Blockchain Integrated Framework for Resolving Privacy Issues in Smart City

Pradeep Bedi, S. B. Goyal, Jugnesh Kumar, and Shailesh Kumar

Abstract Smart City is the concept for improvising the urban cities operating and services efficiency by making use of IoT (Internet of things) which is a modular approach that operates by deploying sensors with significant qualities and integrating them with ICT (Information and Communication Technologies) solutions. The application area for the IoT platform has been in smart building and office management, transportation, environmental degradation surveillance, and smart grid management, etc. However, maintaining an efficient architecture for its operation in a complex environment has been a challenge for several years. This will increase the security and privacy concerns with the increase in smart applications within smart cities. This chapter aims to study the issues related to data integrity and security and the approach used to resolve these issues using blockchain analytics algorithms and architecture. This chapter also gives the future direction towards achieving low-cost architectural management for smart cities. This chapter is mainly focused to analyze such challenges and to identify limitations of the existing secure smart cities framework and to proposes an effective blockchain-based smart city interaction framework.

Keywords Smart cities · Internet of things (IoT) · Blockchain · Distributed ledger technology · Consensus protocol · Authentication · Privacy · Security

P. Bedi
Lingayas Vidyapeeth, Faridabad, India

S. B. Goyal (✉)
City University, Petaling Jaya, Malaysia

J. Kumar
St. Andrews Institute of Technology and Management, Gurgaon, India
e-mail: jugnesh@rediffmail.com

S. Kumar
BlueCrest College, Freetown, Sierra Leone
e-mail: Shailesh.kumar@bluecrestcollege.com

C. Chakraborty et al. (eds.), *Data-Driven Mining, Learning and Analytics for Secured Smart Cities*, Advanced Sciences and Technologies for Security Applications, https://doi.org/10.1007/978-3-030-72139-8_6

1 Introduction

In the past few years, there are many social, environmental, and economic issues that arises due to the quick urbanization of the population of the world. These problems influence the living conditions of people and life's quality significantly. These problems can be resolved by an idea of a smart city. The primary goal of smart cities is the proper utilization of the resources of the public, provide high quality services to citizens, and enhancing the living standard of people. The Information and Communication Technology (ICT) plays a major role in developing the concept of smart cities [1].

A smart city is vulnerable to many security attacks due to the nature of smart devices. It is very necessary to design the secure system to spot those threats and their effects. In this field, many research has been directed like OWASP (Open Web Application Security Project) enlisting generic security attacks, CERT (Computer Emergency Response Teams) giving the probable penetrability in the graphical form, CCSP (Cloud Computer Service Provider) series of G-Cloud is for cloud security. In Smart cities following categories of threat are recognized.

- Availability Threats
- Integrity Threats
- Confidentiality Threats
- Authenticity Threats
- Accountability Threats.

The future technology such as blockchain has varied characteristics like trust independence, democracy, transparency, automation, security, pseudonymity, and automation. These characteristics are very useful for enhancing the services of smart cities and support the evolution of smart cities. Enhancing data security is the key benefit of using blockchain technology. In the world of data, security is the most crucial aspect that needed to be focused by all organizations or institutions. Blockchain technology is capable to solve these issues so the deployment of the mechanism of the blockchain is the solution to these problems [2]. The Effects of blockchain on data security are as follows:

- Considering whole protection: For preventing the data from data-modification attack, blockchain technology is used for encryption of data. The blockchain stores the document as the cryptographic data. This confirms to users that the file is immutable until requesting to save the entire document in the blockchain. The Cross verification of the signature of the file is done by all the blocks due to the decentralized nature of blockchain. If the unauthorized entity tries to modify the file then verification of the signature will fail. The method for authentic and free data verification is undoubtedly given by blockchain. There is no possibility of failure in blockchain technology and cannot be settled by any system because blockchain does not store the record in any central location. The decentralized and scattered ledger of blockchain network modernize regularly in a proportional way. Hackers can fetch all information from a single system or server and attempt

to deal with it in traditional networks, which is not possible with networks of blockchain.

- Decentralized procedure: Blockchain is decentralized in nature so it is independent of any centric authority. Every node preserves an integrated copy of information due to the use of a digital ledger. There is no central control point so the system is suited as extra impartial. For the validation of transactions, various kind of consensus processes. Because it is independent of any middle authority for controlling transactions securely and data are stored in several nodes. Even after failing one or more systems, this technology is intensely secured.
- Communication environment Effects: The blockchain-based environment of IoT is dependent on the techniques of encryption for delivering security when installing consensus on a distributed environment. If anyone wants to append something to the chain then he/she has the allowance to append a block in the chain. Its mechanism complies with an algorithm and instead requests the use of computing power in excess. For example, the power of computation required for implementing the tasks of networking consumes an equal amount of energy as required by the 159 countries in the bitcoin network in comparison with the previous year. It is dominant to about the need for energy in blockchain deployment in the environment of IoT.
- Cost factor: Cost is another important challenge in the IoT environment based on Blockchain. Blockchain programs are not effective in the transaction's accomplishment and the need for components related to energy. For example, the program of bitcoin implements 3–5 transactions in one second and requires a large amount of energy for competing for these transactions while Visa executes transactions about 1,667 per second so it is worst in the performance on comparing with other platforms, therefore the Very high cost is required for establishing the IoT environment based on Blockchain. We cannot spend a huge share of the country's budget to secure certain computing infrastructure. The budget is very high so only some countries have the economy for supporting these types of schemes of communication. We are required to develop effective methods for their deployment in the IoT based on the blockchain so this is one more problem for the working people of the same domain.
- Loads from technology blockchain: Blockchain technology is deployed with the dispersed ledger and the algorithms of cryptography. For operating the transaction more resources and time are needed in the transactions of blockchain. To secure the exchange of information is the main aim of the IoT environment based on blockchain technology, this can be done via the deployment of the mechanism of blockchain, but the transaction processing time in the blockchain is extra. Fast data communication is the main need in some domains like healthcare, battlefield, and rescue operations. If the information exchange and processing require more time then the Conscious recipient will not obtain the information in the required time so the concerned authority will not be capable of decision making in the required reaction time. Convenient cryptographic operations required a low cost of communications, computation, and storage for transaction processing, so the use

of Convenient cryptographic operations can be used for resolving those problems [3–8].

The key contributions of this chapter are as following:

- In this chapter a state-of-the-art about blockchain technology and frameworks are presented along with protocols, applications, and challenges.
- This chapter have illustrated the application of blockchain to facilitate security in smart cities such that it improves the performance.
- This chapter also surveyed application of different blockchain protocols in different sectors of smart city such as healthcare, industries, energy generation, industries, etc.
- This chapter also surveyed the security aspects of existing techniques and illustrated their challenges faced. This chapter mainly aims to identify the open issues and challenges faced while deploying blockchain as a security solution.
- This chapter also proposed the blockchain-based framework is proposed for smart cities to incorporate with security issues and provide a trusted environment for user data transactions.
- In last theoretical comparison of proposed framework is given with existing works that would be beneficial for future research directions.

The remaining section of this chapter are illustrated to be as follows: Sect. 2 introduced the background knowledge of blockchain technology along with that their types, working steps, and protocols are discussed. In Sect. 3 chapter gives an overview of smart cities. Section 4 gives an overview of security issues and challenges faced in smart cities. Section 5 gives an analytical overview about the implementation of blockchain in different applications of smart city. After observing the issues faced during the implementation of blockchain in smart cities, Sect. 6 proposes an architecture to handle security issues in smart cities. Finally, in Sect. 8 conclusion and future research scope are discussed.

2 Overview of Blockchain

In the current time, the living standard of our society has been revolutionized by the latest technologies due to the innovation of semiconductor and communication technologies that allow the devices to link with each other over a network and change the way of association between machines and humans and that concept is Known as IoT. Due to the rapid growth in smart devices and networks with high speed, IoT is in the trend and wide acceptance because low-power lossy networks (LLNs) are used in it. These LLNs can operate the limited resource by very low power consumption. The devices may be remotely controllable to complete the specific task. The sharing of data between the devices is done with the help of a network that employs the communication standard protocols. Properly connected things such as devices have

sensors (Detectors) and chips so they differ from simple wearable equipment to large machines [9].

