Telecommunication Systems (2022) 81:125–173
https://doi.org/10.1007/s11235-022-00938-7

Blockchain-envisioned access control for internet of things applications: a comprehensive survey and future directions

Palak Bagga[1] · Ashok Kumar Das[1,2] · Vinay Chamola[3] · Mohsen Guizani[4]

Accepted: 23 June 2022 / Published online: 20 July 2022

Abstract
With rapid advancements in the technology, almost all the devices around are becoming smart and contribute to the Internet of Things (IoT) network. When a new IoT device is added to the network, it is important to verify the authenticity of the device before allowing it to communicate with the network. Hence, access control is a crucial security mechanism that allows only the authenticated node to become the part of the network. An access control mechanism also supports confidentiality, by establishing a session key that accomplishes secure communications in open public channels. Recently, blockchain has been implemented in access control protocols to provide a better security mechanism. The foundation of this survey article is laid on IoT, where a detailed description on IoT, its architecture and applications is provided. Further, various security challenges and issues, security attacks possible in IoT and their countermeasures are also provided. We emphasize on the blockchain technology and its evolution in IoT. A detailed description on existing consensus mechanisms and how blockchain can be used to overpower IoT vulnerabilities is highlighted. Moreover, we provide a comprehensive description on access control protocols. The protocols are classified into certificate-based, certificate-less and blockchain-based access control mechanisms for better understanding. We then elaborate on each use case like smart home, smart grid, health care and smart agriculture while describing access control mechanisms. The detailed description not only explains the implementation of the access mechanism, but also gives a wider vision on IoT applications. Next, a rigorous comparative analysis is performed to showcase the efficiency of all protocols in terms of computation and communication costs. Finally, we discuss open research issues and challenges in a blockchain-envisioned IoT network.

Keywords Internet of things (IoT) · Blockchain · Access control · Authentication · Key agreement · Security

1 Introduction

The Internet of Things (IoT) is an Internet based service platform or interconnection of heterogeneous objects like smart devices, Global Positioning System (GPS) devices, actuators, mobile devices and sensing nodes together to Internet or cloud to provide a service application. The IoT devices have limited resources, but they possess the Internet Protocol (IP) addresses which help them to communicate in the network. The smart devices are integrated with the physical world and can be accessed remotely. The integration of computer based systems with the outside world, increases the efficiency and accuracy of the network for economic benefits without involving much human interventions. The devices with processing abilities communicate with each other via

✉ Ashok Kumar Das
ashok.das@iiit.ac.in ; iitkgp.akdas@gmail.com

Palak Bagga
palak.bagga@research.iiit.ac.in

Vinay Chamola
vinay.chamola@pilani.bits-pilani.ac.in

Mohsen Guizani
mguizani@ieee.org

[1] Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India

[2] Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA 23435, USA

[3] Department of Electrical and Electronics Engineering and Anuradha and Prashanth Palakurthi Centre for Artificial Intelligence Research (APPCAIR), BITS-Pilani, Pilani Campus, Pilani 333 031, India

[4] Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), Masdar City, Abu Dhabi, United Arab Emirates

device-to-device (D2D) communication [1,2] without using the defined network infrastructure. The interconnected network allows not only Internet connected objects but non IP objects too to interact, send, store, retrieve and share information amongst themselves to co-ordinate in decision making relevant to any application or service. Wireless communication, artificial intelligence, machine learning and embedded systems form pillars of IoT paradigm. The apprehension of the paradigm has improved the quality of life of the people by significantly contributing to their daily routine, leveraging health, increasing self confidence of disabled people, quick health decisions, self staring and self controlling smart home appliances etc [3]. The use of the modern technology has increased efficiency, service level and customer satisfaction [4]. The objects or devices such as smart phones/tablets, smart home appliances, wearable devices, etc are transformed into smart objects by exploiting their backend technologies, embedded devices, embedded electronics, embedded systems, embedded processors and embedded communication systems to create advanced sensing, computation and processing power capabilities. The deployed objects collect the data from their surroundings and send it to the central servers for further processing [5].

1.1 Generic IoT architecture

Figure 1 represents the generic IoT architecture. *IoT smart devices* and *IoT sensors* are deployed in the target fields to execute an IoT application or service. For example in smart home IoT network, smart home appliances are installed in the home at various places, whose services are accessible to the smart home users. As seen in the figures smart devices placed at different target fields become the part of different application such as smart transportation, smart health care, smart grid etc. All the use cases considered, have their own *gateway node* as database repository. Each smart device is registered by a gateway node which is also deployed at some place within the target field. Smart devices and sensors gather the information and acquire sensed data from the surrounding. All the smart devices have the capability to communicate with other devices and to the gateway node after mutually authenticating each other. The data from each device is sent to the nearest gateway node for further processing. The processed data or the information stored, helps in decision making and provide user services. The data is also stored in cloud servers in the Internet to make it accessible to the *IoT users*. The communication between the devices, and between device and gateway node occurs on a wireless open channel. The open public channel is prone to different adversarial attacks discussed in Sect. 3.2. Moreover, any node in the network can be physically captured and compromised to hamper the integrity of the network. Therefore, access control protocols forms the backbone of the IoT network to maintain security and privacy, as it authenticates the nodes before allowing them for communication, and it also allows the nodes to establish a session key for secure communication.

1.2 IoT applications

The advantages, economic benefits and quality of services that IoT provides, has led researchers to implement it in various fields. IoT has been used in fields like smart home, transportation, health care, industrial automation, and emergency response to man made and natural disasters, smart electricity grid, etc. With the evolution of IoT in recent years, IoT applications can be categorized into four major domains which are as follows: (1) Internet of Vehicles (IoV), (2) Machine to Machine Communications (M2M), (3) Internet of Sensors (IoS), and (4) Internet of Energy (IoE). Internet of vehicles is an advanced vehicular adhoc network, which connects vehicles, road side units with the vehicular cloud to provide services like road turn warnings, traffic jam signals, deep curve warning and traffic light management to give best, safe on road experience ensuring safety of passengers and drivers. It also warns the driver on deviating from proper trajectory paths or bumping into objects. Further, such concept enables the automatic emergency notification of nearest road and medical assistance in case of accidents.

In M2M, two machines can communicate or exchange the information without human interaction. Such a communication includes the wireless communication in the industrial Internet of Things (IIoT). IoS is the Internet of sensor nodes, where the traditional wireless sensor networks, social sensor networks and body area sensor networks are included. IoS is interconnection of sensors and the Internet using any IEEE protocols [6]. IoE is the interconnection of smart grids with Internet to manage storage, distribution and monitor energy productions. Figure 2 displays various applications of IoT, some of which are shown as the use cases in Fig. 1.

Use cases of IoT applications Adding to the luxury of the users, IoT in combination with smart meters can also transform home into smart home by installing various IoT sensor nodes for managing and monitoring household stuff. For instance, a user outside his home can still control the equipments at home by getting notified about the activities happening in the house like amount of water in the refrigerator, the temperature of AC, switching on/off of lights, fan and other appliances. It can also be applied to control and monitor power consumptions. Smart metering can also be used to monitor water level and water pressure, gas level, energy production by renewable resources etc. Advancing the notion Li *et al.* in [7] proposed a Smart Energy Theft System (SETS) for the smart home to reduce the common energy thefts. In energy theft, an attacker can hack smart home appliances, or tamper the smart meter readings, to reduce its own smart

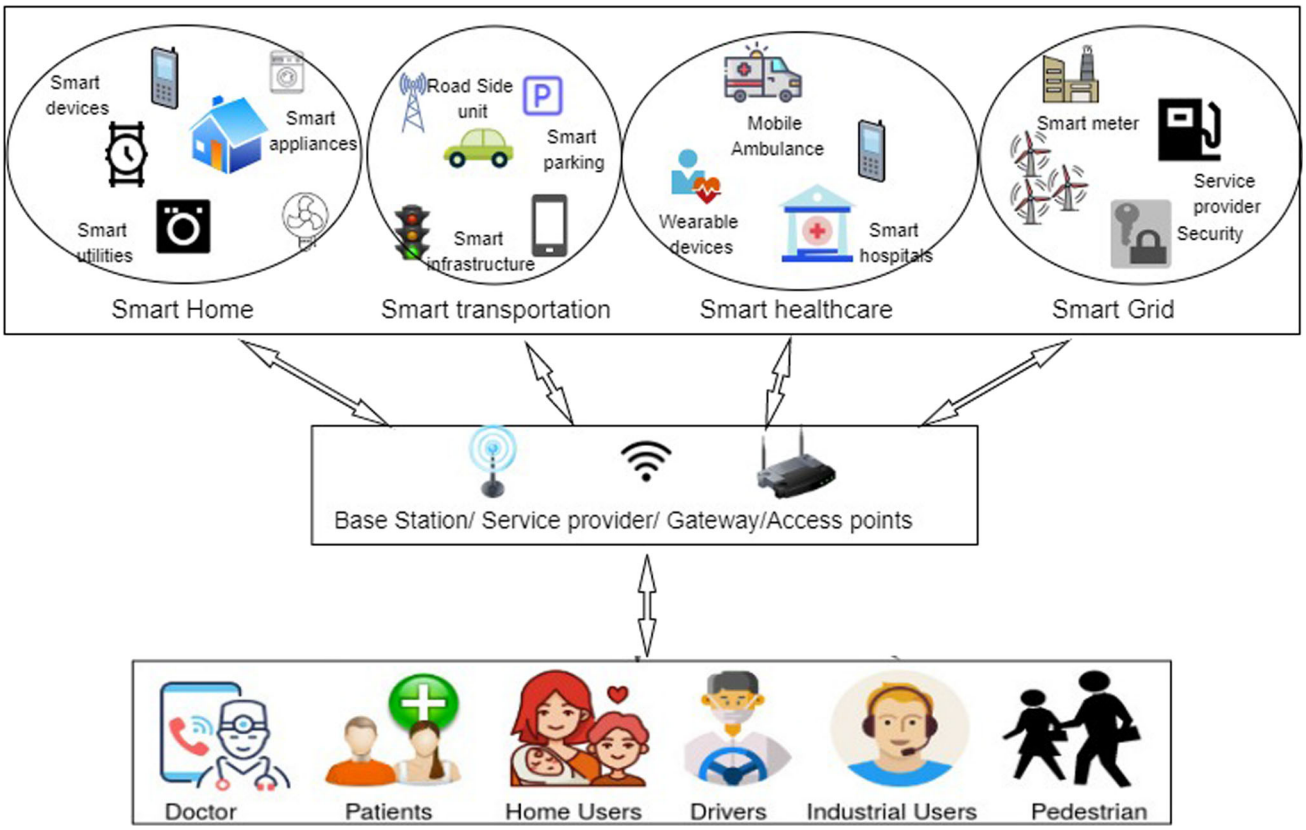

Fig. 1 Generic architecture of IoT

meter's reading; increasing the reading of others in the society so that the total bill of the community remains same. The system in integration with machine learning keeps a check on the energy consumption of the appliances and detects the theft if there is any change in pattern.

IoT can also be implemented to form a smart grid system [8]. Blockchain based smart grid as an application is proposed in [9] where all service providers are assigned the responsibility to validate and add the blocks in the blockchain using consensus algorithm. Service providers also allots the energy and monitors the energy trading system. IoT enabled smart meters controls the power consumption and billing of the customers. The scheme claims to overcome all the limitations of existing power systems by providing a reliable and sustainable system. Under this, power organizations would have full control over power consumption, distribution, transmission and generation.

Coronavirus disease (COVID-19) pandemic which had hit the world in 2020 was a challenge for the health care system through out the world as there was no vaccine or cure of the contagious disease. The only solution to stop and prevent the spread of the disease was home isolation and maintaining physical distance with people around to break the chain of spread. The potential application of IoT can be used to overcome the pandemic situation. The Covid-19 causes respiratory problem, change in body temperature, cough, drop in oxygen saturation, fluctuating heart rate etc and have been proven more easily communicable than SARS which had hit the world in 2003. Better monitoring over the health care and proper surveillance, the communicable disease would have less chance of spreading. Artificial intelligence integrated with IoT could contribute in many ways such as implementing Internet of Drones (IoD) to supply food, necessities and disinfectants avoiding people's access in social places, tracing the contacts and recognition systems, using Bluetooth as a service to calculate distance between people. Vedaei et al. [10] proposed a COVID-FREE framework consisting of IoT nodes, smart phone, fog servers. In the scheme, IoT devices/nodes or wearable devices are used to monitor the symptoms of every individual. A smart phone application notifies the risk factors to the user and advices to maintain distance. Fog servers are used to collect the data to apply machine learning and artificial intelligence, in order to send important information to users. Finally the stored information can be used to control the pandemic.

Another IoT application in smart health care is proposed in [11] where a framework to flexibly monitor electrocardiogram of a heart patient and collect the long distance ECG signal is formulated. The scheme is of economic benefit as the equipment is expensive and would also reduce the need of

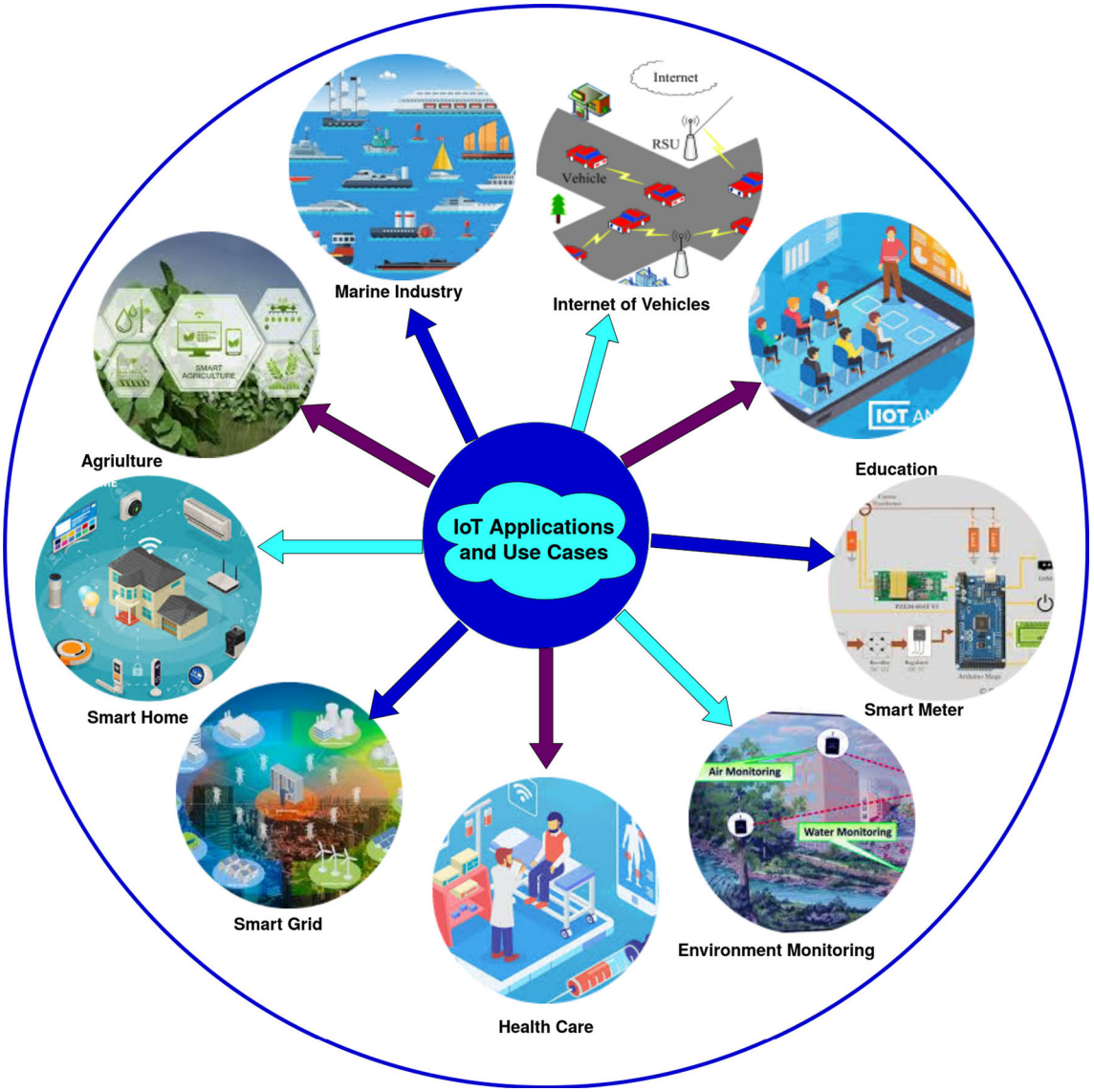

Fig. 2 Various applications of IoT

patients and elderly people to visit the doctors every time for the test. IoT based light weight sensors are used to collect the data and signals which is sent to the health care department using Internet with reduced bandwidth and traffic. In [12] a bio sensing mask is proposed which can be used for recording the facial expressions that can notify the occurrence of pain in the body of user. It connects the patients with their caretakers and health care centers over cloud. They also proposed an extendedly advanced data analytical techniques such as machine learning and big data analysis to synchronize collected data.

IoT could also be used to monitor environmental conditions. It can play a lead role in detecting the occurrence of any kind of natural calamity such as storms, earthquakes, high tides, flash floods, tsunamis, etc. Smart environment management can also be used to detect any forest fire at early stages, estimating snow falls in polar areas, early detection of possibility of land slides to prevent mishappenings, etc. The warning or alarm from such a scenarios can save a lot of man kind through out the world. It can even notify the relief and rescue team to quickly track and reach the affected area to provide help as soon as possible. In [13] authors proposed to collaborate open data source and crowdsensing to aggregate data for end devices to provide valuable services. Moreover, deployed IoT sensors at factories monitor environmental pollution and chemical leaks in water supply, detect smoke and toxic gases and temperature sensors coupled with warning systems to prevent ecological disasters.

With the advancement and evolution in the age of IoT, IoT has also shown progress in marine and naval engineer-

ing. The development has expanded trading of goods via waterways and has increased the sea traffic. The increased sea traffic has vulnerabilities in the communication between the ships and ports, leading to delayed arrival and departures along with major green house emissions and ocean pollution. Internet of Ships (IoS) paradigm is interconnection of smart ships, smart ports, as well as smart transportation that is faster than satellite communication used earlier. IoS would help the ships to communicate with other ships, easy and quick detection of routes, uninterrupted Internet facilities, automatic loading, unloading, berthing , collision avoidance, safety enhancement, real time tracking, collaborative decision making etc. In [14], authors designed an IoS architecture as five layered architecture: sensing layer, heterogeneous network layer, data computation layer, service & application layer, and exhibition layer.

IoT has shown its prominent application in smart agriculture as well. Agriculture is the weapon against hunger and poverty in the country. It forms the backbone of most economy and GDP in India. Implementing IoT in the field of agriculture will not only increase the economic benefits but also the quality of rural agriculture even in antagonistic conditions where the weather and climate is extreme. IoT sensors, devices can be deployed in the soil in agricultural fields which can collect the data regarding weather condition, the quality of soil, amount of insecticides needed to keep the quality of crops maintained. In the paper [15], the authors proposed an intelligent IoT-Based System Design for Controlling and Monitoring Greenhouse Temperature that collects the data and helps the end users to use the data stored in cloud to increase the productivity and also to create an automated system to save energy and cost. The system maintains the temperature inside the green house by monitoring and regulating the outside temperature by monitoring sun rays and energy consumption during peak hours. Ayaz et al. [16] redefined the application of IoT in the field of agriculture by using the potential farming practices integrated with IoT devices through out all the stages from sowing to harvesting to transportation. The sensors can be used for soil preparation, crop status, irrigation, insect and pest detection, aerial crop surveillance and optimising crop yield.

Additionally, another evolving IoT application is in smart mining where autonomous, self-driving mining equipment can be deployed to keep workers away from unsafe areas, while location and proximity IoT sensors allow miners to avoid dangerous situations. The combination of smart transport, smart homes, smart disaster management, smart metering, etc. evolves a city into smart city. Various countries are evolving their cities into smart city to add luxury to the life of citizens by collaborating with their government.

1.3 Motivation

IoT network allows the devices and sensors to communicate with each other to share and collect the information on an open public network. The open network not only allows attacker to passively eavesdrop the network, but also actively attack the network. The scalablity of the network poses a major challenge to use and save the vast rich information effectively and efficiently mostly in real time networks. Since the data is huge in volume, the storage, retrieval, privacy and maintenance are the major issues. Therefore, it becomes utmost important for an IoT application to safeguard secret information in order to provide effective service application [5].

IoT devices like sensors and wearable devices are generally resource constrained and have limited battery capacity. The devices can even be physically captured by an adversary, because they reside in a hostile network where monitoring them in 24×7 is not always possible. Also, IoT applications being scalable in nature allow deployment of new devices. Under this scenario, an adversary might deploy certain malicious devices to harm the integrity of the network by accessing the sensitive data. This can interrupt the smooth flow of information in the network by inserting false data. So, distinguishing between a valid authenticated device and a malicious device is a tedious and an important task.

Access control mechanism is a methodological approach implemented before the deployment of the network, to solve the above stated problems. Access control mechanism controls the flow of false, invalid, illegal and unauthorized information within the network. It manages access permissions, monitors the scalable IoT architecture, handles huge amount of data stream, and also keeps a track of allocation and utilisation of resources in the network. It also ensures that no malicious devices are deployed in the network.

An access control mechanism preserves privacy and security in an IoT environment, as it blocks unauthorized users to access resources, prevents authorized users to access resources illegally. It only permits authorized users to access resources in an authorized manner.

An access control scheme consists of two tasks: *node authentication* and *key establishment*.

- In *node authentication*, a deployed node needs to prove its identity to its neighbor nodes and also to prove that it has the right to access the existing IoT network.
- In *key establishment*, the secret shared keys need to be established between a deployed node and its neighbor nodes to protect secure communications among them.

