that hosts a number of different ledgers. Each ledger in the system is hosted by one or more peers, and each ledger is associated with a number of chain codes that can range from zero to several. As is clear from the above example, P1 acts as the host for the ledgers L1 and L2, as shown here. To gain access to the ledger L1, you will need the chain code S1. To gain access to Ledger L2, you will need the Chain Codes S1 and S2.

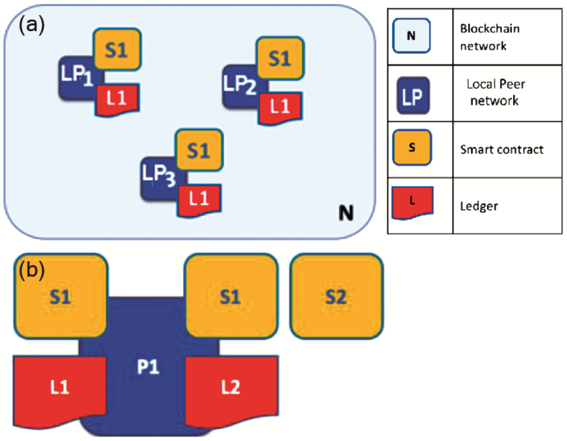

Fig. 2(a-b) — a); Blockchain network elements & b) Multiple ledgers with peer hosting

***Local Peer***: An IoT solution for Local Peer organisations is the Local Peer. It's our idea to break down a single local peer into many smaller ones. Using many instances of Lpeer0 dispersed across various geographical regions may help eliminate a single point of failure. This feature is useful for applications that need consensus on local transactions among a large number of different peering peers. Some ledgers are kept, while others are discarded by secondary Lpeers. Only one device, lpeer0, needs to be found. Users, credentials, and smart contracts are all continually updated in the database. Lpeer0 is the sole member of the ledger who has authorization to read and write blocks. Through interactions with other organisations' anchors, it also addresses inter-organizational issues.

### Ordered & Ordering Services

The organising service is performed at the request of the customer and may include interactions with a number of lepers (if any). It is the responsibility of the ordered, upon receipt of transactions from a variety of applications and/or devices, to incorporate those transactions into a block in the manner specified by the batch instructions. It is where CA certificates and signatures are kept in their entirety. Any user can validate their own transactions by using the ordered, and it will use its certificates and signature to do so. When referring to a "provider who buys resources and then provides them to other miners," the phrase "orderer" should be taken as meaning "a buyer." Participants in the order are responsible for carrying out transactions and generating blocks as part of their duties. In general, miners are the ones who are tasked with certifying bitcoin Blockchains through the use of proof-of-work consensus mechanisms.

***Ledger***: The use of unique serialisation helps to prevent tampering while also keeping track of every transaction. The signing of transactions is the consequence of transactions generated by chaincode invocations given by all parties involved in the company. Ledger is in the same namespace with Lpeer0, who has read/write access to it.

A secondary peer can use the Blockchain to retain a backup copy, which is only used if Lpeer0 goes down. Both Lpeer and BC employ a state database to record the results of every transaction.

***SDK***: Blockchain SDK streamlines the transaction process by using the user's cryptographic credentials. Various applications use the SDK to gather data and transaction information, which is then centralized stored.

***Smart Contract***: A digital agreement between two devices establishes the terms and circumstances of a transaction. The chaincode that implements it is based on asset and business model descriptions. This project utilizes smart contracts as they're defined for international Blockchain networks.[22]

The entire Blockchain process in IoT consists of three phases: a) trade origination, b) verification and validation, and c). Committing phase.

***Phase 1: Trade Origination Phase***

This is the phase where trade proposal preparation and trade proposal execution were discussed.

*i.* *Proposal Preparation:* This section gathers all IoT data and utilises it to generate a business proposal. The SDK formats the data before sending it to chaincode for processing. Trade data, device signatures, destination public addresses, and matching certificates are all included in the payload of the trade agreement packet in Fig. 3.