Yet, as the technologies become prevalent the connectivity between devices is enhancing, and also the infrastructure can become very complex. The cyber-attacks vulnerabilities are increasing due to this complexity. The physical devices are stetted in the unsecured environments in the IoT, which could have no defense method from hackers is a great chance for hackers to change the facts transmitting on the network. So, the authorizations of devices and the information root would be a big problem. In the last few years, blockchain technology becomes a technology with many features to solve the different issues of network devices of IoT [10].

Blockchain maintains the database of records that are distributed. Third-party deprive properly, the demonstration of effort between the nodes of network help in resolving the failure problems of a single point. The public trust and get attracted to the IoT network because It's data cannot be changeable over time and established by the history of networks of IoT. The trust of the public have a very important role in public finance transactions and is the starting of the new world of the divisional economy in the domain of IoT. The blockchain is the series of blocks that hold all the eventful blockchain network transactions. Each block has a block header and block body transaction counter.

Block header contains the following.

- Block version for indicating the version of software and rules of validation.
- Merkle Tree root hash for showing the transaction's hash value and all transaction summary.
- The timestamp contains the current universal time since January 1970 that is epoch time.
- N-Bits represents the bit number necessary for verification of the transaction.
- Any 4-byte number, starting from 0 and rise for every hash of the transaction is known as Nonce.
- The parent block kept the hash value to point to the previous block.

The Transaction counter is efficient to cover all the transactions and the highest number of the transaction depends on the size of the block. Blockchain technology is defined as the public registry and the list of blocks that records all the completed transactions. The list of blocks increases on adding the new block in the list continuously. For the security of the user, Public-key cryptography and distributed consensus algorithms are implemented. Persistency, anonymity, and audit ability are the key features of blockchain technology used for enhancing efficiency and saving cost [11].

2.1 Types of Blockchain

Public blockchain: It is the system based on the permission-less, non-restrictive dispersed ledger. Anyone can access the blockchain platform via registering and signing in with the help of the Internet. A node (user), who is an element of the

public blockchain has the authority to influence records, confirm the transactions, and arrange the mining for the new incoming block. The exchange of cryptocurrencies is the primary use of public blockchain. If the users adhere to the guidelines of security the public blockchain is mostly secured and very risky in the case of users who do not adhere to the guidelines of security. Ethereum, litecoin, and bitcoin are some famous examples of public blockchain [12].

Private blockchain: It works only for closed networks because it is a blockchain with restrictions or permissions. Mostly it is used in the companies or enterprises of selected participants. Authorizations, accessibility, and security are some dominant features used as a command for organization controlling. A private blockchain is similar to a public blockchain, but it has a small or restrictive network. Private blockchain Deployment can be done for performing some fixed operations like management of supply chain, ownership of assets, and voting. Projects of hyperledger and multichain are the example of private blockchain [13].

Consortium Blockchain: It is semi-decentralized so the network of blockchain is managed by many organizations. A private blockchain is operated by only one organization so these both are different in the term of management. In this blockchain, many organizations work as an authority for exchanging and mining the data. These are used in the govt. Companies and banking sectors. R3 and web foundation of energy are some consortium blockchain examples [14–16] (Table 1).

Hybrid Blockchain: The combination of the public and private blockchain platform is represented as the hybrid blockchain. The characteristics of both are appealed in this platform like users can have a "public permission-less system" and "private permission-based system". In the platform of hybrid blockchain, users can be capable to control the acquirement of blockchain stored data. Only Some selected data are publicly accessible and the rest data are kept secret in a private network. It is a malleable system so the merging of private blockchain in several public blockchains can be done by the user easily. The certain network will verify the transaction of a private network in the platform of hybrid blockchain and users can also discharge these transactions in public for the process of blockchain. More verifications requirement and an increase in hashing are done by the platform of public blockchain so the transparency and security of the blockchain network get enhanced. Ex of hybrid blockchain—"Dragon chain".

Table 1 Comparison of blockchain types

Features	Public	Private	Consortium
Nature	Open	Limited	Limited
Transparency	Less	More	More
Energy usage	More	Less	Less
Scalable	Yes	Yes	Not much
Efficiency	Less	More	More
Example	Bitcoin Ethereum Litecoin	Hyperledger	Blockstack

2.2 Working Steps of Blockchain

Nodes communicate with the network of blockchain by compositing private & public keys together. The User for signing his transaction uses his private key and access the network with the public key. Each signed transaction is transmitted by that transaction making node.

All the nodes expect the transaction-making node to verify that transaction in the blockchain network and all the invalid transactions are rejected during this process and this entire process is known as the verification process.

The third step is mining in which every effectual transaction is gathered by the nodes of the network in a fixed time into the block and for a finding of its block, a proof-of-work is implemented. The node transmits the block to all participating nodes after finding the nonce.

A newly generated block is collected by each node to check the block contains transaction is legal and declares the efficiency of the parent block by using the hash value. Nodes will append the block to the blockchain and apply the transactions After the completion of confirmation for keeping the blockchain updated. The projected block is refused and the current mining round ends if the confirmation of the block failed.

Blockchain technology resolves issues of duplication by using the asymmetric cryptography assistant, which has privacy and a public key. The public key is common among all nodes while. The private key remains secret for other nodes. Yet the transaction is signed by a node digitally that makes the transaction and is transited to the whole network of blockchain. All the Accepting nodes will confirm the transactions by signature decrypting with the initializing node public key. The verification of the signature represents the modification in the initializing node.

2.3 Protocols

Proof-of-Work (PoW): The process in this case precisely monitors the node that is intended to be attached with the block that has been recently mined and further with the actual chain that commits the presence of certain proof for such conjunction. This process or architecture works on certain proof-based scenario [17]. The broadcast of blocks by the nodes or collection having equally verified transactions, an ambiguity pops up then the transaction will be put into a block by the node. PoW resolves this matter where the computationally tedious puzzle is solved by nodes for the sake of receiving a chance of linking the freshly constructed block to the existing chain. The hash value of all the entities of a decentralized network is required to be calculated on regular basis through the assistance of various arbitrary values known as ‘nonce’. Because of the struggles levied in the prediction of hashing function based outcome values from the set of predefined and existing input variables that shall allow guessing of an improved one has been a complicated task to be executed. As the nonce that

is desirable has been achieved, the respective block is being broadcasted by miners to verify the solution it is employed by all other network nodes. When the block is approved by all the blocks, it is linked to the existing chain. To guess a suitable nonce value the effort applied by the nodes is called the PoW.

Addition to this, there are many such situations when numerous of miner resolves the puzzle as well as discovers the nonce [18]. In this condition, the block is tried by these miners to broadcast as well as nonce is calculated in the complete network. An ambiguity amidst the miners is the resultant of this network that block must be desired and attached to the current chain that comes out as a "forking problem". The generation of a fork or branch is done for the reason being that only the initial first block is verified by the miners and rests are ignored. For handling the forking problem effectively the longest chain rule is employed by PoW.

The entire scenario may result in circumstances where the nonce finding is achieved by the miner by undergoing the solving procedure number of puzzles at the same time [18]. During the situations described above, the main function of the miner is directed towards broadcasting their block in combination with the nonce that has been determined to the complete network architecture. However, there has been certain vagueness and ambiguity amongst these miners arising due to multiple broadcasting phenomenons where it faces a problem with the decision-making process of which block has to be considered for the addition to the chain present that is often referred to as the "forking issue". The reason for the fork formation is the first consideration of block by the miners and neglecting the remaining others. The forking problem has been tackled by the PoW via the longest chain rule mechanism.

