Chapter 5
Blockchain-Based Fog Computing Model (BFCM) for IoT Smart Cities

R. Venkadeshan and M. Jegatha

5.1 Introduction

With the recent improvement in the urban lifestyle, the smart cities originated for the improvement of the quality of living and to optimize the utilization of cities' resources [1]. There are a lot of improvements that have been carried out on infrastructure and different services which elevated the eminence of life. All these could be possible with the support of the Internet, telecommunication, and advancement in the information technology field [2]. The expectation from the awareness of smart cities includes smart transportation, efficient society services, and better infrastructure results in on-demand accessible and effective interactive services. With the support of the Internet of Things (IoT), the vision of the smart city becomes reality. As a result, many IoT applications have been built up for the smart cities services to interact with the people anytime and anywhere.

The smart cities are deployed with physical objects interconnected with the IoT system. This system emphasizes four pillars in IoT concepts such as things, data, objects, and processes. Hence, the integration of IoT concepts with smart city domain will facilitate the promising services in the near future. Big data analytics is an emerging technique to analyze the massive data generated by IoT-connected devices which could help to sort out the issues of data storage and processing. Fog computing, also referred to as edge computing or fogging, extends the cloud computing services to the enterprise network's edge. It allows the edge devices to transfer a significant amount of data to compute, store, and communicate for the local decision and forward over the Internet.

This chapter discusses a conceptual framework with the dimensions (1) technology, (2) human, and (3) organization and reconnoitering the challenges of digital

R. Venkadeshan (✉) · M. Jegatha
University of Technology and Applied Sciences – Shinas, Shinas, Sultanate of Oman
e-mail: venkadengg@gmai.com

H. L. Gururaj et al. (eds.), *Convergence of Internet of Things and Blockchain Technologies*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-76216-2_5

technologies with the support of blockchain-based fog computing model (BFCM) for smart cities [3]. This model reduces energy consumption and latency in data communication and improves security features. The convergence of blockchain and Internet of Things (IoT) technologies in smart cities ensures the security and privacy of data captured and stored in a cloud-based infrastructure. In the IoT application execution of fog computing, the node called fog node (FN) acts as a basic fundamental entity and an intermediate layer between the cloud and edge devices [4]. Emerging IoT applications require the support of mobility, low latency, geo-distribution, and location awareness. The BFCM architecture targeted to improve the efficiencies of the above parameters by handling most of the data at the network edges rather than transferring to cloud always. Another important service to address is the security of data and devices which could be enhanced by using the blockchain technology. The blockchain technology [5, 6] is organized as a series of blocks and chains of records stored in a shared database which could be secured by cryptographic hash functions. Each block is a group of transactions that had occurred for a while.

5.2 IoT Technologies in Smart Cities

In recent decades, there are several researchers that worked on IoT-related smart cities. Smart cities are one of the rapidly progressing technological revolution and escalation of Internet of Things development in every possible aspect of urban lifestyle [7]. A smart city is designed for providing solutions for the environment, traffic, and other energy management problems by integrating various technologies such as Internet of Things, big data, and blockchain. Simply, the smart city is a network of environment with objects, people, and services sharing the information with one another through the communication technologies like 3G, 4G, and Wi-Fi. Due to the blended heterogeneous devices with different technologies, the deployment of smart cities becomes very much complicated [8]. The large-scale network exponentially increases the difficulties of object's management and tracking which results in an intruder or attacker easily performing security breaches. By taking all these in mind, building a basic infrastructure for a smart city in urban areas needs support from various sensors and technologies [9]. The Internet of Things (IoT) is one among them, considered as a key builder in the development of smart city. The fundamental components and concepts of smart city are given in Table 5.1.

An emerging smart city objective is to make use of the resources like energy and electricity in an effectual way to provide a suitable and comprehensive infrastructure for the human society in day-to-day life. Therefore, the impact of IoT is magnified in various services of smart cities [10]. The smart city is a network of six components: smart environment, smart people, smart governance, smart mobility, smart economy, and smart living (Fig. 5.1). Some of the applications and services where IoT technologies and smart city projects de facto overlap are listed below [11]:

Table 5.1 Fundamental components and concepts of smart city [36]

Components	Descriptions
Policy and purpose	Environmental sustainability: environment pollution, energy efficiency, and resources Economic requirements: education, public security, medical care, social stability, and healthcare Happiness of citizens: asset, new job formation, and system modernization
Key industry	Smart buildings, smart transportation, smart government, smart facilities, and so on
City infrastructure	Sensor networks, operation systems, sensors, and smart devices Telecommunication platforms, data analysis, control systems, and interactive web services

Fig. 5.1 Smart city components [12]

Public services such as public transportation management, citizen services, tourism services and healthcare sector administration, and information services

Sustainability which includes smart wastage management and recycling system, smart metering, smart energy, smart water, and environmental monitoring

Infrastructure services that deal with smart building's structural health monitoring, smart lighting, smart irrigation, smart schools, etc.

