Wireless Personal Communications
https://doi.org/10.1007/s11277-020-07947-2

Blockchain for IoT Access Control, Security and Privacy: A Review

Pradnya Patil[1] · M. Sangeetha[1] · Vidhyacharan Bhaskar[2]

Accepted: 29 October 2020
© Springer Science+Business Media, LLC, part of Springer Nature 2020

Abstract
In modern era, blockchain technology is gaining a major attention among researchers and scientists for different scopes such as access control, data security, privacy and decentralization of the wireless networks. Though blockchain offers several benefits like peer to peer technology, anonymity, increased capacity, better security; the main cause behind being the first choice is its immutable structure. To abolish the role of the reliable third-party within interconnected networks, blockchain can be used as a key technology because of its distributed nature. Hyperledger fabric, IBM Blockchain, Ethereum, Ripple, R3 Corda, multichain are the most prominent blockchain platforms available for implementation. Aforementioned review paper describes and analyzes the existing blockchain based security techniques pertaining to IoT access control, vehicular ad hoc networks, healthcare, and supply chain. The comprehensive survey of use cases of blockchain will serve as a state-of-the-art for the researchers to carry out cutting edge research work in the pursuance of blockchain technology in various fields.

Keywords Access control · Blockchain · Consortium block chain · Data security · Internet of things (IoT) · Privacy

1 Introduction

Among all technologies available for data security and privacy, blockchain is the most efficient one because of its properties like immutability and irreversibility. The blockchain is defiant to modification of data [1]. Whenever there is a change in the ledger using

✉ Vidhyacharan Bhaskar
vcharan@gmail.com

Pradnya Patil
pp1000@srmist.edu.in

M. Sangeetha
sangeetm@srmist.edu.in

[1] Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Kattankulathur, Kancheepuram Dt., Tamilnadu 603203, India

[2] Department of Electrical and Computer Engineering, San Francisco State University, 1600 Holloway Avenue, San Francisco, CA 94132, USA

Published online: 27 November 2020

transactions, changes are distributed to all the nodes to verify and update their particular transcript of the ledger. Once the transaction is verified from all the nodes in the network, it is not possible to change the transaction without altering the later and previous blocks. So, blockchain transactions are irreversible and their data is constantly appended. Each block is connected with a link also known as *a chain*. Subsequent block incorporates hash of the preceding block to visit the chain in the reverse chronological order.

Blockchain uses both decentralized and distributed structure along with cryptographic properties, which makes it work in a unique way. Blockchain technology is preferable where security and confidentiality of the information is the first priority of the network. In IoT, access control can be achieved more efficiently by implementing blockchain [2], which is discussed in the later part of this paper. Further, from literature, it is clear that the use of blockchain will offer many superior results for other use cases like Vehicular Ad hoc Network (VANET), Healthcare, and Supply chain.

The remainder of this paper is organized as follows: Sect. 2 discusses the fundamentals and functioning of the blockchain. Section 3 presents the overview of IoT access control techniques using blockchain. A brief survey on the adoption of blockchain in privacy and security for the use cases mentioned above is provided in Sect. 4. Finally, Sect. 5 presents the conclusion.

2 Basics of Blockchain

2.1 Definition of Blockchain

A blockchain is a time stamped sequence of rigid transactions which is managed by a group of computers using special algorithms. Each computer that participates in this group is called a node and each node shares the same copy of data, which is called as *digital ledger*. Each node maintains the records of transactions in multiple consecutive blocks and uses the same algorithm to reach common agreement. These transactions are saved on every node in a distributed Peer to Peer (P2P) network. Figure 1 shows the general structure of a blockchain with basic block components [3].

Each block consists of version information, nonce value, hash value of the previous block, timestamp, merkle root and transactions. Version number of blockchain is used to maintain changes and updates during the whole duration of the protocol. Nonce is an arbitrary number to which miners will come across as a component of mining. Nonce is a part of cracking the mathematical puzzle first in order to mine the block. Hash is a cryptographic function used

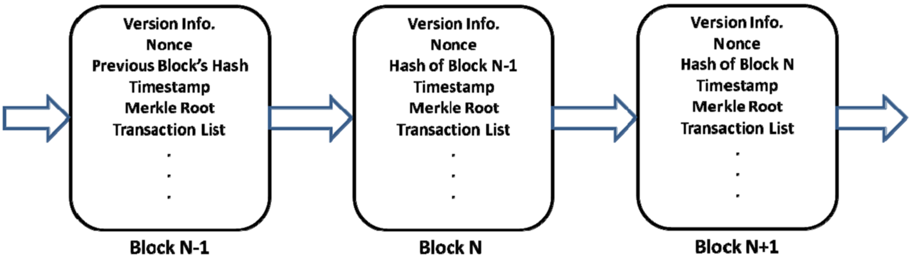

Fig. 1 General structure of blockchain

to secure the chain. Timestamp is used to understand when a particular transaction has been occurred. Merkle Root is obtained by hashing the transaction hashes again. Transaction list refers to the different transactions included in the particular block.

2.2 Functioning of the Blockchain

To implement Blockchain technology, a P2P network needs to be created with the devices (users) that are interested to communicate through blockchain. Each participating device is referred to as a node. Two keys are generated for each node: namely, public and private. As the name implies, public key is acknowledged to all and private key is undisclosed, and is used by a user to produce a signature. In short, asymmetric cryptography is used to accomplish the security demand of the information. Private keys need to be kept protected to avoid possible misuse or tampering of data on a blockchain.

A node initiates the transaction and after signing it with private key, publishes it in the network for getting verified by the peer nodes. These verification methods used are known as consensus algorithms, and vary in different blockchain platforms, depending upon the design objectives. After verification from peers, miner collects the transaction to create a block and that block gets appended to the blockchain with timestamp and unique ID (i.e. hash) to avoid further alterations. Newly added block gets linked up with the earlier block using its hash and upcoming block will establish link with this block and so on [4]. Figure 2 given below depicts the general workflow of blockchain stand on above description.

2.3 Consensus Algorithms

Consensus algorithm is the heart of Blockchain technology since they maintain the integrity and security of the blockchain network. It is a protocol by which network nodes of the blockchain arrive to a standard agreement on current records state of the ledger. Different blockchain platforms use different algorithms to reach the consensus and off course all of them differ in their operation and execution. Figure 3 shows the list of most popular consensus algorithms used in different blockchain platforms.