*ii.* This app talks with CA to produce enrolment certificates (eCert) for users to use after they have joined the Blockchain network of peers.[23]

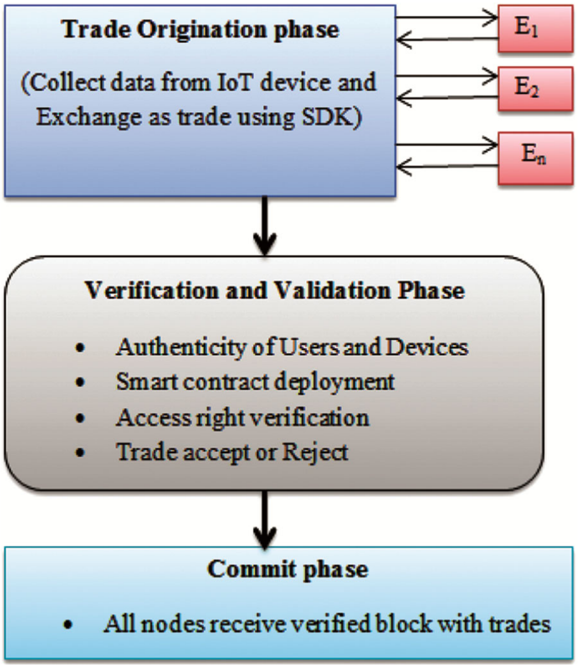
Trade Origination phase
(Collect data from IoT device and Exchange as trade using SDK)
E1
E2
En
Verification and Validation Phase
Authenticity of Users and Devices
Smart contract deployment
Access right verification
Trade accept or Reject
Commit phase
All nodes receive verified block with trades

Fig. 3 — Stages of the IoT Blockchain operational process.

*iii.* The Certificate Authority (CA) issued certificate shows in Fig. 1. Admin approval is required for both Chain code and IoT device installation. This system takes care of administrators, hardware, nodes, and applications all at once.

*iv.* *Proposal Execution:* Each device is accompanied with a business proposition, which is then processed via the channel. A channel is a logical communication tunnel that connects each node and application. Devices without a channel cannot perform transactions since they are channel-specific. Channel setup and maintenance are the responsibilities of the MSP. Nodes are often used to connect IoT devices to prevent them from spending twice in the same blocking session, however they can only do one transaction at a time.[24]

***Phase 2: Verification & Authentication Phase***: The organising service is performed at the request of the customer and may include interactions with a number of lepers (if any). It is the responsibility of the orderer, upon receipt of transactions from a variety of applications and/or devices, to incorporate those transactions into a block in the manner specified by the batch instructions. It is where CA certificates and signatures are kept in their entirety. Any user can validate their own transactions by using the orderer, and it will use its certificates and signature to do so. When referring to a "provider who buys resources and then provides them to other miners," the phrase "orderer" should be taken as meaning "a buyer." Participants in the order are responsible for carrying out transactions and generating blocks as part of their duties. In general, miners are the ones who are tasked with certifying bitcoin Blockchains through the use of proof-of-work consensus mechanisms.

***i. User and Device Authenticity***

Nodes and devices are the two different types of participants that might take part. Since the network was first set up, the administrator has verified their identities using eCert, sign, keys, TLSert, and CAcert. When applications use an admin object to register new nodes or devices, the applications have access to the appropriate eCert. In a similar fashion, the application communicates with the CA and LPEER0 in order to enrol additional nodes.

The Certification Authority generates a variety of certificates (such as TLS CA, eCert, and so on) and hands them over to the device. During the verification process, Lpeer0 stores the information obtained from devices (such as TLS, CA certificates, and signatures) so that it may be used at a later time. By limiting who can connect to the network, this method helps to make sure that only authorised IoT devices can join the local Blockchain network. As a component of the worldwide Blockchain network, the IoT gadget may be used to map and find individuals. LPeer0 is responsible for registering devices with the anchor peer. The registration of devices is handled by the first algorithm. Who is allowed to add blocks and who may raise questions? Because of this, new users and devices won't be able to connect to the network until they have been properly identified.

***IoT Device Registration***: The registration of both IoT device necessity be done through CA and Lpeer0 (as illustrated in Fig. 4) to be part of the system.

Step 1: First, devices should register with CA:

Step 2: CA will create encryption keys and device-specific signatures. TLS CA, eCert, and other certificates, as well as public-private key pairs issued and delivered to the device, must all be developed and certified by the CA.

Step 3: Once the IoT device has registered with the CA, it utilises Lpeer0 to verify the identity of the person making the request. During the verification process, Lpeer0 keeps track of all connected device user credentials (such as TLS, CA certificates, and signatures).

