A Unified Framework for Data Integrity Protection in People-centric Smart Cities

May Altulyan[1], Lina Yao[1], Salil. S .Kanhere[1], Xianzhi Wang[2], and Chaoran Huang[1]

[1] School of Computer Science and Engineering, UNSW Sydney NSW 2052, Australia
[2] m.altulyan@student.unsw.edu.au
{lina.yao, salil.kanhere, chaoran.huang}@unsw.edu.au

Abstract. With the rapid increase in urbanisation, the concept of smart cities has attracted considerable attention. By leveraging emerging technologies such as the Internet of Things (IoT), artificial intelligence and cloud computing, smart cities have the potential to improve various indicators of residents quality of life.However, threats to data integrity may affect the delivery of such benefits, especially in the IoT environment where most devices are inherently dynamic and have limited resources. Prior work has focused on ensuring integrity of data in a piecemeal manner and covering only some parts of the smart city ecosystem. In this paper, we address integrity of data from an end-to-end perspective, i.e., from the data source to the data consumer. We propose a holistic framework for ensuring integrity of data in smart cities that covers the entire data lifecycle. Our framework is founded on three fundamental concepts, namely, secret sharing, fog computing and blockchain. We provide a detailed description of various components of the framework and also utilize smart healthcare as use case.

Keywords: Internet of Things· Smart cities · Blockchain · Data integrity.

1 Introduction

Population growth has become a significant worldwide issue, with an increase in the growth rate from 30% in 1950 to 54% in 2017. The problem is particularly acute in urban areas; the United Nations predicts that in 2050, 66% of the worlds population will live in cities [1]. Public services, infrastructure, and a healthy environment are critical factors for ensuring good quality of life, and these will prove more challenging to deliver as the population grows. One potential solution is the smart city. Devices connected to the Internet of Things (IoT) are essential elements of smart cities. They produce a massive amount of data, which highlights the importance of data integrity in smart cities [2].

Definitions of the smart city vary. In[3], the smart city is said to be able to actively generate novel ideas in an open environment by fostering clusters or open data or by serving as a living laboratory that directly involves citizens in

the co-creation of products or services. The increased importance and usage of various technologies has meant that Smart City applications[4][5][6]are gradually becoming profitable. Some of them, however, present sophisticated challenges to security and privacy; smart health is one example. Hence, the secure collection and transmission of data has become an increasingly critical issue in smart city applications, and ways of securing personal data are being sought. Data integrity for smart cities involves protecting data from various threats, such as external attacks during transmission and receipt of data. This involves minimising the risks before data are exposed to tampering. Methods of guaranteeing data integrity include Checksum and Cyclic Redundancy Check (CRC)[7].

Three main factors significantly impact on data integrity in smart city applications: data quality; data modification; and information flow [8]. Data quality refers to the requirement for all elements, including data, information processing, people, and software to meet a priori quality expectations. Data quality can be evaluated proactively or reactively. In a proactive approach, data timeliness is a critical factor and can only be safeguarded if the data are updated at an appropriate rate. A reactive example can be provided to maintain the quality of the database internals. A reasonable expectation of data quality needs to be established. As the amount of data is no longer a limitation, a mechanism to ensure data quality should be developed to treat massive amounts of data as an advantage. Data modification that is, any improper modification is another concern for data integrity [9]. In relation to information flow, it is necessary to prevent the flow of information from the low-integrity level (where there is a high risk of data contamination or manipulation by authorisers) to a high-integrity level. This can be achieved by employing mechanisms such as a lattice model [8] to guarantee secure information flow. In the context of the smart city, data need to protected from any modification throughout their lifecycle. This presents some unique challenges, as elaborated below.