Proof of Stake (PoS): The PoW based energy competent alternative is the PoS where the miners are assigned to work for the block creation that shall be beneficial in attaining the system hold properly; rather than misspending the computational resources in resolving a complicated mathematical puzzle [19]. The wealth of contributing nodes or their stake in the system is completely responsible for providing possibilities to receive a moment for block validation. Moreover, an abundant stake reduces the chances of any hostile or ill activity that can occur on the network. The selection of a validator is done to consider its hold in the network and this stake helps it to place a bet. When the block is successfully approved, then a fee is received by the validators. Because of the ability of PoS in providing latency, better throughput energy efficiency, it is considered to be imperishable in comparison to PoW. Apart from this, PoS has many shortcomings. At first, the nodes with more wealth might get more block validation chances because validators are selected which is mainly dependent on the stakes and their values. The few nodes are being directed, as per the situation, for governing in the network so that it results in centralization or ill interference. And it has less mining cost use in comparison to PoW which makes this consensus protocol susceptible to ill activities.

Proof of Burn (PoB): PoB designing has been achieved to devastate the cryptographic forms of money. The entire process has been designed in two major forms were first being the cryptocurrency address generation attained by a certain programming algorithm that completely crushes the money received in the produced address. Another way of destroying the unauthorized currency is by generating a function that

is dedicated towards verification of the addresses where the currency is received in crypto. The PoB validators are being rewarded and are even permitted for separate block generation for the events where they can spend the coins by transmitting them to the addresses that are found to be completely public and verified. The process of the PoB is found to be beneficial in handling the coins in the blockchain along with tackling the energy consumption-related problems with the PoW whose result is an increment in the value of the coin. The important tasks associated with the burning system of coins is maintaining a balance of the coins, coin spending if they are unsold, and most importantly including the transaction work.

Practical Byzantine Fault Tolerance (PBFT): The design of the Byzantine Fault Tolerance (BFT) is so achieved that it helps allow the secure transfer of the consensus across the two communicating hubs/nodes despite the presence of certain malfunctioning vindictive hubs/nodes across a certain distribution network. A certain example of the BFT is the PBFT which is an algorithm of replication that is being designed to serve as a consensus protocol. The arrangement in the algorithm of PBFT has been done by the arrangement of nodes in sequential consecutive order and declaring one as the leader with the other as the backups. The functioning of receiving the signal is done by the leader which further transfers it to the backups that undergo processing mechanism and further generate the result to be sent to the originator via leader. Each node in PBFT contributes to the decision in PBFT which depends on maximum votes by nodes which determines the integrity and the origination of the message. In three phases the whole process of PBFT is determined, namely pre-prepared, prepared, and commit. The movement of a node in the network to the next phase is determined by the votes received from two-third of all the nodes. PBFT consensus mechanism is enabled to run efficiently though there is a presence of some malicious byzantine replicas [20] (Table 2).

Proof of Authority (PoA): The designing of PoA has been done as a genealogy forming associations with the protocols for the consensus which are constructed specially for permission blockchain. It gains remarkable execution achieved as it was seen capable of producing messages that are lighter for sending over the network when compared with the BFT algorithms. The algorithm of the PoA has the benefit over the PoW consensus algorithm in terms of reduced dependency as well as a reduction in energy consumption. Certain nodes are equipped with authoritative control all across the other nodes that shall assist in the creation of consensus and new block construction [21].

Table 2 Comparison of blockchain security protocols

Features	Pow	Pos	PoB	PBFT	PoA
Computational speed	High	High	Average	High	Average
Resource consumption	Less	Less	Average	High	High
Energy efficiency	Less	High	Less	High	Less

3 Smart City: An Overview

The population of world living in the cities will be growing up to 50–70%, till the year 2050. The requirements for services are increasing on increasing the population so it is necessary to contemplate the scheme of smart cities taking ICT (information from communication technologies). Smart-cities are implemented by uniting the sensors, networks, electronics, etc. Latest ICTs are dominant for smart cities including smart hospitals, technologies of smartphones, Identification of ratio frequency, artificial intelligence, cloud computing, and infrastructure of IoT.

The network of IoT [22, 23] consists of objects engrossed with electronics, smart sensors, software, and connections among them for exchanging and transferring information. Smart cities based on IoT provide services to administration and the public like smart-homes, surveillance systems, vehicular-traffic, smart-parking, smart grids, smart energy, ecological pollution, and climate systems. Due to the intercommunication of the physical and virtual worlds via electronic devices in houses, buildings, streets, and vehicles. At the current time, There are many problems [23, 24] in establishing the infrastructure of IoT in applications of a smart city. Sensors are constituted to cloud in the architecture of a smart city for inspecting the streaming data for decisions making. The paradigm of cloud computing and IoT works to give information and inputs to tasks for getting executed by mobiles, integrated sensors, vehicles, and humans (Fig. 1).

Qian et al. [25] proposed a framework for Hybrid IoT for computation, proper transmission, and caching of big data provoked by substantial and scattered devices of IoT fixed in the environment of smart cities. The Computation is based on Ultra intensive networking along with providing cloud access for multiple uses. The idea of smart city endorsement is necessary to utilize the control layer of medium access. The research conducted by Fan et al. [26] has focussed on the produces of the random number along with the quadric- residuals, for attaining the cloud-based complete security system that could be further deployed in the healthcare sector. Further, the work by Garg et al. [27] offered a stream for monitoring the transportation framework. They solve the security risk problem in spatial vehicles with the help of run time applications and varying tiers based analytics and calculations. The smart city project may encounter the cyber vulnerability that has been proposed to be solved by the prospective approaches linked with the data structure model to carry out the recognition of such threats. The data has been provided by the ultra spatial vehicles that tend to procure the information from various vehicles and the task of security has been achieved by the aggregators on the time of receiving of data by the edge devices by the transmission of the load. The work by the author however guarantees security during the vehicle's abnormal movements as well. The work on the architecture of the drone and its security issues are being dealt with by Lin et al. [28] whore research is directed towards the working of an unmanned vehicle operation. The issues of data security, its integrity, and the process of accessing it, has been solved by the simple cryptography procedure. The energy-saving problem associated with the smart cities development program shortly has been brought up by Kumar et al. [29]. They have

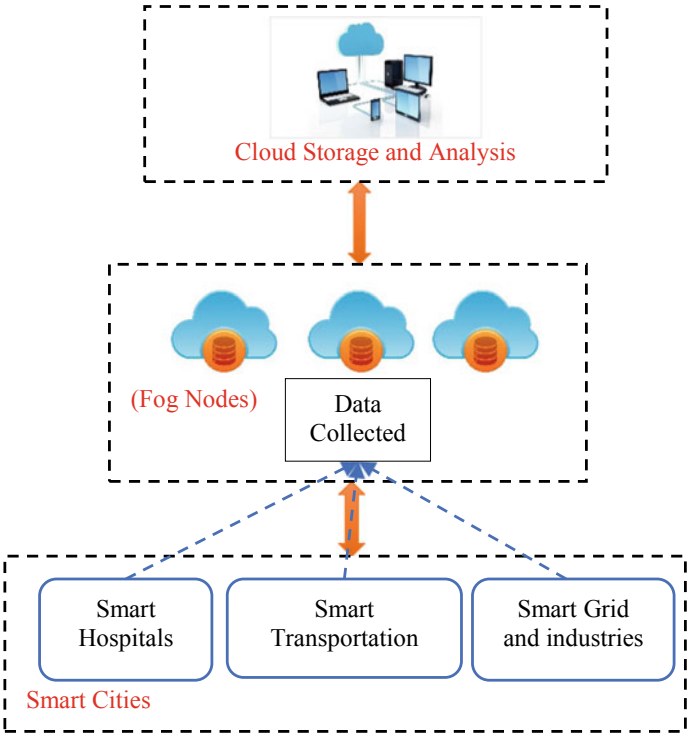

Fig. 1 The architecture of smart cities

used an infrastructure based on the cloud for decisions making to scrimp the energy for various devices. They aim to reduce the main grid overload by providing the capacity of continuous DC To all the machines of low voltage and having less support on the main grid. The process of development during its peak energy requirement is being analyzed and solved, by making the system more continual to tackle the energy demand evenly. Dener [30] inspected various researches for defining the importance of cloud computing in giving the application of computing, storage, numerous, and database for internet accessibility. These services given by the cloud are used for combining and transferring information among various smart city systems. Further, the research done by Khattak et al. [31] resulted in the development of a model for integrating clouds of vehicular-networking with IoT. The article properly describes the importance associated with the applications of the real-world that includes the formation of smart homes, smart city, and smart lighting of traffic for robotization and simple controlling and its combination with IoT-VC. Daniel et al. [32] offered a policy of management for maintaining small operational latency up to possibility and reducing the latency of the request in the architecture that employs the IoT mechanism linked with the server on the cloud itself in the development of smart cities. The main research is being focused in the article is on the parameters that