Transportation services that handle smart traffic management, coordinating the connected vehicles on the road, smart road system, pollution and noise control management, and so on

Safety services which are video surveillance, disaster recovery system, environmental screening, and telemedicine system

IoT technologies in Table 5.2 provide IT solutions for automatic electricity services, telecommunication services and construction, vehicle telematics, smart healthcare, and other business services [12].

Table 5.2 IoT technologies for smart cities

Technologies	Descriptions
User interface technology	Communication between sensors, objects, machines, and humans
Context awareness technology	Provide services based on the understandability of current situation data collected from various sensors, objects, and machines
Wired and wireless connection gateway	It's a home gateway technology used to provide communication between the different network platforms like Ethernet, 3G, 4G, LTE, Wi-Fi, and Zigbee
System-on-Chip (SoC) technology	It's a microcontroller for controlling and integrating with computers objects for sensing the environment. Mostly used in the mobile computing and edge computing markets
Optimized sensor design technology	It's a sensor technology used for collecting environmental values on object transformation and personal information.
Sensor fusion and converging technology	Used for converging more than one sensor's functionality in an object
Analytical technology	Sensors generating massive amount of data which are collected on cloud server for big data analytics

5.3 Fog Computing for Smart Cities

The Internet of Things (IoT) connects billions of everyday automation objects/things to collect and exchange massive amount of data over the Internet. All those collected data are pushed into the cloud for further analysis and knowledge discovery for future purpose [10]. Moreover, the amount of gathered data becomes overwhelming to store and manage, requiring high-processing computing devices to forward to cloud, and will have limitations such as resources wastage (e.g., storage, bandwidth), unreliable latency, and data security. The result of fog computing or edge computing offers different solutions to these limitations. The main goal of Fog computing technology is to improve the effectiveness and minimize the amount of information sent over the Internet to the cloud for analysis, processing, and storage by performing data analytics at the network edges [13]. Edge devices are easy to control, manage, and self-govern at the local network. Therefore, the network traffic and data processing have been reduced considerably by moving the services to the edge of the local network. In smart cities development, the fog computing plays a potential role in processing a variety of volume of data swiftly and most securely.

Figure 5.2 illustrates the various elements of smart city that applies fog computing technology to support low latency, location awareness, and mobility to the end users.

Smart cities achieve the below listed benefits through the incorporation of fog computing technology [14]:

Reduced the amount of data being sent to cloud: Fog computing uses intelligent sensing and filtering technique to allow only the useful and most needed information to the cloud; the remaining will be available at the local fog devices in the network premises.

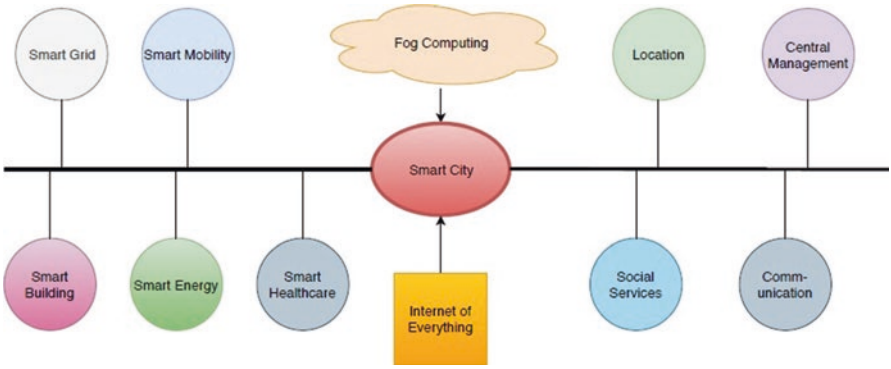

Fig. 5.2 Fog computing for sustainable smart cities [3]

Low latency: Fog devices are capable of data processing and decision-making and sending back results without depending on the remote cloud services. Especially, these characteristics save a lot of time considerably in IoT automated environment.