Note: It is essential to have a solid understanding that this strategy only enables IoT devices to join the local Blockchain network if they have been given permission to do so. As a component of the worldwide Blockchain network, the IoT gadget may be used to map and find individuals. LPeer0 is responsible for registering devices with the anchor peer. The Blockchain serves as the foundation for the IoT architecture that is managed by Algorithm-1.

***Algorithm-1 Device registration***

```
Input: DeviceID'seg:$d_1$, $d_2$
Output: $Peer_{id}$, $Device_{id}$
Step 1: Assign: $Device_{id}$- -> $d_{i,}$ $Peer_{id}$- - >$Lpeer^0$
Request sign & certificates of $d_i$- -> CA
If $d_i$ (sign & certificates)
then
$d_i$- ->$Lpeer^0$ (sign($d_i$ ), $d_i$ )
If
$Lpeer^0$ (sign($d_i$ ),then
Comment:
Device $d_i$; registered with Lpeer
return Peer $_{id}$: $Device_{id}$= $Lpeer^0$: $d_i$
else
$d_i$ sign or certificates is not valid
end
else
Request Cancel
end
```

***Smart Contract Deployment***: An administrator will install and activate the Chain Code software on a node. The instantiation policy will be applied by declaring the name and version of the smart contract. The process for the installation and instantiation of chain code in Hyperledger is the same as the workflow for a conventional invocation. This implies that the endorsement, validation, and commit activities take

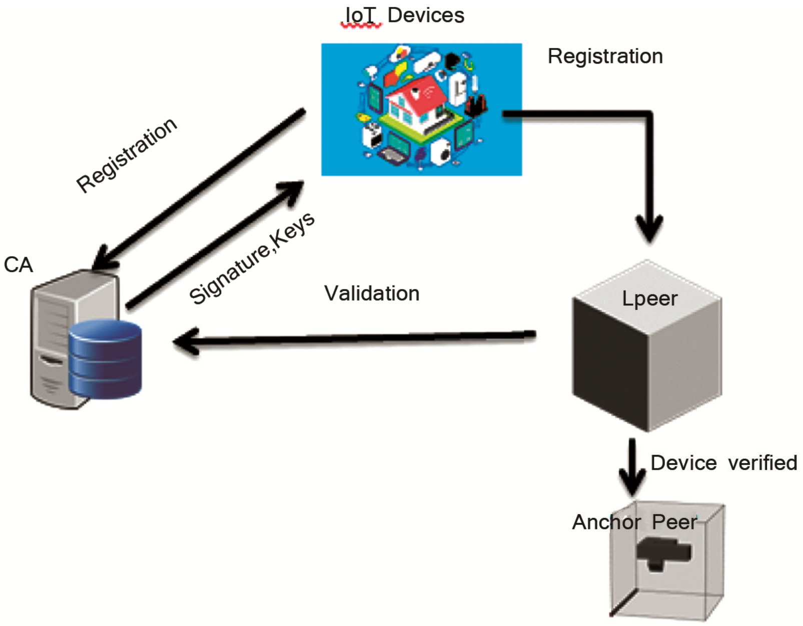

Fig. 4 — IoT devices registration process

place in the order that they were listed. However, installation results in alterations, which in turn pose a significant security risk because the capability to confirm transactions is dependent on the smart contract. Chain code plays an essential role in the overall process because it is responsible for the administration of several commercial regulations. The trade execution rules between the devices are, to a large extent, put into practise by these regulations, which are part of the agreements that were formed between the participating devices. Our method stipulates that the decision-making process for every modification to the smart contract follows the exact same format as that for a single trade. At least 51% of the nodes have expressed their approval for the contract amendment.

***User Account Validation:***

The smart contract script will then define the access privileges based on the channel used. You may only talk to other devices using a channel that uses the MSP credentials you generated. Because the admin assigns the channel, it's impossible to reach any nodes or devices that aren't already linked. To determine if the transaction came from a genuine user, Lpeer0 validates each transaction it receives. The process of verifying the devices is handled by Algorithm 2 if they are registered.

***Algorithm 2: Device Verification***

```
Input: Requested ($Peer_{id}, d_{id}$)
Output: Approved or Denied
Step 1: if ($(Peer_{id}.d_{id}) = Lpeer$
then
if sign ($Lpeer_{admin}$)and sign($d_i$ ) is verified
then
return Approved
else
return denied
end
else
return denied
end
```

***Acceptance or Rejection***

The customer gets simultaneous trades by several nodes also creates a new block attached towards the register.