- Changeable data.
  In the smart city context, data are constantly being transmitted, some of which will be stored and shared with third parties to provide services for users. Data integrity must be ensured over their lifecycle.
- Malicious activities.
  In the smart city, multiple interfaces of service access can lead to security vulnerabilities. Attackers can alter or remove data stored in the systems. For example, malicious programs can be introduced into the system, resulting in data loss. Smart city systems need to minimise this possibility to secure data integrity.
- Data quality.
  This is key to the quality of services in the system. Multiple processes may be involved in the data lifecycle in smart cities, and appropriate mechanisms should be employed to reject data that do not meet the relevant criteria.
  The security requirements for a smart city framework include data confidentiality, data integrity, data availability, and authentication. Although several frameworks have been proposed, few focus on data integrity protection. Liu

et al. suggested a framework to resolve data integrity concerns in cloud storage services to eliminate the need for a trusted third-party authority by using blockchain technology [10]. However, this framework only works on a small scale, and focuses on cloud storage services. Other framework focuses on securing data communication in a distributed environment based on blockchain technology [11]. This framework uses blockchain to protect data in a distributed way.

In this paper, we propose a hierarchical framework to guarantee data integrity in smart cities. We divided the framework into three layers: Secret Sharing Layer, Fog Computing Layer and Blockchain Layer. The framework provides whole lifecycle data integrity. The main contributions of this paper are summarized as follows:

- We present a framework for data integrity in the smart city based on three leading technologies: (1) Secret sharing, (2) Fog computing and (3) Blockchain.
- We aim to protect data of IoT devices (first layer) by using Secret Sharing technique. This technique will ensure data integrity as well as reduce the energy consuming. In this layer is classified as sensitive data and normal data. Secret sharing will be applied only on sensitive data.
- We adopt Fog computing to conceal data to help with Blockchain overload. It also performs roles in storing the normal data and sending the sensitive data into blockchain without understanding the content of the messages, and with no complex preprocessing.
- Blockchain technique is employed in the third layer for the safety of data storage in addition to decentralized feature.

The remaining of this paper include the related works in Section 2, the proposed framework in Section 3, the smart healthcare use case in Section 4, and the discussion and conclusion in Section 5.

2 Related work

Data integrity is considered one of the critical security issues in smart city systems, involving both data storage and data transmission. In this paper, we focus on ensuring data integrity for the smart city over its whole lifecycle. Previous literature has considered security frameworks for the smart city. We have grouped these into two categories according to their primary goals: securing communication and securing data storage.

In the category of securing communication, Chakrabarty and Engels presented a framework that focuses on resolving vulnerabilities in traditional IoT systems. Because of resource constraints in IoT nodes, it is not feasible to apply all security measures on every IoT node. Their framework has only four fundamental blocks: black networks; trusted SDN controller; unified registry; and key management system hence it can be easily deployed [12]. Jararweh et al. exploited two techniques, Data Fusion (DF) and Software Defined Systems (SDS),

in the IoT environment to propose a future smart city framework [13]. The DF technique is used to reduce data flow in the network by keeping only useful data, while SDS minimises complexity from the end users side. It does so by separating the data layer from the control layer. Biswas and Muthukkumarasmay proposed a secure smart city framework that used blockchain technology to secure communications between smart devices [11]. They also discussed a potential solution to address the challenge of integrating existing communication protocols and blockchain. Song et al. proposed an improved privacy preserving protocol for smart home systems. The protocol not only protects privacy and security but also requires less overhead computation and power consumption and has good scalability [14]. Gope and Hwang proposed an authentication protocol to investigate the network security requirements in healthcare systems. The protocol has two phases: a registration phase which is responsible for securing the communication channel, and an anonymous authentication phase to secure the data before it is transmitted [15].