There could be various access control methods like hierarchical data confidentiality, managing accessing objects manually, assigning resources based on rules, assignment

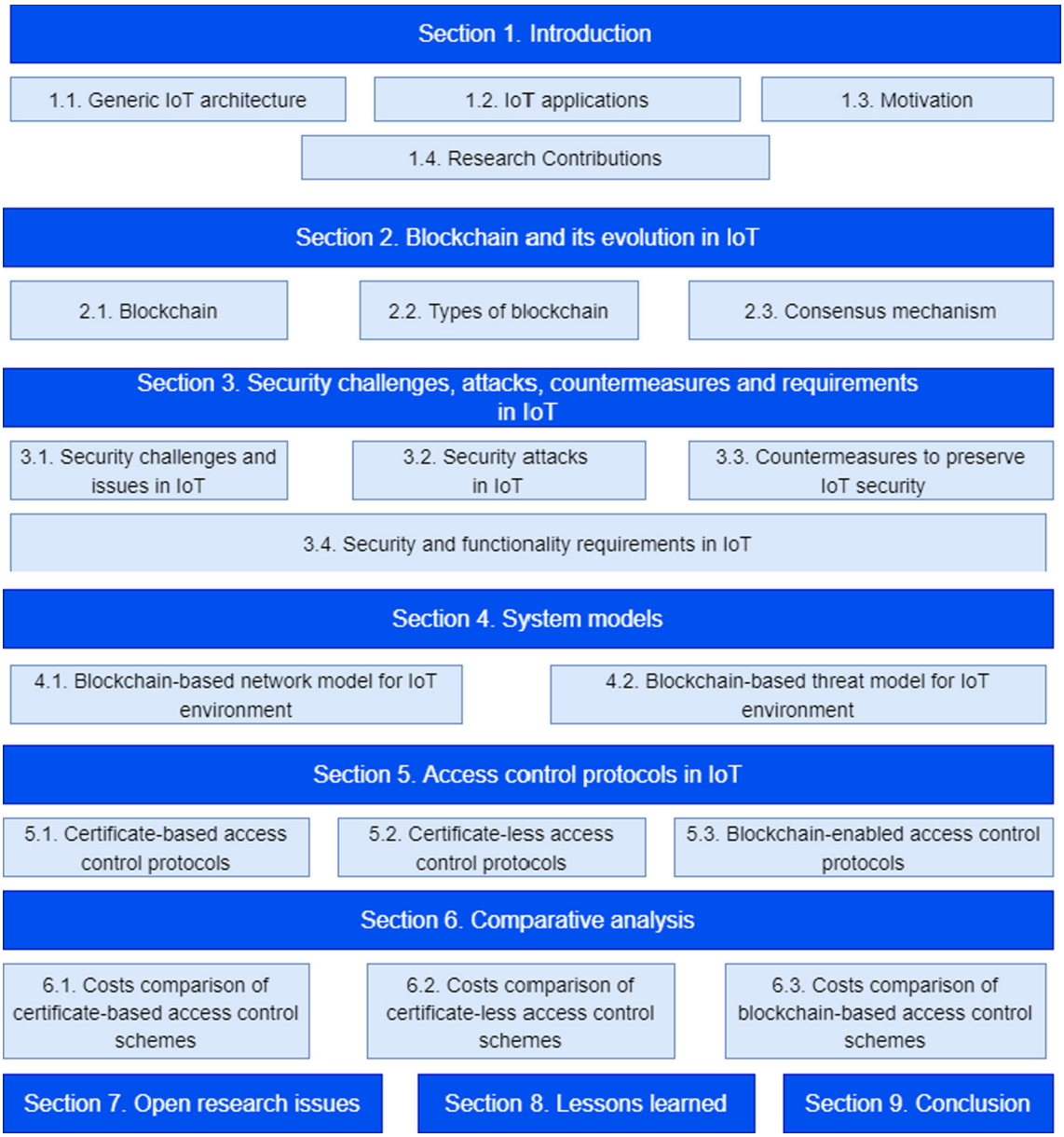

Fig. 3 Roadmap of the paper

based on roles, creating assigning rules based on attributes of the users etc.

In this paper, we summarize few access control mechanisms with their comparative analysis. The readers would be benefited with proper understanding of how access control mechanism can be applied in almost all applications of IoT. Figure 3 presents the roadmap of the paper.

1.4 Research contributions

1.4.1 Existing surveys on security protocols in IoT

In the recent times lots of surveys are already performed on IoT and blockchain technology. Table 1 compares existing surveys on security protocols in IoT environment against our survey. The comparison includes the key areas like IoT applications, security and privacy issues and requirements, IoT attacks and countermeasures, threat models, blockchain in IoT and future research directions/ open issues etc. We also summarize the key areas covered in each survey. It can be seen that our survey excels in coverage of information than the other existing surveys in content and comprehension.

1.4.2 Main contributions

The main contributions of the paper are listed in following points-

Table 1 Existing surveys on security protocols in IoT environment

References and year	IoT applications	Security and privacy issues and requirements	IoT attacks and countermeasures	Threat models	Blockchain in IoT	Future research directions/open issues	Key areas covered
[17], 2015	×	✓	×	×	×	✓	Analysis of technologies currently being used.
[3], 2015	×	Protocols at different layer	×	×	×	✓	Summarizes most relevant protocols and application issues and on how different protocols fit together to deliver desired functionalities.
[12], 2017	×	Security at different layers	✓	×	×	×	IoT security at different layers is discussed. Also covers limitations of IoT devices.
[18], 2017	✓	✓	✓	×	×	✓	Describes IoT reference models. List of attacks and countermeasures against them on the edge-side layer of IoT.
[19], 2018	✓	✓	✓ (only attacks)	✓	×	✓	Taxonomy of various security protocols in IoT is provided.
[20], 2019	×	✓	✓	×	×	×	Explains IoT protocol architecture and provides various IoT solutions to attacks.
[21], 2019	✓	Security at different layers	✓	×	✓	✓	States improvement and enhancements for upcoming IoT applications.
[22], 2019	✓	×	×	×	✓	✓	Discusses the new paradigm as synthesis of blockchain and IoT as Blockchain of Things (BCoT). Taxonomy of blockchain systems is provided.

Table 1 continued

References and year	IoT applications	Security and privacy issues and requirements	IoT attacks and countermeasures	Threat models	Blockchain in IoT	Future research directions/open issues	Key areas covered
[23], 2019	✓	✓ (blockchain-IoT)	Only attacks	✓	✓	✓	Covers taxonomy and a side-by-side comparison of the state-of-the-art methods toward secure and privacy-preserving blockchain technologies.
[24], 2020	×	×	✓	×	✓	×	Prevention, detection, and mitigation of attacks towards IoT classified according to different layers is excellently conveyed.
Our survey, 2021	✓	✓	✓	✓	✓	✓	Comprehensive survey on IoT paradigm, blockchain technology, evolution of blockchain in IoT and blockchain envisioned access control protocols.

- The main aim of the paper is to provide a thorough understanding on access control protocols in IoT applications.
- First, we give a detailed overview on IoT, its architecture, various security and functionality features. We also highlight security issues, threats and attacks possible in IoT paradigm along with their counter measures.
- Then, we discuss on blockchain and its evolution in IoT. We explain types of blockchain, various consensus mechanisms and their characteristics. We also emphasize on how blockchain can resolve some of the vulnerabilities of IoT.
- To analyze the access control protocols, we present a generic blockchain based access control architecture for IoT applications. In addition to this, we also put the spot light on the threat models considered for blockchain based IoT network.
- Next, we perform a detailed survey on existing access control protocols in IoT. For better organization and understanding we have classified the protocols as certificate based, certificate less and blockchain envisioned access control protocols. We discuss on the mechanism of some recent schemes under each category.
- The paper also elaborates on each use case like smart home, smart grid, health care, smart agriculture etc while describing access control mechanism. The detailed description clearly explains the implementation of access mechanism.
- Subsequently, we also perform a rigorous comparative analysis of the existing schemes and compare them in terms of computation and communication costs.
- Finally, the study opens up few challenges and research directions for future.

2 Blockchain and its evolution in IoT

The communication in an IoT environment takes place openly in an unsecure environment, so it becomes very easy and approachable for the adversary to perform security attacks on the network. Not only this, but an adversary can even trace the messages exchanged in the network. Therefore, blockchain based solutions are one of the most optimistic approach to provide security in an IoT environment and also maintains functionality features like traceability and anonymity.

2.1 Blockchain

Blockchain are basically distributed database whose copy exists in parallel on different nodes in the network [25]. The blocks are added one after the other in a chain such that each block is linked to the hash value of the previous block. The root block in the blockchain known as genesis block. Any

Block Header	
Block Version	$BVer_i$
Previous Block Hash	PBH_i
Timestamp	TS_i
Merkle Tree Root	MTR_i
Owner of Block	OB_i (ES_m)
Public key of signer	Pub_{ES_m}
Block Payload (Transactions)	
List of n_t transactions and their signatures	$\{(Tx_i, Sig_{Tx_i}) \mid i = 1, 2, \cdots, n_t\}$
Signature on all transactions (Tx_i)	Sig_{Block_i}
Current Block Hash	CBH_i

Fig. 4 Generic structure of a block [26]

block of the blockchain consists of version of the block, hash value of the previous block, timestamp value, a random nonce value, and number of transactions within the block. Figure 4 shows the content of a complete block. After the block is formed every node validates the block and the validated block is added to the blockchain and is linked to the previous block by the parent hash value. Therefore, any block added in the chain is impossible to tamper with, and no block can be added in between two already added blocks. This way the records stored in the block are both open and secure at the same time.

Blockchain technology embedded with IoT serves several advantages like transparency, immutability, confidentiality etc.

- *Transparency* For a public blockchain any user can participate to add or validate the block in the blockchain. Similar to this any transaction or block added to the blockchain is accessible to all the users. In private blockchain the data is only open the private authorized users. Also it is easy to track the transactions made by an entity even when it's real identity is secured.
- *Immutability* It means that once a block is inserted into public or private blockchain it is impossible to modify or tamper it later. As the blocks consist of the hash value of the previous block, so any change of the value in a block would affect validity of all the consecutive blocks. Moreover the copy of blockchain is present with every user of the network so conflict in copies could easily be identified.
- *Traceability* Verifying/tracing the data stored in blockchain is possible due to the presence of nonce and also the fact that the data is mapped to the timestamped value.
- *Interoperability* IoT consists of heterogeneous devices thus it faces one major challenge to inter operate with each other. The decentralization feature of IoT makes it a challenging task to exchange data. Blockchain allows various IoT systems and devices to communicate amongst themselves by exchanging data.
- *Reliability* The data stored within the blocks of a blockchain is valid and can be trusted as various cryptographic techniques like hashing, encryptions form the underlying basis for storing data in the blockchains.
- *Decentralization* Traditional database systems were depended on any third party or agency for validation, where as blockchain technology is unique and works independently by using a distributed ledger that validates the transaction within the nodes without consulting or requiring a third party. Using decentralized blockchain technology in an IoT network, reduces the overall communication overheads and also makes proper use of the shared resources within the network.
- When a transaction is added to the block it is digitally signed using private key of the miner which can only be verified by the public key. So, no node can deny the digitally signed transaction added by it into the block.
- Blockchain technology reduces time, cost, dependency on the third party, and security of the data.

Due to above stated advantages of Blockchain, it is implemented in several fields like supply chains [27,28], financial administrations [29–31], VANETs [32,33], UAVs [34,35] medicinal services [36], governments and numerous different ventures, trailblazers, energy, health and medical care [37,38], IoT, digital asset trading, security [39,40], property right protection and education, personnel big data management system [41], truth discovery [42], etc. Figure 5 shows the applications of blockchain in various fields.

Blockchain has shown prominent benefits in IoT paradigm. The shortcomings faced by IoT paradigm are overcome and complemented by the advantages of blockchain technology. Table 2 shows how blockchain can be used to solve various vulnerabilities and shortcomings of IoT security.

2.2 Types of blockchain

Blockchain technology can be categorised into three categories: public blockchain, private blockchain and consortium blockchain.

- **Public blockchain** Public blockchain also known as permission less blockchain works in an open environment like Ethereum, Bitcoin where anyone is allowed to join and write the shared blocks. Every participant in public blockchain is given equal privileged in drawing a consensus in consensus mechanism. Public blockchains completely abide by the properties like non-repudiation, transparency and traceability. Scalability is an issue in

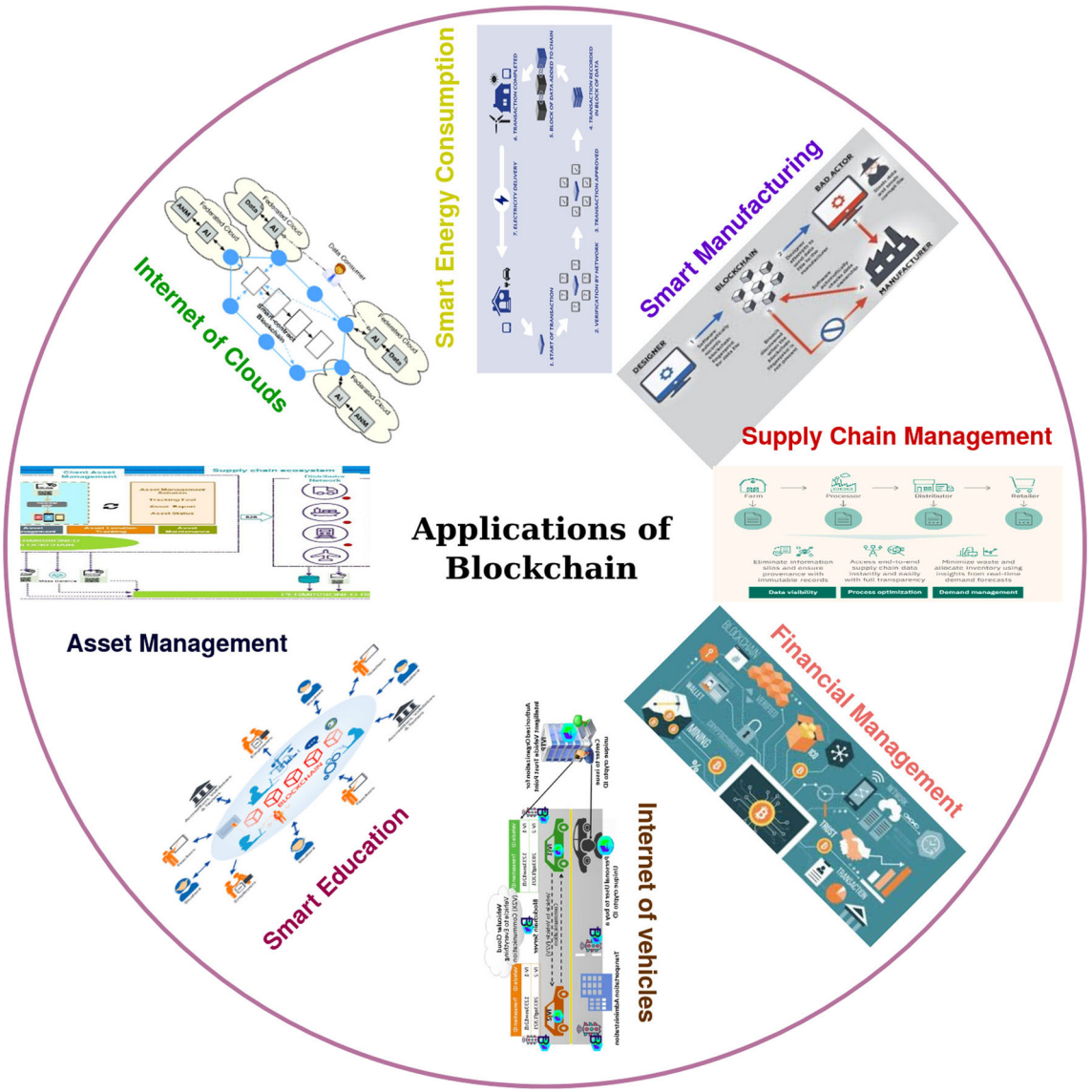

Fig. 5 Various applications of blockchain in IoT environment

such types of blockchains, as the rate of validation of blocks increases with increase in number of nodes.

- **Private blockchain** Private blockchain [43] like Hyperledger, multichain fabric works in a closed environment where all the participants allowed in the process are well known. Private blockchain is also known as Business blockchain [44]. Public and private blockchain differ in the way they allow users to access, store, modify, send, receive transactions. Public blockchains are open to all, that is anybody can access the blockchain, where as in private blockchain only trusted entities are allowed to access the blockchain thus forming a trusted network. In private blockchain only the authoritative entity assigns specific tasks to the trusted entities to perform. Private blockchains are more scalable than public as the users are monitored by a centralized group.
- **Consortium blockchain** A hybrid approach combining both public and private blockchain in order to reach to consensus in a peer to peer network is called consortium blockchain. The access in consortium blockchain is given to pre-defined set of nodes. Any new node that wishes to join the network should be authenticated and authorized. Private and consortium blockchain are known as permissioned blockchain.

2.3 Consensus mechanism

Blockchain technology does not rely on the third party for validation and verification. Unreliability on the third party

Table 2 Blockchain as a solution for IoT security

IoT security issue	Blockchain as a solution
Stored heterogeneous data in the cloud is open and prone to attacks	Blockchain can be used to store and transmit data as it is immutable and hashed data is stored in the chain. Also Enhances interoperability as the data exchange via blockchain is flexible.
IoT application is spread over vast areas and is based on cloud for storing	As IoT application can have a single point failure so blockchain can help by providing decentralisation and easy storing of data irrespective of the distance
Security of data	The transactions compiled in the block are encrypted and blockchain stores the hash of the data, and so these are secured against threat on data. Any change in the data would change the hash value of blocks.
Validity of data stored	The data stored in blocks of a blockchain is verified by many miners so the probability of storing fabricated or corrupted data is less.
Data can be lost or misused	Blocks once added to the blockchain cannot be deleted or removed and the users in the blockchain are registered initially so no adversary can imitate being an authenticated user to spoof the data.
Unauthorized data access	The data stored in blockchain is stored using public-private keys, so no unintended user can access the actual content of the data. It also provides non repudiation.
Privacy of an IoT application	Private and public blockchain can be used for IoT application designed for private users and for application that is open for all .

is due to the mechanism which is followed to validate the information and add the transactions to the block and the blockchain. The mechanism is called as *consensus mechanism* [45]. Consensus means a process to arrive at an agreement in a decentralized or distributed network platform where the nodes cannot trust each other. Consensus mechanism is a procedure like a state machine running on every node in the network so that every individual concludes on the same output. Consensus mechanism is an algorithm which helps the miners to validate a transaction and come to the conclusion of adding or dropping a block in the blockchain. It ensures a tamper free environment where one version of the truth should be agreed upon. It solves the problem of trust in blockchain, as all the non trusted miners participating in the process undergo a similar algorithm to agree on the validity of the block. Consensus algorithm also mitigates the effect of presence of faulty nodes in the network. All the nodes must reach to an agreement about the state of blockchain.

A consensus mechanism should have following properties.

- **Consistency** The result of a consensus algorithm is such that all nodes should agree on the same block.
- **Validity** The agreed block should be the block that receives the majority consensus.
- **Liveliness** Eventually the algorithm should terminate; that is, the nodes should decide on some block.

Choosing appropriate consensus algorithm is the most important part of implementation of effective blockchain solution. The choice of the consensus algorithm is based on various factors like [46]-

- Type of blockchain: public, private or consortium.
- Scalability of the network.
- Tolerance to withstand attack or failures like node failures, partition failure or byzantine failure.
- Low latency
- High throughput
- Low bandwidth
- Less complex
- Minimum energy consumption.

Consensus algorithm basically can be classified into two types: (1) Proof based and (2) Voting based. In proof based consensus algorithm, the nodes having the highest compu-

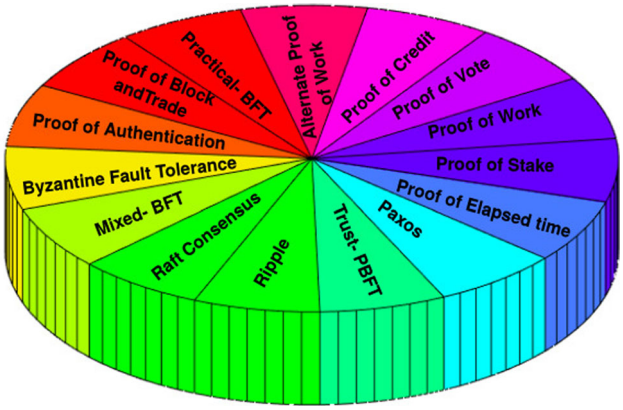

Fig. 6 Various consensus mechanisms in Blockchain technology

tational power is given the right to append the block to the blockchain. Proof based consensus is basically used in public blockchains. Voting based algorithm are preferred in private blockchains, where a block can be added to the blockchain only after threshold number of nodes have agreed on it. Any node who wishes to append a block needs vote of its peer nodes to get the consensus to add the block [47].

Figure 6 represents different consensus mechanisms in blockchain environment.

We briefly discuss few consensus algorithms.