***Phase 3: Commit Phase***

Everything comes to an end here. All nodes in the network may get a block when the consensus PoBT is completed, which they may add in their own PoBT books.

***Block Distribution:*** The orderer won't consent to the new block being added to the Blockchain until the PoBT algorithm has validated it as valid, at which point it will be broadcast to all of the network nodes along with the orderer's signature. Each node adds the block to its repository after verifying the signature of the block.

**Structure of transaction and processing:**

It examines each transaction that Lpeer0 receives in order to ascertain whether or not the trade was carried out by a genuine user. In the event that the devices have been registered, the Algorithm 2 will handle the verification process on your behalf. Together with the sender's device and the device of the receiver, as well as the private and public keys that were specified in the message, a message was successfully transferred. The same is true for the transaction proposal, which identifies the private keys of the peers, the public key of the user, and the administrator of the connected device in the peer. Additionally, it also identifies the public key of the user. In the event that a transaction proposal is sent, the peer will validate it and decode it using a private key in the event that it was communicated.[25] In addition to verifying all of the certificates that were previously stored, after decryption it checks the signatures of both the administrator and the device. After it has been established that all of the verification results are satisfactory, it will send a favorable answer to the applicant that initiated the verification process.

**Trade Processes and the Ledger's Scalability:**

The Local Blockchain is designed to disseminate blocks to each and every node that is part of the network. The whole of the network's transactions is included within the blocks that are then distributed. Because of this, the amount of memory that is necessary for the ledger will increase in a manner that is proportional to the number of nodes that are now operational. Memory needs are governed by a variety of distinct factors, including the kind of transactions, the storage policy, the data that is contained inside transactions, and the number of times blocks are produced. According to the information that is displayed in this image, the quantity of memory that is required to store committed blocks sees a significant increase as the size of the network increases. Because the amount of data that is transferred may vary from one IoT application to the next, the amount of RAM that is required may range anywhere from hundreds of terabytes to hundreds of petabytes. In other words, the amount of RAM that is required may be anywhere in the range of hundreds of thousands of gigabytes (e.g., 10 KB trades compared to 5 KB trades). There's a chance that adding more nodes will make the network safer, but the extra memory that will be needed to store transactions might make it harder to use.

Let us represent the size of trade-in terms $Tr_w$ and the weight of the block header $B_w$ and trades per block Tr. The ledger weight measures how much weight a ledger is $Ld_w$ (in bytes) motivation growth for a particular amount of time following Eq. (1), where i =1,2, 3,…The symbol n represents the number of blocks in a certain time series.

$$Ld_w = \sum_{i=1}^{n} \sum_{j=1}^{\bar{T}r} Tr_w^j + B_w^i \quad \dots (1)$$

If the average transaction acceptance rate per second is, as previously stated, $Tr_r$ As a result, the ledger increase rate per second becomes

$$Ld_{w/s} = (Tr_w + \frac{B_w}{Tr_n}) \times Tr \quad \dots (2)$$

## Results and Discussion

Each transaction represents a block, as we learned from the experimental evaluation of Hyperledger Fabric which approximately is 5 - 10 KB, and blocks are produced at a pace of 500 trades per each block of 4.5 KB. Based on Eq. (1) we can estimate a ledger growth rate of 50–100 KB/sec. If you have hundreds of IoT nodes, this one won't do you much good. The solution to this problem is to split up the transactions amongst different nodes and different gadgets. Trade execution is determined by $N_{sd}$ during the trade creation step. The process of confirming local trade and creating blocks are depicts in Fig. 5. The $N_{sd}$ represents the node closest to the user, while Ni € represents a non-selected node.

All through the set-up procedure, we tested our idea using Hyperledger Fabric (v1.0.2). In this study, we'll use two distinct devices, each of which will