Basic working principle behind these algorithms is as given below:

i. *Proof of Work (PoW)* In PoW, nodes with more computing power administers the network.
ii. *Proof of Stake (PoS)* In PoS, nodes with more money administers the network.
iii. *Proof of Authority (PoA)* In PoA, arbitrary chosen trustworthy nodes administers the network.
iv. *Proof of Elapsed Time (PoET)* In PoET, nodes who have finished specific waiting period administers the network.
v. *Delegated Proof of Stake (DPoS)* In DPoS, Nodes elected by delegates through voting administers the network.

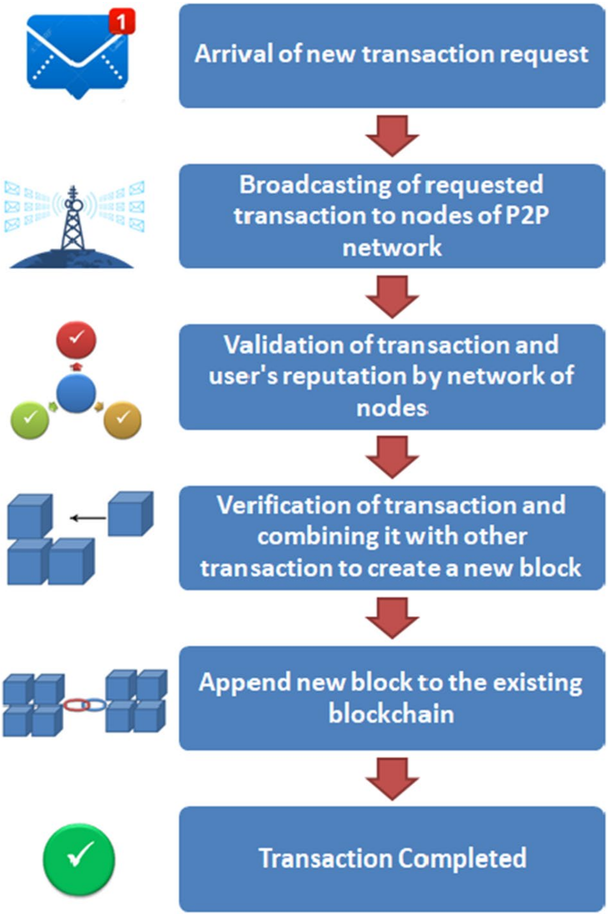
Arrival of new transaction request
Broadcasting of requested transaction to nodes of P2P network
Validation of transaction and user's reputation by network of nodes
Verification of transaction and combining it with other transaction to create a new block
Append new block to the existing blockchain
Transaction Completed

Fig. 2 General workflow of blockchain

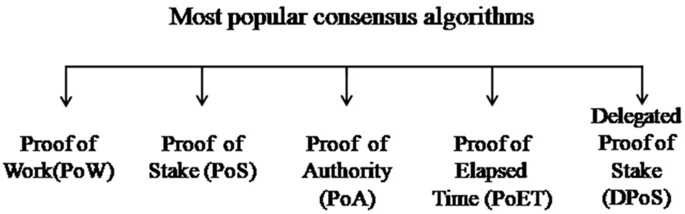
Most popular consensus algorithms
Proof of Work(PoW)
Proof of Stake (PoS)
Proof of Authority (PoA)
Proof of Elapsed Time (PoET)
Delegated Proof of Stake (DPoS)

Fig. 3 Most popular consensus algorithms

3 Blockchain Based IoT Access Control Methods

The surge of growing objects in communications and networking technology has caused a huge growth in IoT research. Interconnecting different smart devices over the Internet offers many advantages like data sharing, ease of access, and remote monitoring [5]. One of the major issues faced by IoT is its centralized structure i.e. the client–server model. Lack of trust between different participating devices may cause failure of the entire network, and so a credible solution is needed to avoid this issue. In recent years, several approaches have been proposed, in which blockchain is gaining popularity due to its properties like decentralized structure, security, and immutability.

3.1 Attribute Based Access Control (ABAC)

Attribute Based Access Control (ABAC) design is proposed to make access management simpler in IoT [6]. In this work, blockchain technology is implemented to append and preserve the distribution of attributes that includes user attributes, resource attributes and object attributes based on user's requirement. ABAC extracts uniqueness or representations into a set of attributes which are published by attribute authority. Each set of attributes is represented by Boolean formulae which defines different access policies. These access policies are used for valid and authorized access. It eliminates the stress of allocating roles or making access control list for all devices in the system. The performance analysis given in this paper shows that the ABAC scheme provides high degree of confidentiality, resiliency, flexibility and scalability.

In [7], authors have proposed Attribute bases Access Control method consisting of five main components namely Consortium Blockchain Network, Authority Nodes (AN), IoT Devices, Chaincode and Public Ledger and Access Tree. Authority nodes are part of Consortium Blockchain Network and are responsible for handling all the interactions with the Blockchain Network on behalf of IoT Devices. When requester sends access request to the target it gets forwarded to the AN by that target. Chaincode is queried by the AN and registered access credentials are retrieved to check the legitimacy of the requesters' uniqueness and the target's access rule. After that the access tree is constructed by AN to make authorization. Blockchain is used to record final access information with the authorization result followed by which results are sent to the requester by AN.

Here, attribute based Access Control is achieved by maintaining three closely related key-value database including Device database, Attribute database, and Access database. Attribute name is given to the Attribute after its registration and individual owner lists are maintained for each attribute when that is assigned to any device. Performance analysis shows that presented scheme is lightweight as well as efficient due to reduced storage and computation overhead.

3.2 Fair Access

To facilitate the users to have control on their own data, a completely pseudonymous technique without central governance is introduced in [8]. To achieve pseudonymity, bitcoin resembling addresses are used for identification of all interacting entities and access control policies are defined in the smart contract and then saved in blockchain. Blockchain also circulates endorsement tokens which are used as a unique identification, demonstrating the connection permission for admittance to a specific resource. Transaction integrity checks and double spending detection mechanism are enforced to detect forgery and reuse of tokens. The proposed framework relieves the constrained IoT devices from the trouble of managing a massive load of admittance control data.