included the rush hours, outages along with the probability factor that has been considered on periodicity for demonstrating the latency factor of the operation that is found to be small in the contest without any reason to inspected articles. Perera et al. [33] describe the requirement of fog integration and computing on the cloud. In contemplation of characteristics and main advantages of computing fog like higher availability, management of latency, reducing the priority-based big data that hold up the use case scenarios. The sustainability for IoT based smart cities are suggested by the author. Kaur et al. [34] offered architecture that focussed on the development of smart cities by making use of the IoT platform along with the cloud servers. The research article depicts the usage of the IoT framework to bring about an enhancement in the performance of smart cities. The key framework adopted in the methodology selected the cost of the infrastructure and the investment capital as its objective function to be minimized. The Dubai smart city case study is taken by the author with some scenarios based on applications and offered healthcare architecture in a smart city. The work done by the article written by Elhoseny et al. [35] learning approach has been deployed to develop the smart city project. It is feasible to alter the method of learning to advanced technologies i.e. internet of things, big data, and cloud, but making the system of smart learning is the very problematic task of smart cities. The author offered the big data-based model of smart learning that is capable to work in the environment of the smart system. Massobrio et al. [36] proposed an inspection of the smart city-based big data with the help of the infrastructure of cloud computing. Hadoop framework is used for implementation and use of map minimized parallel model. The key focussed area is anticipating the matrix linking the origin to destination services as well as public transport services.

4 Security and Privacy Issues in IoT

In the present century 'The Internet of Things (IoT)' is considered as a technology having much disruption. It is also like the incursion of devices for the city to make it smart which are further integrated with the servers on the cloud for monitoring the functionalities comprising of the system software and applications that are programmed to collect the data and deliver it to the servers. The conclusion that can be made about the IoT is that it can work on the platform of the internet whose infrastructural overview has been shown in Fig. 1. The platform of the internet offers the facility of locating the device easily and IoT is considered to be well supplied with low power, the storage is also limited and restricted processing capacity. There are gateways in IoT employing the connection and linking of various devices with the servers and cloud on the internet and are programmed to communicate with each other during operation. The linking and shrinking of the world into a small village has been gained with the help of IoT, smarter, and therefore extraordinarily effective. The sensors having a cheap rate and this linkage between "things" produce much more data than they produced ever. In this way, the information carried by these data creates an analytical as well as smart environment. Like, analyzing the data accumulated for

providing every individual customized service. The IoT has attracted the attention of researchers as well as industries and thus experiencing extreme growth. Famous and successful corporations like Amazon AWS IoT and Google Cloud IoT have invested billions of dollars in the construction of IoT platforms. IoT has brought much ease to governments as well as individuals; likewise, the handling of the enormous number of devices delivering consequently enormous data on the cloud becomes an uphill task as they are interlinked with a grid of complex connections. The hackers could try to perforate the vast range of IoT devices. In this way, in the system of IoT, the hackers can target the devices that have low security as well as the linkage between smart devices can be. Besides, if the generated data is not stored appropriately then there is much chance for the exposition of privacy of the user and so becomes a matter of concern. There is a threat of safety in IoT like in the year 2016, a company named Dyn has focussed on the development of certain thrust that deploys myriad devices performing interlinked with the online internet platform such as monitors, routers, and cameras. The service was referred to as a distributed denial of service (DDoS). In an IoT system security is the most desirable properties therefore it must be carefully considered [37–40]:

Data Integrity: The production of the data by IoT systems of any company is of great worth which includes trade secrets that are vital for the prosperity of the company so that confidentiality is maintained from outsiders. Therefore it is a must to keep data confidentially and as it is for its use in the future. The integration of traditional centralized storage into IoT architecture can be performed for example cloud storage because it tends to inherent vulnerabilities. The centralized server is prone to risk and so that it may experience a single point of failure. Apart from this, if many devices are linked to a central server model then it can create many-to-one traffic jams, and therefore can suffer from delayed response as well as system scalability problems. The mechanism of the blockchain on the IoT platform can serve as a key solution in dealing with the hindrances of data getting deleted or copied. There have been myriad explorations and researches for the development of distributed storage systems for the data.

Data Sharing: The main objective of an IoT system is to share details among objects, which helps to manufacture, transport, and it also allows businesses to give good service to the daily life of people [9]. Data production is huge in IoT systems. The research and study performed by a certain businessman from the US, the global index shows 35% of the businessmen that relay their business decisions on the data being procured online from various sensors. But, these data are not free data that is why a suitable, as well as the fair technique of fair data trading, is a must.

Authentication and Access Control: The challenge of IoT systems is their security issue. The definition of security issues may deploy accessing the data and resources that require prior permission for such approvals. For granting traditional authentication and for giving access control to the external resources that mainly rely on a centralized system that produces an appropriate key that relies on access policies. When the quantity of devices increases immensely than the IoT system makes centralized approaches bottleneck and because the tendency of IoT is energetic and powerful

so its use leads to complicated trust management, which requires the renunciation of the scalability of the system.

Privacy: With the use of a wide range of smart devices as well as sensors, an IoT system accumulates data for making a broad determination based on customized requirements. But if the configuration of the IoT system is complex then there are many chances that privacy can be violated easily, for example, raw data processing, data acquisition, and data exchange. If there is an abuse of data given by IoT devices then it consequently may try to violate user privacy. Therefore we can say that in IoT systems the conservation of privacy means the privacy of data as well as privacy of entity, which is important and challenging also.

5 Blockchain Usage in Smart City

In the world of IoT security, the emergent blockchain may bring new freedom. A promising blockchain is being explored for IoT security by many companies and researchers. Blockchain is an append-only decentralized digital ledger based on cryptography. To do trusted transactions without a third-party Blockchain offers a platform in which all the tasks, all the transactions, and all the requests are recorded on the chain with a digital signature for the verification of the public. All entity of the system generates and maintains a ledger. In decentralized networking Blockchain is the fundamental techniques with vast excellence, like:

- Blockchain is disseminated and that's why it permits various peers to connect the network with no registration, so it has become trouble-free in comparison to traditional centralized systems [41].
- The dependence on the third party systems for ensuring the creation of trust and security is avoided by the mechanism of the blockchain and the work is achieved by the implantation of the trust in the service system by proof of work (PoW) or Proof of stack (PoS) that form a part of consensus algorithm.
- Blockchain is inflexible. The bock chain architecture makes use of the entire information as a process them as a copy or shared data. The data when is finally integrated with the chain, information can't have tampered and it is all because of given attributes of blockchain, in many applications blockchain act as the fundamental mechanism like those included in the determination of cryptocurrencies, the asset management in a company and the decision making segment in the business. The inference about the efficiency of the blockchain can be brought about for revolutionary response in the economics and business sectors.