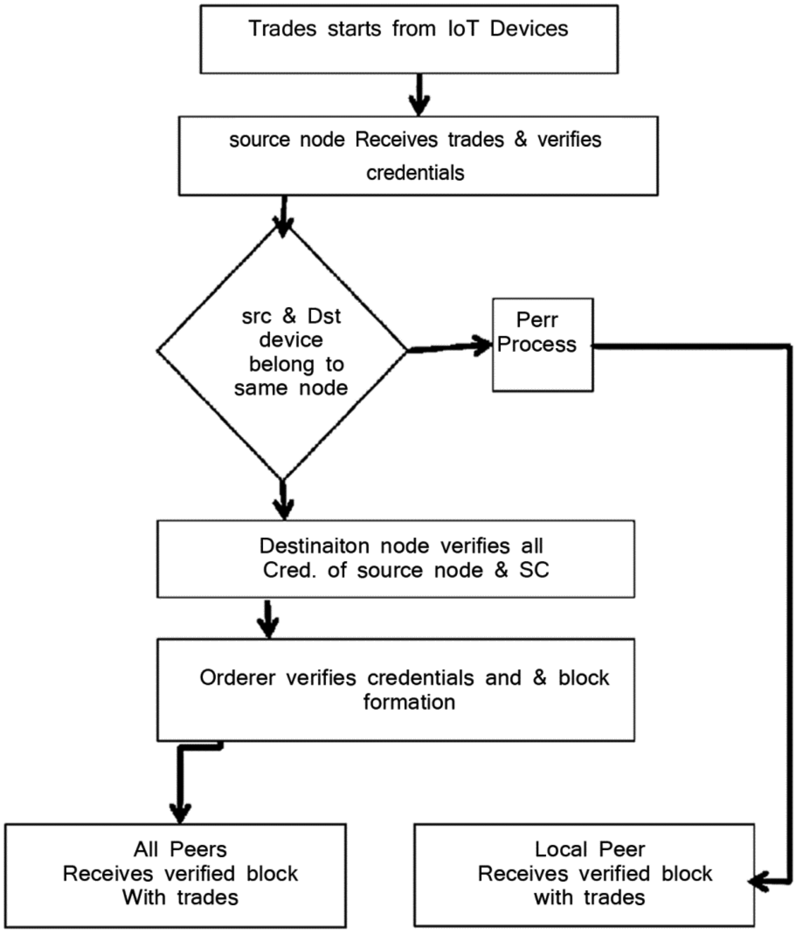
Trades starts from IoT Devices
source node Receives trades & verifies credentials
src & Dst device belong to same node
Perr Process
Destinaiton node verifies all Cred. of source node & SC
Orderer verifies credentials and & block formation
All Peers Receives verified block With trades
Local Peer Receives verified block with trades

Fig. 5 — Flow model

simulate a certain set of characteristics: The Lpeer Network takes cues from the first example, while the global Blockchain looks to the second as an inspiration. Ubuntu-based container virtualization was employed to power the peers.[1] This research aims to discover how the scalability of Blockchain technology might boost the IoT's efficiency in its operational processes. The size of the ledger can be reduced and the processing of financial transactions can be sped up by having fewer peers engage in transactions and by enhancing the rate at which transactions are processed. The reader to keep in mind that both Blockchain and the IoT are in a constant state of development and the process is shown in Fig. 6. The rapid evolution in the architectures of the many available platforms will have an impact on the assessments. In the present day, a Blockchain for the IoT can process ten transactions per second.[26]

$N_{sd}$ will ask the orderer to select a random node Ni to cross-validate the trades after it has determined that the source DS and destination Dd IoT devices are related. The only way to get everyone on the same page is via this method. This method of random selection guarantees that each node is distinct and prevents a negotiated $N_{sd}$ from selecting a preferred validator. After the transaction has been validated, the orderer Ni receives it, preventing a compromised $N_{sd}$ from bypassing the check. The legitimacy of the signatories on an order must be verified before processing may begin. The memory of other nodes is not tapped for these deals. By doing so, the memories of other nodes are spared from the exchange.

The ordering system may give any node's requested block ID with correct authorization by keeping a list of local and global transaction IDs internally. To attain these three fundamental features, the method requires verification/consensus, communication, and computing which improves the Scalability of the ledger. Calculation of Computing Time: The length of time necessary to validate numerous nodes has an effect on the transaction throughput of the system as well as its overall dependability. The time required to validate a trade between two nodes is the first thing that will be measured by the proposed system. After that, it verifies the transaction with the Ns while the consensus is being built. The total amount of time spent on computing, which is denoted by Tb, can be found by:

$$T_b = \sum_{i=1}^{\bar{T}_r} T_r^i(t) + \sum_{i=1}^{\frac{N_s}{2}+1} N_s^i(t) \qquad \dots (3)$$

$T_r^i(t)$ It is time for a single trade, and $N_s^i(t)$ It's time for consensus verification by Ns. Likewise, the computation time for Hyperledger fabric $T_b^{Fab}$ Can be used to compute

$$T_b^{Fab} = \prod_{j=1}^{\bar{T}_r} \sum_{i=1}^{Ns} N_s^i(t) \qquad \dots (4)$$

Because it uses a different implementation for getting trade and endorsing node information than existing state-of-the-art Fabric solutions Eq. (3), the suggested technique takes less time to verify Eq. (3) and Eq. (4).