- In *Proof of Work* [48], the miner has to do some heavy computational work to calculate a nonce value based on previous block's hash value to add the block in the blockchain. The work to add/tamper the block is based on all the blocks in the blockchain, and should be heavy and not be possible to be performed in generic environment to discourage an attacker. PoW requires heavy energy consumption which makes it infeasible to apply in IoT environment.
- *Proof of Stake (PoS)* [22], [49] mechanism chooses the miner based on economic stake or bit coins that it holds. Adversaries can increase number of transactions to increase stake which might also lead to unfair method of choosing a leader.
- Similar and better to PoS, is *Proof of Credit (PoC)* [58] consensus protocol, where credit does not depends on the bits or account balance of the miners but on their behavior. No attacker can deliberately increase the credit, it only depends on the positive behaviour of the nodes in favour of the network. It requires less power consumption than PoW.
- To reduce the amount of energy and resources, an *Alternative to PoW* Alt-PoW [60] is proposed. The main idea followed in Alt-PoW is- instead of performing heavy computation at once to win a chance to mine a block, a miner has to mine multiple chain problems to reach to mine a block. This way there can be multiple chains where the miners can start computing their chain parallely. The miner who finishes up first through all the rounds in the chain makes up to mine a block. Others can drop or change their chosen chain in initial rounds to avoid wastage of energy and resources.
- *Paxos* [50], another consensus algorithm implemented in private blockchain is used to choose a single value. A proposal node chooses a value and sends it for majority to accept it. Once the accepter nodes accept the value, the value is announced to the learner nodes.
- In *Raft* [51] algorithm, one of the nodes is elected as sender based on the majority of votes on the request messages received from volunteering nodes. Rest nodes become the follower nodes. The leader node chooses a value for the follower nodes to reach the consensus. PoW cannot be applied in IoT application as it requires energy efficient computing, real time decision making.
- *Proof of Authentication (PoAh)* [57] is a light weight consensus mechanism which is applied in IoT application which authenticates the block after following the traditional method of consensus. The miner nodes can be used for authenticating the block, and a reward is given to the node that authenticates the block first.
- To overcome the limitations and to justify decentralization property of blockchain, *Proof of Vote (PoV)* [59] consensus mechanism is proposed for consortium blockchains. The network nodes are categorized into four categories: 1.Butler, 2.Butler candidate, 3.Commissioner, 4.Ordinary User. Several enterprises form a consortium network and commissioners are the members of the league. A butler is a node that can create a block like miners in PoW. A butler is chosen out of the butler candidates by a commissioner unlike PoW where they have to prove their power. A node can willingly become a candidate by registration and recommendations. A block is added to the blockchain based on the votes of commissioners. Ordinary user can only distribute the message but cannot take part in the block formation.
- *Proof of Elasped Time (PoET)* [61], another consensus mechanism which depends on random waiting time. The first node that finishes waiting is elected as a leader.
- *Proof of Space* [62] elects the member as a leader which offers maximum disk space.
- *Byzantine fault tolerance (BFT)* [52] algorithm helps a group of nodes within a closed network to reach a consensus even in the presence of faulty nodes. The algorithm runs in pre-prepare, prepare and commit phases. Once the message sent in the pre-prepare phase is accepted by $2f + 1$ nodes where f is the number of faulty nodes, the message is accepted.
- *Practical Byzantine fault tolerance (PBFT)* [53] algorithm is a variant of BFT and it reaches to consensus

with $3f + 1$ accepting nodes. The consensus is reached in pre-prepare, prepare and commit phases. PBFT has low scalability.

- To overcome the scalability issue, *EigenTrust-Based Practical Byzantine Fault Tolerance (T-PBFT)* [54] algorithm only includes the group of nodes with higher trust value. The algorithm performs node trust evaluation process using Eigen trust model [63] based on the transaction history between nodes which have direct or indirect connection, followed by construction of consensus group including the nodes with highest trust value and finally consensus process.
- *Mixed Byzantine fault tolerance (MBFT)* [55] is another consensus algorithm which improves the scalability issue. It follows sharding technique and a two layered process, by dividing the whole network into two groups as low level consensus group and high level consensus group. Each node in the network is either a verifying node or synchronizing node or backup node. Verifying nodes have high trustworthiness and have won election and are responsible to verify the transaction and package a block. Back up nodes verify the block packaged by verifying nodes. Rest, synchronizing nodes or clients initiate requests.
- *Ripple protocol* consensus algorithm is another voting based consensus algorithm. All participating nodes maintain a list of trusted nodes called as "Unique node list". Participant nodes receives the transaction constantly throughout the process. If the transaction is valid, it is added to the candidate set. All the participating nodes exchange their candidate set with each other as proposals. On receiving proposal, the transaction is checked for validity only if it comes from the trusted neighbouring node. A transaction that gets more than 80 percent of votes is added to the block.
- Specifically for IoT application, Biswas *et al.* proposed a *Proof of Block & Trade (PoBT)* [56], a light weight consensus protocol which provides security during the verification of the trade as well as block. The protocol works in two steps. Initially, the trade received is verified by the source node and then the verified trade is added to the block. Finally, consensus is performed on the candidate block that contains several verified trades by the orderer node whose responsibility is to integrate the verified trades into the block.

Various blockchain consensus mechanisms and their applications are then summarized in Table 3.

3 Security challenges, attacks, countermeasures and requirements in IoT

In this section, we discuss various security challenges and issues, attacks and their countermeasures, and also security and functionality requirements related to an IoT environment.

3.1 Security challenges and issues in IoT

Security and privacy issues including key management, authentication and access control are vital issues in various networking environments. Various schemes proposed in the past had tried to overcome the issue by providing a solution. In [64], an authentication scheme for medicine anti counterfeiting system used for checking the authenticity of pharmaceutical products is proposed. Similarly, a secure password-based authentication and key agreement scheme using smart cards for the telecare medicine information system is proposed in [65]. Another healthcare solution is provided in [66]. Odelu *et al.* in [67] designed a secure and efficient authentication protocol for near-field communication (NFC) applications using lifetime-based pseudonyms. Further, in [68], an access control protocol for wireless sensor networks is also proposed. This scheme is secured against various attacks. A lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment based on bitwise exclusive-or (XOR), one-way cryptographic hash and bitwise rotation operations is provided in [69]. Few other schemes like the scheme in [70] was designed to provide a key establishment mechanism. Another solution in the field of Internet of Drones (IoD) is provided in [71] that explains a mechanism to secure data delivery and collection. The overall security and privacy issues, and a taxonomy of IoT are provided in [19], [72].

IoT involves data accumulation, information integration, processing and storing for data analysis. The data is made available to anywhere and everywhere through out the processing [20]. Other features of IoT such as centralized control, transparency, poor interoperability creates privacy and security issues including energy trading between untrusted/non-transparent networks [21]. There are various security challenges in an IoT network which makes the network more vulnerable to attacks, which are discussed below.

- *IoT hardware* Various IoT devices such as sensors, wearable devices, digital gadgets, microcontrollers like

Table 3 Blockchain consensus mechanisms and their applications

Consensus mechanism	Algorithm	Advantages/limitations	Type of blockchain
PoW [48]	Chooses the first miner who finds a nonce value based on computation of mathematical problems	*Advantage:* Works well for real time applications	Public Blockchain
		Limitation: Suffers from Sybil attack and DoS attack.	
PoS [22], [49]	Chooses the node with highest stake (bit coins)	*Advantage:* It solves monopoly problem	Public blockchain
		Limitation: Suffers from Nothing-at-stake attack	
Paxos [50]	Proposal node chooses a value to have a consensus on	*Limitations:* Suffers from Starvation	Permissioned blockchain
		No consensus can be reached if$(N/2-1)$ nodes fail.	
Raft [51]	Elected node becomes a leader and chooses a value to agree on	*Advantage:* Highly efficient	Private blockchain
		Limitation: Does not support byzantine nodes	
BFT [52]	Pre-prepare, prepare and commit phases to reach consensus.	*Advantages:* Consumes less power during computation.	Private blockchain
	Reaches consensus if (2f+1) nodes accept message, f:number of faulty nodes		
PBFT [53]	Variant of BFT algorithm	*Advantage:* The algorithm consumes less energy	Private blockchain (Tendermint Core)
	Reaches consensus if (3f+1) nodes accept message, f:number of faulty nodes.	*Limitation:* The algorithm is non scalable and suffers from sybil attack.	
TBFT [54]	Consensus amongst the nodes with high trust value	*Advantages:* Optimal byzantine fault tolerance rate and is highly scalable	Consortium blockchain
MBFT [55]	A two layered consensus process based on sharding technology.	*Advantage:* The scheme is scalable.	Permissioned blockchain
		Limitation: Does not block forking of the blockchain	
PoBT [56]	Two step process of trade verification followed by consensus formation	*Advantages:* Does not allow malicious nodes to commit.	Private blockchain
		Validation of blocks in decreased time.	
PoAh [57]	The block undergoes authentication after traditional consensus.	*Advantage:* Best for resource constraint application like IoT	Public blockchain
PoC [58]	Node with positive behaviour has the maximum credit and wins the chance to mine.	*Advantage:* Fair election method in favour of the network.	Private blockchain
PoV [59]	Members are allowed to vote, block with highest votes is added to the chain.	*Advantages:* Low power consumption, latency	Consortium blockchain

Table 3 continued

Consensus mechanism	Algorithm	Advantages/limitations	Type of blockchain
		No bifurcation or forking in blockchain	
Alt-PoW [60]	Multiple chains of multiple small problems to add a block in the chain .	*Advantages:* Avoids wastage of resources and power	Public blockchain
		Nodes can back off and mine in some other chain in which they have more chance of winning.	

Arduino, Raspberry pi and embedded hardware are small in size with other hardware constraints. The devices are connected to Internet almost all the time so users are at continuous risk. Hardware life cycle, software updates, access control and device authentication are other challenges that the enterprises and manufacturing industries should take care of.

- *IoT software* The software designed for various IoT devices is based on purely the requirement of the sensor nodes it is installed in. The security issues are not properly dealt with within an IoT software. Storage capacity, huge volume of data are some of the other concerns. Installing firewall or gateway could be possible solutions to protect the software attacks.
- *Open communication* IoT network gives a privilege to any device to communicate with any other device, just by providing IP addresses. But the communication is open and the network is all time exposed to the attacker. Due to increase in IoT devices every year, it is impossible to set a boundary around a network. Therefore, protecting the network from the attackers is again a huge task.
- *Open Cloud storage* The data collected by the sensors is collaborated and stored in the cloud for further analysis. The data can be also shared to other entities. So if a cloud is not configured properly, it may lead to data leakage. A continuous cloud monitoring is requires as a preventive measure.
- *Limited upgradation capacity* IoT devices should be able to upgrade the software with minimal intervention of a user, whenever they are connected to the Internet [73].

In addition, authentication, confidentiality and integrity are also the major security issues in IoT. The following issues raise which we consider such security issues [74]:

- *Devices with restrained capacity* The IoT devices are generally wearable devices or sensors that have limited battery capacity. Running heavy computations on such devices can lead to sensor drops and weak connectivity links [75].
- *Non-trusted network* An IoT network is a group of heterogeneous devices that are varied in both nature and location. Therefore, management of trust amongst non trusted nodes becomes an important issue.
- *Heterogeneity* The IoT network is a Device to Device (D2D), Human to Device (H2D) network that consist of devices of diversified functionalities. Therefore, compatibility between the entities should be managed [76].
- *Secured access control* The data collected by the sensors is generally stored on cloud for further analysis. The stored data can be used by any entity or process. Secured access by authorized entities can safeguard the open network.
- *Privacy management* To have a safe flow of communication within an IoT network, management of identities to maintain anonymity is important. The identities of entities should be hidden so that attacker cannot trace their actions to misuse them illegally [21].

3.2 Security attacks in IoT

Due to the above discussed issues and challenges, few possible security attacks on IoT are stated as follows [77], [19] [78].

- *Replay attack* Under a replay attack, an attacker records the messages flown in the network and then sends the already sent message again without decrypting in order to get an unauthorized access in the network. Timestamps, random numbers is used in some schemes to resist replay attacks.
- *Man-in-the-middle attack* An attacker in man-in-the-middle attack takes control over the communication channel between two legitimate honest nodes without their knowledge. He can listen intercept/modify/delete the messages in between before the message reaches the intended receiver. Authentication protocols, symmetric polynomials, establishing pairwise session keys, makes it difficult for the adversary to perform man in the middle attack [79].

- *Impersonation attack* In an impersonation attack, an attacker monitors the messages sent by a legitimate node in the previous session. Then he/she modifies and uses the content of the message (basically the identity) to create a valid request to access the network illegally on behalf of an honest node. Impersonation attack can be user impersonation attack, sensor impersonation attack. Biometric and passwords and using anonymous identities resist impersonation attacks. Hashing as mechanism of authentication can also be used to avoid impersonation attack in sensor network.
- *Forging attack* Through forgery attack an attacker can steal confidential information [80].
- *Cloning attack* Extension to impersonation attack is cloning attack under which an attacker creates multiple clones or replicas of a compromised node whose identity is known to him. Attacker gets more opportunity to explore the network, moreover the network suffers from storage overheads, high computation etc.
- *Stolen verifier attack* Registration entity generally stores the user's login id and password in a table to use it further for verification. Under stolen verifier attack, an attacker might steal the stored information and use it to access the network illegally. Therefore in an user authentication scheme, registering entity should not store password tables in order to resist stolen verifier attack.
- *Password guessing attack* An adversary via password guessing attack, guesses the password of the user in an online or offline mode by the help of the content in the messages flown in the network. Once an adversary fetches the password, he/she can access the network illicitly.
- *Activity tracking attack* In activity tracking attack, the attacker monitors the behavior and activities of the genuine user by continuously tracking the session or the messaged exchanged by them. An attacker can then use the monitored stored information to launch other attacks.
- *Message modification attack* In message modification attack, an adversary changes the data or information in the message to misguide the network entities.
- *False message attack* In false message attack, an attacker misleads the receiver by sending false messages continuously to exhaust the receiver's cache.
- *Session key leakage attack* In session key leakage attack, an attacker eavesdrops the session key and other ephemeral secrets and can use the credentials to create a new session disguising the legitimate honest node.
- *Node capture attack* It is the kind of an attack where an intruder captures few nodes in the the network and can compromise the entire network. The resilience against the node capture attack states that even when few nodes in the network are compromised, it should not compromise secure communication links not involving the compromised nodes directly [81].
- *Denial-of-Service (DoS) attack* Under DoS attack, an attacker overwhelms the network by sending multiple requests to a node more than the network's capacity. DoS attack makes the system unavailable for the legitimate user obstructing availability of the network. DoS attack can be caused due to hardware failure, software bugs or exhausting resources. Flooding messages in the network is a type of DoS attack.
- *Distributed DoS attack* DDoS attack is an advanced version of DoS attack where an attacker uses a huge network to bottle neck the existing network so that the server gets overwhelmed and denies to provide service to legitimate users. IoT botnets can be used to perform DDoS attack [82].
- *Privileged insider attack* Any privileged user of the edge server can find out the genuine login details or credentials of the user to create a valid login request to launch an insider attack.
- *Masquerade attack* An attacker creates a fake login request by spoofing, stealing the legitimate user's identity, password or behaviour and convinces the server that it genuinely came from the legitimate user. It creates two different senders of same identity [83].
- *Eavesdropping attack* An eavesdropping attack is a passive attack where an attacker eavesdrops or spies the messages that are exchanged during mutual authentication or key establishment phases. It can be an active attack, if the attacker tries to modify the message by injecting some false data in the message.
- *Sybil attack* An attacker in sybil attack uses multiple identities of the existing or non existing nodes for single malicious device to give an essence of multiple devices in the network. The attack effects distributed storage, availability, consensus voting and fair resource allocations. Using token based authentication mechanism and cluster based approach helps to resist sybil attack [84].
- *Wormhole attack* Under a wormhole attack also known as a tunneling attack, an attacker fakes its closeness to the targeted device by advertising it's wrong location. Thus all the messages are forwarded to the malicious node before anywhere else in the network. The malicious node can replay those messages or can even modify or delete the messages increasing the latency and packet drop ratio in the network.
- *Node replication attack* An attacker in node replication attack can deploy many replicas of the a single device on various places in the network. For this an attacker captures few end devices, fabricates the data and deploys its replicas in targeted positions for further malicious activities. Node replication attack may distort the topology

of the network, data aggregation, resource allocation and may even effect routing protocols.

- *Routing attack* Under routing attack an attacker creates false fake routes misleading the driver to take wrong routes.
- *Phishing site attacks* One of the easiest attacks is the phishing attack as it requires minimal effort by the adversary to launch this attack. The major goal of an attacker in this type of a attack is to compromise the user password and identity so as to compromise the IoT system as a whole.
- *Sniffer attack* An adversary tries to access the user confidential data by monitoring and controlling the network through a sniffer application.

3.3 Countermeasures to preserve IoT security

The increase in IoT devices has led to a vast and open IoT network. Each device can be connected to any and every other device in the network to provide specific service. The devices collect the data and store it in the cloud for future reference or to share it with with other autorised entities of the network. Therefore, open communication and cloud storage makes the network vulnerable and weak against various malicious attacks described in Section 3.2.

Various methods and processes can be followed as general countermeasures to protect IoT applications against various attacks. Some of them are stated briefly below cite-Butun2020, [85].

- The data that is collected and stored in the cloud by various devices, sensors etc should not be stored in the form of plain text. But it should be *encrypted* and stored as cipher text so that the adversary cannot get the meaningful information behind the cloud data, even when the data is exposed.
- Once an IoT device is deployed it becomes difficult to protect it against various false data injection attack and up-gradation of the software or hardware is also critical. Therefore to secure devices against various attacks *rigorous penetration testing* should be performed to be sure of the device to be secured and safe.
- The communication within IoT devices occurs over an open insecure channel. Therefore the data flowing over the network is exposed to the adversary. The best solution to save the data from the attacker is to encrypt the data before exchanging it.
- Another measure to have seamless secure network is to apply an *authentication protocol* always before allowing any device to enter the network [86].
- IoT network is an expanding network as everyday new IoT devices are connected in the network. The paradigm allows any device to connect by providing an IP address to it. So according to this, an IoT network could expand in proportion with the increase in number of devices. So a test to check the *scalability* of the system should be performed to avoid a threat on availability on number of users.
- Using AI based technique can also be incorporated in the future to have a secure IoT network.
- Fog computing in IoT is a collaboration of cloud computing and IoT network. Using *fog computing* storage and integration of data in the cloud is secure and easy to manage. *Edge computing* is also a solution which is different from fog computing as various edge servers are placed between the cloud and IoT devices. Not all activities are performed by cloud as some are taken over by edge servers [87].

Table 4 Attacks and their countermeasures

Attack	Its countermeasure
Tampering	Self destruction mechanism
	Tamper proofing methods
Collision attack	Error collecting code
Flooding attack	Client puzzles
Sink hole attack	Geo routing protocol
Worm/ Black hole attack	Authorisation
	Monitor redundancy
	Using multiple routing paths
Gray hole attack	Immediate acknowledgements
Message injection attack	Pre-testing
DoS attack	Intrusion Detection System
	Firewalls
	Rate limitation
	De-patterning
Sybil attack	Rule based anomaly detection [88]
Node Replication attack	Cryptographic schemes
	(Public key encryption)
Impersonation attack	Attribute based signatures
Man-in-the-middle attack	Secure mutual authentication
Modification attack	Using MAC
Replay attack	Freshness of key pairs
	Using timestamps
Eavesdropping	Blocking
	Personal firewalls
Side channel attack	Timing based methods
	Physical unclonable functions

Table 4 shows few specific countermeasures of few common attacks.

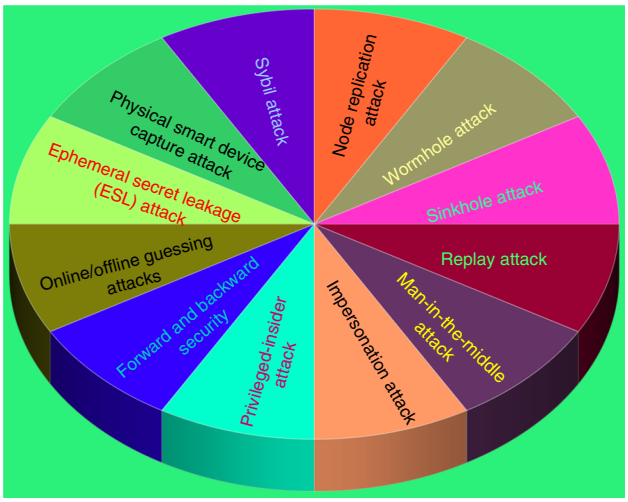

Fig. 7 Various potential attacks in an IoT environment

3.4 Security and functionality requirements in IoT

The security and functionality requirements in an IoT network under an access control are as follows [19]:

- **Resilient against eavesdropping attack** As an IoT network allows multiple heterogeneous devices to connect in the network, it is highly possible that an attacker might eavesdrop or inject false messages into an existing network.
- **Resilient to node capture attacks** If few nodes in an IoT network are compromised then the resilience against node capture attack is measured by fraction of secure communications that are compromised not including the compromised nodes directly. Briefly, for a scheme to be secured against node capture attack, it should not be highly possible for an attacker to decrypt the messages flowing between two non compromised nodes u and v if c nodes are compromised.
- **Resilience against new node deployment attack** IoT is a dynamic network where new nodes connect in the network and old ones leave the network every now and then. Therefore, while deploying a new node in the existing network it becomes very important that the new deployed node should not be a malicious node. The malicious node could be the new node or the the existing compromised node. The deployment of a fair node in the network, resists Sybil attack, worm hole attack, node replication attack etc.
- The entities or the device connected in an IoT network should *mutually authenticate* each other.
- There should be high connectivity within the nodes of network such that it should be easy for the nodes to derive a secret pair wise *session key* to have a secure communication.
- The scheme should inculcate *low storage overhead* on the entities.
- To implement a scheme in practical environment, the number of messages flown in the network to mutually authenticate and to establish a pair wise session key should be minimum. Hence an efficient scheme should have *low communication overheads*.
- Mutual authentication between the nodes followed by pair wise key establishment should involve *low computational overhead.*
- IoT network is a growing network as new nodes or devices are added in the network. So no matter how many nodes are added and the network grows large, the communication and computation cost should remain low.
- To resist the attack by an adversary a scheme should abide by *anonymity and untraceability*, which means that if an adversary gets exposed to the messages flown in the network he should not be able to know about the real sender of the message by the content of the message data.

4 System models

In this section, we describe the general network model and threat model that are used to discuss blockchain envisioned IoT protocols in further section.