In Fig. 2 a typical structure of blockchain is shown. Peers connect blockchain with unique private–public key pairs. A block consists of a block header and a block body and that is formed of few transactions signed by a user with her private key which could be cross-checked with the public key. Few fundamental details about the block like block size, version number, timestamp, and transaction numbers are contained by a block header. For generating a hash value of sell and purchase in the

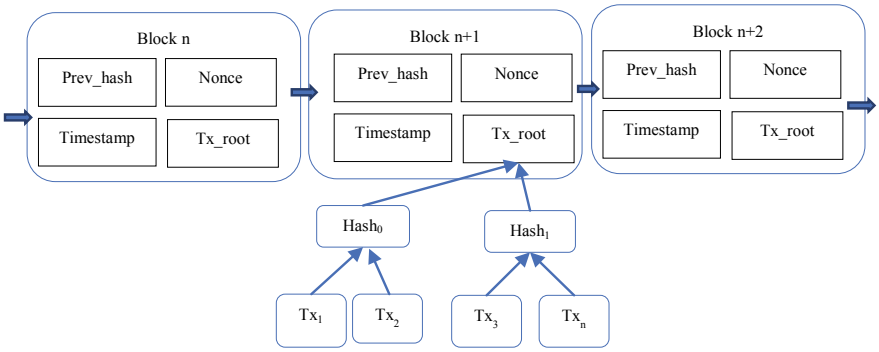

Fig. 2 Blockchain architecture

given block a Merkle hash tree is generally used for the sake of reducing storage overhead of the chain. The hash value of the past block is also contained by a block for the linkage of the two blocks. The block is propagated to miners as soon as it is generated, which is a must for validating all transactions in the block.

After the transactions in blocks are validated, the consensus protocol, such as PoW, is employed by searching a nonce which makes the hash of the block start with a definite number of zeros. Then the block is linked to the chain and at the same, it telecast all the nodes in the system. The other nodes assent the given block by employing its hash as part of the newly produced block. The main approaches of blockchain are Ethereum and Bitcoin. The main distinction between the both is, to track the transfer of ownership of cryptocurrencies whereas Ethereum blockchain mainly targets running programming codes on the platform, that obtains very robust functions like voting and ballots. The Ethereum system works for an account-based model with state transitions, and these accounts are of two types, one is private and another is coded in contracts. The accounts which are externally owned are administered by private keys and contract accounts are administered by codes in contracts. Contracts are generated by transactions with a special "to" address.

5.1 Applications of Blockchain

The area of communication and accordingly operation deploys the ides of IoT (Internet of Things) in which different kind of computing devices, people and electromechanical devices interacts and transfer the information over an internet vie the identities like IP address associated with these objects without any interference of human. These associated identities are responsible for making these objects efficient for this work. The Smart cities or IoT based on Blockchain has several functionalities in cities (Fig. 3).

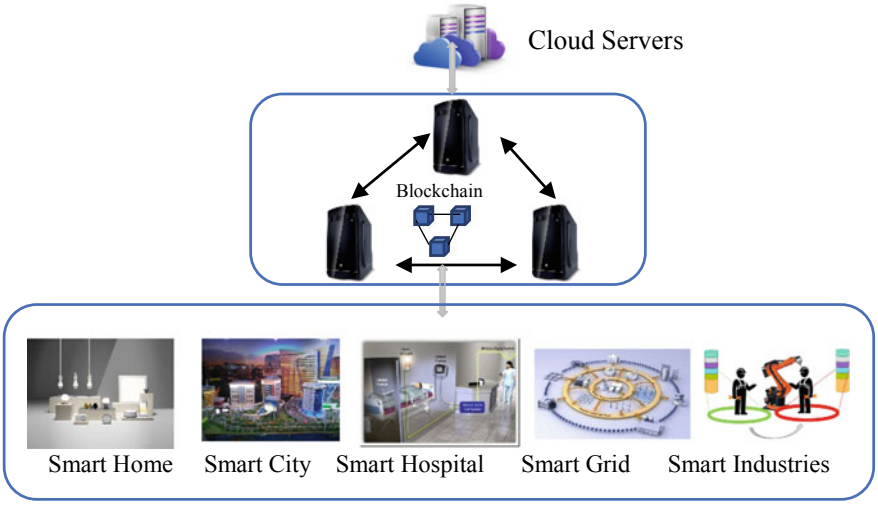

Fig. 3 Blockchain application in smart cities

Smart Healthcare comprising of Blockchain: Another probable application of IoT (Internet of Things) is the intellectual and smart system of healthcare. Many smart healthcare devices (wearable health devices and implantable medical devices) are used in these types of environments of communication and they also consist of different kinds of users, Doctors for a medicinal recommendation, health staff (nurses and other staff) for monitoring the health of the patient. All the data are received and transmitted in a secure technique. The system of recommendation can be established in the communication environment for managing the system in absence of doctors. There are many problems with the intellectual or smart system of healthcare-related to privacy and security. In these types of systems, the data is encrypted and saved in blockchain, with a private key gives access only to the authority. The information of surgery is saved in a blockchain and dispatched as delivery proof to the companies of insurance. Ledger is also used in the system for management of general healthcare like drug inspection, adherence of the rules of consent, recording of the tested results, and healthcare supplies management. So, for securing the data communications in the smart system of healthcare, the blockchain approach is useful.

Blockchain in Smart Transportation: The intelligent or smart system of transportation includes automated vehicles (like automatic cars), fog/cloud servers, and roadside units. These devices can interact with each other with the help of the internet. This is a vast system of network of several antennas, embedded software, sensors, and technologies used for sophisticated route navigation. All decisions of accuracy, speed, and consistency decisions are taken by the System's intelligent units. So these type of environments of communication supplies a journey safe and comfortable for the passengers. In a system of intelligent transportation, communications become secured and authentic from threats from inside and outside the network.

Table 3 Contribution of blockchain in smart cities applications

References	Application	Technique	C	I	Sc	Sh	ExT
[42]	Smart healthcare	Consortium blockchain	No	No	No	Yes	–
[43]	Smart transport	Hyperledger	No	No	Yes	Yes	2 s
[44]	Smart industries	Ethereum	Yes	–	No	–	–
[45]	Smart healthcare	–	Yes	No	Yes	No	–
[46]	Smart grid	Bitcoin	Yes	Yes	–	–	~0.15 s
[47]	Smart grid	Bitcoin	No	Yes	–	–	–
[50]	Smart home	Smart contract	Yes	Yes	–	–	–
[51]	IoT application	–	Yes	No	Yes	–	~3 s
[52]	Smart cities	–	Yes	Yes	Yes	–	~60 ms
[53]	Smart grid	–	Yes	Yes	Yes	Yes	~40 s
[54]	IoT application	–	Yes	Yes	Yes	–	~2000 ms
[55]	Smart cities		Yes	Yes	–	–	~3 ms

C Confidentiality; *I* Integrity; *Sc* Scalability; *Sh* Sharing; *ExT* Execution Time

Blockchain in Smart Industries: The combination of devices and connected machines like manufacturing machines, gas, oil, power generation system is known as a smart Industrial system. Sometimes the system failures and Unplanned downtime in an industry cause the lives of working people so the deployment of the industries based on the IoT is the technique for averting these problems. A System with sensing devices and smart monitoring provides a safe and faithful environment for work. Gateway nodes, many servers, and intellectual IoT devices are included in the environment of IoT. The devices rich in resources like servers can implement the algorithms of machine learning and make a phenomenal prediction. The communications done in these types of environments of communication are penetrable to various types of attacks. So we use the scattered ledger in a blockchain for making communications more reliable and secure against intruders.

Some of the major contributions of research work in the field are given in Table 3.

Technological initiatives presented by blockchain are presented to make smart cities more efficient, robust, secure, etc. Table 4 represents the technological innovation of blockchain in smart city applications.

5.2 Problem Domains in Blockchain

In the above sections, blockchain-based security applications in smart cities are discussed. These existing works are focused on the general application of blockchain in smart cities.