Whenever a session comes to an end, a batch of transactions is sent out to all of the nodes in the network. To put it another way, the memory requirements of the ledger rise according to the size of the network. Memory use during a transaction can be affected by a number of factors, including the storage policy, the kind of transaction being performed, and the rate at which new blocks are produced and it is demonstrated Fig. 7 that the number of committed blocks that must be stored with a 10-node network. It

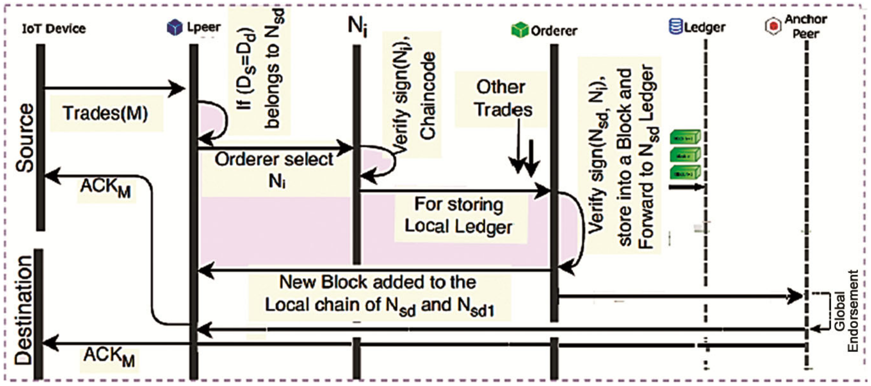
IoT Device
Lpeer
$N_i$
Orderer
Ledger
Anchor Peer
Source
Destination
Trades(M)
If ($D_S$=$D_d$) belongs to $N_{sd}$
Orderer select $N_i$
Verify sign($N_i$), Chaincode
Other Trades
For storing Local Ledger
Verify sign($N_{sd}$, $N_i$), store into a Block and Forward to $N_{sd}$ Ledger
$ACK_M$
New Block added to the Local chain of $N_{sd}$ and $N_{sd1}$
$ACK_M$
Global Endorsement

Fig. 6 — Sequence structure

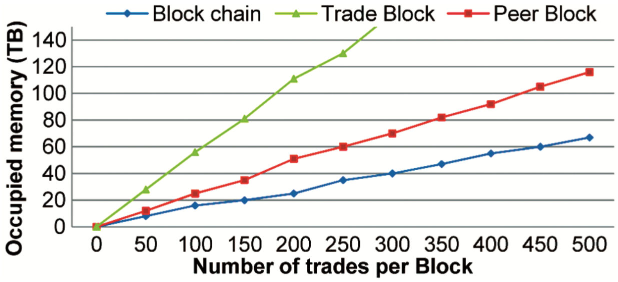

Fig. 7 — Ledger memory scalability

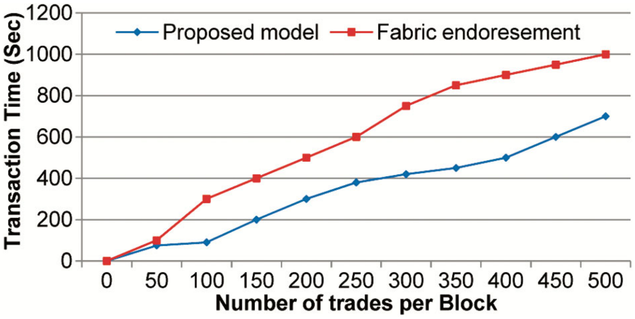

Fig. 8 — Fixed numbers of nodes

requires significantly more storage space for the committed blocks because of the huge rise in the number of blocks that must be saved. Because various IoT applications deal with transactions of varying sizes, the amount of RAM required to store such transactions might reach several hundred terabytes (e.g. 10 KB trades compared to 5 KB trades). However, keep in mind that the memory required to retain these trades might be an issue owing to the size and capabilities of the nodes. This could be a concern because more nodes mean more validating nodes, which suggests better security.