Reduced bandwidth: Forwarding and processing of sensed data require huge amount of bandwidth in cloud computing. But, in the case of fog computing, this issue does not exist because most of the data are stored and processed by the fog nodes inside the local network which significantly reduces the consumption of total network bandwidth.

Security enhancement: Fog computing restricts the outreach of most sensible and confidential data exposed to the vulnerable public network (Internet) which results safeguard the data from cyberattacks and hacking.

Henceforth, fog computing provides relief to the smart city components by achieving reliable and faster data communication. In succession, the urban areas called as fog (edge) computing smart city proliferate the communal sectors such as healthcare, manufacturing, education, transportation, energy, and utilities [15].

5.4 Blockchain-Based Fog Computing Model (BFCM)

The blockchain-based fog computing model (BFCM) for the smart cities is introduced to connect the Internet of Things (IoT) and fog nodes. This model is an on-demand service that provides high performance with low latency and secure device management and data privacy in a distributed form of infrastructure [16]. It will result in the improvement of lifestyle quality of the citizens and meeting the expectations of day-to-day activities.

5.4.1 Blockchain: A Study

A blockchain technology is a decentralized distributed database with special data structure which forms all transactions into blocks with secure distinctive hash code and transmits them to every node [17]. It works with different elements like network, authentication, and transactions to store the sensitive data. It also enables the network's authorized members to validate the transaction data at any time and to quickly store it as a digital information which is easy to manage against any forgery and attacks. A public key cryptographic technique is used to sign all the transaction on a distributed ledger linked blocks of records known as blockchain [18]. Once the data is transferred, it cannot be changed, and it provides better security to the information. For smart cities management, various frameworks support Internet of Things (IoT) technology but face multiple issues like security, resource management, heterogeneous devices and data, multiple application assistance, and platform independence. The BFCM-based infrastructure secures sensitive information with authentication, edge computing, encryption, and blockchain.

5.4.2 Structure of Blockchain

Generally, a blockchain is nothing but consecutive list of records, called blocks, that contains the detailed transactions linked using cryptography in a network. In Fig. 5.3, each record, or block, consists of a header and a body, where the header comprises the previous record or block's identity and the body portion encompasses stored data/transactions that are being transferred [6]. The chain of blocks is connected as linked list to transfer over the network.

Intuitively, blockchain technology offers desirable features such as decentralization, immutability, distributed ledger, and fault tolerance. Intrinsically, BFCM

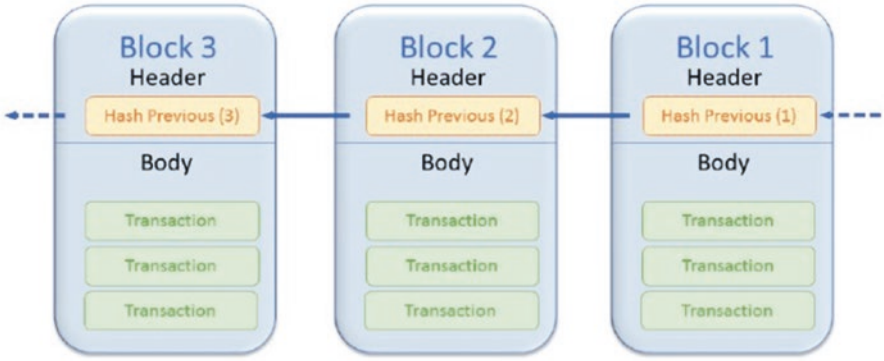

Fig. 5.3 Structure of blockchain [6]

promotes transparency and trust on smart city elements and helps to provide on-demand services to the citizens [19].

Decentralization—A blockchain technology is a decentralized database network which does not have any governing authority or entity at the framework to manage and control the transactions of data among the smart city components. So, the data storage and analytics integrate the security and trust on decision-making processes.

Immutability—It is one of the exciting key features of blockchain technology, where the network is permanent, uncorrupted, and unaltered. The chain of immutable blocks contains the secured data with digital ledger ensuring the validity and corruption-proof. IoT-enabled smart city infrastructure struggles with handling massive data being generated, safety and security of carrying sensitive information such as financial transaction, health-related data, traffic information, and so on. With the support of immutability in smart cities, the communication becomes tamper-free where an attacker would have to compromise all the devices within the network to alter any records in the blockchain.