Table 4 Technological initiatives of blockchain in smart cities applications

Application area	Technological initiatives of blockchain
Economy and employment of city	• Sustainable supply management in a smart city • Transparency and trust in employment history as well as employment policies • Increase of ease and decreasing the cost of doing business
Healthcare	• Secure, flexible, and trustworthy environment for patients and health providers • Better control and monitoring for healthcare • Transparency and trust for better deployment of healthcare
Education	• Blockchain-based educational systems ensure flexible management • Secure and shared educational system
Transportation	• Decentralized and secure public transport system management • Real-time monitoring of automobiles such as accident detection, automatic number plate detection, etc.
Energy	• Decentralized management for power supply • Secure fault diagnosis management

These works don't focus on the trustworthiness of the IoT applications of smart cities. After analyzing the above application and their challenges following problems (Fig. 4). If any bugs are found in blockchain applications such as contract code then

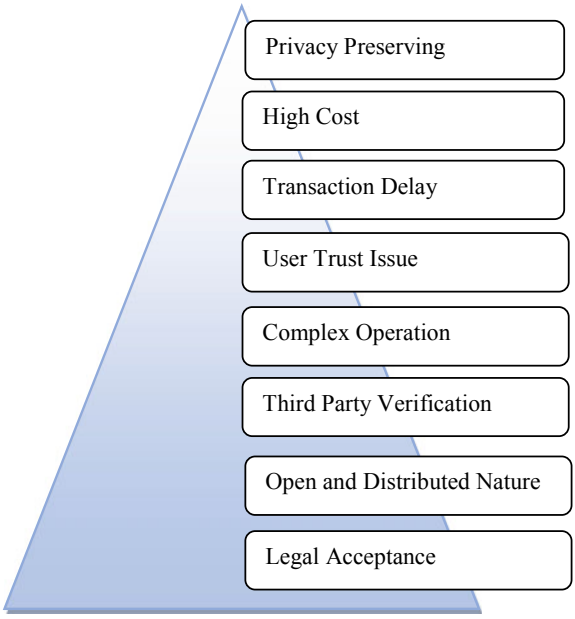

Fig. 4 Problems identified in blockchain technology

it will become a challenging task. At edge nodes of the network, the blockchain model is implemented whose function is to track and authorize all sensor nodes transmitted and received data. If any malicious nodes attempt to attack and mimic an authentic node then blockchain can easily identify it. There is a need to keep all records to identify the origin of malicious activities. So, this work is associated with the implementation of blockchain technology for smart city applications.

6 Proposed Architecture

In this work blockchain-based framework is proposed for smart cities to incorporate security issues and provide a trusted environment for user data transactions. The proposed cross-layer architecture designing for the smart city platforms through which the data transfer is made more reliable. There are three layers within this approach, sensor layer, application layer, and network layer whose coordination can enhance the IoT performance. Also, different IoT systems utilize different architectures that can lead to problems in convergence; the designing of a generic IoT structure for all the platforms can be cost-effective. Figure 5 illustrated the proposed architecture.

The steps for the proposed blockchain secure framework is described as below:

1. Authentication application to access files is sent to the authority server.
2. The authority server checks the credentials and forwards the request to the owner.

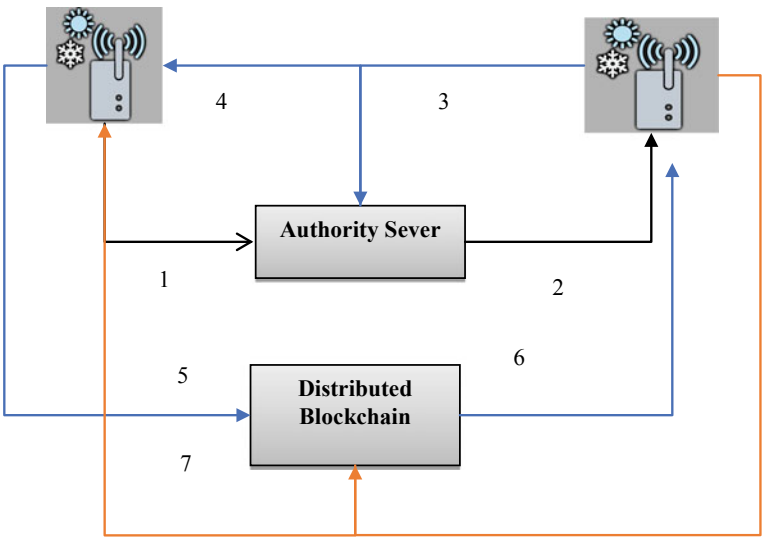

Fig. 5 Proposed blockchain-based architecture

Table 5 Security features comparison with existing techniques

References	Application	C	I	Auth	Sc	Sh
[42]	Smart healthcare	No	No	No	No	Yes
[43]	Smart transport	No	No	No	Yes	Yes
[44]	Smart industries	Yes	No	No	No	No
[46]	Smart grid	Yes	Yes	No	No	No
[51]	IoT application	Yes	No	No	Yes	No
[52]	Smart cities	Yes	Yes	No	Yes	No
[53]	Smart grid	Yes	Yes	No	Yes	Yes
[54]	IoT application	Yes	Yes	No	Yes	No
[55]	Smart cities	Yes	Yes	No	No	No
Proposed	Smart cities	Yes	Yes	Yes	Yes	Yes

C Confidentiality; *I* Integrity; *Sc* Scalability; *Sh* Sharing; *Auth* Authentication

3. The data owner sends the license to access the data file in the cloud.
4. License is sent back to the data used to access the file.
5. Then the user initiates the smart contract to the blockchain unit for secure access (transaction) of the file.
6. Blockchain retrieves the file from the cloud and informs the data owner.
7. Finally, the encrypted data is transmitted to the user with a decryption key to access the data file.

Table 5 illustrates the theoretical comparison over existing works. The implementation of proposed architecture will show improvement over existing techniques in terms of security features or aspects.

7 Challenges and Future Research Directions

Many existing reviews or surveys are presented on blockchain technology and smart cities that can be extensively used to study. The existing surveys are mainly focused on issues related to blockchain and its application in smart cities. There are no past works that have provided a profound description of blockchain and smart cities along with the broad application of blockchain in smart cities. This chapter also explores the technological innovations that are done with blockchain integrated smart city. This chapter gives a brief description of challenges and issues related to blockchain implementation in smart cities. To resolve these issues, this chapter also proposed architecture and also redirects the researchers towards future research scopes. Table 6 represents the state-of-art reviews related to blockchain applications in smart cities. This table represents the all review aspects that are presented in existing surveys.

Rather than an all-embracing summary of the area under study, the existing research ideas need to be understood for potential research. This chapter gives a

Table 6 Comparative analysis of features included in existing survey

References	Year	1	2	3	4	5	6	7	8	9	10	11
[56]	2018	✓	✓	✓	✓	–	–	–	–	–	–	–
[57]	2019	✓	✓	✓	✓	–	–	–	–	–	–	–
[58]	2019	✓	–	✓	–	✓	✓	✓	✓	–	✓	–
[59]	2019	✓	–	–	–	–	✓	✓	✓	–	✓	–
[60]	2019	✓	✓	✓	–	–	✓	✓	–	✓	✓	–
[61]	2019	–	–	–	✓	✓	–	–	–	–	✓	–
[62]	2019	✓	–	✓	–	–	✓	✓	✓	✓	–	–
[63]	2020	✓	✓	–	–	–	✓	✓	✓	–	–	–
[64]	2020	✓	–	–	–	–	✓	✓	✓	–	✓	–
[65]	2020	✓	✓	–	–	–	✓	–	–	–	–	–
This chapter		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

1 = Blockchain description and types, 2 = Blockchain issues and challenges, 3 = Protocols, 4 = Smart city basics, 5 = Smart city security issues, 6 = Blockchain in smart healthcare, 7 = Blockchain in smart transportation, 8 = Blockchain in smart grid, 9 = Blockchain in industries, 10 = Problem domains in blockchain, 11 = Proposed solution

brief overview about blockchain and its issues while implementing in smart cities. Some of the challenges for future research work are presented in Fig. 6. In this chapter a comprehensive framework is proposed which can give direction for future research work. Besides, some of the fields overlap and communicate with one another. In the interest of conciseness, this chapter does not explore these overlaps and interactions. For the same reason, an in-depth discussion of subjects that, while relevant, are not unique to smart cities, such as the use of blockchain to counter the outbreak of pandemics, was also not discussed. Consequently, the system should not be seen as a model that determines the limits of current research but as an inspiration for future research to take up a subject and to carry out an in-depth analysis. To explore the value that blockchain can create in combination with various architectures such as cloud, fog, and edge computing, IoT [48, 49]. Further research is also needed. This particularly applies to the scalability problem solution given by such architectures. Likewise, blockchain and Artificial Intelligence (AI) combinations present exciting new research possibilities for many areas of application.