In the category of secured data storage many frameworks utilise integrity assurance techniques.[16] presents a comprehensive review of techniques for protecting and verifying the integrity of data from external parties in the cloud. In [10], the authors proposed a framework for providing data integrity services for cloud-based IoT platforms. It uses blockchain technology to eliminate the need for third party involvement and ensure service availability. It also provides data integrity as a service for cloud platforms. Nevertheless, eliminating the third party does not mean that distributed systems cannot be compromised; data integrity can still be at risk. The authors in [17] define a complete architecture using blockchain to protect the data collected by IoT devices. Its principal components are a cloud server, publishers, subscribers, smart contracts and blockchain. The architecture aims to reduce the time needed to validate transactions in blockchain systems. It takes advantage of the database in the system to improve performance, as well as using the publishers as a gateway to connect all IoT devices to the blockchain. There are commonly three types of smart contracts: publishers, subscribers and the client. Each contract has a central role in the blockchain. In [18], the authors proposed an architecture for a vehicle network based on blockchain in the smart city, called a Block-VN. The model has four main components: block controller nodes, blockchain vehicle network, revocation authority and department of motor vehicles. It enables some key features to be exploited by some other existing approaches. For example, it allows vehicles to discover and change their resources by themselves, without the intervention of the third party. The blockchain is used here to provide decentralisation, security, privacy and fault tolerance. Hybrid blockchain was exploited in [19] to address the five potential issues for both IoT devices and blockchain: scalability, security, decentralisation, network limits, and efficiency. The authors divide the blockchain into sub blockchains, each of which is connected to a group of devices and used as a proof of work (PoW) consensus mechanism to proof a new block. They also use Byzantine fault tolerance (BFT) consensus mechanism to connect the sub blockchains. Dorri et al. optimised the efficiency of classic blockchain

with IoT applications by eliminating the overhead issue while retaining most of its privacy and security benefits. The proposed blockchain reduces the delays in transaction processing by eliminating mining [20]. In [21] blockchain is used to ensure data integrity of IoT datasets and IoT systems. The authors proposed a framework to address the dataset challenges of data integrity and data lifetime, in which blockchain and the owners maintain the only a Reference Integrity Metric(RIM) that can remove data at any time. In IoT systems, blockchains are also used to sustain RIM and update firmware.

The research in these two categories often has a single focus, while our work can be a hybrid of the two. This paper aims to solve the data integrity issue for the smart city over its whole lifecycle.

3 Proposed Smart City Framework

We first provide an overview of the three main techniques used in our framework, followed by a detailed description of the framework.

3.1 Preliminaries techniques

1. *Blockchain*
   Blockchain is an emerging technology that consists of sequential chained blocks including ledgers that are replicated in each node of a peer to peer network and are primarily used to store financial transactions that are shared by all users. Consequently, any modifications in these transactions can be easily detected. The typical workflow of a blockchain system is shown in Fig.1. When a transaction is created, a block is made. All nodes in the network receive a broadcast about this block and one of the nodes (called miner) validates the block and broadcasts it to all nodes. The block is added to the chain by the nodes when they verify that it has a hash number to connect with the previous block [21].
   Blockchain technologies are categorised as public, private and consortium blockchain. Each one has a main feature and specific consensus mechanisms [22]. However, blockchain cannot be directly adapted to IoT, so several problems and challenges need to be addressed. First, mining in blockchain requires complex computation in which some IoT devices have restricted resources. Second, mining is time-consuming, which is not desirable in IoT applications. Third, blockchain is scalability while IoT that be connected to the network is increased. Finally, blockchain protocols may still be insufficient in the IoT environment.
   Despite these challenges, blockchain has been adapted for use in different domains of the IoT, including the smart city. Blockchain has several advantages as a potential solution to the problem of protecting data integrity. First, it uses a peer to peer network so there is no single point of failure. If any node fails, the other nodes will complete the operation without any ill effects. This feature is consistent with decentralisation in smart cities, where

data should be available to provide services at any time. Second, blockchain has a distributed database that records all transactions. All participating devices keep an identical copy of the records to ensure the integrity of these data in the case of attacker activities. Although 51% of an attack[23] can accrue in the blockchain, only transactions within the past few blocks can be modified by an attacker. Third, the history of all transactions can be traced by blockchain and all transactions can be stored permanently. This feature helps to repair corrupted software by replacing the corrupted code with a similar code. Finally, IoT devices in the smart city are always connected to a network, and they need to be updated. Authentication should be investigated to prevent unauthorised modification. Authentication is achieved in blockchain using existing tools such as smart contracting.