Distributed Ledger—Generally, the term DLT stands for distributed ledger technology, used to keep multiple copies of single ledger in a distributed manner. So, all the ledger holders should ensure the data integrity and the data cannot be altered in between. The DLT provides data sharing and smart services in building a smart city infrastructure that are supported by blockchain and IoT.

Fault Tolerance—The distributed nature of blockchain technology allows the nodes to tolerate the malicious behavior for certain threshold. Blockchain peers will automatically reject the blocks if any tampering occurred. The fault tolerance servers are imperative in providing continuous services and operations to maximize the value of smart industries. Since the data are shared, replicated, and synchronized across the participating devices, any failure in one or more devices in a smart network does not affect the performance of entire system.

5.4.3 Blockchain and IoT Technology

Basically, the Internet of Things (IoT)-technology-supported network works as a centralized architecture for communication where the data is collected, processed, and analyzed in various forms from different millions of devices. Yet, this technology suffers with numerous issues like security and privacy of massive data, scalability of devices, and scarcities in resource management at IoT edge network. Fortunately, the blockchain technology with distributed nature offers countermeasures for all the above listed issues and secures the data from tampering embedded into real-time IoT applications [20]. Nevertheless, using blockchain technology in the smart city's infrastructure requires huge amount of energy to generate blocks of live records and to verify its integrity with the use of energy-constrained IoT devices. The smart city infrastructure enhances these technologies to support and provide sustainable solutions for the new era. The BFCM plays a prominent role in the rapid

moving environment of smart cities [21]. Blockchain technology could be incorporated in three ways:

- *Public* **blockchain:** It is also named as "Permissionless Blockchain"; a decentralized environment allows everyone to keep a replica of blocks and take part in validating new blocks.
- **Private blockchain:** It is referred as "Permissioned" or "Private" or "Closed" blockchain; the access to the blocks of records are restricted to some specific participants. It supports three types of permissions to setup a blockchain:

  Read—allows to access and see the transactions of ledger records
  Write—allows to access, modify, and see the transactions of ledger records
  Commit—allows the ledger records to update the state after modification

- **Consortium blockchain:** It is like private blockchain where the permission is required to access the blocks. The main role of consortium blockchain is to synchronize the distributed databases and to keep track of data exchanged between the participants in the network. It provides faster latency and more auditability for the chains of blocks in the networks.

5.4.4 Challenges in Blockchain-Based IoT

On the other side, there are some challenges in the integration of blockchain with IoT technology. The IoT technology visualizes the smart city as collection of connected smart devices or sensors or things that interacts and shares data with each other using smart applications. IoT-based solutions are being incorporated in many of the smart city components such as smart industries, smart grid, smart transportation, smart healthcare, and smart environment to optimize the performance and digitizing of the communication [22]. The smart applications that generate huge data require uninterrupted connectivity and continuous power that lead to excessive number of challenges. Integrating the blockchain with IoT technology will enrich the infrastructure by providing trustable sharing services; reliable information can be traceable at any point. The challenges [6] in an integration of both technologies are summarized in Table 5.3 [23].

5.5 BFCM-Based Smart City Architecture

The objective of BFCM-based model is to incorporate the IoT-based smart cities with blockchain and fog computing technologies to solve traffic-, energy-, and environment-related problems and to enhance and better the lifestyle of the citizens. The smart city network is composed of different components like smart healthcare, smart transportation, smart banking, and smart industries using different

Table 5.3 Integration challenges of blockchain and IoT [6]

Category	Challenges
Integration	Layer of integration of two different systems into single coherent model that supports energy constraints, compatibility, and heterogeneity
Device management and deployment	Building the infrastructure to provide failure recovery, remote monitoring and auditability, sensor's extensibility, and flexibility
Storage and scalability	Devices are being scalable every day in smart cities and generating gigabytes of data in a real-time environment which creates a barrier to blockchain technology to provide security
Security	Different formats of data from different devices in smart city component are very much hard to handle. There is no single security model to protect against all the cyberattacks and breeches
Anonymity	Smart city applications work mostly with sensitive and confidential data like healthcare and banking. The problems of providing data privacy is transparent, and the public blockchains of cryptographic security for software devices should be safeguarded