3.3 Distributed Access Control

Oscar Novo [9] proposed a new approach which provides decentralized access control method linked to geographically distributed sensor networks. It is a combination of Wireless Sensor Networks, Manager Nodes, Agent node, Smart contract, Blockchain network and Management hubs.

i. *Wireless Sensor Networks* It is a group which consists of different IoT equipments and can be linked to the blockchain system over the management hub.
ii. *Manager Nodes* Managers are lightweight nodes which are liable to administrate the access control regulations.
iii. *Agent Node* Particular node bound to set up the smart contract in blockchain network which is the possessor of the smart contract through the life span of the access control system.
iv. *Smart Contract* It is a piece of code deployed in blockchain network which determines each and every operation related to access management.
v. *Blockchain network* Private block-chain network is used to save and handle admittance regulation policies.
vi. *Management hubs* It is a link which modifies Constrained Application Protocol (CoAP) messages initiated by the IoT equipments to JavaScript Object Notation Remote Procedure Call (JSONRPC) protocol messages recognizable by the blockchain nodes. IoT devices can request data access from the blockchain using management hub.

In this approach, authors have exercised blockchain for storage and distribution of access control information. An exclusive and non-destroyable single smart contract is used to describe all the actions certified in admittance regulatory system. Smart contracts are contacted by the managers to describe the admittance rules of the structure. The main advantage in this approach is its increased scalability since multiple systems can be linked to the blockchain set-up simultaneously using special nodes called management hubs.

Hwang, D. et al. in [10] proposed a method for interchanging information between geographically distant IoT devices. Instead of sending information request directly to the particular device, it is sent to the management hub which in turn checks for the access permission stored in blockchain. If the request is granted, management hub accesses the information from that device and sends it to the requesting device. This method is suitable for distant devices, where direct communication between devices is not feasible. Also, dynamic policy generation is proposed for the devices whose access control policies are not registered. Improved scalability has been achieved as an upshot of this scheme.

3.4 Distributed Key Management

For privacy oriented IoT systems, distributed key management design based on blockchain is proposed in [11]. Based on the deployment fields different side blockchain are formed in the fog layer to quicken the verification and to save storage space. Fog computing is included to cut down waiting time and collective blockchains are implemented in cloud layer to achieve cross-domain access. Compared to hierarchical schemes, extensibility is found higher along with higher communication and computational overhead.

3.5 Token Based Access Control

Access control by means of tokens using smart contract is presented by Fotiou, N. [12] to build an extensive event-based Internet of Things (IoT) control structure. Mapping between device operations and functions is included in smart contracts. Whenever any function is called by a client, smart contract generates a relative blockchain event. The corresponding IoT gateways receive the events which gradually results in an action in the suitable IoT equipment access. Fluctuating monetary cost and transaction delays are the issues faced by this method. It can be improved by direct interaction between client and IoT gateways.

Smart contract based blockchain solution using Ethereum is used [13] to provide successful access to the IoT devices for legitimate client. Access control and authentication scheme consists of smart contract which authenticates the client by means of his/her ethereum wallet address. Access token and ethereum address of the sender is published by smart contract, only if client is legitimate. This published information is received by the client and IoT equipments. The client develops a combination which encloses the ethereum public key, user Internet Protocol (IP) address, access token, and access duration. This combination is endorsed by ethereum private key followed by transmission of the related public key. Endorsement of the combination is essential in this setting to protect the integrity. When the IoT equipment obtains this information, after verification, it assigns the admittance to the client against the sender's IP address for the interval stated. The appeal or enquiry is abandoned when any of the verification check fails. Improved availability and scalability has been observed from the evaluation of proposed system.

Permission authorization method for IoT data by means of trusted oracles and blockchain is presented by Albreiki, H. et al. [14]. Oracles are used as gateways which act as an interface between blockchain, service providers, and remote clients. Multiple smart contracts are used which governs the interaction and right to use the IoT data. They also provide reputation count and enrollment of new oracles. Users send request to smart contract for accessing IoT data. Right of access to IoT data is validated by smart contracts after verifying the access control policies. After verification smart contracts issue Access tokens to the oracles and end-users to confirm the right of access. Access control based on oracles supports heterogeneous storage and offers distributed access control with dynamic policy management.

3.6 Control Chain

Control Chain [15] architecture which is a combination of four different blockchains is introduced for IoT access authorizations. Public recommendation and dealings of the entire individuals are stored within relationship blockchain. Context blockchain is used to store environmental information like refined data, physical inputs, and sensor reports which is useful for taking decisions about authorization. Confirmation regarding acceptance or rejection of admittance is stored in accountability Blockchain. Endorsement regulations specified by owners to their device or by device to themselves are stored in blockchain which is dedicated for rules. This architecture is more scalable, user-transparent and well-suited through wide variety of admittance control representations engaged in IoT.

3.7 Attribute Update Oriented Access Control

Immutable nature of the blockchain is the biggest challenge faced for embracement of Attribute Based Encryption (ABE) in fine grained access control due to its conflict with attribute updates or revocation of ABE. Novel multilayer blockchain based IoT system with Chameleon Hash algorithm is proposed in [16] to facilitate the attribute updates in fine grained access control. This scheme is capable of preventing revoked members or miners from stepping into the upcoming data as well as the precedent data without violating the integrity of the blockchain.

3.8 Ripple Protocol Consensus Algorithm (RPCA) Based Access Control

To resolve the security and privacy concerns in Internet of Drones (IoD) network, access control scheme with blockchain implementation is designed by Basudeb Bera [17]. It provides two types of access control: First is among two nearby drones in the same flying area and secondly within the drone and its Ground Station Server (GSS). GSS collects the real time data from the drones and create blocks containing the transactions. These blocks are then forwarded to the cloud server. Cloud server which acts as leader amongst all cloud servers will verify the block and add it to the blockchain using Ripple Protocol Consensus Algorithm (RPCA). Proposed scheme is protected for "replay" and "man in the middle" attacks together as per the simulation reports.

3.9 Multiple Smart Contracts Based Access Control

Authorized access control along with the permission based sharing of services is achieved using Ethereum blockchain by Tanzeela Sultana [18]. Three types of smart contracts named Access Control Contract (ACC), Register Contract (RC) and Judge Contract (JC) are framed to offer proficient access control administration. Secure sharing of services is accomplished by setting several permission levels to provide permissioned access rights for IoT users. Results show that, the system is cost efficient and less complex for access control and data sharing between the IoT devices. Summary of Blockchain based IoT access control methods and its performance analysis are given in Table 1 and 2 respectively.