4.1 Blockchain-based network model for IoT environment

A general blockchain-based access control architecture in IoT is represented in Figure 8. The model is a layered architecture, with four layers described as follows.

- *IoT domain layer:* This layer is generally the front end layer, which consists of IoT smart devices and sensors connected to each other and the user to form an IoT network. IoT network can be for any application like smart home, smart health care, smart grid, Internet of vehicles etc. The mode of communication is usually wireless using IEEE 802.11p. The sensors and smart devices collect the information, which is passed to the second layer for further processing.
- *Communication layer:* The second layer of the architecture consists of two types of nodes. The first sublayer consists of gateway nodes, Road side units, base stations etc which accepts the information from the first layer and pass it to the upper sub layer. The upper sub layer consists of trusted authorities which are fully trusted. The IoT sensors and devices in the first layer are deployed after registering by trusted authorities via gateway/relay nodes. The communication in this layer is wired and secured. For certificate based protocols, the certificate

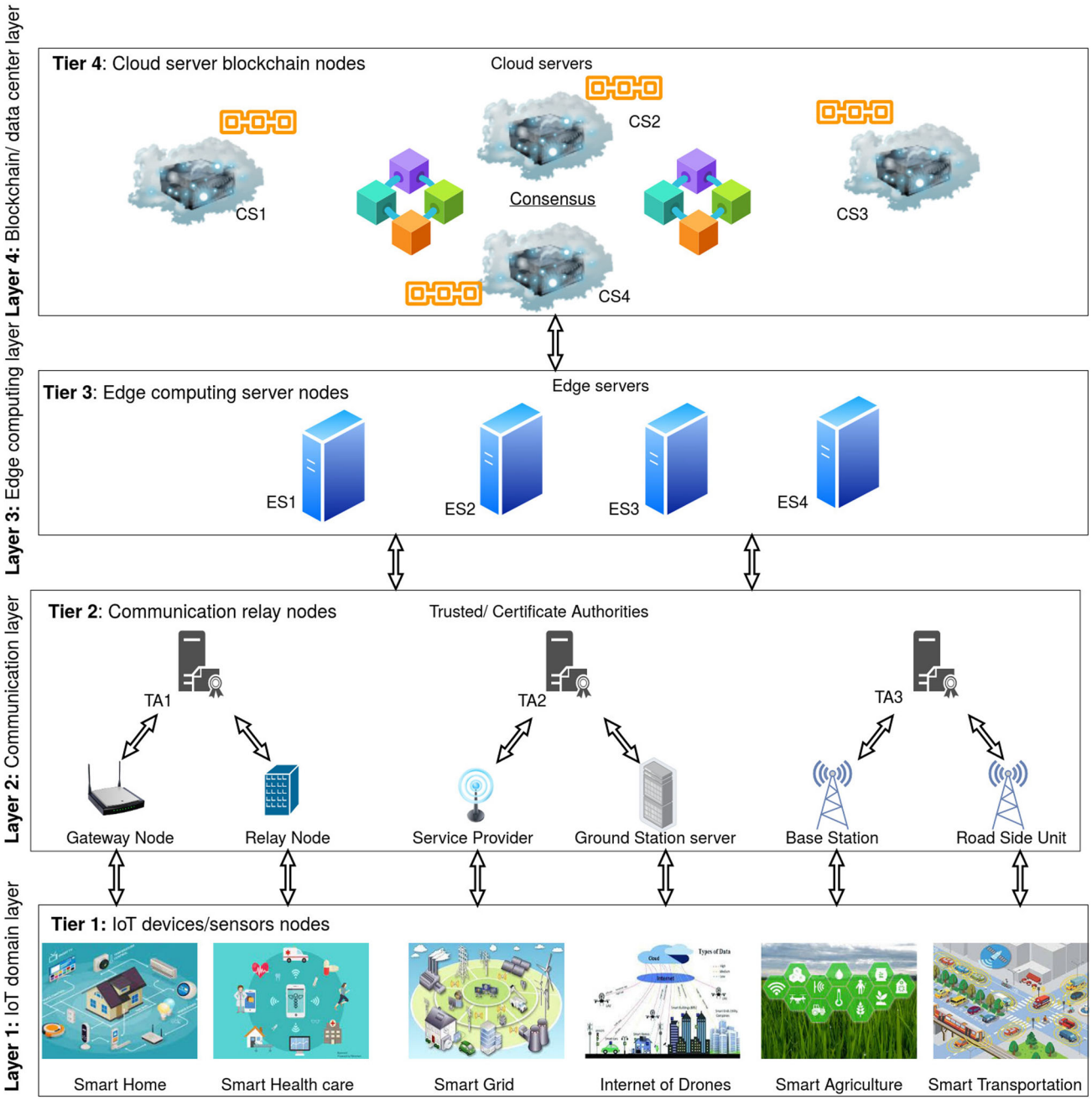

Fig. 8 Blockchain based architecture of IoT

to the IoT devices are issued by upper sub layer via lower sub layer. Lower sub layer acts as mediator nodes. The access control protocol is implemented at this layer where IoT devices are mutually authenticated by the second layer and a session key is established for secured communication between first and the second layer.

- *Edge computing layer:* IoT applications always produce high amount of data. So to increase the efficiency of data processing, the third layer of the architecture consists of edge servers. The data from the second layer is passed to the edge servers after encryption. Edge servers validate the data and form transactions. The transactions are packed into partial blocks which are passed to the blockchain layer. This layer adds decentralization, anonymous privacy protection, scalability, capability to handle huge amount of data efficiently by lowering computation cost in any IoT application. Some schemes skip this layer, and the data from the communication layer is directly sent to the fourth layer.

- *Blockchain/ data center layer:* The last layer of the architecture is the blockchain or the data center layer. This layer contains cloud servers. The main purpose of this layer is to form blocks and blockchains. All cloud servers form a peer-to-peer network. The partial blocks received from edge computing layer are verified and full blocks are formed. After that, cloud servers implements any consensus mechanism (discussed in Section 2.3) to add the verified blocks to the blockchain. The data received from the first layer is finally stored in the blockchain which is transparent and immutable. In recent times, this data can also be used for *big data analytics*.

4.2 Blockchain-based threat model for IoT environment

There can be following attack models, that can be considered in blockchain based access control protocols.

- **Dolev Yao threat model** Under the widely-recognized "Dolev-Yao threat (DY) model" [89], the adversary $\mathcal{A}$ is capable to intercept the messages exchange during communication. An adversary can also modify, fabricate and delete the messages that are exchanged in IoT environment. In addition to this, under this model, the end points communicating parties are not trusted and can be compromised by the adversary. Once the credentials are exposed to the adversary, various attacks like impersonation, man-in-the-middle attack can be launched.
- **CK-adversary model** Recently, the "Canetti and Krawczyk's adversary model (CK-adversary model)" [90] is considered as another contemplated *de facto* model to analyse IoT networks. According to this model, adversary can not only intercept, modify, delete messages as in DY model but also can compromise the secret keys and session credentials that are available in the storage memory of the entities during access control phase.
- **Physical IoT device capture attack** Another possible attack, that can be launched in blockchain based IoT architecture is physical IoT device capture attack. According to this attack, an adversary can physically capture and compromise the IoT devices and sensors deployed in hostile environment. The sensitive credentials stored in the memory of the devices can be exposed to the attacker, using power analysis attacks [91]. Under simple power analysis attack, various inputs are provided to cryptographic based devices. The power consumed by devices to produce the output is inspected to get through the stored credentials.

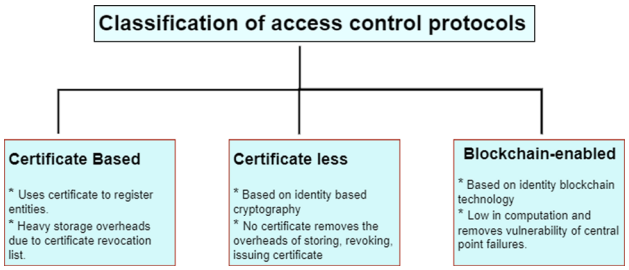

Fig. 9 Classification of access control protocols

5 Access control protocols in IoT

In this section we discuss access control protocols in IoT. The security protocols are classified as certificate based, certificate less and blockchain envisioned access control protocols. Figure 9 shows the categories of access control mechanism considered. We describe the mechanism of recent schemes under each category in Sections 5.1, 5.2 and 5.3, respectively.

5.1 Certificate-based access control protocols

The schemes in which a certificate is issued to the entities during registration are certificate based scheme. They generally follow public key cryptography technique where a certificate is issued by any trusted authority. Few certificate based access control protocols on recent use cases are discussed below.

Malani *et al.* [92] proposed a light weight access control scheme based on certificates, elliptic curve cryptography and one way hash functions. Gateway node initializes the system parameters and registers other entities or smart devices. The smart devices are provided with certificates including public key, private key and other parameters that are used to establish a pair wise secret key. In device access control phase, smart devices authenticate themselves to each others and then establish pair wise key to have a secure communication. A smart device i sends its signature, certificate to the other device j. The smart device j verifies the certificate and signature using public parameters provided by gateway node. After the successful verification a secret key SK_{ji} is computed by j and sent to the sender device i along with the signature. The device i checks the signature sent by j to check the authenticity. Further, it computes the secret key SK_{ij}. If the secret key received SK_{ji} matches with the secret key computed SK_{ij}, a pair wise key is established. Smart device i can communicate with smart device j using the established secret key $SK_{ji} = SK_{ij}$. Any new device before deployment, undergo the same steps. The scheme is secured against device impersonation attack, physical capture attack, replay attack, resists to malicious node deployment attack, as

it is impossible for the attacker to create a certificate without knowing the private key of gateway node.

Das *et al.* [93] proposed a certificate based lightweight access control and key agreement protocol in IoT environment (LACKA-IoT). A certification authority (CA) is completely dedicated to issue certificates to gateway nodes and sensor devices. CA initially sets up the public parameters along with its own key pairs. Following to this, CA registers the devices and gateway nodes by choosing a private, public key pair and creating a certificate for each. The certificate along with the key pairs is pre-loaded in the memory of the devices before their deployment. After this, device access control phase is specifically performed between the devices that wish to communicate without the mediation of gateway node. An authentication message request consisting of certificate, signature and timestamp is sent to the other device. The receiving device verifies the signature, and sends an authentication reply message including session key, verifier of the session key and it's certificate. After that a session key is computed, and agreed on by sending an acknowledgment message to accomplish mutual authentication. Similarly if a sensor device has to communicate with the nearest gateway node, it has to undergo similar access control phase.

Chaudhry *et al.* [94] later exposed the weakness of Das *et al.* [93] lightweight access control and key agreement protocol in IoT environment (LACKA-IoT). They claimed and proved that the scheme [93] is vulnerable to device impersonation attack and man in middle attack. The messages exchanged in their scheme can expose the original certificate to the adversary, which can let the adversary to create a valid request and generate a session key. Further, they proposed an improved lightweight access control and key agreement protocol in IoT environment (iLACKA-IoT) which is secured against related well known attacks. The scheme has the same phases as [93], with a difference in device access control phase. The computation steps includes the secrecy of random nonce, secret key and the assigned certificate. Therefore, authentication request message and authentication reply message sent in the phase does not include certificate of the initiating or responding devices. This does not allow adversary to form a valid request on behalf of any device. The authors claimed that in all cases even when the certificate is exposed, the adversary cannot form a valid request.

In [95], a certificate based demand response (DR) management authentication scheme (DRMAS) to manage demand response in smart grid-based systems is proposed. The scheme manages the data/energy flow between utility service providers, smart grid devices and clients. A malicious intruder might try to create a loop between the demand and supply of the energy. To manage seamless demands, the scheme allows the flow of sensitive information only after when the entities are authenticated and a session key is established. The network model consists of trusted authority similar to other schemes, utility control to manage the energy flow and smart meter devices to provide correct energy estimation to the clients. Alike public key infrastructure, trusted authority registers the utility controls and smart grid devices. In the next authentication phase, SG (smart grid) device creates a random certificate and sends a message using the pseudo identity to utility control. The utility control verifies the identity from the stored verifier table and checks the validity of the certificate. After the validation of the certificate, session key is computed and verified and agreed at both ends. New device deployment phase is also explained by the authors.

In an heterogeneous environment like IoT, authentication and key establishment becomes a tedious task. As everything can be connected to each other in an IoT network; restricting the entry of unauthenticated node and restricting the flow of data within the authorized legitimate nodes requires huge computation and communication cost. Huge overheads schemes are not suitable for such paradigm as real time implementation is required. So Siddhartha *et al.* in [96] proposed a light weight authentication protocol using implicit certificates for securing IoT systems. Implicit certificates are reduce sized certificate of identity, and are suitable for less resource constrained nodes. Certification authority assigns implicit certificate to the nodes which help them to create their key pairs. A node requests the CA for implicit certificate. CA verifies the integrity of the identity and data, and sends an *authenticator*: $< encrypted\ certificate, signature >$ using its private key. The node decrypts it using public key of CA and generates its key pairs. Next in key pair establishment phase two nodes mutually authenticate each other by verifying authenticator, hash of the authenticator and identities of each other. Then both the nodes compute a secret key by the derived parameters.

The deployment of malicious nodes in a network can invite lot of attacks on the security of the network. Malicious nodes can pretend legitimate to inside nodes and can illegally access the data and limited resources. To control the deployment of malicious nodes in the wireless sensor network, Zhou *et al.* in [97] proposed a protocol based on boot strapping that prohibits the deployment of malicious nodes in the network and also differentiates new nodes from the old nodes existing in the network. To commence the protocol, certificate authority (CA) initialises the system parameters and its own key pairs. For deploying sensor nodes, it creates a certificate that uniquely identify the node. In the memory of the node, public parameters, its key nodes, certificate and a bootstrapping time is loaded. A bootstrapping time is the time when a device bootstraps itself as soon as it is deployed in the network or about to start a new communication. Sensor nodes are deployed in the group so the bootstrapping time for the nodes within the group might be similar and different to the nodes belonging to other group. The authors have proposed

Table 5 Summary of characteristics of certificate-based access control protocols

Scheme	Year	Techniques	Network model entities	Phases or steps	Benefits and limitations
Malani et al. [92]	2019	*One way hash functions	*Front end devices	*Set up phase	*A light weight protocol which resists deployment of malicious nodes.
		*ECC	*Communication infrastructure	*Device enrollment phase	*The scheme has low computation and communication cost.
			*Gateway nodes	*Device access control phase	
				*Device addition phase	
Das et al. [93]	2019	*One way hash functions	*Certification authority	*Set up phase	*The scheme resists various attacks like replay attack, device physical capture attack, man in middle attack but is insecure against device impersonation and man in middle attacks.
		*ECC	*Gateway nodes	*Device registration phase	
			*Smart devices	*Device access control phase	
				*Dynamic device addition phase	
Chaudhry et al. [94]	2020	*One way hash functions	*Certification authority	*Set up phase	*The scheme resists various attacks like replay attack, device physical capture attack, man in middle attack, device impersonation and man in middle attacks.
		*ECC	*Gateway nodes	*Device registration phase	
			*Smart devices	*Device access control phase	

Table 5 continued

Scheme	Year	Techniques	Network model entities	Phases or steps	Benefits and limitations
Chaudhry et al. [95]	2020	*One way hash functions	*Trusted authority	*Setup phase	*The scheme controls the malicious activities in demand response in a smart grid network.
		*ECC	*Utility control (UC)	*UC Registration	*With less computation cost, it is also secured against replay attack, stolen SG device attack, SG device impersonation attack and man in the middle attack.
			*Smart grid (SG) devices	*SG Device Registration	
				*Authentication	
				*SG Device dynamic addition	
Siddhartha et al. [96]	2019	*ECC	*Certification authority	*Implicit certificate generation phase	*The scheme is a light weight scheme using implicit certificates of reduced size.
		*Hash function	*Nodes	*Pair wise key establishment phase	*The scheme ensures untraceability and anonymity along with reslience to impersonation, known key, DoS attack.
				*Mutual authentication phase.	

Table 5 continued

Scheme	Year	Techniques	Network model entities	Phases or steps	Benefits and limitations
Zhou et al. [97]	2007	*ECC	*Certificate Authority	*Predeployment phase	*The scheme ensures that no new malicious node can be deployed in the network and no old node's identity can be used maliciously.
		*Hash function	*Sensor nodes	*Node deployment	*The scheme has huge communication overheads and might even suffer through bottleneck.
				*Node authentication	
				*Key establishment	
Song et al. [98]	2010	*SPKI certificates	*Home appliances	*Service request	*The scheme uses the advantages of both gateway nodes and distributed home appliances based model.
			*Gateway node	*Issue relevant certificates	*The categorisation of policies secures the privacy of the residents according to their preferences.
			*Requester	*Certificate reduction	*The certificate management creates huge computational overheads.
				*Grant service	
Porambage et al. [99]	2013	*MAC	*Cluster head	*Implicit Certificate Generation	*The scheme allows secure authentication even when the nodes dynamically change their locations in a wireless sensor network.
		*Hash function	*Sensor nodes	*Pairwise Link Key Establishment.	*The scheme is secured against impersonate and masquerade attacks but might suffer from man in the middle attack.

two access control protocols; one for mutual authentication between new nodes and other for mutual authentication between old and new node. When a new node N_i wants to communicate in the network, it bootstraps and sends a message containing identity, certificate and bootstrap time to the neighboring node. If a neighboring node N_j in also new node, handshake between new nodes is followed. Both the nodes compare the bootstrap time of each other. If it is greater than or equal, the certificate of the sender node is verified using using challenge response procedure under hardness of ECDLP problem. A session key is shared after successful verification . If the receiving node is an old node, then handshake between new and old node is followed where only new nodes bootstrap time is checked.

Song *et al.* proposed another SPKI certificates [100] based access control scheme for home network [98]. A home network consists of home appliances which provide services to the requester based on the access control policies. The scheme allows the residents to frame access control policies according to their own preferences and choices. SPKI certificates are basically authorization certificate which are provided to the requesters according to their delegation rights. SPKI certificate is an 5-tuple certificate signed by issuer's private key $< Issuer, Subject, Delegation, Authorization, Validity >_{s(Issuer)}$. Issuer issues the certificate to the requester or the subject for certain authority for specified time mentioned in validity. Delegation is a boolean value that shows the subject could delegate or not. There are two types of policies: one are the general policies which are low security policies for which the residents have no issue even if they are exposed, other are privacy policies, which are related to privacy of the residents and are of high security. Home appliance issue the certificate to requester or gateway node. The scheme collaborates gateway model and distributed appliances model. In case of general policy, delegation certificate is issued by household appliance to the requester via gateway node using *5-tuple reduction rule*, where as for privacy policies, private certificate is directly give to the requester by the appliance. When a requester wishes and attempts to use a service it searches for a certificate and sends it to the household appliance. If the requester does not possess a certificate, a request to gateway node is sent to issue a certificate. If the request falls under general policy, gateway issues a certificate and delegates the request. And if the request falls under privacy policy, it transfers the request to household appliance for privacy certificate. By dividing the policies into general and private categories, the security of the residents is preserved according to resident's choice and preferences.

Wireless sensor nodes are limited in terms of resources and computational power. They are mobile; that is they can change their locations dynamically and can still communicate within the network. To support the same, Porambage *et al.* in [99] proposed a "Certificate-Based Pairwise Key Establishment Protocol for Wireless Sensor Networks". A legitimate node whenever wishes to initiate the communication or changes the location, it obtains a certificate from the certificate authority (CA) after sending certificate request. It then establishes a pair wise key to have a secure communication. Each node is deployed in pre decided particular cluster, where a resource rich node becomes a cluster head and acts as a CA for that cluster. CA issues the certificate to the requester sensor node and also communicates with the base station. The public parameters are stored in the memory of each sensor in an offline mode before their deployment. A sensor node that wants to communicate or renovate the existing certificate, generates a request message which is sent to CA (cluster head) along with the MAC on its identity. CA verifies the the correctness of the MAC, and sends a certificate to sensor nodes. Requester nodes fetches its private and public key by exploiting the parameters in the certificate. Further when sensor node U wants to communicate with sensor node V, U and V checks the legitimacy of each other's certificate, MAC and computed session key.

A summary of characteristics of discussed certificate-based access control protocols is provided in Table 5.

5.2 Certificate-less access control protocols

Certificate less access control schemes, are the scheme which remove the overheads of storing, revoking, issuing certificate and might work on identity based cryptography. Few certificate-less access control protocols on recent use cases are discussed below.

The security and privacy of the user and data accumulated by the sensor devices are of big concerns while creating a wireless body area network. Any malicious activity like exposing the data collected by sensors or deploying malicious sensor devices in the network can be life threatening and might directly affect the health of the user. In same context, Ali et al. [101] proposed a certificate less, robust authentication and access control protocol for securing wireless health care sensor networks. Trusted authority (TA) registers the sensor nodes and users via public key cryptography and biometric authentication respectively. A user sends a log in message to TA along with the details of the sensor node. TA verifies the credentials of user and sensor node and then exchanges the credentials to create session between an authenticated user and the authenticated node. User and sensor node, both store the received values in their memory. Finally in access control and encryption phase, an authenticated user sends an access request to the sensor node. The sensor node validates the request against the saved credentials and sends the response to the user if the request is valid. The scheme also proposes user credentials update phase and new user addition, revocation and re-registration phase in case the

credentials are compromised. Dynamic node addition phase adds new nodes in the network.