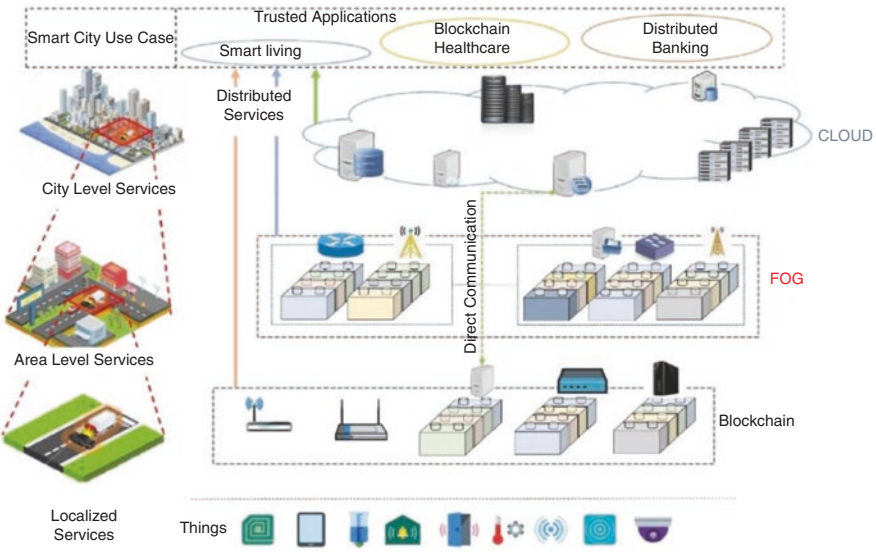

Fig. 5.4 BFCM-based smart city architecture [37]

communication model of IoT technology [24]. The smart city use cases are broadly categories into three levels of services as depicted in the Fig. 5.4, which includes (1) localized services, (2) area-level services, and (3) city-level services, to understand how the BFCM model is acting as digital technology transformation in data transmission and its communication [25]. The lower-level localized services are populated with the highly reliable, low-cost IoT smart objects and sensors like RFIDs, IR sensors, GPS, and cameras deployed across the smart cities horizontals such as generation, distribution, transmission, and consumption. The security to the data

generated by sensor devices is achieved through blockchain technology where the information is stored as blocks of records called ledger. The next level is the integration of computing services and blockchain technology to provide distributed area-level services for handling substantial amount of data communication and analysis through fog computing framework [26]. As shown in the figure, not all data are to be processed and handled at the network edge; some of the data as per the user's requirements can be transferred directly called as "Direct Communication" to the cloud storage and analysis without fog computing in the edge of network.

The blockchain provides guarantee to the data integrity and transactions between the local network and the cloud. Blockchain strengthens the security and privacy of the internal information by using SHA (Secure Hash Algorithms) [27]. Smart cities are growing exponentially with the emergence of Internet of Things (IoT) technology. Every edge device should cover up the sensors to perform local traces and instant analysis. The outcomes of fog layer may either have transferred fully to the smart city's IoT application processing at cloud or may be off-loaded in the network edges. The distributed environment at city-level services experienced massive raise of data storage and data processing. Cloud computing is a solution to handle huge amount of data storage and processing in on-demand and anytime and anywhere basis. It supports centralized monitoring and control of information with high performance and different behavioral analysis. The topmost level is the trusted event-driven applications that impeccably integrate the IoT technologies, spatiotemporal analytics, and complex-event processing for the different smart city's components present to the end users.

5.5.1 Blockchain IoT Applications and Platforms

Emerging technologies such as blockchain fog and cloud computing have been improvising the IoT applications particularly in security domain, e.g., data integrity and data reliability. This has resulted in an enlightenment of increasing electronic devices or smart devices deployment in many areas and stepping into the digital world. The smart devices can be able to sense, actuate, and communicate over the Internet without any human interventions [28]. The end users connected with the IoT applications, which are more specific in features and characteristics, generate large amount of data and expected high connectivity and electric power for long periods. The smart cities are the collection of different components such as smart healthcare, smart home, smart transportation, smart education, and smart grid [2]. Each component is embedded with IoT sensors that can communicate with each other using BFCM model. The presented figure is a multitier architecture that illustrates the detailed layout of smart city infrastructure with the technologies, Internet of Things (IoT), fog computing, blockchain, telecommunication, and cloud services (Table 5.4).