4 Blockchain for Other Use Cases

4.1 Vehicular Ad-Hoc Networks (VANET)

VANET is a breed of Mobile Ad-Hoc Networks (MANET) formed with moving automobiles. VANET facilitate a broad collection of functions, essentially avoidance of crashing, security, sightless crossings and dynamic traffic supervision. It also provides Internet affinity to automobiles. Critical security requirements of VANET includes authentication of a sender node, non-repudiation and uprightness of the messages sent from the nodes in the network. Different methods have been proposed in literature to resolve the security related concerns of VANET. Some of them are discussed below (Table 3).

Table 1 Summary of blockchain based IoT access control methods

Study	Research interest	Solution		Remarks
		Blockchain platform adopted	Testing tool	
[6]	Data Tampering & single point failure	Hyperledger Fabric	AVISPA	Secure scheme for practical applications and it is useful and competent to implement stringent access control in IoT
[7]	Flexible and fine-grained authorization	Hyperledger Fabric	Hyperledger Caliper	Insubstantial and suitable scheme for aceess control with less storage overhead
[8]	Security and privacy of data	Bitcoin [as implementation of the bitcoin protocol]	Regtest	Users control over their personal data is achieved by encrypting it with keys which just client holds and governs
[9]	Distributed access control and scalability	Ethereum	CoAPBench	Fully decentralized scheme which provides an expandable, broad, and smoothly governable access control system for IoT
[11]	Auditability, scalability, extensibility and privacy	Not Applicable	OMNeT++ 5.4.1	An efficient approach for IoT access control is proposed by combining blockchain with cloud computing and fog computing
[12]	Security and resilience	Ethereum	Ropsten Rinkeby	Access control using tokens with ethereum blockchain is implemented which is convenient and with less overhead
[13]	Authentication and secure communication	Ethereum	Mythril	Effective approach of aunthication for secure communication and also overcomes drawbacks of conventional authentication mechanisms
[14]	Decentralized control and trusted management	Ethereum	Remix IDE	Blockchain and trusted oracles are implemented for decentralized access control. Heterogeneous storage is an added advantage of this approach
[16]	Update/Revocation aligned access control	Not Applicable	Python-based testbed	Blockchain based access control method to stop the revoked users from accessing future data as well as past data is designed for the first time
[17]	Security and privacy of Internet of Drones (IoD) environment	Not Applicable	AVISPA	Improved security and privacy for IoD environment along with efficient access control is proposed using blockchain
[18]	Secure data sharing and access control	Ethereum	Remix IDE	Cost effiecient access control with less complexity

Table 2 Performance analysis of blockchain based IoT access control methods

Study	Scalability	Decentralization	Privacy	Extensibility	Reduced computational overhead
[6]	✓	✓	✓	N/A	✓
[7]	✓	✓	✓	N/A	✓
[8]	✓	✓	✓	✓	N/A
[9]	✓	x	x	N/A	N/A
[11]	✓	✓	✓	✓	x
[12]	x	✓	x	✓	x
[13]	✓	✓	✓	x	N/A
[14]	x	✓	x	x	N/A
[15]	✓	✓	x	x	✓
[16]	✓	✓	✓	N/A	✓
[17]	x	✓	✓	N/A	✓
[18]	x	✓	✓	N/A	N/A

Reputation system based on blockchain to access data creditability of the message is proposed by Yang Z. [19]. Reputation of a particular node is calculated from the rating generated by a provisional core node whichever is nominated as a miner by using specific rules. Ratings are the representation of consensus of all vehicular nodes on each vehicle reputation. Vehicles will judge arriving messages as either correct or fake, depending on sender's reputation rate. The ratings are packed into a block by a miner after winning an election and broadcasted to all vehicular nodes in a network for their consensus. If miner qualifies some predefined equation, then vehicles will allow the arriving block and appends it to the blockchain. Here, blockchain is implemented to store the score which is used to compute the reputation value of the sender and in turn trustworthiness of the communication.

In [20] blockchain is used to stock up trust values of moving automobiles. Bayesian inference model is used for validation of received messages from neighboring vehicles. Depending upon the validation result each vehicle will receive some rating. Trust values are calculated from these ratings and packed into blocks to store in the blockchain.

Use of public blockchain in VANET is proposed in [21] to accumulate node reliability and communication reliability. Record of safety incident messages alongside the confidence rank of the vehicles is stored within blockchain in this approach to protect communication distribution in VANET.

Blockchain-based Anonymous Reputation System (BARS) for privacy of vehicle's identity is presented by Lu Z. [22]. Utilization of three types of blockchain is proposed for different purposes. Blockchain named MesBC is used to store all messages broadcasted by vehicles. CerBC is used to store the issued certificates and RevBC is a blockchain which serves as a public ledger for each and every revoked public key.

The consortium blockchain system is proposed in [23] for information safety contribution and efficient storage system. The proposed scheme is enhanced for extensive record storage in VANET, and the disseminated protection is implemented to tackle the safety impositions induced through a centralized database. Sharma P.K., [24] presented vehicular network design built on blockchain called Block-VN to improve the performance of

Table 3 Summarized literature review for blockchain based VANET

Study	Approach	Proposed technique	Performance metrics	Limitations
[19]	Reputation based trust management	Blockchain with Distributed consensus	**MDA**: Message Detection Accuracy **RTH**: Reputation Threshold	Security analysis is not done
[20]	Reputation based trust management	Blockchain with PoW and PoS	Storage overhead	Privacy preservation along with trust management is not considered
[21]	Node as well as message trustworthiness	Blockchain with PoW	Storage overhead Block generation time	Real time critical event message dissemination is absent
[22]	Reputation based trust management	Blockchain with PoW	Storage overhead Time consumption for authentication	Use of two Blockchain increases the complexity of the system.
[23]	Distributed data storage and security	Blockchain with pBFT(practical Byzantine Fault Tolerance	Verification delay Transcation confirmation time	Absence of real time message authentication
[26]	Secure message communication and node reputability prediction	Blockchain and Sea Lion Explored-Whale Optimization Algorithm	Rejection ratio Accuracy	Two level evaluation process is used which leads to system complexity
[27]	Revocable message authentication	Blockchain and cuckoo filter and node selection algorithm KUNodes	Computation and communication cost Execution time	System is more complex due to combination of different techniques
[28]	Secure data sharing and trust management	Blockchain with PoA (Proof of Authority)	Average trust rate Gas consumption cost	Less-efficient in terms of expenditure as it increases with size of the data
[29]	Optimal content catching	Blockchain with PoU (Proof of Utility) and Deep Reinforcement Learning	Block verification time % successful content catching	Communication time increase linearly with remoteness between vehicle and PoU chosen leader

large-scale vehicular networks in smart city. This method grants vehicles to determine and allocate their assets to form a network on which they work jointly to create value-added benefits.