From the comparison of the above result, analysisisessential with the Hyperledger material for the calculation time (from the validation of trade to the closing of blocks). The system's overall number of nodes is 10, while transactions per block are 1 to 500. The results in the necessary time compared to the growing number of trades per block are presented in Fig. 8. The scale is logarithmic; it should be noted. If there are 100 competitor trades, it may be seen that approval is required for ~200 ms, although our suggested model entails ~80 ms.

Similarly, the time needed for endorsement is 500 trades per ~1000 ms. Whereas the proposed model necessitates ~590 ms, which is half the value of Fabric. The endorsement time increases in direct proportion to the volume of transactions. The proposed model, on the other hand, takes a lot less time to compute than Fabric. The time required to complete a trade under two dissimilar adjustable conditions is illustrated in Fig. 9. The X-axis indicates the number of employments per block (which can range between 5 and 250) and the number of agreement participants associated with each trade (ranging from 2 to 50). This is critical since the number of endorsers has a direct effect on the system's performance.[2] In the first instance, the time required to execute five deals with two endorsers for every session is ~4 ms and ~3.6 ms which are nearly equivalent. However, when the number of endorsers per every session is 20 and the number of trades is 100, the time required for endorsements grows significantly is ~189 ms, for Fabric, the proposed model requires only ~85 ms. When nodes are 50 for 250 transactions, the endorsement time is approximate. But from the preceding study, it is clear that the suggested work outperforms the competition in terms of the time necessary to execute the trade. As a result, the proposed method scales better as the number of trades and participating nodes increases.

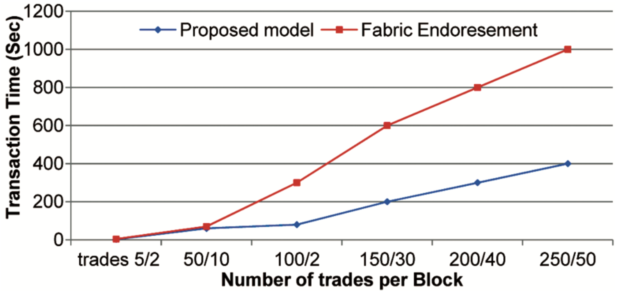

Fig. 9 — Variable numbers of nodes and trades

## Conclusions

Scalable, secure Blockchain technologies will be needed for the IoT. A block must be approved by the majority of its peers before being built. Massive networks take longer to understand. Hyperledger, a commercial Blockchain solution, reduces network peers and limits verification to transactions, solving this problem. A secure transaction-based communication system built on Blockchain technology may soon be possible. This study found that Blockchain technology and the IoT are incompatible and the model emphasizes on establishment of peer networks at the neighborhood level. The simulation affects TPS and ledger weight both positively and negatively. This allows the IoT to handle more commercial transactions without needing more memory.

It will be an exciting direction based on the outcomes of the experimental inquiry, whether to have a uniform transaction structure that is optimized for various types of business chains or specialized structures but with interoperability among multiple chains. Regardless of which option is chosen, it will be a direction that will be exciting. In either case, the path that is taken will be one that is defined by the findings of the investigation.

## References

1 Xu R, Chen Y, Li X & Blasch E, A secure dynamic edge resource federation architecture for cross-domain IoT systems, *Int Conf Comput Commun Netw* (ICCCN) (Manchester Metropolitan University, United Kingdom) 2022, 1–7, doi: 10.1109/ICCCN54977.2022.9868843.

2 Mallick S R & Sharma S, EMRI: A scalable and secure Blockchain-based IoMT framework for healthcare data transaction, *19th* OITS *Int Conf Inf Technol* (OCIT) (IEEE) 2021, 261–266, doi: 10.1109/OCIT53463.2021.00060.

3 Al Nuaimi K & Kamel H, A survey of indoor positioning systems and algorithms, *Proc Int Conf Innov Inf Technol* (IEEE) 2011, 185–190.

4 Misra P & Enge P, Global positioning system: signals, measurements & Performance, *IEEE Aerosp Electron Syst Mag*, **17(10)** (2002) 36−37.

5 Zhen F, Zhan Z, Peng Q & Yuguo Z, Analysis based on RSSI ranging, *Chin J Sens Actuators*, **20(11)** (2007) 2526−2530.