Table 5.4 Blockchain- and fog-based architecture network characteristics [3]

Type	Architecture	QoS	Technology	Latency	Bandwidth	Mobility	Storage	Delay
Primary	Centralized	High	Wi-Fi/4G/5G	Low	Medium	Yes	Yes	Very low
Inter- primary	Centralized	High	Zigbee/Bluetooth/Wi-Fi	Very low	High	Yes	No	Very low
Secondary	Distributed	Very	5G/4G	Low	Low	No	Yes	Low

5.5.2 Challenges and Security Features for Device Management in BFCM

A smart city is a network that consists of complicated and heterogeneous urban devices connected with the Internet that have the capacity to send and receive the data using Internet of Things (IoT) technology and can exponentially increase the security problems where the attackers can perform several cyberattacks [30, 31]. Some of the security measures for device administration security in a smart city are as follows.

Confidentiality. A wide range of devices across the smart cities will sense, collect, store, and process data that could contain more sensitive information [29]. Confidentiality means providing security and privacy over those data and enabling only authenticated and authorized entities to access that information. One of the general methods to provide confidentiality is relying on cryptography technique. Since the BFCM model uses blockchain technology, that integrates the cryptography with private and public keys in the list of records to strengthen the sensitive information.

Integrity. The data exchanged between the smart devices are reliable, accurate, consistent, and integrity to ensure the transferred data are delivered without any modification. The blockchain technology is designed to prevent the data modification using hash functions: the data does not get changed once it is added into the chain.

Availability. Sensors act as a backbone of smart cities, and continuous collection of massive data from different geographic areas requires high availability to the authorized entities. The BFCM model is deployed as distributed decentralized infrastructure and provides data availability with no single point of failure.

Accounting. Blockchain technology is a distributed P2P database system; the data is stored and managed as a record with timestamp called block. A block is a data structure that accounts all the records of transactions between the smart devices. So, the blockchain provides efficient accountability for data management.

Latency. In BFCM, the data are gathered and processed at the edge of the network in geographic proximity. Due to that, it enhances the performance of the network by reducing the latency and provides higher bandwidth in transaction.

Adaptability. The smart city operates on open interconnected heterogeneous smart devices and technologies that result in interoperability issues. But the BFCM enables decentralized architecture to manage cross-disciplinary IoT systems.

5.5.3 Privacy-Conserving Blockchain and Fog Computing

It is to all appearances that the main challenge in IoT is to overcome the downsides associated with privacy, security, and vulnerability aspects. Moreover, the blockchain technology requires enormous amount of energy to process and verify each

block of record that are difficult to handle with resource-constrained IoT devices and real-time data applications [32]. Due to the public ledger system, blockchain discloses the privacy of the stakeholder's data though it is secure from data alteration. Fog computing technology reduces the complexity of data privacy at cloud computing by populating the real-time applications data at the network edges. However, due to handling of massive data, distributed environment, and shortage of enough resources made, this model endlessly suffers from abundant security and privacy issues [33]. Remarkably, blockchain technique provides strong countermeasures to these security issues and protects data against any tampering even in distributed nature of IoT. It is very difficult to provide message delivery in end-to-end connectivity without the cooperation of network devices. But, some selfish devices in the network become reluctant in data transmission due to minimum resources utilization such as energy consumption [34]. The BFCM provides remote data integrity verification which allows the remote users to validate the reliability of the transmission data. The authors [31] proposed homomorphic encryption for data aggregation scheme in fog-assisted IoT devices. There are several articles that addressed the various techniques used to preserve the privacy of information through blockchain and fog computing. Some of them are listed below:

Identity privacy—A user's identity in IoT environment should be preserved and protected from impersonate attacks. The authors [30] present various pseudonym techniques to preserve identity privacy.

Data privacy—There are algorithms run between the fog and cloud services to preserve the information transferred. But the reality is this algorithm consumes massive amount of resources at the network edge devices. At the local edge, same encryption method can be deployed without decryption to allow privacy preservative collection [31].

Usage privacy—Additional important concern in blockchain-based fog computing model is user's resource usage privacy pattern. Let us consider that the smart energy meter in smart industry reads and stores a massive amount of data continuously that are user's private data, energy consumption, user unavailability, and other online and offline appliances status at home, which are threat to user's privacy [34].

Location privacy—However, the fog clients and remote monitoring nodes are in different location; there are rare possibilities that the path route may be revealed to fog nodes. One method to hide the fog node's location is to obscure the identity of fog client [35].