Intelligent traffic system using blockchain is implemented in [25] for transmission of data as well as for transfer of lane property rights between vehicles. Peer to Peer network is used to eliminate the need of central computing authority. Each node can communicate with every other node directly. In [26], authors have introduced novel trust management structure in two stages: protected message broadcast and node authenticity calculation. Data sanitization process combined with privacy preservation model guarantees the secure message transmission. Key required for sanitization procedure is improved by a new fusion algorithm termed Sea Lion Explored-Whale Optimization Algorithm, which is the combination of Whale Optimization Algorithm and Sea Lion Optimization Algorithm, respectively. The blockchain technology is served for the management of the keys originated from the nodes. Two-level assessment procedure through rule based and machine learning based approach was used later, to calculate authenticity of the node.

Current practices in certificate-less signature schemes for security and privacy of the VANET are facing some difficulties owing the use of expensive bilinear pairing and absence of the efficient revocation mechanism. Resource constrained nature of the On Board Unit (OBU) is also a major factor which demands the efficient certificateless signature scheme to improve the message processing in VANETS. Proficient pairing-free online/offline certificate-less signature scheme is employed in [27] as the core technique for message verification. To enhance the effectiveness of the message verification procedure cuckoo filter is used which allows authenticating messages using the notifications from the RSU without checking each and every signature by itself. Also OBU can conduct the complex cryptographic operations offline accordingly they can sign the messages whenever needed using the pre-computed values. Revocation issue is addressed by updating time keys of the revoked users after certain period. Node selection algorithm named KUNodes is implemented to reduce the burden of Key Generation Centers (KGC). Implementation of blockchain is proposed here to store the revocation list in order to enhance transparency and integrity of the revocation list.

In [28], authors proposed blockchain based VANET for trustworthy data sharing between normal nodes with limited resources. Edge nodes with added computational potential are used to handle service provisioning. Normal node vehicles contacts edge node vehicles for required services after which edge node vehicles connects to the Rode Side Units (RSU) and responds to the particular request. Using Intelligent Vehicle Trust Point (IVTP), the trust values of the vehicles are calculated and authenticity of the same is determined. Ethereum blockchain is implemented to store a list of all the registered vehicles as well as reviews given by the ordinary node vehicles against services provided to them, and the whole process is automated using smart contracts without inclusion of the third party. Application of Interplanetary File System (IPFS) to reserve the large amount of data generated by nodes and provision of caching facility at edge nodes to store repeatedly used services are also measurable inputs of the scheme in increasing efficiency of the system.

In [29], authors presented a mixed approach with the integration of permissioned blockchain and Deep Reinforcement Learning (DRL) into VANETS for smart and safe content catching. In proposed permissioned blockchain structure, vehicles act as a catching requester and catching providers while Base Stations (BS) does the role of verifiers to keep up the blockchain. To monitor and understand the dynamic network environment DRL approach has been used; which further helps in scheming finest content catching scheme among the catching requesters and providers.

4.2 Healthcare

Existing healthcare systems suffers from ample number of confrontations concerning privacy, security, efficiency and exchange of data between different healthcare entities. At present time, designing a smart and secure healthcare system is the foremost intent of researchers to get rid of above mentioned constraints obligated by conventional healthcare systems. Combination of promising technologies such as blockchain, edge computing, and artificial intelligence can offer great features to overcome the constraints of the existing healthcare systems. Some of the research work based on integration of blockchain with a few additional technologies is presented below.

Reduction in computational and communication overhead is achieved in [30] for healthcare via isolating the network members in clusters and only one copy of ledger for each cluster is kept. Blockchain network is implemented using Hyperledger Fabric platform in [31] for storing the collected health records securely and to handle the access control in order to maintain the patient's privacy.

Blockchain based framework is developed by Patel V. [32] for cross domain image distribution without any central authority. This concept can enable secure transfer of different medical records between various entities under the supervision of patients.

A brief discussion on the crucial role of Electronic Healthcare Record (EHR) management in healthcare industry and current gaps in EHR management is provided in [33]. Blockchain based architecture is proposed in [34] which facilitates the storage of data hash and access policies in blockchain to increase the integrity and accessibility of the users' data. Single point failure and Denial of Service (DoS) attack can be avoided through this approach as per given security analysis. Separate ledgers are used to store hashes and access policies. Multiple rounds of voting are applied using practical Byzantine Fault Tolerance (pBFT) consensus algorithm by all nodes to boost the network security and efficiency.

In [35], consortium blockchain interconnecting patients, health bureau, healthcare communities and hospitals, combined with Parallel Healthcare System (PHS) is proposed to offer data integrity, interoperability, scalability, security, with improvement in the precision diagnosis and efficient treatment. Presneted framework of parallel healthcare systems (PHSs) is based on the Artificial systems, Computational experiments and Parallel execution (ACP) approach. In this method, Blockchain is employed only to store the hash value of the data which in turn cuts down the storage space. Delegated Proof of Stake (DPoS) mechanism is used to reach the agreement among network nodes.

Blockchain based framework labeled as HaBiTs [36] for telesurgery using smart contracts has been proposed by Rajesh Gupta. Interoperability issue in traditional systems is resolved in this approach by assigning one block for each surgeon where complete information about surgical procedure executed by the doctors is saved.

A new decentralised record management structure to deal with Electronic Health Records, using blockchain technology called MedRec is presented in [37]. The system gives patients an ample, unalterable record and trouble-free right to entry to their medical reports across providers and treatment sites. MedRec maintains authentication, confidentiality, accountability and data distribution which are essential properties while handling receptive information. Further parallel effort is attempted in Medicalchain [38] which campaigns the application of blockchain technology in electronic healthcare industry.