Most of the access control schemes proposed in the IoT environment assume that all the communicating nodes are in the same domain using the same system parameters and following the same cryptographic technique. Luo et al. in [102] proposed a secure and efficient "access control scheme for wireless sensor networks in the *cross-domain* context of the IoT". IoT user resides in a certificate less cryptography environment and other sensor nodes in an identity-based cryptography (IBC) environment. Key generation center (KGC) and Private key generator (PKG) runs the initial set up phase to randomly select different system parameters. The user residing in a certificate less cryptography environment registers itself via key generation center (KGC) and receives a partial private key and the sensor nodes are registered via private key generator (PKG). After the registration, any Internet user that wishes to access the sensor nodes creates a request message and performs a signcryption algorithm and sends a cipher text to the gateway node of the corresponding sensor node. The gateway node verifies the freshness of the received request and forwards the authenticated encrypted request to the wireless sensor node. The sensor nodes encrypts the required information and forwards to the user. The scheme maintains confidentiality, non repudiation and authentication in cross domain environment. If the partial private key is exposed, a key revocation phase is also defined.

Similar to [102], a heterogeneous access control scheme that allows communication between the entities lying in different cryptographic environment is proposed by Li et al. in [103]. The scheme is based on signcryption, bilinear pairing and identity-based access control (IBAC) model. A fully trusted service provider (SP) acts as a Key generation center (KGC) and Private key generator (PKG) in certificate less based environment and identity based environment respectively. During setup phase, it generates identities and private keys for sensor nodes as they belong to identity based environment, where as identities, partial private keys for users as they belong to CLS environment. A user computes its private key and public key after the registration process. User sends an encrypted access request consisting of cipher text, timestamp and identity to the honest gateway. The authenticated request is forwarded to the specific sensor node for information. The sensor node decrypts and verifies the plain text using bilinear pairing and computed session key. The scheme also attains confidentiality as the signcryption algorithm does not allow the content of the message to be revealed to anyone throughout the process. The revocation process defined in the scheme is too flexible as an expiry date is assigned along with the identities of the entities.

An access control scheme should monitor the deployment of the new nodes in the network keeping the node identities disclosed to ensure privacy. One such access control scheme, called as access control with node (identity) privacy (ACP) is proposed by Kumar et al. [104]. The whole network is divided into cells with one co-ordinator (C) each. Sensor nodes deployed in the network belong to a particular cell. Base station manages the whole network and commences the initial setup phase. Base station provides an identity, key identifier, secret salt value and the cell information to the node before their deployment. Similarly the coordinator is also informed about assigned senor nodes in its cell, identity of the cell etc. The coordinator acts as a mediator between the sensor nodes and base station to exchange sensory information. In the authentication phase, the sensory nodes hashes and encrypts identity with an asymmetric key to form a hashed authentication message. The message is decrypted by the coordinator after receiving, to verify the legitimacy of the sensor nodes against the saved information about the assigned nodes. Similarly the coordinator is also verified by the nodes by exchanging encrypted messages. After the successful mutual authentication, a key is computed and agreed for future communication between the sensory nodes and the coordinator. The scheme also flexibly deploys new nodes in the network via new node addition phase. [104] resists message replay attack, legal node masquerading attack, message forgery attack, identity threat, sybil attack, node capture and fabrication threat.

Integration of IoT with health care industry has provided extreme benefits to the users including both doctors and patients. With the recent years, IoT health care has collaborated with cloud computing to exploit its advantages like storage and processing. At the same time, it brings lots of security and privacy issues related to accessing data. In context to IoT health care, the sensitive data of the patients health is recorded in electronic health records (EHR) which should only be accessible to doctors and other authorized role players.

For the same scenario Riad et al. [105] proposed a "Sensitive and Energetic IoT Access Control (SE-AC)" mechanism for managing cloud electronic health records. The protocols fits for an IoT based health care systems where the privacy is maintained by using secure encryption mechanism. The data is accessible to the requesting users only by granting permissions. The scheme divides the authorities into various authorities named as Organization Central Authority (OCA), System Authorities (SA) like Emergency (EA), General Surgery (GSA), Neurology (NA), Gynecology and users in Custodian Domain (CD) like physicians, pharmacy etc to avoid delays and bottleneck like situations. An Organization Central Authority (OCA) is the core of the hospital organization. OCA sets up the parameters and creates public key of SA, *patient id* of patients and private key of the users in CD. SA have the responsibility to store the encrypted EHR in the cloud. The user of any domain that wishes to access the data sends the data access request to the OCA. Whenever

OCA receives the access request from the user, it forwards it to corresponding SA along with other details like Requested Operation (OP) (permission), Purpose of Use (PoU). SA runs an algorithm to generate a token that would help to decrypt the encrypted data on the cloud. The user receives a token and decrypts the information stored in cloud using its secret key.

At times, health care environment have to deal with many emergency situations like a patient might not be able to give access to the rescuer because of his health and the doctor cannot diagnose him without accessing his medical file. In such a situation, a problem in accessing the file might delay the treatment and can even be life threatening. To deal with such situations a term called as "break-glass" is introduced, which means dodging the usual access scheme and allowing the unauthorized access to any non designated person in exceptional circumstances. For the above described situation, Yang et al. [106] proposed a lightweight break-glass access control (LiBAC) system that defines two access control protocols one for both normal and the other for emergency circumstances. The patients store their medical records on the cloud after encrypting with a key and the chosen password. In normal situations, attribute based method is followed where, a secret key is assigned to the designated users like staffs, or the friends and relatives of patient, during the registration phase by KGC. The secret key helps them to decrypt the files stored in cloud after the consent from Cloud platform (CP) and Health care infrastructure provider (HIP). CP provides a partially decrypted file if the user successfully abides by the access policy. For emergency situations the patients choose some emergency contacts and share the password with them. Later, the Emergency contact persons (ECPs) contact with CP to decrypt the data using shared password and break-glass key.

An alternative category of access control protocols could be schemes based on *Group key Management (GKM)*. A GKM scheme assigns a group key only to a group of legitimate users to provide a controlled access. The users/subscribers only with a group key will be able to access the services from a particular device. GKM schemes are centralized and require lot of computation in rekeying process as every time a member leaves or joins the group, group key needs to be updated. Centralization and heavy computations makes GKM based schemes inefficient for a dynamic IoT paradigm where multiple users keep joining and leaving multiple group according to their needs and interest. To remove the rekeying computation burden and achieve decentralization, Dammak el al. exploited the features of the current mechanism and introduced a new "Decentralized Lightweight Group Key Management Architecture for Access Control, called DLGKM-AC" [107]. The scheme follows a hierarchical approach where, multiple devices form a device group (DG) and multiple users form Users group (UG). Key distribution center (KDC) initializes the system by choosing a master key and assigning slave keys to communicate with Sub-key distribution center (SKDC). KDC also provides Traffic encryption key to the devices during their registration. SKDC performs the similar steps to assign keys and slave tokens to multiple users. Any new device or user joining the network is assigned to a group with same features, attributes and interests. KDC manages the distribution of keys to devices using Logical key hierarchy (LKH). LKH arranges the devices of a group in a tree and distributes a Traffic Encryption Key to devices for encrypting the data. To mitigate single point of failure SKDC manages the distribution of keys in multiple users using master key encryption (MKE) which allows multiple decryption keys to decrypt the message encrypted using one master key. Every time the for updation, only the master key can be updated reducing the computation overheads. The scheme maintains forward secrecy, as every time a new user joins a network, SKDC updates the KDC about the event and assigns a slave token to new user according to the updated group key which can be used to decrypt the data. When a user leaves a group slave token of the user is deleted without affecting the existing users. Existing users can still manage to decrypt the data using their assigned slave tokens. Exit/entry of IoT devices is managed by KDC by rearranging and updating the part of LKH tree to update the Traffic encryption key.

With the advancement in technology, IoT is now even used for personal economic profit. Owners of the IoT devices have started lending their device for use to earn profits. The shared IoT devices are installed in the network which can be given for use on shared basis. To manage the same, unlike traditional IoT scenario the owners are now even concerned about the usage of their devices. Access control on such usage becomes an import security concerns as a greedy adversary might deploy malicious devices for profits, on the other hand even the users might not give enough money for the services. For same context, Liu et al. proposed a secure and efficient access control scheme for IoT in sharing economy environments [108]. The scheme is based on identity based authentication with anonymous signatures to preserve users privacy. Any user that wishes to access any shared device sends a signature and an authentication request via gateway nodes. Initially a central server is used to register the gateways and shared IoT devices and provides them key pairs. As the number of times a user is accessing a shared device needs to be tracked, users are given many secret keys which is used only once to produce one time signatures per usage. To decrease storage overheads and burden of producing huge number of secret keys, central server provides original key pair and corresponding 'pids' depending upon the payment, using which user can produce new key under bitmap every time he wants to access the device. In the next phase shared IoT device mutually authenticate gateway by sending an

authentication request, and a signature to the gateway. After this, to ensure legitimacy of user and gateway, identity based mutual authentication between user and gateway takes place. Finally, user sends a one time signature based on the service it needs to the gateway. The gateway helps the user to access the service and also provides a feedback to the owner of the shared device. The service provided by devices that remain in their position terminates after the execution. The authors have even proposed a solution where the user might take the IoT device to some other place. To maintain the accountability of various shared devices, gateways send the aggregated one time signatures to central server. Central server can even revoke the identity of the malicious gateways or user or IoT shared device by deleting the secret keys.

The communication between IoT users and smart devices occur on insecure open communication channel. Therefore, the security of the data exchanged is at risk. The data or messages can be modified, fabricated or even deleted. So restricting the access of the users on the data becomes important so as to allow only authorized users access the data. Mandal et al. [109] proposed a new three-factor certificateless signcryption-based user access control scheme for an IoT environment (CSUAC-IoT). The scheme allows the real time authorized users to access the data or avail the services directly from the smart devices after the mutual authentication between users and devices successfully accomplishes. IoT devices are installed in groups referred to as cells in the paper. Each cell is assigned a gateway node. Trusted Authority (TA) registers users, devices and gateway nodes. During the enrollment of devices with TA, credentials such as public private keys, identity along with an assigned gateway node and a secret value is stored in the memory of the devices. The users undergo certificate less cryptographic technique to register itself via TA, by receiving partial private key XORed with expiry date of public key, from TA and calculates its private-public keys. User is also provided with identities of list of IoT devices. Next, users generate biometric key and password using fuzzy extractor generation function in his/her mobile device. Subsequently, access control phase occurs which will help user and sensor device to agree on a session key. User creates two signatures $Sign_G$ and $Sign_{S_i}$ for gateway node and sensor device by signcryption algorithm which is sent to intended gateway node. GWN verifies the message and signature and forwards the message to particular sensor node. Sensor node runs unsigncryption algorithm and creates a session key and its verifier. Finally, the user runs session key verifying algorithm to verify the session key. The data collected by sensor nodes is securely sent to cloud server for further analysis and decision making and is also made available to authorized users. The scheme also supports dynamic node addition phase, user revocation phase and users password/biometric update phase.

Braeken et al. [110] proposed "eDAAAS: Efficient distributed anonymous authentication and access in smart homes based on symmetric key cryptography". The home owner (O) is responsible for managing the end home devices. The users are the temporary residents or permanent residents or guests. Owner acts as a key distribution center and registration center which allows the access of end nodes/ home devices to the users. The authentication mechanism lies on two factors; one is the users password and the other is the possession of the user device. Any communication between the entities should be done via shared secret key which can either be shared by physical contact or by public key infrastructure. The secret key is shared between the owner and the user, owner and the end device which is saved in an encrypted form. Each end node is pre-installed with the secret key and other secret parameters chosen by the owner. Users register themselves to the owner and receive capability token based on their access rights ad other materials related to the end node they wish to access after successful verification. Capability token contains an identifier to uniquely identify the token, issuing time, details of the subject (user) and device, signature on token and access rights. Possession of capability token gives permission to the user to access the device. The user logs in their device using the set password and then generate authentication request which is sent along with the capability token to the gateway and then is forwarded to end device without interference of the owner. End device verifies the received message and token and answers the request to accomplish mutual authentication. User also verifies the end device, and after mutual authentication, user is provided with the required information. The scheme can update the password of the user and can revoke the capability token whenever required. The scheme solves three purposes; it ensures the authenticity of the data, access control on the users accessing the smart home facility, also preserves anonymity.

At the end, a summary of characteristics of the discussed certificate-less access control protocols is given in Table 6.

5.3 Blockchain-enabled access control protocols

The schemes defined in the previous section can be prone to central single point failure. And, as IoT devices are low in computation and power, so it becomes too easy for an adversary to compromise them. Therefore trusting access policies might not be a complete solution. To suppress the above issue, blockchain technology can be used to provide distributed and trustworthy access control. Few blockchain based access control protocols on recent use cases are discussed below.

IoT enabled health care [111] is an important application of blockchain. Access control on the sensitive information related to patients health becomes utmost important. The information related to a patient should be accessible only to

Table 6 Summary of characteristics of certificate-less access control protocols

Scheme	Year	Techniques	Network model entities	Phases or steps	Benefits and limitations
Ali et al. [101]	2020	*Bilinear pairing	*Trusted authority	*Setup phase	*The scheme is secured against privileged insider attack, impersonation attacks, stolen smart card attack.
		*ECC	*User	*Sink node pre deployment registration	*The scheme does not propose device to device authentication phase.
		*Non invertible hash function	*Sensor nodes	*User registration phase	*Moreover, use of bilinear pairing incurs heavy computational cost.
		*Biometric authentication		*Login phase	
				*Verification phase	
				*Access control and encryption phase	
				*User credentials update phase	
				*New user addition, revocation phase	
				*Dynamic node addition phase.	
Luo et al. [102]	2018	*Bilinear pairing	*Internet user	*System initialization phase	*The scheme supports the communication in a cross domain environment where user and sensor device can be in different cryptographic environment.
			*Gateway	*User registration phase	*The scheme does not support mutual authentication anonymity and untraceability.
			*Wireless sensor node	*Authentication with key establishment phase	
			*Key generation center	*Leaked key revocation phase	
			*Private key generator		
Kumar et al. [104]	2016	*ECC	*Sensor nodes	*System initialization phase	*The scheme controls the access and deployment of new sensor nodes in the network along with managing privacy by hiding their identities.
		*Hashing	*Coordinator	*Authentication and key establishment phase and	*The scheme does not take care of message confidentiality and unforgeability at the same time.
		*AES encryption	*Base Station.	*New node addition phase.	

Table 6 continued

Scheme	Year	Techniques	Network model entities	Phases or steps	Benefits and limitations
Riad et al. [105]	2019	*Hashing	*Organization central authority.	*Set up	*The scheme proposes to execute the phases in parallel to have a real time execution with no delay.
		*Encryption and decryption	*System authorities.	*Key generation	*The scheme is scalable as it divides authorities within the network.
			*Cloud storage.	*Encrypted data upload	
			*Custodian domains.	*Data access request	
				*Token generation	
				*Decrypting cipher text.	
Li et al. [103]	2016	*Bilinear pairing	*Service provider	*Initialization phase	*The scheme controls the illegal data access by unauthorized users and achieves confidentiality, integrity, authentication and non repudiation.
		*Signcryption algorithms	*Internet user	*Registration phase	*The scheme does not support mutual authentication, anonymity and untraceability.
			*Sensor nodes	*Authentication and authorization phase	*Verification of requests by gateway can become a bottleneck in case of increased access requests.
				*Revocation phase	
Yang et al. [106]	2018	*Bilinear pairing	*Key generation center (KGC)	*System Setup	*The scheme works well in emergency situations in health care environment.
		*One way Hash function	*Cloud platform (CP)	*Key Generation for User and Delegation	*The openness of the scheme to violate access policies during emergency might also become an abuse and lead to uncontrolled accesses.
			*Healthcare Infrastructure Provider (HIP)	*Password based Break glass Key Generation and Key Extraction	
			*Patient (PA)	*Encryption	
			*Data users	*Decryption with Attribute Key and Verification	
			*Emergency contact person (ECP).	*Decryption with Break glass Key and Verification	

Table 6 continued

Scheme	Year	Techniques	Network model entities	Phases or steps	Benefits and limitations
Dammak et al. [107]	2020	*Logical key Hierarchy	*Key distribution center (KDC)	*Initialization	*The scheme effectively manages the dynamic and decentralised nature of IoT network.
		*Master Key Encryption (MKE)	*Sub key distribution center (SKDC)	*Device group registration	*The joining, leaving of devices and users is managed with low computation costs suiting the light weight need of the network.
		*Generalized Chinese Remainder Theorem (GCRT)	*Users	*User group registration	
			*IoT Devices.	*Dynamic changes in users' membership (Join/Leave)	
				*IoT device changes (Join/Leave).	
Liu et al. [108]	2020	*Bilinear pairing	*Shared IoT devices	*System initialization	*The access control scheme allows sharing/accessing IoT devices along with preserving privacy of the users through identity based authentication.
		*Encryption	*Central server	*Entity registration	*Through one time signatures computed using secret keys, a check on number of accesses on particular device can be made.
			*Gateway	*Service discovery	
				*Service request	
				*Command execution	
				*Service termination	
				*Service accounting	
				*Entity revocation	
Mandal et al. [109]	2020	*ECC	*Users	*System initialization phase	*The scheme ensures authentication by using three authentication factors user's password, personal biometrics and mobile device.
		*Fuzzy extractor	*IoT smart devices	*Enrollment phase	*The scheme incurs less communication cost making it affordable to use practically.
			*Gateway	*User registration phase	
			*Cloud servers	*Login and access control phase	
				*Dynamic device addition phase	
				*User revocation phase	
				*User password / biometrics update phase	

Table 6 continued

Scheme	Year	Techniques	Network model entities	Phases or steps	Benefits and limitations
Braeken et al. [110]	2016	*Symmetric cryptosystem	*User	*Installation phase of end nodes	*The scheme solves three purposes; it ensures the authenticity of the data, access control on the users accessing the smart home facility and preserves anonymity.
		*One way cryptographic hash function	*Users device	*Registration of the user	*The scheme accomplishes in low computation cost but its communication cost is high.
			*Gateway	*Definition of the capability token	
			*IoT devices or end nodes	*Derivation of secure key material by the owner	
				*User log in and answer by the end node	
				*Information retrieval.	

authorized persons and should also be immutable. Saha *et al.* proposed a "Blockchain-Based Access Control Protocol for IoT-Enabled Health care Applications" [112]. The scheme considers a hospital authority (HA) which receives the confidential data of the user securely via proposed access control mechanism. HA saves the data of the users in blocks under private blockchain technology. Trusted HA of any hospital sets the public parameters and also shares a shared key with HA's of other hospitals. Next in the registration phase any user like patient, nurse, staff members, doctor creates a secret biometric key, password in their sensor/mobile devices and register themselves with TA by sending an request message containing hashed ID, password, temporary ID. In response, HA sends the registration response message, after storing the registration tuple in its database. The user initiates the process of authentication and key establishment by logging into the mobile device using password and biometric. After the successful log in, the user sends an access control request to HA by creating a signature on private and public credentials. HA verifies the identity of the user from the database and verifies the signature. If valid, it computes a session key and temporal random identity and sends in response message. Finally, the user also computes the session key and agrees on the key if the received key matches to the computed one. The computed session key is used by user to send encrypted message to HA for secure communication. HA decrypts the message with same session key and forms an encrypted transaction, to store in blockchain. Practical Byzantine Fault Tolerance (PBFT) algorithm is used to come to consensus to add new blocks. Other HA's can verify the legitimacy of the block by recalculating the Merkle root and hash value of previous verified block.

Another scheme similar to [106] for emergency situation when patient is unconscious and health care providers need some necessary information about the patients to give correct line of treatment is proposed by Rajput et al. [113]. They designed a health care system based on the permissioned blockchain Hyperledger Composer framework, where the patient can store and manage access rules/permissions for patient health record (PHR) data. Under normal conditions patients can decide access control rules so as to allow the doctor to access his data. For emergency situations, patients beforehand impose various access control policies/permissions via smart contract to permit the access of his PHR data to health providers, emergency doctor, other authorized staff members to get immediate treatment when he would be unconscious. The patients and doctor register themselves by adding the required detail like ID, name. Blockchain transaction processing function (TPF) is called to complete the registration. The patients even enter the Emergency Access Time Constraints to restrict the time limit on emergency access. The emergency doctors (ED) register themselves via license number and when a request to access

the patients data is made the ED enters its ID and license number. The data request is checked for permissions and validity of license number. The patients data is granted only if access permissions allows for time equals to the access time constraint limit, otherwise the access is denied.

For the smart grid [114] application Bera *et al.* proposed a novel decentralized blockchain-based access control protocol in IoT-enabled smart-grid system, called DBACP-IoTSG [9]. A registration authority registers the smart meters (SM) and service providers (SP) in offline mode and provides them with certificate, temporal credentials, key pairs, random and temporal identity. Smart meters are provided to users to monitor energy consumption and service providers to manage smart meters. The access protocol basically provides a mechanism to securely store the data between smart meters and service providers. The communication between users and SM's is secured, but the communication between SM's and SP's is open and needs to be secured so that no attack is possible. SP's collect the data from the SM's and then form a block of transactions to save data. Then SP's together form a peer to peer network and add the block to the blockchain via consensus algorithm amongst themselves. To accomplish this, SM and SP undergo an access control and mutual authentication phase initiated by SM. SM sends an authentication request message to SP containing certificate, and temporal identity. SP then verifies the received values and certificate and further creates a session key and its verifier which is sent as an authentication response message. SM recomputes the session key via some computations and sends a session key acknowledgement message. If the received session key is equal to the computed one SP declares the agreed session key for future communication. Then SM uses the same session key to send encrypted data securely to the SP. SP will transform the information received in the form of transaction in the transaction pool until a threshold on the number of transaction is received. A leader is selected based on Secure Leader Selection algorithm. The selected leader forms a block and sends the block for validation to all SP's. SP's send a *VerStatus* to the leader if they find the block to be valid by verifying it against their pool. Finally, a leader sends a commit message to add a block only if 2n+1 SP's agree on it. The scheme claims that no fake block can be added to the chain as it wont be verified by all SP's.