5.6 Conclusions

With the support of emerging technologies like Internet of Things (IoT), fog computing, blockchain, and cloud computing, the world is moving toward the digital electronic era of communication. The smart city projects uplift the use of all these

technologies in a common citizen's day-to-day lifestyle to share information and data communication among the smart devices between cities. In smart cities, there are abundant Internet of Things (IoT)-related applications along with smart sensors, actuators, and controllers that provide energy-aware, scalable, and low-latency network to the society. We started with the impact of Internet of Things (IoT) technology in smart city's infrastructure which generate huge amount of data that should be handled by fog computing nodes at the network edges to provide state-of-the-art security and privacy to meet the limitations. In addition, next, we discussed the role of blockchain technology as an emerging solution to the security issues in fog-enabled IoT environment. At the end, we addressed some of the challenges in integration of blockchain-based fog computing model (BFCM) in the IoT platform. To conclude, BFCM provides many advantages in smart city infrastructure and networks in terms of data computation and information storage with minimal energy consumption.

References

1. Albino, V., Berardi, U., et al. (2015). Smart cities: Definitions, dimensions, performance, and initiatives. *Journal of Urban Technology*, 3–21. https://doi.org/10.1080/10630732.2014.942092.
2. Nguyen, D. C., & Pathirana, P. N. (2020). Blockchain for 5G and beyond networks: A state of the art survey. *Journal of Network and Computer Applications*. https://doi.org/10.1016/j.jnca.2020.102693.
3. Singh, P., Nayyar, A., et al. (2020). Blockchain and fog based architecture for internet of everything in smart cities. *Future Internet*. https://doi.org/10.3390/fi12040061.
4. Hussain, M., & Beg, M. M. S. (2019). Fog computing for internet of things (IoT)-aided smart grid architectures. *Big Data and Cognitive Computing, 2019*(3), 8. https://doi.org/10.3390/bdcc3010008.
5. Shen, C., & Pena-Mora, F. (2018). Blockchain for cities—A systematic literature review. *IEEE Access.* https://doi.org/10.1109/ACCESS.2018.2880744.
6. Aloqaily, M., & Otoum, S. (2020). Blockchain for managing heterogeneous internet of things: A perspective architecture. *IEEE Network*. https://doi.org/10.1109/MNET.001.1900103.
7. Sanchez, L., Muñoz, L., et al. (2014). IoT experimentation over a smart city testbed. *Computer Networks*, 217–238. https://doi.org/10.1016/j.bjp.2013.12.020.
8. Anton, R. (2018). Intelligent communication and patterning in smart cities. *IntechOpen*. https://doi.org/10.5772/intechopen.79629.
9. Biswas, K., & Muthukkumarasamy, V. (2016). Securing smart cities using blockchain technology. In *Conference: 14th IEEE International Conference on Smart City*. https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198.
10. Karim, S., & Ahamed, F. A. S. (2019). Smart city architecture and applications based on IoT: A theoretical overview. *International Journal of Scientific and Engineering Research, 10*(1), 1815–1820.
11. Alvarez, M. G., Morales, J., et al. (2019). Integration and exploitation of sensor data in smart cities through event-driven applications. *Sensors*. https://doi.org/10.3390/s19061372.
12. Samih, H. (2019). Smart cities and internet of things. *Journal of Information Technology Case and Application Research*. https://doi.org/10.1080/15228053.2019.1587572.
13. Perera, C., Qin, Y., et al. (2017). Fog computing for sustainable smart cities: A survey. *ACM Computing Surveys*. https://doi.org/10.1145/3057266.