6 Jeon K E, She J, Soonsawad P & Ng P C, BLE, beacons for internet of things applications: Survey, challenges, and opportunities, *IEEE Internet Things J*, **5(2)** (2018) 811–828.

7 Qiu Y, Zhao C C, Dai G L & Hu C J, Research on localization technology for wireless sensor networks, *Comput Sci*, **35(5)** (2008) 47−50.

8 Akyildiz I F, Su W, Sankarasubramaniam Y & Cayirci E, A survey on sensor networks, *IEEE Commun Mag*, **40(8)** (2002) 102–114.

9 Li Y, Meng M Q H, Li S, Chen W & Liang H, Particle filtering for range-based localization in wireless sensor networks, *Proc* 7th *World Congress on Intelligent Control and Automation* (IEEE) 2008, 1629–1634.

10 Sahinoglu Z & Gezici S, Ranging in the *IEEE* 802.15.4a standard, *Proc Microw Technol Conf (WAMICON)* (IEEE) (2006), 1−5.

11 Chen W, LiW, Shou H & Yuan B, Weighted centroid localization algorithm based on RSSI for wireless sensor networks, *J Wuhan Univ Technol*, **30(2)** (2006) 256–268.

12 Iyengar R & Sikdar B, Scalable and distributed GPS free positioning for sensor networks, *Proc Int Conf Commun* (ICC'03) (IEEE) 2003, 338–342.

13 Chen Y, Li X, Ding Y, Xu J & Liu Z, An improved DV-Hop localization algorithm for wireless sensor networks, *Proc13th IEEE Conf Ind Electron Appl (ICIEA)* (IEEE) 2018, 1831–1836.

14 Wang Z M & Zheng Y, The study of the weighted centroid localization algorithm based on RSSI, *Proc IEEE Int Conf Wirel Commun Sens Netw* (IEEE) 2014, 276–279.

15 Chapre Y, Mohapatra P, Jha S & Seneviratne A, Received signal strength indicator and its analysis in a typical WLAN system (short paper), *Proc IEEE LCN annu Conf Local Comput Netw* (IEEE) 2013, 304–307.

16 Al Nuaimi K & Kamel H, A survey of indoor positioning systems and algorithm, *Proc IEEE Int Conf Innov Inf Technol* (IEEE) 2011, 185−190.

17 Misra P & Enge P, Global positioning system: signals measurements & performance, *IEEE Aerosp Electron*, **17(10)** (2002) 36–37.

18 Zhen F, Zhan Z, Peng Q & Yuguo Z, Analysis based on RSSI ranging, *Chin J Sens Actuators*, **20(11)** (2007) 2526–2530.

19 Jeon K E, She J, Soonsawad P & Ng P C, BLE beacons for internet of things applications: Survey, challenges, and opportunities, *IEEE Internet Things J*, **5(2)** (2018) 811–828.

20 Qiu Y, Zhao C C, Dai G L & Hu, C J, Research on localization technology for wireless sensor networks, *Comput Sci*, **35(5)** (2008) 47–50.

21 Akyildiz I F, Su W, Sankarasubramaniam Y & Cayirci E, A survey on sensor networks, *IEEE Commun Mag*, **40(8)** (2002) 102–114.

22 Li Y, Meng M Q H, Li S, Chen W & Liang H, Particle filtering for range-based localization in wireless sensor networks, *Proc IEEE 7th World Congress on Intell Control Autom* (IEEE) 2008, 1629–1634.

23 Sahinoglu Z & Gezici S, Ranging in the *IEEE* 802.15. 4astandard, *Proc IEEE Microw Technol Conf* (WAMICON) (2006), 1–5.

24 Chen W, Li W, Shou H & Yuan B, Weighted centroid localization algorithm based on RSSI for wireless sensor networks, *J Wuhan Univ Technol*, **30(2)** (2006) 256–268.

25 Chen Y, Li, X, Ding Y, Xu J & Liu Z, An improved DV-Hop localization algorithm for wireless sensor networks, *Proc13th IEEE Conf Ind Electron Appl (ICIEA)* (IEEE) 2018, 1831–1836.

26 Iyengar R & Sikdar B, Scalable and distributed GPS free positioning for sensor networks, *Proc IEEE Int Conf Commun (ICC'03)* (IEEE) 2003, 338–342.