To elliminate the drawbacks of conventional Smart Helathcare System (SHS) authors in [39] proposed a new blockchain based architecture called Secured and Smart

Healthcare System (S2HS) in which various healthcare data generated by different entities are encrypted using cryptographic properties of blockchain and stored in decentralized manner instead of centralized database. Only legitmate users can access this stored data and doctors or clinitians will be granted the access to it only after the patients consent. All the entities in proposed framework are connected through Wireless Sensor Network (WSN).

Attribute based signature scheme with attribute revocation facility is proposed in [40] to protect the patients identity in Blockchain based healthcare systems. Attribute master key represents the users identity along with attributes set and is capable of resisting atrribute collusion attacks. Attribute update key is related to the attribute revocation. Users independently calculate the attribute signature by combining attribute master key and update key which in turn avoids the leakage of signature key. Revocation of the attributes is made effective by means of KUNodes algorithm. This scheme involves relatively few paring operations and is free from central authority.

Integration of edge computing with blockchain to facilitate the trade of huge amount of healthcare records produced from different entities is proposed in [41]. Patients privacy is the main moto behind this work. Priority based secure data sharing scheme is designed by the authors to reduce the service latency introduced due to blockchain. Table 4 Summerizes the work done till date in Blockchain based healthcare system.

4.3 Supply Chain

In supply chain scenario, cooperation between suppliers, manufacturers, carriers, retailers, and customers is necessary for efficient functioning of the system. On another side, real time product tracking has always been a major challenge in supply chain management which requires prominent and trustworthy solution to meet the requirement. Blockchain based solutions for supply chain available in the literature are given below:

In [42], Industrial IoT (IIoT) devices are connected to the blockchain for real time data recording and supervising of the data which is later stored in the system through smart

Table 4 Summary of blockchain based healthcare systems

Study	Type of data	Blockchain purpose	Blockchain platform used
[30]	Personal medical record	Data integrity Privacy	Not applicable
[31]	Personal medical record from wearable and medical devices	Privacy Data integrity	Hyperledger fabric
[32]	Medical images	Access control Privacy	Not applicable
[34]	Personal medical record	Access control	Not applicable
[35]	Personal medical record	Data integrity Access control	Not applicable
[36]	Personal medical record	Security Privacy Interoperability	Hyperledger fabric
[39]	Clinical data from sensors	Access control	Not applicable
[40]	Electronic health record	Privacy of the patient's identity	Not applicable
[41]	Personal medical record	Privacy	Private blockchain with DPoS

contracts. The access policies are defined in smart contracts and only those companies satisfying the attributes criteria can have access to the smart contracts and in turn access to the transactions facilitating secure sharing scheme for supply chain.

Quality of the agriculture products is degrading day by day in today's era due the use of uncertified chemicals and artificial mechanisms used to ripen the product. Considering consumer's health it is necessary to track the origin of the agriculture products. For this purpose, blockchain based approach is developed using Ethereum platform in [43].To assure data sharing and quality control from a supply chain perspective, blockchain-based Supplier Continuous Quality Improvement (SCQI) framework consisting of four layers namely data layer, IoT sensor layer, business layer and contract layer as discussed by Chen S. [44].

Implementation of a supply chain tracking system using smart contract on ethereum blockchain is demonstrated by S.R. Niya [45]. A platform-independent technique which adjusts various object combinations and conversions to be tracked is provided by means of Decentralized Application (Dapp). Integration of the blockchain and Enterprise Resource Planning (ERP) systems is implemented using hyperledger composer [46] to automate the payments between distributers and retailers. Use of smart contract is demonstrated to automate transactions between distributor and retailer.

A foremost challenges encountered by transport industry are misplacing of cargo and immense loads in cargo checks for illegitimate movements and possible terrorist offenses. Blockchain-based cargo management scheme can be used as effective solution against these threats as suggested by Xu L. [47].

An approach that makes use of the Ethereum blockchain and smart contract to expertly perform industry dealings for soybean tracking and traceability over the agricultural supply chain is proposed in [48]. Designed approach terminates the necessity of a faithful central authority, mediators and produces transactions ledger with higher reliability and better competence. Smart contracts are executed to handle and organize the entire interactions and dealings between all the members concerned in the supply chain environment. A food traceability system based on blockchain and IoT is proposed in [49] to incorporate the employment of fuzzy logic and blockchain-IoT technology into a whole shelf lifespan management structure to manage faster decaying food. Summary of Blockchain based schemes in supply chain management is presented in Table 5.

5 Conclusion

Automation and data dependency is escalating at a faster pace to conquer the limitations such as manual operations, trust, security, and privacy. Even though many conventional state of the art technologies exist, issues like single point failure and tampering of the data is yet to be resolved. Blockchain technology along with IoT, cloud computing, big data and machine learning can offer an extended solution for these issues.

This review paper presents diverse blockchain based methods offered in literature for IoT access control as well as privacy and security enhancement of VANET, healthcare and supply chain networks. Also it examines available methods for various performance metrics such as scalability, privacy, extensibility, accuracy, storage overhead and computation overhead. At the same time we cannot compare all the methods under common criteria due to variability of solutions proposed by the researchers. Consortium blockchain along with

Table 5 Summary of blockchain based supply chain management schemes

Study	Objective	Contribution	Implemented blockchain platform
[42]	Access control	Privacy and security of the supply chain network is enhanced by combining blockchain, attribute-based encryption and Industrial IoT	Ethereum
[43]	Traceability	Increased transparency and traceability of the food product in organic food supply chain is achieved using blockchain	Ethereum
[44]	Supply chain quality management	New framework is proposed for supply chain quality management	Not applicable
[45]	Supply chain tracking	A hardware-and platform-independent technique which adjusts various object combinations and conversions to be tracked is provided by means of Decentralized Application. (DApp)	Ethereum
[46]	Payment automation	Automatic payment system between distributers and retailers is developed by combining Blockchain and ERP system	Hyperledger Composer
[47]	Cargo security	Blockchain based cargo management system is proposed to overcome safety threats like cargo mishap and higher burdens in cargo assessments	Not applicable
[48]	Traceability	Designed approach terminates the necessity of a faithful central authority, mediators and produce transactions ledger with higher reliability and better competence	Ethereum
[49]	Traceability	Effective food traceability system is proposed which combines blockchain, IoT and fuzzy logic to achieve entire traceability for storage life of the food	Not applicable

effective consensus algorithm could be the enhanced solution for different scenarios as per our study.