14. Neagu, I. M. (2018). Sustainable smart cities: A fog computing framework for a smart urban transport network. *Studia Universitatis Vasile Goldis Arad – Economics Series*. https://doi.org/10.2478/sues-2018-0021.
15. Yu, W., et al. (2018). A survey on the edge computing for the internet of things. *IEEE Access*, 6900–6919. https://doi.org/10.1109/ACCESS.2017.2778504.
16. Miraz, M. H. (2020). Blockchain of things (BCoT): The fusion of Blockchain and IoT technologies. In S. Kim & G. Deka (Eds.), *Advanced applications of Blockchain technology. Studies in big data* (Vol. 60). Singapore: Springer. https://doi.org/10.1007/978-981-13-8775-3_7.
17. Li, X., Jiang, P., et al. (2018). A survey on the security of blockchain systems. In *Future generation computer systems*. https://doi.org/10.1016/j.future.2017.08.020.
18. Tariq, N., Asim, M., et al. (2019). The security of big data in fog-enabled IoT applications including blockchain: A survey. *Sensors*. https://doi.org/10.3390/s19081788.
19. Oliveira, T. A., & Oliver, M. (2020). Challenges for connecting citizens and smart cities: ICT, E-governance and blockchain. *Sustainability, 12*, 2926. https://doi.org/10.3390/su12072926.
20. Iftikhar, M. Z., Iftikhar, M. S., et al. (2019). Efficient resource utilization using Blockchain network for IoT devices in smart city. *International Conference on Broadband and Wireless Computing, Communication and Applications BWCCA, 2019*, 521–534. https://doi.org/10.1007/978-3-030-33506-9_47.
21. Jang, S. H., Guejong, J., Jeong, J., & Sangmin, B. (2019). Fog Computing Architecture Based Blockchain for Industrial IoT. In J. Rodrigues et al. (Eds.), *Computational Science – ICCS 2019. ICCS 2019. Lecture Notes in Computer Science* (Vol. 11538). Cham: Springer. https://doi.org/10.1007/978-3-030-22744-9_46.
22. Lu, K., Heung, A., Lashkari, H., et al. (2017). A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT. *IEEE Access*, 3302–3312. https://doi.org/10.1109/ACCESS.2017.2677520.
23. Reyna, A., Martín, C., et al. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, 173–190. https://doi.org/10.1016/j.future.2018.05.046.
24. Košt'ál, K., Helebrandt, P., et al. (2019). Management and monitoring of IoT devices using blockchain. *Sensors*. https://doi.org/10.3390/s19040856.
25. Gong, S., Tcydenova, E., et al. (2019). Blockchain-based secure device management framework for an internet of things network in a smart city. *Sustainability*. https://doi.org/10.3390/su11143889.
26. Jayasinghe, D., Lee, G. M., et al. (2019). TrustChain: A privacy preserving block-chain with edge computing. Hindawi. *Wireless Communications and Mobile Computing*. https://doi.org/10.1155/2019/2014697.
27. Theodorou, S., & Sklavos, N. (2019). Blockchain-based security and privacy in smart cities. *Smart Cities Cybersecurity and Privacy*. https://doi.org/10.1016/B978-0-12-815032-0.00003-2.
28. Marsal-Llacuna, M.-L., Colomer-Llinàs, J., et al. (2015). Lessons in urban monitoring taken from sustainable and livable cities to better address the smart cities initiative. *Technological Forecasting and Social Change*, 611–622. https://doi.org/10.1016/j.techfore.2014.01.012.
29. Khan, M., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 395–411. https://doi.org/10.1016/j.future.2017.11.022.
30. Lin, X., Sun, X., et al. (2008). TSVC: Timed efficient and secure vehicular communications with privacy preserving. *IEEE Transactions on Wireless Communications*, 4987–4998. https://doi.org/10.1109/T-WC.2008.070773.
31. Lu, R., Liang, X., et al. (2012). EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications. *IEEE Transactions on Parallel and Distributed Systems*, 1621–1631. https://doi.org/10.1109/TPDS.2012.86.
32. SmartCity. (2018). *Blockchain–train of innovative thoughts transforming smart cities*. Smart City Press. https://www.smartcity.press/blockchain-implementations-in-smart-cities/.

33. Nitti, M., Pilloni, V., et al. (2017). IoT architecture for a sustainable tourism application in a smart city environment. *Mobile Information Systems*. https://doi.org/10.1155/2017/9201640.
34. Pick, J. B. (2017). Smart cities in the United States and worldwide: A rich arena for MIS studies. *Journal of Information Technology Case and Application Research, 19*(3), 133–144. https://doi.org/10.1080/15228053.2017.1363597.
35. Lee, B., & Lee, J. H. (2017). Blockchain-based secure firmware update for embedded devices in an internet of things environment. *The Journal of Supercomputing, 73*, 1152–1167. https://doi.org/10.1007/s11227-016-1870-0.
36. Andrea, Z., Nicola, B., Angelo, C., Lorenzo, V., & Zorzi, Michele, Z. (2012). Internet of things for smart cities. *Internet of Things Journal, IEEE. 1*. https://doi.org/10.1109/JIOT.2014.2306328.
37. Jayasinghe, U., Lee, G. M., MacDermott, Á., & Woo Seop Rhee, W. S. (2019). TrustChain: A privacy preserving blockchain with edge computing. *Wireless Communications and Mobile Computing, 2019, 17*. https://doi.org/10.1155/2019/2014697.