8 Conclusion

The increasing number of smart devices number leads to increased challenges amongst the IOT services and their efficient performance. One of the emerging applications of IoT is smart cities that are designed to scale up the urban environment and ultimately improve the life of the citizens. With the growing development in IoT based resources, the challenges associated with security is the key concern of

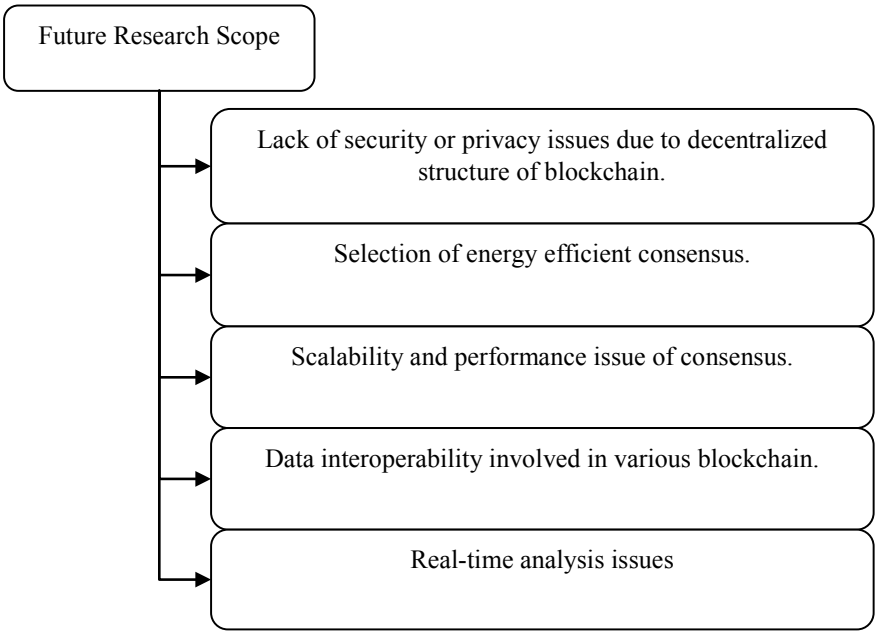

Fig. 6 Current challenges in blockchain integrated smart cities

the research area. The problems and consequences however are found to be resolved using the mechanism of the blockchain in these systems. In this chapter, the architecture of blockchain and its application in different areas are illustrated which showed up their benefits. Along with that a blockchain security model is proposed for future direction in this field. The proposed algorithm can be fruitful in providing a better quality of services even in a complex environment.

References

1. Bibri SE, Krogstie J (2017) Smart sustainable cities of the future: an extensive interdisciplinary literature review. Sustain Cities Soc 31:183–212. Elsevier Ltd. https://doi.org/10.1016/j.scs.2017.02.016
2. Naphade M, Banavar G, Harrison C, Paraszczak J, Morris R (2011) Smarter cities and their innovation challenges. Computer (Long Beach Calif) 44(6):32–39. https://doi.org/10.1109/MC.2011.187
3. Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M (2014) Internet of things for smart cities. IEEE Internet Things J 1(1):22–32
4. Shen M, Tang X, Zhu L, Du X, Guizani M (2019) Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. IEEE Internet Things J 6(5):7702–7712
5. Deep G, Mohana R, Nayyar A, Sanjeevikumar P, Hossain E (2019) Authentication protocol for cloud databases using blockchain mechanism. Sensors (Switzerland) 19(20)

6. Petrolo R, Loscrì V, Mitton N (2014) Towards a smart city based on cloud of things. In: WiMobCity 2014—proceedings of the 2014 ACM international workshop on wireless and mobile technologies for smart cities, co-located with MobiHoc, pp 61–65
7. Biswas K, Muthukkumarasamy V (2016) Securing smart cities using blockchain technology. In: International conference on high performance computing and communications. IEEE international conference on smart city. IEEE international conference on data science and systems, pp 1392–1393
8. Lalit G, Emeka C, Nasser N, Chinmay C, Garg G (2020) Anonymity preserving IoT-based COVID-19 and other infectious disease contact tracing model. IEEE Access 8:159402–159414
9. Decker C, WattenhoferR (2013) Information propagation in the Bitcoin network. IEEE P2P 2013 proceedings, Trento, pp 1–10
10. Dinh TTA, Liu R, Zhang M, Chen G, Ooi BC, Wang J (2018) Untangling blockchain: a data processing view of blockchain systems. IEEE Trans Knowl Data Eng 30(7):1366–1385
11. Saini H, Bhushan B, Arora A, Kaur A (2019) Security vulnerabilities in information communication technology: blockchain to the rescue (A survey on Blockchain Technology). In: International conference on intelligent computing, instrumentation and control technologies (ICICICT)
12. Maesa DDF, Mori P (2020) Blockchain 3.0 applications survey. J Parallel Distrib Comput 138:99–114
13. Yuan Y, Wang F-Y (2018) Blockchain and cryptocurrencies: model, techniques, and applications. IEEE Trans Syst Man Cybern Syst 48(9):1421–1428
14. Vora J, Nayyar A, Tanwar S, Tyagi S, Kumar N, Obaidat MS, Rodrigues JJ (2018) BHEEM: a blockchain-based framework for securing electronic health records. In: IEEE Globecom workshops (GC Wkshps)
15. Huang X, Zhang Y, Li D, Han L (2019) An optimal scheduling algorithm for hybrid EV charging scenario using consortium blockchains. Futur Gener Comput Syst 91:555–562
16. Wang Q, Zhao H, Wang Q, Cao H, Aujla GS, Zhu H (2019) Enabling secure wireless multimedia resource pricing using consortium blockchains. Futur Gener Comput Syst
17. Memon R, Li J, Ahmed J (2019) Simulation model for blockchain systems using queuing theory. Electronics 8(2)
18. Saleh F (2018) Blockchain without waste: proof-of-stake. SSRN Electron J
19. Wang X, Weili J, Chai J (2018) The research on the incentive method of consortium blockchain based on practical byzantine fault tolerant. In: International symposium on computational intelligence and design (ISCID)
20. Gramoli V (2017) From blockchain consensus back to Byzantine consensus. Futur Gener Comput Syst
21. De Angelis S, Aniello L, Baldoni R, Lombardi F, Margheri A, Sassone V (2018) PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain. In: Italian conference on cyber security
22. Rathore MM, Paul A, Hong W, Seo H, Awan I, Saeed S (2018) Exploiting IoT and big data analytics: defining smart digital city using real-time urban data. Sustain Cities Soc 40:600–610
23. Mohanty SP, Choppali U, Kougianos E (2016) Everything you wanted to know about smart cities: the Internet of things is the backbone. IEEE Consum Electron Mag 5(3):60–70
24. Bhushan B, Khamparia A, Sagayam KM, Sharma SK, Ahad MA, Debnath NC (2020) Blockchain for smart cities: a review of architectures, integration trends and future research directions. Sustain Cities Soc 61:102360
25. Qian LP, Wu Y, Ji B, Huang L, Tsang DHK (2019) HybridIoT: integration of hierarchical multiple access and computation offloading for IoT-based smart cities. IEEE Netw 33(2):6–13
26. Fan K, Zhu S, Zhang K, Li H, Yang Y (2019) A lightweight authentication scheme for cloud-based RFID healthcare systems. IEEE Netw 33(2):44–49
27. Garg S, Singh A, Batra S, Kumar N, Yang LT (2018) UAV-empowered edge computing environment for cyber-threat detection in smart vehicles. IEEE Netw 32(3):42–51
28. Lin C, He D, Kumar N, Choo KKR, Vinel A, Huang X (2018) Security and privacy for the internet of drones: challenges and solutions. IEEE Commun Mag 56(1):64–69