References

1. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access, 4*(1), 2292–2303.
2. Fernandez-Carames, T. M., & Fraga-Lamas, P. (2018). A review on the use of blockchain for the internet of things. *IEEE Access, 6*(1), 32979–33001.
3. Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system. [Online]. http://www.bitcoin.org/bitcoin.pdf
4. Zheng, Z., Xie, S., Dai, H., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *Proceedings of 2017 IEEE international congress on big data (BigData Congress)*, Honolulu, HI, USA, pp. 557–564.
5. Kumar, N. M., & Mallic, P. K. (2018). Blockchain technology for security issues and challenges in IoT. *Procedia Computer Science, 132*(1), 1815–1823.
6. Ding, S., Cao, J., Li, C., et al. (2019). A novel attribute-based access control scheme using blockchain for IoT. *IEEE Access, 7*(1), 38431–38441.
7. Zhang, Y., Li, B., Liu, B., et al. (2020). An attribute-based collaborative access control scheme using blockchain for IoT devices. *MDPI Electronics, 1*(1), 1–22.
8. Ouaddah, A., Abou Elkalam, A., & Ait Ouahma, A. (2017). FairAccess: a new blockchain-based access control framework for the internet of things. *Security and Communication Networks, 9*(18), 5943–5964.
9. Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal, 5*(2), 1184–1195.
10. Hwang, D., Choi, J., & Kim, K. (2018). Dynamic access control scheme for IoT devices using blockchain. In *Proceedings of 9th international conference on information and communication technology convergence*, Maison Glad Jeju, Jeju Iceland, Korea, pp. 713–715.
11. Ma, M., Shi, G., & Li, F. (2019). Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario. *IEEE Access, 7*(1), 34045–34059.
12. Fotiou, N., Pittaras, I., & Siris, V. A., et al. (2019). Secure IoT access at scale using blockchains and smart contracts. In *Proceedings of 20th IEEE international symposium on a world of wireless, mobile and multimedia networks*, Washington DC, USA, pp. 1–6.
13. Ourad, A. Z., Belgacem, B., & Salah, K. (2018). Using blockchain for IoT access control and authentication management. In *Proceedings of international conference on internet of things,* Seattle, USA, pp. 150–164.
14. Albreiki, H., Alqassem, L., & Salah K., et. al. (2019). Decentralized access control for IoT data using blockchain and trusted oracles. In *Proceedings of IEEE international conference on industrial internet*, FL, USA, pp. 248–257.
15. Pinno O. J. A., Gregio A. R. A., & De Bona L. C. E. (2018). ControlChain: Blockchain as a central enabler for access control authorizations in the IoT. In *Proceedings of IEEE global communications conference*, Abu Dhabi, UAE, pp. 1–6.
16. Yu, G., Zha, X., & Wang, X. (2020). Enabling attribute revocation for fine-grained access control in blockchain-iot systems. *IEEE Transactions on Engineering Management, 1*(1), 1–18.
17. Bera, B., Chatterj, D., & Das, A. K. (2020). Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment. *Computer Communication, 1*(1), 229–249.
18. Sultana, T., Almogren, A., Akbar, M., et al. (2020). Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices. *MDPI Applied Sciences, 1*(1), 1–21.
19. Yang, Z., & Zheng K., et al. (2017). A blockchain-based reputation system for data credibility assessment in vehicular networks. In *Proceedings of IEEE international symposium on personal, indoor and mobile radio communications*, Montreal, QC, Canada, pp. 1–5.
20. Yang, Z., Yang, K., et al. (2019). Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet of Things Journal, 6*(2), 1495–1505.
21. Shrestha, R., Bajracharya, R., Shrestha, A. P., et al. (2019). A new type of blockchain for secure message exchange in VANET. *Digital Communications and Networks, 2019*(1), 1–14.
22. Lu, Z., Liu, W., Wang, Q., et al. (2018). A privacy-preserving trust model based on blockchain for VANETs. *IEEE Access, 6*(1), 45655–45664.

23. Zhang, X., & Chen, X. (2019). Data security sharing and storage based on a consortium blockchain in a vehicular ad hoc network. *IEEE Access, 7*(1), 58241–58254.
24. Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Block-VN: A distributed blockchain based vehicular network architecture in smart city. *Journal of Information Processing Systems, 13*(1), 184–195.
25. Ren, Q., Man, K. L., & Li, M. et al. (2019). Using blockchain to enhance and optimize IoT-based intelligent traffic system. In *Proceedings of international conference on platform technology and service,* Jeju, Korea, pp. 1–4.
26. Malik, N., Nanda, P., He, X., et al. (2020). Vehicular networks with security and trust management solutions: proposed secured message exchange via blockchain technology. *Wireless Networks, 26*(6), 1–20.
27. Li, K., Lau, W. F., Au, M. H., et al. (2020). Efficient message authentication with revocation transparency using blockchain for vehicular networks. *Computers and Electrical Engineering, 86*(1), 1–11.
28. Javed, M. U., Rehman, M., Javaid, N., et al. (2020). Blockchain-based secure data storage for distributed vehicular networks. *MDPI Applied Sciences, 1*(1), 1–22.
29. Dai, Y., Xu, D., Zhang, K., Maharjan, S., & Zhang, Y. (2020). Deep reinforcement learning and permissioned blockchain for content caching in vehicular edge computing and networks. *IEEE Transactions on Vehicular Technology, 69*(4), 4312–4324.
30. Ismail, L., Materwala, H., & Zeadally, S. (2019). Lightweight blockchain for healthcare. *IEEE Access, 7*(1), 149935–149951.
31. Liang, X., Zhao, J., & Shetty, S., et al. (2018). Integrating blockchain for data sharing and collaboration in mobile Healthcare applications. In *Proceedings of IEEE international symposium on personal, indoor and mobile radio communications*, Bologna, Italy, pp. 1–5.
32. Patel, V. (2018). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Informatics Journal, 25*(4), 1398–1411.
33. Dasaklis, T. K., Casino, F., & Patsakis, C. (2018). Blockchain meets smart health: Towards next generation healthcare services. In *Proceedings of 9th international conference on information, intelligence, systems and applications*, HongKong, China, pp. 1–8.
34. Hossein, K. M., Esmaeili, M. E., & Dargahi T. (2019). Blockchain-based privacy-preserving healthcare architecture. In *Proceedings of IEEE Canadian conference of electrical and computer engineering*, Edmonton, Canada, pp. 1–4.
35. Wang, S., Wang, J., & Wang, X. (2018). Blockchain-powered parallel healthcare systems based on the ACP approach. *IEEE Transactions on Computational Social Systems, 5*(4), 942–950.
36. Gupta, R., Member, S., & Tanwar, S., et al. (2019). HaBiTs: Blockchain-based telesurgery framework. In *International conference on computer, information and telecommunication systems*, Beijing, China, pp. 1–5.
37. Azaria, A., Ekblaw, A. & Vieira, T. et al. (2016). MedRec: Using blockchain for medical data access and permission management. In *Proceedings of 2nd international conference on open and big data*, Vienna, Austria, pp. 25–30.
38. Ammbr, T., Token, P. & Has, S. et al. (2018). MedicalChain. Whitepaper.
39. Gautami, T., Mohd, A. A., & Sara, P. (2020). S2HS-A blockchain based approach for smart healthcare system. *Healthcare, 8*(1), 1–11.
40. Su, Q., Zhang, R., Xue, R., & Li, P. (2020). Revocable attribute-based signature for blockchain-based healthcare system. *IEEE Access, 8,* 127884–127896.
41. Abdellatif, A. A., Al-Marridi, A. Z., Mohamed, A., Erbad, A., Chiasserini, C. F., & Refaey, A. (2020). ssHealth: Toward secure, blockchain-enabled healthcare systems. *IEEE Network, 34*(4), 312–319.
42. Wen, Q., Gao Y., & Chen, Z. et al. (2019). A blockchain-based data sharing scheme in the supply chain by IIoT. In *Proceedings of IEEE international conference on industrial cyber physical systems*, Cologne, Germany, pp. 695–700.
43. Basnayake, B. M. A. L., & Rajapakse, C. (2019). A blockchain-based decentralized system to ensure the transparency of organic food supply chain. In: *Proceedings of IEEE international research conference on smart computing and systems engineering*, University of Kelaniya, Sri Lanka, pp. 103–107.
44. Chen, S., Shi, R., & Ren Z., et al. (2017). A blockchain-based supply chain quality management framework. In *Proceedings of IEEE International Conference on E-Business Engineering*, Shanghai, China, pp. 172–176.