Another blockchain based access control scheme for a general Home Area Network (HAN) is proposed by Zhou *et al.*. HAN consist of a smart meter associated with every user to manage their energy consumption and communication with energy provider. The communication is two ways between HAN users and energy providers where power is supplied to users by the providers and users can return or sell excess power back. A consensus algorithm based on Proof of Stake (POS) between HAN users and servers selects a private key generator amongst themselves. Each node registers itself to national level organisation and is bifurcated into master or slave nodes depending upon social and behavioural credits possessed by them. All master nodes participate in PKG election but slave nodes are just used to confirm the selection of PKG. PKG then initiates the scheme by setting up the initial parameters hash function its own private and public key pair, also allots public and private key pairs to energy providers and users via SSL layer in online mode. An expiration date is also provided which sets the expiration time of the key pairs. Next in the data access step three different scenarios are used. When a user wants to sell excess power to providers, it creates and sends an anonymous query message and a signature to the provider. Similarly an encrypted query message is created when energy providers wishes to access data of the user and signcrypted query request (signature and encrypted message) when he wants to store user's data to the cloud storage server. The verification of the request on both user and server side, takes place via bilinear pairing. Lastly, users and providers are automatically revoked according to expiry date of the keys associated to them in the registration phase. The scheme only uses one key in all scenarios saving the storage space.

Smart home is another emerging concept and application of IoT. Security and privacy of devices, data is important here too. Xue et al. [115] formulated a secure and auditable access control scheme for smart home systems, called PBAC. The service providers provide services related to management of smart home devices where the data from sensor devices is collected by SP for auditing and managing. Malicious and irresponsible service provider can be a threat to smart home. The scheme ensures the validity/legitimacy of service providers by mutual authentication and enables the integrity, accuracy, security and timeliness of access record by blockchain technology. Any new service provider who wishes to access data from smart devices are considered as visitors. The valid visitor is provided with the data from sensor devices via smart home administrator. Visitor sends a signcrypted message to administrator. Administrator checks the identity and access rights of the visitor against the list stored and the policy header. A token, shared secret key is generated along with the expiration date and is sent to the visitor. Visitor sends the data request to the device encrypted using the secret key received during registration. Smart device decrypts the request message to fetch the identity and sends the data package to the visitor. Finally an administrator, creates a block to be added in private blockchain by adding multiple signatures of the visitor on the data package. As a part of consensus, a signature on whole block is created by the visitor and is sent to administrator which is finally added to the blockchain. A visitor is revoked after the expiry of secret key and can even forcibly be revoked where the list of the administrator needs to be updated. The scheme

does not support key agreement, anonymity or untraceability preservation.

To prevent illegal access and unauthorized attacks, Mbarek et al. proposed an agent based blockchain-based access control for IoT in smart home systems. Agents remove the intervention of human by automatically processing blockchain transactions. The implementation is done on integrated Hyperledger Fabric-based Blockchain and IoT network. The scheme is best suited for scenario where parents can monitor their children's activity on home appliances. A blockchain based solution has three roles: endorsing peers, the ordering service, and committing peers. The endorsing peers endorse a transaction proposal based on access policies set by any family and on the functioning of the agents. A transaction that gets enough endorsements is sent to ordering services. The transactions are ordered in a block and is further sent to committing peers to add to the blockchain. Each committing peer update their ledger by updating their list of transactions. Two agents are used in the scheme. One is a static agent which resides in the peer device say parents and other is mobile agent. Without any manual verification, static agent verifies the received transaction by comparing it with predefined policies. Mobile agents are used to monitor devices in real time. They migrate to targeted device to control manage and monitor real time user activities, perform actual computations, accomplish the tasks, say activities of the children. To summarize, consider an example, when a child wishes to use any household appliance, the request in the form of smart contract goes to the static agent residing in the endorse peer or parent's mobile phone. The static agent if approves the request, response goes to ordering service. After collecting the endorse response, a block is created and added to the blockchain on validation. A notification reaches to peer nodes (parents), thereafter parent's static agent creates a mobile agents and sends it to targeted device requested by child. It runs the code on each control sensors, and can even deny the services if malicious activity is detected.

Application of IoT in the field of agriculture has given huge amount of benefits to people dependent on it for income, directly or indirectly by reducing crop disasters. Human activities, sudden unexpected change in climatic conditions such as floods or drought, random changes in temperature, humidity, improper irrigation facility etc have reduced the yield in the crop production a lot. Artificially maintaining the condition for crop yielding using multiple sensors to maintain, detect and gather temperature, light, mugginess, acidity, amount of nitrogen, amount of fertilizers and soil dampness etc would be of a great help. The collected information would help the professionals or farmers to take necessary action to have high yields and reduce crop destructions. Deployment of malicious devices and illegal data access or fabrication can be of equal danger. Wrong information or delay in the information due to malicious activities can even force the farmers to take wrong decisions that can destroy the crops. Authentication and access control are important pillars to maintain security [16].

In the field of agriculture, Arshad et al. proposed a private blockchain based secure access control for agriculture growth. The system model consists of sensor devices installed in agricultural field that collects the data in the surroundings. Gateways are installed in connection to users, which collects the data from the wireless sensors and forwards the data to the authorized user. Initially the system is initialised by a system administrator, followed by two way authentication process. In two way authentication the sensor's legality is validated and ensured along with the authentication of the user. The visitor user proves its identity by signcrypting the message. Administrator stores the access control list and a header containing the access right for each user. A key is assigned to a visitor from the administrator through a signcrypted message if his identity is proven valid and users access rights are declared. The data is collected and stored in a private blockchain maintained by the administrator. The private blockchain is different from the traditional blockchains as no nonce, or Merkle root is stored. Instead, the block contains information like smart agriculture device data and visitor access records which are periodically created. The transactions within the block contains data and record. Data includes information from devices and visitors access at a certain time. Record is defined as a multi-signed access record for a visitor and administrator authorized by the smart agriculture owner. To add the block, Proof of work is replaced by low overhead consensus mechanism because of limitation of resources. As proof of work is not used, low computation power of adversary can even arbitrarily tamper in creation of blocks. To avoid unknown addition and deletion of blocks from malicious devices, entire block is signed after its creation again before adding into blockchain. After the successful authentication, when a data is requested, the administrator checks it against the list and the policy header stored to grant access to the legitimate users.

Drones an unmanned aerial vehicle, is being currently applied in the field of military, aerial photography, traffic control and management and cinematography etc. Drones are connected to different devices processors, sensors, wireless transceivers etc. The connection of drones to various devices makes Internet of drones a part of IoT, forming IoT enabled Internet of drones network. AS a part of IoT, security issues becomes an important concern in IOT enabled IoD [116] also. Bera et al. proposed a new blockchain-based access control mechanism for the IoD environment based on certificates [117]. A control room (CR) is a trusted authority which is used to register Drones (DR_j) and Ground Station Server (GSS). CR initialises system parameters and registers drones and GSS by loading identities, temporal credentials, key pair, certificate on secret key, polynomial function in their mem-

ory before their deployment. The authors proposed access control phase between drone to drone (D2D) and drone to GSs (D2GSS) for secure data collection. For D2D access control a drone D_i sends a message to another drone D_j containing random nonce, certificate, it's identity over public channel. D_j verifies the certificate and computes a session key and its verifier to send as a response along with its certificate and identity. D_i verifies certificate and computes session key and its verifier. If the computed session key is equal the received, an acknowledgement is sent to agree on the same session key for future communication. Similar steps occur in D2GSS access control phase. Incase of drone failure or physical capture, new drones can be deployed in the same flying zone via dynamic drones addition phase. GSS forms a block of transactions after collecting real time data from DR's using the established session key. The block containing hash value of the information stored, encrypted transactions, signatures via ECDSA is sent to cloud server (CS). Peer to peer cloud server (P2P CS) network choose a leader by a selection algorithm and then apply Ripple consensus mechanism to verify the block. If the leader receives more than threshold value that is 80 percent of the votes on a particular block, it is added in the blockchain.

An essential part of smart city is Internet of vehicles (IoV) [77] that manages traffic, improves transportation, energy consumption, efficiency, saves cost and time of customers, reduces fatal occurrences saving lives. Vehicles upload traffic related information in data center for traffic analysis. Vehicles can even fetch information from the data center via road side unit (RSU) to take traffic relate decisions. Wrong information might lead to loss of life, time and economy. Therefore, authenticity of vehicles and RSUs is important to ensure the correctness if the information stored and preserve the privacy of the customers.

In smart cities, there are multiple TA's that manage the vehicles in their domain avoiding bottleneck problem that could occur in one TA architecture. With multi TA architecture, cross TA authentication problem occurs when a vehicle goes from one TA zone to another. To support the decentralized nature of IoV and solve the above problems, Xu et al. proposed a blockchain-based Roadside Unit-assisted authentication and key agreement protocol for Internet of Vehicles [118]. Vehicle nodes (VN) are equipped with on board units (OBU) which communicates with RSUs over open channel. System administrator innitialises the system parameters used to register VNs before their deployment. VNs register themselves to their nearest TA. The registration information about VNs are stored in data center. DC broadcasts the pointer/block identifier to information to other TAs. TAs are the miners to form private blockchain containing information about registration and encrypted traffic related data. All TAs store the pointers to vehicle information in a block linked to the previous block, and adds in a blockchain or distributed ledger based on Proof of Stake consensus mechanism. During authentication phase, VN sends an authentication request to RSU in its communication range. RSU forwards some credentials from the request message to TA. TA checks for the presence of pointer to the vehicle in its blockchain, and sends the authentication parameters of VN retrieved from DC to RSU. RSU authenticates TA and VN, and sends the updated parameters to TA and VN. Next, TA authenticates RSU and vehicles authenticates TA simultaneously. TA updates the data center and sends an acknowledgement signal to RSU. Finally both TA and VN agree on a session key for future communication. The scheme preserves anonymity and untraceability also is resistant to eavesdropping, impersonation and replay attacks. The proposed scheme is efficient, as RSUs assist TAs during authentication to avoid bottleneck problem, also TAs maintain common distributed ledger to store data to diminish cross domain authentication problem.

Finally, a summary of characteristics of the discussed blockchain based access control protocols is also provided in Table 7.

6 Comparative analysis

Under this section, we evaluate the performance of discussed access control protocols in Section 5 in terms of computation and communication overheads. Computation cost is calculated by finding the total time taken by all cryptographic operations in the scheme. Communication cost is calculated by finding the number of messages and total number of bits exchanged.

For calculating computational cost, the description of the notations used for various cryptographic operations for comparison is shown in Table 8. To measure the computational time of various cryptographic primitives we used testbed experiments using "Multi-precision Integer and Rational Arithmetic Cryptographic Library (MIRACL)". The configuration and other settings of the testbed is shown in Figure 10. To calculate the cost of each primitive we ran each operation 100 times. Figure 11 shows the maximum, minimum and average time (in milliseconds) observed for each primitive out of 100 experimental observations. The cost of T_{fe} is assumed similar to T_{ecm}. We use the average time of each operation to calculate the computational costs of all schemes.

We evaluate the communication overheads of all the discussed access control schemes which involve the number of messages and the number of bits of the transmitted messages. We assume that the one-way cryptographic hash function (using SHA-1 hashing algorithm [122]) produces an output of 160-bit hash value. Since 160-bit elliptic curve cryptography (ECC) provides same security as that of 1024-bit RSA public key cryptosystem [123], we consider 160-bit ECC for communication and computation comparisons of

Table 7 Summary of characteristics of blockchain based access control protocols

Scheme	Year	IoT-based application	Techniques	Network model entities	Phases or steps	Benefits and Limitations
Bera *et al.* [9]	2020	Smart grid	*ECC	*Registration Authority	*System setup	*The scheme applies blockchain to securely save data in open communication environment.
				*Smart meters	*Registration of smart meters and service providers	*No fake block can be added due to a voting consensus algorithm.
				*Service providers	*Access control *Key management among service providers	*Session key established is secured under CK adversary model.
				*Users	*Block formation and addition in the blockchain	
					*New smart meters addition after initial deployment in the smart grid environment	
Zhou *et al.* [119]	2019	Smart grid	*Bilinear pairing	*Private key generator	*Initial phase	*The scheme allows two way communication between smart meter of the user and energy provider where user gets the power from the providers and may also return the excess power back.
			*Hash functions	*HAN users	*Registration phase	*The scheme is vulnerable to ESL attack and does not support dynamic nodes addition after initial deployment.
			*ECC	*Energy providers	*Data creation phase	
					*Data access phase	
					*Withdrawal phase	
Rajput *et al.* [113]	2019	Smart healthcare	*Hyperledger Composer	*Patients	*Patients registration	*The emergency accessing of PHR data does not involve any third party.
				*Doctors	*Doctors registration	*It ensures the security and availability of patient's PHR data as the access permissions depend on the access policies/rules defined by patients.

Table 7 continued

Scheme	Year	IoT-based application	Techniques	Network model entities	Phases or steps	Benefits and Limitations
				*Emergency doctors	*Emergency doctors registration	*The scheme does not establish session key for future communication.
					*Get patient data	
Saha *et al.* [112]	2020	Healthcare	*ECC	*Hospital Authority	*Registration/Enrollment Phase	*The scheme proposes an access control mechanism for IoT based health care applications.
			*Fuzzy extractor	*User	*Login and Access Control Phase	*It mutually authenticates entities, creates a session key and preserves anonymity and untraceability.
					*Private Blockchain Formation	
Xue *et al.* [115]	2018	Smart home	*Bilinear pairing	*Administrator	*Initialization phase	*PBAC implements a private blockchain to provide an unforgeable and auditable foundation for smart home systems, that resists illegal data access.
			*ECC	*Visitor	*Authentication phase	*But it does not preserve anonymity and untraceability.
				*Devices	*Access phase	*The scheme utilises high communication and computation cost.
					*Blockgen phase	
					*Revocation phase	

Table 7 continued

Scheme	Year	IoT-based application	Techniques	Network model entities	Phases or steps	Benefits and Limitations
Mbarek *et al.* [120]	2020	Smart home	*Hyperledger fabric based blockchain	*Endorsing peers	*Submit endorsement request	*The blockchain based scheme automatically manages access control of smart devices at home without human interventions using two agents: static and mobile agents.
			*Agent based approach	*Ordering service	*Send proposal response	*Mutual authentication and key establishment is not aforementioned.
				*Committing peers	*Request block creation	
					*Collect endorsements and create block	
					*Send created block to committing peers	
Arshad *et al.* [121]	2020	Smart agriculture	*Hyper ledger	*Sensor devices	*Initialisation	*The scheme is a private blockchain-based secure access control for agriculture to increase the crop production and reduce crop destruction by monitoring different climatic parameters phase.
			*Hash function	*Users	*Authentication phase	*The authors did not elaborate the phases for better understanding
					*Access control	
					*BlockGen	
					*Revocation	

Table 7 continued

Scheme	Year	IoT-based application	Techniques	Network model entities	Phases or steps	Benefits and Limitations
Bera *et al.* [117]	2020	Internet of Drones	*ECC	*Ground server station (GSS)	*System initialization phase	*The scheme manages the mutual authentication and access control (key establishment between drones and drone and GSS).
			*Hash function	*Drones	*Drone registration	*The scheme is resilient to drone and GSS impersonation attack, man-in-the-middle attack, physical drone capture attack etc.
			*ECDSA	*Control server	*GSS registration	
			*Ripple consensus mechanism	*Cloud server	*Drone to drone (D2D) access control	
					*Drone to GSS (D2GSS) access control	
					*Dynamic drones addition phase	
					*Block construction and addition in blockchain.	
Xu *et al.* [118]	2021	Internet of Vehicles	*ECC	*Data center	*Initialization phase	*The proposed scheme is efficient, as RSUs assist TAs during authentication to avoid bottleneck problem, also TAs maintain common distributed ledger to store data to diminish cross domain authentication problem.
			*One way hash function	*Vehicle nodes	*Registration phase	*The authentication phase exchanges 5 communication messages, thus the scheme incurs a a little communication overheads.
				*Trusted authority	*Authentication phase	
				*Road side units		

Table 8 Notations and their descriptions

Notation	Description
T_{ecm}	Elliptic curve point multiplication
T_{epa}	Elliptic curve point addition
T_{mtp}	Map-to-point operation
T_{bp}	Bilinear pairing
T_h	One-way hash function
T_{exp}	Modular exponentiation
$T_{enc/dec}$	Symmetric encryption/decryption
T_{fe}	Fuzzy extractor function
T_{exp}	Modular exponentiation

Model: MacBook Pro (15-inch, 2019)
CPU Architecture: 64-bit
Processor: 2.3 GHz Intel Core i9
Memory: 32 GB
OS: macOS Mojave 10.14.6

Fig. 10 Configuration of the testbed

Cryptographic operation notation	Minimum time(in milliseconds)	Maximum time(in milliseconds)	Average time(in milliseconds)
T_h	.023	.053	.024
T_{ecm}	.337	.54	.382
T_{epa}	.001	.003	.002
$T_{enc/dec}$	.001	.002	.001
T_{bp}	5.715	8.616	6.353
T_{mtp}	.075	.127	.084
T_{exp}	.037	.071	.039
T_{mul}	.002	.035	.004
T_{add}	0	.004	.002

Fig. 11 Computation costs of cryptographic primitives using MIRACL

the authentication schemes. With this consideration on ECC, the communication overhead to transmit an elliptic curve point $P = (P_x, P_y)$ is of $(160 + 160) = 320$ bits, where P_x and P_y are the x and y co-ordinates of the point P. We also assume that the entity's real identity, random nonce and timestamp are of 160-bit, 160-bit and 32-bit, respectively. For symmetric key encryption/decryption, the Advanced Encryption Standard (AES-128) has been used [124]. All the entities and their bit sizes are provided in Table 9.

Table 9 Message fields and their sizes in bits used in comparison of communication costs

Description	Size (in bits)
Message digest (hash value)	160
Elliptic curve point	320
Random or pseudo identity	160
Timestamp	32
Random nonce	160
AES plaintext/ciphertext block	128
Message length	160

6.1 Costs comparison of certificate-based access control schemes

In Tables 10 and 11, we have compared the computation and communication costs of the Chaudhry et al. [95], Chaudhry et al. [94], Siddhartha et al. [96], Malani et al. [92], Das et al. [93], Porambage et al. [99], Zhou et al. [97].

6.2 Costs comparison of certificate-less access control schemes

In Tables 12 and 13, we have compared the computation and communication costs of Mandal et al. [109], Ali et al. [101], Luo et al. [102], Li et al. [103], Braeken et al. [110], Kumar et al. [104]. The computational cost of Luo et al. [102], Li et al. [103] is huge due to the use of bilinear pairings.

6.3 Costs comparison of blockchain-based access control schemes

The schemes of Bera et al. [117], Bera et al. [9], Zhou et al. [119] have resource constrained devices like drones, smart meters. IoT devices communicate and register themselves to gateway/servers or service providers. We calculate the computation cost of smart devices, by experimenting on Raspberry PI3 to find the computation time of each cryptographic primitive. The configuration settings of Raspberry PI3 is as in Fig. 12. Figure 13 shows the maximum, minimum and average time (in milliseconds) observed for each primitive out of 100 experimental observations. We use average time to perform our comparisons. For calculating the computation cost of gateway/servers and service providers, we consider the time of MIRACl, thus we use the same values as in the Table 11. In [117], T_{poly} is the time to evaluate an t-degree univariate polynomial over finite field. We compute T_{poly} by finding $t(T_{mul} + T_{add})$, where t is the degree of polynomial.

In Tables 14 and 15, we have compared the computation and communication cost of the Bera et al. [117], Bera et al.

Table 10 Comparative computational costs analysis of certificate-based access control schemes

Scheme	Total cost (in milliseconds)	Estimated time
Chaudhry et al. [95]	$9T_{ecm} + 8T_h + 2T_{epa}$	≈ 3.634 ms
Chaudhry et al. [94]	$10T_{ecm} + 8T_h + 6T_{epa}$	≈ 4.024 ms
Siddhartha et al. [96]	$7T_{ecm} + 5T_h + 2T_{epa} + 2T_{enc/dec}$	≈ 2.800 ms
Malani et al. [92]	$6T_{ecm} + 8T_h + 2T_{epa}$	≈ 2.488 ms
Das et al. [93]	$7T_{ecm} + 6T_h + 3T_{epa}$	≈ 2.824 ms
Porambage *et al.* [99]	$6T_{ecm} + 9T_h + 2T_{epa}$	≈ 2.512 ms
Zhou et al. [97]	$3T_{ecm} + T_h + 2T_{enc/dec}$	≈ 1.172 ms

Table 11 Comparative communication costs analysis of certificate-based access control schemes

Scheme	Number of messages	Number of bits
Chaudhry et al. [95]	2	1344
Chaudhry et al. [94]	3	2944
Siddhartha et al. [96]	6	6336
Malani et al. [92]	2	2144
Das et al. [93]	3	3296
Porambage et al. [99]	4	3584
Zhou et al. [97]	5	4608

[9], Zhou et al. [119], Saha et al. [112], Xu et al. [118] and Xue et al. [115].

The comparison of computation and communication costs clearly shows the complexity of the schemes. Out of the discussed certificate based access control schemes, Zhou et al. [97] takes roughly 1.172 ms of computation time which is least of all other schemes. On the other side, Chaudhry et al. [95] incurs the minimum communication cost of 1344 bits. For certificate less access control schemes, the computation cost of Braeken et al. [110] is ≈ 0.554 ms which is lesser than all other certificate less schemes and all certificate based schemes. As the revocation, issuing certificates takes time therefore certificate less are better in terms of computation time. The least computation time out of all discussed schemes from all categories which are certificate based, certificate less or blockchain based, Xu et al. [118] which is blockchain based accomplishes in minimum time of 0.456 ms roughly.

Table 13 Comparative communication costs analysis of certificate-less access control schemes

Scheme	Number of messages	Number of bits
Mandal et al. [109]	3	3136
Ali et al. [101]	5	3264
Luo et al. [102]	2	3040
Li et al. [103]	2	3488
Braeken et al. [110]	3	3552
Kumar et al. [104]	3	2240

Model: Raspberry PI 3 B+ Rev 1.3
CPU Architecture: 64-bit
Processor: 1.4 GHz Quad-core, 4 cores
Memory: 1 GB
OS: Ubuntu 20.04 LTS, 64-bit

Fig. 12 Configuration of Raspberry PI3

7 Open research issues

In this section, some potential future research directions that need to be addressed in Blockchain envisioned IoT security protocols are discussed as follows.