29. Kumar N, Vasilakos AV, Rodrigues JJPC (2017) A multi-tenant cloud-based DC nano grid for self-sustained smart buildings in smart cities. IEEE Commun Mag 55(3):14–21
30. Dener M (2019) The role of cloud computing in smart cities. Eurasia Proc Sci Technol Eng Math 7:9–43
31. Khattak HA, Farman H, Jan B, Ud Din I (2019) Toward integrating vehicular clouds with IoT for smart city services. IEEE Netw 33(2):65–71
32. Sun D, Li G, Zhang Y, Zhu L, Gaire R (2019) Statistically managing cloud operations for latency-tail-tolerance in IoT-enabled smart cities. J Parallel Distrib Comput 127:184–195
33. Perera C, Qin Y, Estrella JC, Reiff-Marganiec S, Vasilakos AV (2017) Fog computing for sustainable smart cities: a survey. ACM Comput Surv 50(3):1–43
34. Kaur MJ, Maheshwari P (2016) Building smart cities applications using IoT and cloud-based architectures. In: International conference on industrial informatics and computer systems, CIICS 2016
35. Elhoseny H, Elhoseny M, Riad AM, Hassanien AE (2018) A framework for big data analysis in smart cities. Adv Intell Syst Comput 723:405–414
36. Massobrio R, Nesmachnow S, Tchernykh A, Avetisyan A, Radchenko G (2018) Towards a cloud computing paradigm for big data analysis in smart cities. Program Comput Softw 44(3):181–189
37. Assiri A, Almagwashi H (2018) IoT security and privacy issues. In: International conference on computer applications and information security, ICCAIS 2018
38. Kaushik K, Dahiya S (2018) Security and privacy in IoT based e-business and retail. In: International conference on system modeling and advancement in research trends, SMART, pp 78–81
39. Hameed A, Alomary A (2019) Security issues in IoT: a survey. In: International conference on innovation and intelligence for informatics, computing, and technologies, 3ICT 2019
40. Apare RS, Gujar SN (2018) Research issues in privacy preservation in IoT. In: IEEE global conference on wireless computing and networking, GCWCN, pp 87–90
41. Rizvi S, Kurtz A, Pfeffer J, Rizvi M (2018) Securing the internet of things (IoT): a security taxonomy for IoT. In: IEEE international conference on trust, security and privacy in computing and communications and IEEE international conference on big data science and engineering, Trustcom/BigDataSE, pp 163–168
42. Wang S, Wang J, Wang X, Qiu T, Yuan Y, Ouyang L, Guo Y, Wang FY (2018) Blockchain-powered parallel healthcare systems based on the ACP approach. IEEE Trans Comput Soc Syst 5(4):942–950
43. Gao F, Zhu L, Shen M, Sharif K, Wan Z, Ren K (2018) A blockchain-based privacy preserving payment mechanism for vehicle-to-grid networks. IEEE Netw 32(6):184–192
44. Longo F, Nicoletti L, Padovano A, d'Atri G, Forte M (2019) Blockchain-enabled supply chain: an experimental study. Comput Ind Eng 136:57–69
45. Li X, Huang X, Li C, Yu R, Shu L (2019) EdgeCare: leveraging edge computing for collaborative data management in mobile healthcare systems. IEEE Access 7:22011–22025
46. Aggarwal S, Jindal A, Chaudhary R, Dua A, Aujla GS, Kumar N (2018) EnergyChain: enabling energy trading for smart homes using blockchains in smart grid ecosystem. In: ACM MobiHoc workshop on networking and cybersecurity for smart cities, smart cities security 2018
47. Rottondi C, Verticale G (2017) A privacy-friendly gaming framework in smart electricity and water grids. IEEE Access 5:14221–14233
48. Sanjukta B, Sourav B, Chinmay C (2019) IoT-based smart transportation system under real-time environment, IET: big data-enabled internet of things: challenges and opportunities, Ch. 16, pp 353–373
49. Banerjee S, Chakraborty C, Chatterjee S (2019) A survey on IoT based traffic control and prediction mechanism. Intelligent systems reference library, vol 154. Springer Science and Business Media Deutschland GmbH, pp 53–75
50. Fakhri D, Mutijarsa K (2018) Secure IoT communication using blockchain technology. In: International symposium on electronics and smart devices (ISESD), Bandung, pp 1–6

51. Zhaofeng M, Jialin M, Jihui W, Zhiguang S (2020) Blockchain-based decentralized authentication modeling scheme in edge and IoT environment. IEEE Internet Things J
52. Chen R, Li Y, Yu Y, Li H, Chen X, Susilo W (2020) Blockchain-based dynamic provable data possession for smart cities. IEEE Internet Things J 7(5):4143–4154
53. Jindal A, Aujla GS, Kumar N, Villari M (2020) GUARDIAN: blockchain-based secure demand response management in smart grid system. IEEE Trans Serv Comput 13(4):613–624
54. Rahman A et al (2020) DistB-Condo: distributed blockchain-based IoT-SDN model for smart condominium. IEEE Access 8:209594–209609
55. Yu S, Lee J, Park K, Das AK, Park Y (2020) IoV-SMAP: secure and efficient message authentication protocol for IoV in smart city environment. IEEE Access 8:167875–167886
56. Reyna A, Martín C, Chen J, Soler E, Díaz M (2018) On blockchain and its integration with IoT. Challenges and opportunities. Futur Gener Comput Syst 88:173–190. https://doi.org/10.1016/j.future.2018.05.046
57. Salman T, Zolanvari M, Erbad A, Jain R, Samaka M (2019) Security services using blockchains: a state of the art survey. IEEE Commun Surv Tutor 21(1):858–880. https://doi.org/10.1109/COMST.2018.2863956
58. Xie J et al (2019) A survey of blockchain technology applied to smart cities: research issues and challenges. IEEE Commun Surv Tutor 21(3):2794–2830. https://doi.org/10.1109/COMST.2019.2899617
59. Ferrag MA, Derdour M, Mukherjee M, Derhab A, Maglaras L, Janicke H (2019) Blockchain technologies for the internet of things: research issues and challenges. IEEE Internet Things J 6(2):2188–2204. https://doi.org/10.1109/JIOT.2018.2882794
60. Ali Syed T, Alzahrani A, Jan S, Siddiqui MS, Nadeem A, Alghamdi T (2019) A comparative analysis of blockchain architecture and its applications: problems and recommendations. IEEE Access 7:176838–176869. https://doi.org/10.1109/ACCESS.2019.2957660
61. Sookhak M, Tang H, He Y, Yu FR (2019) Security and privacy of smart cities: a survey, research issues and challenges. IEEE Commun Surv Tutor 21(2):1718–1743. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/COMST.2018.2867288
62. Aggarwal S, Chaudhary R, Aujla GS, Kumar N, Choo KKR, Zomaya AY (2019) Blockchain for smart communities: applications, challenges and opportunities. J Netw Comput Appl 144:13–48. Academic Press. https://doi.org/10.1016/j.jnca.2019.06.018
63. Sengupta J, Ruj S, Das Bit S (2020) A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. J Netw Comput Appl 149:102481. Academic Press. https://doi.org/10.1016/j.jnca.2019.102481
64. Moniruzzaman M, Khezr S, Yassine A, Benlamri R (2020) Blockchain for smart homes: review of current trends and research challenges. Comput Electr Eng 83:106585. Elsevier Ltd. https://doi.org/10.1016/j.compeleceng.2020.106585
65. Alam Khan F, Asif M, Ahmad A, Alharbi M, Aljuaid H (2020) Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. Sustain Cities Soc 55:102018. https://doi.org/10.1016/j.scs.2020.102018