45. Niya, S. R., Dordevic, D., Nabi, A. G., Mann, T., & Stiller, B. (2019). A platform-independent, generic-purpose, and blockchain-based supply chain tracking. In *Proceedings of IEEE international conference on blockchain and cryptocurrency* Seoul, Korea, San Diego, USA, pp. 11–12.
46. Kaid, D., & Eljazzar, M. M. (2019). Applying blockchain to automate installments payment between supply chain parties. In *Proceedings of international computer engineering conference: Secure smart societies*, Giza, Egypt, pp. 231–235.
47. Xu, L., Chen, L., Gao, Z., Chang, Y., Iakovou, E., & Shi, W. (2018). Binding the physical and cyber worlds: A blockchain approach for cargo supply chain security enhancement. In *Proceedings of 2018 IEEE international symposium on technologies for homeland security*, Woburn, MA USA, pp. 1–5.
48. Salah, K., Nizamuddin, N., Jayaraman, R., et al. (2019). Blockchain-based soybean traceability in agricultural supply chain. *IEEE Access, 7*(1), 73295–73305.
49. Tsang, Y. P., Choy, K. L., Wu, C. H., et al. (2019). Blockchain-driven IoT for food traceability with an integrated consensus mechanism. *IEEE Access, 7*(1), 129000–129017.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Pradnya Patil has received her Bachelors and Masters degree in Electronics and Telecommunication engineering from Shivaji University, Kolhapur, India in 2007 and 2010 respectively. Currently she is pursuing her PhD degree at SRM Institute of Science and Technology, Chennai. Her current research interests include Blockchain Technology, IoT Security, Information Security and Cryptography.

Dr. M. Sangeetha is a senior IEEE member, who received her PhD degree from S.R.M. University, Kattankulathur, Chennai, India in 2014. She was a gold medalist in her M.Tech degree. Her research interests include Wireless Chaotic Communications, Signal Processing application for Wireless Communication Systems, Internet of Things (IoT) and Machine Learning(ML) algorithms for IoT. Currently, she is working as an Associate Professor in the Department of Electronics and Communication Engineering at S.R.M. Institute of Science and Technology (formerly known as SRM University), Kattankulathur, India. She has published 18 International Journal papers, presented 15 International Conference papers and presented 5 papers in National Level Conferences.

Dr. Vidhyacharan Bhaskar received the B.Sc. degree in Mathematics from the University of Madras, Chennai, India in 1992, M.E. degree in Electrical & Communication Engineering from the Indian Institute of Science, Bangalore in 1997, and the M.S.E. and Ph.D. degrees in Electrical Engineering from the University of Alabama in Huntsville in 2001 and 2002, respectively. During 2002–2003, he was a Post Doctoral fellow with the Communications research group at the University of Toronto, Canada, where he worked on the applications of space–time coding for wireless communication systems. During 2003–2006, he was an Associate Professor in the Department of Information Systems and Telecommunications at the University of Technology of Troyes, France. From Jan. 2007 to May 2014, he was a Full Professor in the Department of Electronics and Communication Engineering at S.R.M. University, Kattankulathur, India. Since 2015, he is a Professor in the Department of Electrical and Computer Engineering at San Francisco State University, San Francisco, California, USA. His research interests include MIMO wireless communications, signal processing, error control coding and queuing theory. He has published 131 Refereed Journal papers, presented around 72 Conference papers in various International Conferences over the past 20 years, published a book on "Adaptive Rate Coding for A-CDMA Systems" in Jan 2011, a book on "Higher-Order s-to-z mapping functions for digital filters," in March 2013, and has also co-authored a book on MATLAB in 1998. He has 894 Google scholar citations. He has advised 50 Masters students, 11 Doctoral students, and 3 Senior design projects. He is an IEEE Senior member (SM-IEEE) and is a member of IET (M-IET, UK). He is a Fellow of Institute of Electronics and Telecommunication Engineers (F-IETE), and a Fellow of Institute of Engineers (F-IE), Kolkata, India. He is also a Life member of the Indian Society of Technical Education (LM-ISTE) and a member of the Indian Science Congress (M-ISC).