7.1 Scalability

IoT applications like smart home, smart city or smart grid are $24X7$ running real time applications. These applications

Table 12 Comparative computational costs analysis of certificate-less access control schemes

Scheme	Total cost (in milliseconds)	Estimated time
Mandal et al. [109]	$T_{fe} + 14T_{ecm} + 28T_h + 8T_{epa}$	≈ 6.418 ms
Ali et al. [101]	$2T_{fe} + 3T_{ecm} + 16T_h + 2T_{bp}$	≈ 15.000 ms
Luo et al. [102]	$3T_{ecm} + 4T_h + T_{epa} + T_{exp} + 4T_{bp}$	≈ 26.695 ms
Li et al. [103]	$3T_{ecm} + 2T_h + 2T_{epa} + 5T_{bp}$	≈ 32.963 ms
Braeken et al. [110]	$23T_h + 3T_{enc/dec}$	≈ 0.554 ms
Kumar et al. [104]	$2T_{ecm} + 6T_h + 6T_{enc/dec}$	≈ 0.914 ms

Cryptographic operation notation	Minimum time(in milliseconds)	Maximum time(in milliseconds)	Average time(in milliseconds)
T_h	.0274	.643	.309
T_{ecm}	2.206	4.532	2.288
T_{epa}	.015	.021	.016
T_{enc}	.017	.038	.018
T_{dec}	.009	.054	.014
T_{bp}	27.606	32.79	32.084
T_{mtp}	.381	.406	.385
T_{exp}	.178	.493	.228
T_{mul}	.009	.016	.011
T_{add}	.008	.013	.010

Fig. 13 Computation costs of cryptographic primitives using Raspberry PI3

produce abundance amount of data every second. Storing huge sized data in blockchain not only vary the size of the blockchain, but also creates encumbrance on whole working process of blockchain technology. Literally, each node of the network should contain copy of transactions related to data produced by the IoT device. However, storing all the produced data in the blockchain is impossible, and would unnecessary increase the overheads. Moreover, the miner nodes would have to process whole amount of data against their limited storing, computation capacity affecting the network performance. This has led to various issues like long queuing time, more computation time, high block generation latency, high utilization of energy resources etc. Therefore, the increase in number of smart IoT devices and smart applications has welcomed scalability as a challenge, while designing security protocols in blockchain based IoT system. So, the need of the hour is to design a system that analyses, differentiates, optimizes and channelizes data while storing that can be easily retrieved and extracted as and when asked for. Also, the processing of the large amount of data should not affect the overall efficiency of smart applications and suppress the benefits of blockchain technology.

7.2 Security and privacy

IoT is a vulnerable network which is prone to various types of attacks. Any security scheme designed for an IoT application should be able to handle major security issues like integration, availability and access control. Integrating blockchain and IoT provides us integration and availability because of the inherent properties of blockchain technology using digital signatures and public blockchains, but the privacy and access control is still a major concern. Firstly, privacy of the data is questionable because the data in form of transactions are passed to the ledger publicly after verification. However private keys are used, still there are lots of public information that can be a trouble for identity based information. Very few solutions using gateways and homomorphic computation etc is provided in recent years as in [125], [126]. But still there is a lot of scope to design a light weight, resource restricted full privacy preserving mechanism that is suitable for sensitive IoT platforms. Secondly, to control the unauthorized and authorized access, each transaction is verified which cause a concern in scalability (discussed in Sect. 7.1). Therefore, we need to design an access control scheme that eliminates overheads, lowers the latency, increases availability, and is able to persist real time data delivery. One such solution is provided in [127] using Software Defined Networks (SDN).

7.3 Trust management and malware detection

The trust among the nodes in a network is established, after they communicate with each other for quite a considerate amount of time. But in the case of an IoT network, the nodes are dynamic (wireless sensor networks, IoV, IoD, etc.) and so is the candidacy of a node in any network. Due to the inter-

Table 14 Comparative computational costs analysis of blockchain-based access control schemes

Scheme	Total cost (in milliseconds)	Estimated time
Bera et al. [117]	Drone : $4T_{ecm} + 5T_h + T_{epa} + T_{poly}$	$\approx 10.713 + 0.021t$ ms
	Gateway Server : $4T_{ecm} + 5T_h + T_{epa} + T_{poly}$	$\approx 1.65 + 0.006t$ ms
Bera et al. [9]	Smart Meter: $4T_{ecm} + 11T_h + T_{epa}$	≈ 12.567 ms
	Service provider: $4T_{ecm} + 11T_h + T_{epa}$	≈ 1.794 ms
Zhou et al. [119]	Smart Meter: $3T_{ecm} + 2T_h + T_{epa} + T_{mtp} + 3T_{bp}$	≈ 104.135 ms
	Service provider: $3T_{ecm} + 2T_h + T_{epa} + T_{mtp} + 3T_{bp}$	≈ 34.374 ms
Saha et al. [112]	$3T_{ecm} + 16T_h + T_{epa} + T_{fe}$	≈ 1.914 ms
Xu et al. [118]	$19T_h$	≈ 0.456 ms
Xue et al. [115]	$6T_{ecm} + 7T_h + 2T_{epa} + 6T_{bp} + 6T_{enc/dec} + 3T_{exp}$	≈ 40.705 ms

Table 15 Comparative communication costs analysis of blockchain-based access control schemes

Scheme	Number of messages	Number of bits
Bera et al. [117]	3	1888
Bera et al. [9]	4	3040
Zhou et al. [119]	3	2464
Saha et al. [112]	2	1472
Xu et al. [118]	4	4448
Xue et al. [115]	5	9344

mittent nature of IoT nodes, trust management becomes an important issue. Blockchain when integrated with IoT system has been a perfect choice to manage reputation and trust. But blockchain envisioned IoT system still faces a challenge while managing trust as the system is decentralized and the participants keep changing. Moreover, as IoT is more or less a sensor based network, the mechanism of processing data and integrating information is different for every node. So validating each particular transaction is difficult and prone to mistakes. Hence, to detect malicious nodes and develop trust easily, a malware detection mechanism is required.

7.4 Regular software upgrade

IoT devices have software running in them which needs updation on regular basis as and when the services or the network size increases. The updation of software needs to be synchronized so that the availability of the network is not hampered. With integration of blockchain in IoT system the upgradation is a big challenge, as simultaneous upgradation of IoT devices is not possible because of decentralized feature. Hence the IoT devices loose their updation and become prone to malware attacks. For this decentralized periodic run time system needs to be developed to upgrade the system as a whole.

7.5 Hybrid systems

IoT devices are restricted in terms of computation and storage capacity. So, storing full sized blockchain would be infeasible for them as they cannot use/store whole data. Also, IoT devices are heterogeneous in functionality and architecture. So one infrastructure or a protocol would not fulfill the requirements. To manage these issues, we need a hybrid system with following solutions.

- It provides a blockchain specific IoT infrastructure that allows the storage of large data into the blockchains.
- It should be adaptable to the existing IoT application framework and offers enhanced security solutions.
- It should provide hybrid mining solution that works both in centralized and decentralized environment.
- The system should be adaptable to the existing IoT ecosystem and its underlying popular device to device connection protocols.
- High energy consuming blockchain nodes impacts on the total energy consumption of the IoT network. Therefore the system should be able to manage between the number of blockchain and IoT nodes such that energy consumption is moderate [128].

7.6 Reformed consensus algorithms

One of the major research areas in the field of Blockchain envisioned IoT is designing a consensus algorithm that works fast and quickly comes to conclusion. IoT devices are generally the part of real time application where the communication or exchange of message should happen within limited time. For example in Internet of Vehicles scenario, any accident warning should be reached to the vehicle node in minimalistic time period. So to align with the speed of communication, consensus mechanism in blockchain should be such that the miners should be able to validate and add the block before due time for information exchange. Therefore, the research in the field of designing an optimized blockchain consensus mechanism is required, that designs the consensus mechanism which is suitable for quick real time applications and resource constrained environments as IoT.

7.7 Future blockchain cloud of things (BCoT)

The evolution of IoT has overwhelmed the world with new commercial applications and services such as smart homes, smart cities, smart industries, smart governance etc. The exceptional properties of blockchain has promoted the usage of these applications in our lives. But the resources of IoT devices are limited. therefore, the processing of data is deputed to cloud computing. The integration of cloud computing and IoT has led to the merging revolution of Cloud of Things (CoT) paradigm. The integration has extremely improved the efficiency of the services provided by IoT. But great functionalities are often tailed by some limitations. The major drawback of CoT is the utilization of the central cloud or any third party for data processing and storage. Due to this, the data processing time creates obstructions while implementing it in practical use cases. Therefore blockchain can be used to decentralize CoT and create a novel future paradigm of blockchain and cloud of things integration framed as BCoT. BCoT can support the present needs as it increases data availability, enhances security and privacy, decentralization etc. In future, BCoT might have lost of research directions like designing a light weight consensus protocols to increase the efficiency, machine learning in BCoT, big data analytics in BCoT etc [129].

7.8 Additional research areas

Other research areas and future challenges in Blockchain envisioned IoT are *sharding in blockchain* [130], *blockchain for 5G IoT* [131], *skyline query processing in blockchain* [132], *energy efficient mining*, *artificial intelligence/ machine learning trends in blockchain* etc.

8 Lessons learned

The main motive of the comprehensive survey drafted in this article is to provide a complete understanding of IoT, and its security and privacy issues. We elaborated on how blockchain technology can be used to enhance and upgrade the IoT applications by providing various security solutions. The expected lessons learned from this comprehensive survey are as follows.

- The foundation of the paper is on IoT, so the starting section of the paper gives a detailed description on IoT, its architecture, applications. Further, various security challenges and issues in IoT are documented. Since there are many security attacks possible in IoT, the paper gives a detailed description on various attacks possible and their countermeasures along with other functionality features.
- Next, the evolution of blockchain in IoT paradigm is explained. Under the same section, we explained the types of blockchain as public, private and hybrid, and various consensus mechanisms that are applicable to reach consensus. The section would give a clear understanding on how blockchain can resolve some of the vulnerabilities of IoT.
- The main goal of the paper is to analyse various access control protocols, for which we provide system models that include a generic blockchain based access control architecture and threat models considered for blockchain based IoT network.
- Later in the paper, we focus to provide a wider vision on existing access control protocols in IoT by classifying them as certificate based, certificate less and blockchain envisioned access control protocols. While explaining the access control protocols, each use case like smart home, smart grid and health care is also elaborated.
- Finally, an analysis of the existing schemes is performed where we compare the computation and communication costs of the state of art schemes. The computation and communication costs give a clear understanding on the complexity of the schemes.

9 Conclusion

In this survey, a comprehensive study has been conducted on access control protocols in various IoT applications. A detailed overview is provided on IoT applications, security challenges, functionality requirements, security attacks and their counter measures. Further, we elaborate on blockchain technology, consensus mechanisms and its evolution in IoT. The study gives a thorough understanding on how blockchain is a rescue to vulnerabilities faced by IoT applications. Further, for better understanding we have classified the access control protocols into certificate based, certificate less and blockchain envisioned access control protocols. For each classification, some existing schemes are reviewed in detail and a comparative analysis on computation and communication costs is also provided. The description of the mechanism of each access protocol is done on a wider vision by elaborating to each use case. This will let the readers not only understand the access mechanism but also clear issues with the use cases of IoT applications. Finally, the study provides a few challenges and research directions for the future.

Acknowledgements This work was supported by the Ripple Centre of Excellence Scheme, CoE in Blockchain (Sanction No. IIIT/R&D Office/Internal Projects/001/2019), IIIT Hyderabad, India and by the Mathematical Research Impact Centric Support (MATRICS) project funded by the Science and Engineering Research Board (SERB), India (Reference No. MTR/2019/000699). The authors would like to thank the anonymous reviewers and the associate editor for their valuable comments and suggestions which helped us to improve the presentation and quality of the paper.

Declarations

Conflict of interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Wazid, M., Das, A. K., Odelu, V., Kumar, N., Conti, M., & Jo, M. (2018). Design of secure user authenticated key management protocol for generic IoT networks. *IEEE Internet of Things Journal, 5*(1), 269–282.
2. Hassija, V., Saxena, V., & Chamola, V. (2021). A mobile data offloading framework based on a combination of blockchain and virtual voting. *Software: Practice and Experience, 51*(12), 2428–2445.
3. Al-Fuqaha, A., Guizani, M., Mohammad, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies. *Protocols, and Applications, IEEE Communications Surveys Tutorials, 17*(4), 2347–2376.
4. Kamilaris, A., & Pitsillides, A. (2016). mobile phone computing and the internet of things: A survey. *IEEE Internet of Things Journal, 3*(6), 885–898.
5. Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S., & Fang, B. (2020). A survey on access control in the age of internet of things. *IEEE Internet of Things Journal, 7*(6), 4682–4696.

6. Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., & Shu, L. (2017). Authentication Protocols for Internet of Things: A Comprehensive Survey, Security and Communication Networks, Article ID 6562953, 41 pages, https://doi.org/10.1155/2017/6562953.
7. Li, W., Logenthiran, T., Phan, V., & Woo, W. L. (2019). A novel smart energy theft system (SETS) for iot-based smart home. *IEEE Internet of Things Journal, 6*(3), 5531–5539.
8. Morello, R., De Capua, C., Fulco, G., & Mukhopadhyay, S. C. (2017). A smart power meter to monitor energy flow in smart grids: The role of advanced sensing and iot in the electric grid of the future. *IEEE Sensors Journal, 17*(23), 7828–7837.
9. Bera, B., Saha, S., Das, A. K., & Vasilakos, A. V. (2021). Designing blockchain-based access control protocol in iot-enabled smart-grid system. *IEEE Internet of Things Journal, 8*(7), 5744–5761.
10. Vedaei, S. S., Fotovvat, A., Mohebbian, M. R., Rahman, G. M. E., Wahid, K. A., Babyn, P., Marateb, H. R., Mansourian, M., & Sami, R. (2020). COVID-SAFE: An IoT-based system for automated health monitoring and surveillance in post-pandemic life. *IEEE Access, 8*, 188538–188551.
11. Xu, G. (2020). IoT-assisted ECG monitoring framework with secure data transmission for health care applications. *IEEE Access, 8*, 74586–74594.
12. Yang, G., Jiang, M., Ouyang, W., Ji, G., Xie, H., Rahmani, A. M., Liljeberg, P., & Tenhunen, H. (2018). IoT-based remote pain monitoring system: From device to cloud platform. *IEEE Journal of Biomedical and Health Informatics, 22*(6), 1711–1719.
13. Montori, F., Bedogni, L., & Bononi, L. (2018). A collaborative internet of things architecture for smart cities and environmental monitoring. *IEEE Internet of Things Journal, 5*(2), 592–605.
14. Aslam, S., Michaelides, M. P., & Herodotou, H. (2020). Internet of ships: A survey on architectures. *Emerging Applications, and Challenges, IEEE Internet of Things Journal, 7*(10), 9714–9727.
15. Subahi, A. F., & Bouazza, K. E. (2020). An intelligent IoT-based system design for controlling and monitoring greenhouse temperature. *IEEE Access, 8*, 125488–125500.
16. Ayaz, M., Ammad-Uddin, M., Sharif, Z., Mansour, A., & Aggoune, E. M. (2019). Internet-of-Things (IoT)-Based Smart Agriculture: Toward Making the Fields Talk. *IEEE Access, 7*, 129551–129583.
17. Granjal, J., Monteiro, E., & Sá Silva, J. (2015). Security for the internet of things: A survey of existing protocols and open research issues. *IEEE Communications Surveys Tutorials, 17*(3), 1294–1312.
18. Mosenia, A., & Jha, N. K. (2017). A comprehensive study of security of internet-of-things. *IEEE Transactions on Emerging Topics in Computing, 5*(4), 586–602.
19. Das, A. K., Zeadally, S., & He, D. (2018). Taxonomy and analysis of security protocols for internet of things. *Future Generation Computer Systems, 89*, 110–125.
20. Cynthia, J., Parveen Sultana, H., Saroja, M. N., & Senthil, J. (2019). *Security Protocols for IoT* (pp. 1–28). Cham: Springer.
21. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures, IEEE. *Access, 7*, 82721–82743.
22. Dai, H., Zheng, Z., & Zhang, Y. (2019). Blockchain for internet of things: A survey. *IEEE Internet of Things Journal, 6*(5), 8076–8094.
23. Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2019). Blockchain Technologies for the Internet of Things: Research Issues and Challenges. *IEEE Internet of Things Journal, 6*(2), 2188–2204.
24. Butun, I., Österberg, P., & Song, H. (2020). Security of the internet of things: Vulnerabilities. *Attacks, and Countermeasures, IEEE Communications Surveys Tutorials, 22*(1), 616–644.
25. Hanif, M., & Song, H. (2019). Blocks' Network: Redesign Architecture Based on Blockchain Technology, In *IEEE International Conference on Industrial Internet (ICII), Orlando, FL, USA*, pp. 34–39.
26. Vangala, A., Bera, B., Saha, S., Das, A. K., Kumar, N., & Park, Y. (2021). Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems. *IEEE Sensors Journal, 21*(14), 15824–15838.
27. Hassija, V., Chamola, V., Gupta, V., Jain, S., & Guizani, N. (2020). A survey on supply chain security: Application areas, security threats, and solution architectures. *IEEE Internet of Things Journal, 8*(8), 6222–6246.
28. Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., Song, H., Alshamari, M., & Cao, Y. (2021). A survey on blockchain technology: Evolution, architecture and security. *IEEE Access, 9*, 61048–61073.
29. Hassija, V., Chamola, V., Krishna, D. N. G., Kumar, N., & Guizani, M. (2020). A blockchain and edge-computing-based secure framework for government tender allocation. *IEEE Internet of Things Journal, 8*(4), 2409–2418.
30. Nerurkar, P., Patel, D., Busnel, Y., Ludinard, R., Kumari, S., & Khan, M. K. (2021). Dissecting bitcoin blockchain: Empirical analysis of bitcoin network (2009–2020). *Journal of Network and Computer Applications, 177*, 102940.
31. Hassija, V., Chamola, V., & Zeadally, S. (2020). Bitfund: A blockchain-based crowd funding platform for future smart and connected nation. *Sustainable Cities and Society, 60*, 102145.
32. Hassija, V., Gupta, V., Garg, S., & Chamola, V. Traffic jam probability estimation based on blockchain and deep neural networks, IEEE Transactions on Intelligent Transportation Systems.
33. Hassija, V., Saxena, V., Chamola, V., & Yu, F. R. (2020). A parking slot allocation framework based on virtual voting and adaptive pricing algorithm. *IEEE Transactions on Vehicular Technology, 69*(6), 5945–5957.
34. Alladi, T., Chamola, V., Sahu, N., & Guizani, M. (2020). Applications of blockchain in unmanned aerial vehicles: A review. *Vehicular Communications, 23*, 100249.
35. Hassija, V., Chamola, V., Krishna, D. N. G., & Guizani, M. (2020). A distributed framework for energy trading between uavs and charging stations for critical applications. *IEEE Transactions on Vehicular Technology, 69*(5), 5391–5402.
36. Karunarathne, S. M., Saxena, N., & Khan, M. K. Security and privacy in iot smart healthcare, IEEE Internet Computing.
37. Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K.-K.R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & Security,* 101966.
38. Chamola, V., Hassija, V., Gupta, V., & Guizani, M. (2020). A comprehensive review of the COVID-19 pandemic and the role of IOt, drones, AI, blockchain, and 5g in managing its impact. *IEEE Access, 8*, 90225–90265.
39. Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019). A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications, 126*, 45–58.
40. Hassija, V., Bansal, G., Chamola, V., Kumar, N., & Guizani, M. (2020). Secure lending: Blockchain and prospect theory-based decentralized credit scoring model. *IEEE Transactions on Network Science and Engineering, 7*(4), 2566–2575.
41. Chen, J., Lv, Z., & Song, H. (2019). Design of personnel big data management system based on blockchain. *Future Generation Computer Systems, 101*, 1122–1129.
42. Tian, Y., Yuan, J. & Song, H. (2019). Secure and Reliable Decentralized Truth Discovery Using Blockchain, In *IEEE Conference*

on Communications and Network Security (CNS), Washington, DC, USA, pp. 1–8.
43. Panda, S. S., Mohanta, B. K., Satapathy, U., Jena, D., Gountia, D., & Patra, T. K. (2019). Study of Blockchain Based Decentralized Consensus Algorithms, In *TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), Kochi, India*, pp. 908–913.
44. Mougayar, W. (2016). *The business blockchain: Promise, practice, and application of the next internet technology*. Wiley.
45. Basu, S., Maulik, U., & Chatterjee, O. (2016). Stability of consensus node orderings under imperfect network data. *IEEE Transactions on Computational Social Systems, 3*(3), 120–131.
46. Chaudhry, N., & Yousaf, M. M. (2018). Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities, In *2018 12th International Conference on Open Source Systems and Technologies (ICOSST), Lahore, Pakistan*, pp. 54–63.
47. Pahlajani, S., Kshirsagar, A., & Pachghare, V. (2019). Survey on Private Blockchain Consensus Algorithms, In *2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT), Chennai, India*, pp. 1–6.
48. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System, Cryptography Mailing list at https://metzdowd.com.
49. King, S., & Nadal, S. (2012). PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, Accessed on March 2021. https://decred.org/research/king2012.pdf.
50. Lamport, L. Paxos Made Simple, Sigact News - SIGACT 32.
51. Huang, D., Ma, X., & Zhang, S. (2020). Performance analysis of the raft consensus algorithm for private blockchains. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50*(1), 172–181.
52. Veronese, G. S., Correia, M., Bessani, A. N., Lung, L. C., & Verissimo, P. (2013). Efficient byzantine fault-tolerance. *IEEE Transactions on Computers, 62*(1), 16–30.
53. Zhang, L., & Li, Q. (2018). Research on Consensus Efficiency Based on Practical Byzantine Fault Tolerance, In *10th International Conference on Modelling, Identification and Control (ICMIC)*, Guiyang, China, pp. 1–6.
54. Gao, S., Yu, T., Zhu, J., & Cai, W. (2019). T-PBFT: An eigentrust-based practical Byzantine fault tolerance consensus algorithm. *China Communications, 16*(12), 111–123.
55. Du, M., Chen, Q., & Ma, X. (2020). MBFT: A New Consensus Algorithm for Consortium Blockchain. *IEEE Access, 8*, 87665–87675.
56. Biswas, S., Sharif, K., Li, F., Maharjan, S., Mohanty, S. P., & Wang, Y. (2020). PoBT: A lightweight consensus algorithm for scalable iot business blockchain. *IEEE Internet of Things Journal, 7*(3), 2343–2355.
57. Puthal, D., & Mohanty, S. P. (2019). Proof of authentication: IoT-friendly blockchains. *IEEE Potentials, 38*(1), 26–29.
58. Han, X., Yuan, Y., & Wang, F. (2019). A fair blockchain based on proof of credit. *IEEE Transactions on Computational Social Systems, 6*(5), 922–931.
59. Li, K., Li, H., Hou, H., Li, K., & Chen, Y. (2017). Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism Consortium Blockchain, In *2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Bangkok, Thailand*, pp. 466–473.
60. Sharkey, S., & Tewari, H. (2019). Alt-PoW: An Alternative Proof-of-Work Mechanism, In *IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), Newark, CA, USA*, pp. 11–18.
61. Kumar, M. A., Radhesyam, V., & SrinivasaRao, B. (2019). Front-End IoT Application for the Bitcoin based on Proof of Elapsed Time (PoET), In *Third International Conference on Inventive Systems and Control (ICISC), Coimbatore, India*, pp. 646–649.
62. Park, S., Kwon, A., Fuchsbauer, G., Gaži, P., Alwen, J., & Pietrzak, K. (2018). *SpaceMint: A Cryptocurrency Based on Proofs of Space* (pp. 480–499). Berlin Heidelberg, Berlin, Heidelberg: Springer.
63. Kamvar, S., Schlosser, M., & Garcia-molina, H. The EigenTrust Algorithm for Reputation Management in P2P Networks, The EigenTrust Algorithm for Reputation Management in P2P Networks.
64. Wazid, M., Das, A. K., Khan, M. K., Al-Ghaiheb, A.A.-D., Kumar, N., & Vasilakos, A. V. (2017). Secure authentication scheme for medicine anti-counterfeiting system in iot environment. *IEEE Internet of Things Journal, 4*(5), 1634–1646.
65. Das, A. K., & Bruhadeshwar, B. (2013). An improved and effective secure password-based authentication and key agreement scheme using smart cards for the telecare medicine information system. *Journal of Medical Systems, 37*(5), 1–17.
66. Chaudhary, R., Jindal, A., Aujla, G. S., Kumar, N., Das, A. K., & Saxena, N. (2018). LSCSH: Lattice-based secure cryptosystem for smart healthcare in smart cities environment. *IEEE Communications Magazine, 56*(4), 24–32.
67. Odelu, V., Das, A. K., & Goswami, A. (2016). SEAP: Secure and efficient authentication protocol for NFC applications using pseudonyms. *IEEE Transactions on Consumer Electronics, 62*(1), 30–38.
68. Chatterjee, S., & Das, A. K. (2015). An effective ECC-based user access control scheme with attribute-based encryption for wireless sensor networks. *Security and Communication Networks, 8*(9), 1752–11771.
69. Jangirala, S., Das, A. K., & Vasilakos, A. V. (2020). Designing secure lightweight blockchain-enabled rfid-based authentication protocol for supply chains in 5G mobile edge computing environment. *IEEE Transactions on Industrial Informatics, 16*(11), 7081–7093.
70. Das, A. K. (2012). A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks. *International Journal of Information Security, 11*(3), 189–211.
71. Bera, B., Saha, S., Das, A. K., Kumar, N., Lorenz, P., & Alazab, M. (2020). Blockchain-envisioned secure data delivery and collection scheme for 5g-based Iot-enabled internet of drones environment. *IEEE Transactions on Vehicular Technology, 69*(8), 9097–9111.
72. Zeadally, S., Das, A. K., & Sklavos, N. (2021). Cryptographic technologies and protocol standards for internet of things. *Internet of Things, 14*, 100075.
73. Goswami, S. A., Padhya, B. P., & Patel, K. D. (2019). Internet of Things: Applications, Challenges and Research Issues, In *Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India*, pp. 47–50.
74. Abdul Sattar, K., & Al-Omary, A. (2020). A survey: security issues in IoT environment and IoT architecture, In *3rd Smart Cities Symposium (SCS 2020)*, Vol. 2020, Online, pp. 96–102.
75. Tewari, N., & Datt, G. (2021). A Systematic Review of Security Issues and challenges with Futuristic Wearable Internet of Things (IoTs), In *2021 International Conference on Technological Advancements and Innovations (ICTAI), Tashkent, Uzbekistan*, pp. 319–323.
76. Mishra, N., & Pandya, S. (2021). Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access, 9*, 59353–59377.
77. Bagga, P., Das, A. K., Wazid, M., Rodrigues, J. J. P. C., & Park, Y. (2020). Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges. *IEEE Access, 8*, 54314–54344.
78. Deogirikar, J., & Vidhate, A. (2017). Security attacks in IoT: A survey, In *International Conference on I-SMAC (IoT in Social,*

Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, pp. 32–37.
79. Okul, S., & Ali Aydın, M. (2017). Security Attacks on IoT, In *International Conference on Computer Science and Engineering (UBMK), Antalya, Turkey*, pp. 1–5.
80. Shim, K.-A. (2019). Universal forgery attacks on remote authentication schemes for wireless body area networks based on internet of things. *IEEE Internet of Things Journal, 6*(5), 9211–9212.
81. Bera, B., Das, A. K., Garg, S., Jalil Piran, M., & Hossain, M. S. (2022). Access control protocol for battlefield surveillance in drone-assisted IoT environment. *IEEE Internet of Things Journal, 9*(4), 2708–2721.
82. Samad, A., Alam, S., Shuaib, M., & Bokhari, M. (2018). *Internet of Vehicles (IoV) Requirements*. New Delhi: Attacks and Countermeasures.
83. Nosouhi, M. R., Sood, K., Grobler, M., & Doss, R. (2022). Towards spoofing resistant next generation Iot networks. *IEEE Transactions on Information Forensics and Security, 17*, 1669–1683.
84. Murali, S., & Jamalipour, A. (2020). A lightweight intrusion detection for sybil attack under mobile rpl in the internet of things. *IEEE Internet of Things Journal, 7*(1), 379–388.
85. Khanam, S., Ahmedy, I. B., Idna Idris, M. Y., Jaward, M. H., & Bin Md Sabri, A. Q. (2020). A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things. *IEEE Access, 8*, 219709–219743.
86. Bagga, P., Das, A. K., Wazid, M., Rodrigues, J. J. P. C., Choo, K.-K.R., & Park, Y. (2021). On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system. *IEEE Transactions on Vehicular Technology, 70*(2), 1736–1751.
87. Goudarzi, M., Wu, H., Palaniswami, M., & Buyya, R. (2021). an application placement technique for concurrent IoT applications in edge and fog computing environments. *IEEE Transactions on Mobile Computing, 20*(4), 1298–1311.
88. Sarigiannidis, P., Karapistoli, E., & Economides, A. A. (2015). Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information. *Expert Systems with Applications, 42*(21), 7560–7572.
89. Dolev, D., & Yao, A. (1983). On the security of public key protocols. *IEEE Transactions on Information Theory, 29*(2), 198–208.
90. Canetti, R., & Krawczyk, H. (2001). Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels, In *Advances in Cryptology – EUROCRYPT, Springer Berlin Heidelberg, Innsbruck (Tyrol), Austria*, pp. 453–474.
91. Messerges, T. S., Dabbish, E. A., & Sloan, R. H. (2002). Examining smart-card security under the threat of power analysis attacks. *IEEE Transactions on Computers, 51*(5), 541–552.
92. Malani, S., Srinivas, J., Das, A. K., Srinathan, K., & Jo, M. (2019). Certificate-based anonymous device access control scheme for IoT environment. *IEEE Internet of Things Journal, 6*(6), 9762–9773.
93. Das, A. K., Wazid, M., Yannam, A. R., Rodrigues, J. J. P. C., & Park, Y. (2019). Provably secure ECC-based device access control and key agreement protocol for IoT environment. *IEEE Access, 7*, 55382–55397.
94. Chaudhry, S. A., Yahya, K., Al-Turjman, F., & Yang, M. H. (2020). A secure and reliable device access control scheme for IoT based sensor cloud systems. *IEEE Access, 8*, 139244–139254.
95. Chaudhry, S. A., Alhakami, H., Baz, A., & Al-Turjman, F. (2020). Securing demand response management: A certificate-based access control in smart grid edge computing infrastructure. *IEEE Access, 8*, 101235–101243.
96. Siddhartha, V., Gaba, G. S., & Kansal, L. (2020). A lightweight authentication protocol using implicit certificates for securing IoT systems. *Procedia Computer Science, 167*, 85–96.
97. Zhou, Y., Zhang, Y., & Fang, Y. (2007). Access control in wireless sensor networks. *Ad Hoc Networks, 5*(1), 3–13.
98. Song, Bin, Yu, In-Kwan, Son, Jiseong, & Baik, D. (2010). An effective access control mechanism in home network environment based on SPKI certificates, In *2010 IEEE International Conference on Information Theory and Information Security, Beijing, China*, pp. 592–595.
99. Porambage, P., Kumar, P., Schmitt, C., Gurtov, A., & Ylianttila, M. (2013). Certificate-Based Pairwise Key Establishment Protocol for Wireless Sensor Networks, In *2013 IEEE 16th International Conference on Computational Science and Engineering, Sydney, NSW, Australia*, pp. 667–674.
100. Ellison, C., Frantz, B., Lampson, B., Rivest, R., Thomas, B., & Ylonen, T. (1999). RFC2693: SPKI Certificate Theory.
101. Ali, Z., Ghani, A., Khan, I., Chaudhry, S. A., Islam, S. H., & Giri, D. (2020). A robust authentication and access control protocol for securing wireless healthcare sensor networks. *Journal of Information Security and Applications, 52*, 102502.
102. Luo, M., Luo, Y., Wan, Y., & Wang, Z. Secure and Efficient Access Control Scheme for Wireless Sensor Networks in the Cross-Domain Context of the IoT, Security and Communication Networks.
103. Li, F., Han, Y., & Jin, C. (2016). Practical access control for sensor networks in the context of the internet of things. *Computer Communications, 89–90*, 154–164.
104. Kumar, P., Gurtov, A., Iinatti, J., Sain, M., & Ha, P. H. (2016). Access control protocol with node privacy in wireless sensor networks. *IEEE Sensors Journal, 16*(22), 8142–8150.
105. Riad, K., Hamza, R., & Yan, H. (2019). Sensitive and energetic IoT access control for managing cloud electronic health records. *IEEE Access, 7*, 86384–86393.
106. Yang, Y., Liu, X., & Deng, R. H. (2018). Lightweight break-glass access control system for healthcare internet-of-things. *IEEE Transactions on Industrial Informatics, 14*(8), 3610–3617.
107. Dammak, M., Senouci, S. M., Messous, M. A., Elhdhili, M. H., & Gransart, C. (2020). Decentralized lightweight group key management for dynamic access control in IoT environments. *IEEE Transactions on Network and Service Management, 17*(3), 1742–1757.
108. Liu, Y., Xue, K., He, P., Wei, D. S. L., & Guizani, M. (2020). An Efficient accountable, and privacy-preserving access control scheme for internet of things in a sharing economy environment. *IEEE Internet of Things Journal, 7*(7), 6634–6646.
109. Mandal, S., Bera, B., Sutrala, A. K., Das, A. K., Choo, K. R., & Park, Y. (2020). Certificateless-signcryption-based three-factor user access control scheme for IoT environment. *IEEE Internet of Things Journal, 7*(4), 3184–3197.
110. Braeken, A., Porambage, P., Stojmenovic, M., & Lambrinos, L. (2016). EDAAAS: Efficient distributed anonymous authentication and access in smart homes. *International Journal of Distributed Sensor Networks, 12*(12), 1–11.
111. Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. (2015). The internet of things for health care: A comprehensive survey. *IEEE Access, 3*, 678–708.
112. Saha, S., Sutrala, A. K., Das, A. K., Kumar, N., & Rodrigues, J. J. P. C. (2020). On the Design of Blockchain-Based Access Control Protocol for IoT-Enabled Healthcare Applications, In *2020 IEEE International Conference on Communications (ICC), Dublin, Ireland*, pp. 1–6.
113. Rajput, A. R., Li, Q., Taleby Ahvanooey, M., & Masood, I. (2019). EACMS: Emergency access control management system for personal health record based on blockchain. *IEEE Access, 7*, 84304–84317.
114. Chen, S., Wen, H., Wu, J., Lei, W., Hou, W., Liu, W., Xu, A., & Jiang, Y. (2019). Internet of Things Based Smart Grids Supported by Intelligent Edge Computing. *IEEE Access, 7*, 74089–74102.

115. Xue, J., Xu, C., & Zhang, Y. (2018). Private blockchain-based secure access control for smart home systems. *KSII Transactions on Internet and Information Systems, 12*, 6057–6078.
116. Gharibi, M., Boutaba, R., & Waslander, S. L. (2016). Internet of drones. *IEEE Access, 4*, 1148–1162.
117. Bera, B., Chattaraj, D., & Das, A. K. (2020). Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment. *Computer Communications, 153*, 229–249.
118. Xu, Z., Liang, W., Li, K.-C., Xu, J., & Jin, H. (2021). A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles. *Journal of Parallel and Distributed Computing, 149*, 29–39.
119. Zhou, Y., Guan, Y., Zhang, Z., & Li, F. (2019). A Blockchain-Based Access Control Scheme for Smart Grids, In *2019 International Conference on Networking and Network Applications (NaNA), Daegu, South Korea*, pp. 368–373.
120. Mbarek, B., Ge, M., & Pitner, T. (2020). Blockchain-Based Access Control for IoT in Smart Home Systems, In *International Conference on Database and Expert Systems Applications (DEXA'20), Linz Austria*, pp. 17–32.
121. Arshad, J., Siddique, M. A. B., Zulfiqar, Z., Khokhar, A., Salim, S., Younas, T., Rehman, A. U. , & Asad, A. (2020). A Novel Remote User Authentication Scheme by using Private Blockchain-Based Secure Access Control for Agriculture Monitoring, In *2020 International Conference on Engineering and Emerging Technologies (ICEET), Lahore,Pakistan*, pp. 1–9.
122. May, W. E. (2015). Secure Hash Standard, FIPS PUB 180-1, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, April 1995. Accessed on June 2020 . http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.
123. Barker, E. (2021). Recommendation for Key Management, special Publication 800-57 Part 1 Rev. 4, NIST, 01/2016. Accessed on September 2021. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf.
124. Advanced Encryption Standard, FIPS PUB 197, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, November 2001. Accessed on June 2020. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
125. Zhou, L., Wang, L., Sun, Y., & Lv, P. (2018). BeeKeeper: A blockchain-based IoT system with secure storage and homomorphic computation. *IEEE Access, 6*, 43472–43488.
126. Cha, S.-C., Tsai, T.-Y., Peng, W.-C., Huang, T.-C., & Hsu, T.-Y. (2017). Privacy-aware and blockchain connected gateways for users to access legacy IoT devices, In *IEEE 6th Global Conference on Consumer Electronics (GCCE), Nagoya, Japan*, pp. 1–3.
127. Sharma, P. K., Chen, M.-Y., & Park, J. H. (2018). A software defined fog node based distributed blockchain cloud architecture for IoT. *IEEE Access, 6*, 115–124.
128. Sankaran, S., Sanju, S., & Achuthan, K. (2018). Towards Realistic Energy Profiling of Blockchains for Securing Internet of Things, In *IEEE 38th International Conference on Distributed Computing Systems (ICDCS), Vienna, Austria*, pp. 1454–1459.
129. Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Integration of blockchain and cloud of things: Architecture applications and challenges. *IEEE Communications Surveys Tutorials, 22*(4), 2521–2549.
130. Zheng, P., Xu, Q., Zheng, Z., Zhou, Z., Yan, Y., & Zhang, H. (2021). Meepo: Sharded Consortium Blockchain, in: IEEE 37th International Conference on Data Engineering (ICDE), Athens, Greece, pp. 1847–1852.
131. Hewa, T. M., Kalla, A., Nag, A., Ylianttila, M. E., & Liyanage, M. (2020). Blockchain for 5G and IoT: Opportunities and Challenges, In *IEEE Eighth International Conference on Communications and Networking (ComNet), Hammamet, Tunisia*, pp. 1–8.
132. Hua, J., Zhu, H., Wang, F., Liu, X., Lu, R., Li, H., & Zhang, Y. (2019). CINEMA: Efficient and privacy-preserving online medical primary diagnosis with skyline query. *IEEE Internet of Things Journal, 6*(2), 1450–1461.

Palak Bagga received her Ph.D. degree in computer science and engineering from IIIT Hyderabad, India, in 2022. She also received her M.Tech. degree in Computer Science and Engineering from Uttar Pradesh Technical University, India. She is currently working as a Senior Engineer at Qualcomm, Hyderabad, India. She was a gold medalist in academics and also awarded by a Certificate of Merit. Her research interests include network security, and security in Internet of Things and Internet of Vehicles. She has published several journal articles in her research areas.

Ashok Kumar Das received a Ph.D. degree in computer science and engineering, an M.Tech. degree in computer science and data processing, and an M.Sc. degree in mathematics from IIT Kharagpur, India. He is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, IIIT, Hyderabad, India. He is also working as a visiting faculty with the Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA 23435, USA. His current research interests include cryptography, system and network security including security in smart grid, Internet of Things (IoT), Internet of Drones (IoD), Internet of Vehicles (IoV), Cyber-Physical Systems (CPS) and cloud computing, blockchain and AI/ML security. He has authored over 305 papers in international journals and conferences in the above areas, including over 265 reputed journal papers. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He was/is on the editorial board of IEEE Systems Journal, Journal of Network and Computer Applications (Elsevier), Computer Communications (Elsevier), Journal of Cloud Computing (Springer), Cyber Security and Applications (Elsevier), IET Communications, KSII Transactions on Internet and Information Systems, and International Journal of Internet Technology and Secured Transactions (Inderscience). He also severed as one of the Technical Program Committee Chairs of the first International Congress on Blockchain and Applications (BLOCKCHAIN'19), Avila, Spain, June 2019, International Conference on Applied Soft Computing and Communication Networks (ACN'20), October 2020, Chennai, India, and second International Congress on Blockchain and Applications (BLOCKCHAIN'20), L'Aquila, Italy, October 2020. His Google Scholar h-index is 67 and i10 index is 194 with over 12,960 citations.

Vinay Chamola is currently Assistant Professor in Dept. of Electrical and Electronics Engg., BITS-Pilani, Pilani campus. Vinay received his B.E. degree in Electrical & Electronics Engineering and Master's degree in communication engineering from Birla Institute of Technology & Science (BITS), Pilani, India in 2010 and 2013 respectively. He received his Ph.D. degree in Electrical and Computer Engineering from the National University of Singapore, Singapore, in 2016. From June to Aug. 2015, he was a visiting researcher at the Autonomous Networks Research Group (ANRG) at the University of Southern California (USC), USA. After his PhD, he worked as a postdoctoral researcher at the National University of Singapore in the area of Internet of Things. His research interests include IoT security, Blockchain, 5G resource management, Drones, VANETs and BCI. He is an Associate Editor of various journals including Ad Hoc Networks, IEEE Internet of Things Magazine, IEEE Networking letters, IET Networks, and IET Quantum Communications.

Mohsen Guizani received the B.S. (Hons.) and M.S. degrees in electrical engineering and the M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He is currently a Professor with the Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), Masdar City, Abu Dhabi, United Arab Emirates (UAE). Previously, he has served in different academic and administrative positions for the Qatar University, University of Idaho, Western Michigan University, the University of West Florida, the University of Missouri-Kansas City, the University of Colorado-Boulder, and Syracuse University. He is the author of nine books and more than 1100 publications in refereed journals and conferences. He guest edited a number of special issues in IEEE journals and magazines. His research interests include wireless communications and mobile computing, computer networks, mobile cloud computing, security, and smart grid. He is also a Senior Member of ACM. Throughout his career, he received three teaching awards and four research awards. He was a recipient of the 2017 IEEE Communications Society Wireless Technical Committee (WTC) Recognition Award, the 2018 AdHoc Technical Committee Recognition Award for his contribution to outstanding research in wireless communications and Ad-Hoc Sensor networks, and the 2019 IEEE Communications and Information Security Technical Recognition (CISTC) Award for outstanding contributions to the technological advancement of security. He was the Chair of the IEEE Communications Society Wireless Technical Committee and the Chair of the TAOS Technical Committee. He has served as a member, the chair, and the general chair of a number of international conferences. He is also the Editor-in-Chief of the IEEE Network. He serves on the editorial boards for several international technical journals. He also serves the Founder and the Editor-in-Chief for Wireless Communications and Mobile Computing journal (Wiley). He has also served as the IEEE Computer Society Distinguished Speaker. He is also the IEEE ComSoc Distinguished Lecturer. He is an Associate Editor of various journals including Ad Hoc Networks, IEEE Internet of Things Magazine, IEEE Networking letters, IET Networks, and IET Quantum Communications.