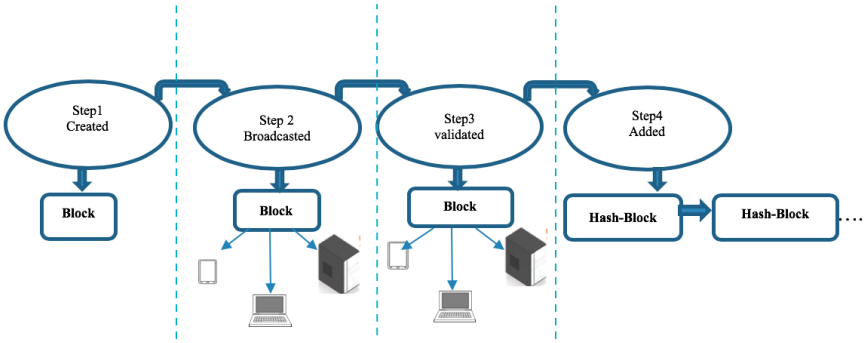

Fig. 1. Exemplary blockchain process[21].

2. *Fog computing*
   Fog computing is an extension of the cloud computing paradigm that enables connection and interaction with the network without the third party. Fog computing includes mobile cloud computing (MCC) and mobile-edge computing (MEC) and their various features, such as mobility, interface heterogeneity, network and communication protocols and interaction with the cloud. Fog computing has several advantages, such as reducing big data, low latency, and availability. The use of fog computing with IoT has recently attracted considerable attention, especially for the smart city, where it not only provides low latency and location awareness but also provides better real-time services. In [24], the authors explain several promising scenarios for the use of fog computing in the smart city. Nonetheless, as with other technologies, some issues with fog computing need to be addressed [25].
3. *Secret sharing*
   The smart city uses sensors in several kinds of applications in domains such as smart health applications. Sensor nodes produce a massive amount of data, either sensitive data (such as medical sensors) or normal data. When sensor nodes are compromised, they are referred to as malicious sensor nodes

and the sensory data may be lost or modified. In the smart city, sensory data integrity is essential to ensure that the content data are not revealed during data aggregation[26]. There are two approaches to protecting data aggregation: the end to end scheme [27] and the hope by hope scheme [28]. In our work, we consider the end to end scheme based on secret sharing because the data do not need to be encrypted, thus reducing energy. Secret sharing schemes are an important cryptography tool to investigate several security requirements [29]. Shares are distributed among parties by a dealer, but only authorised subsets of parties can perform the secret reconstruction.[30] proposed two approaches based on secret sharing: sign share and sham share. Sign share could be adapted in our framework to provide data integrity for smart cities. The sign-share approach has four phases: setup, secret sharing signature, aggregation, and verification decoding. In the setup phase, numbers of parameters are initially loaded into each node. The second phase encodes the sensory data then splits the encoded data into four parts, encoding each using one of these parameters, finally signing each byte and sending data in a tuple to the next phase. The aggregation phase is responsible for collecting the four parts and sending them to the base station. In the last phase, the data are constructed by the base station. Each of these phases is included in the secret sharing layer of our framework.

3.2 Overview the Framework Structure

Here we propose a hierarchical framework for data integrity in the smart city and explain the detailed specifications of the proposed model. [31] proposed a distributed cloud based on the blockchain model to address traditional network architecture issues such as high scalability, security, resiliency, and low latency. It combines three emerging technologies: blockchain to provide safety; fog computing to manage the raw data of IoT devices; and software-defined networking (SDN) to control the fog nodes. Based on [31], we propose a smart city framework that consists of three technologies: secret sharing, fog computing, and a blockchain. Secret sharing is used to decode and split the sensory data. Fog computing nodes provide services and interact with blockchain, as well as reducing overload of the blockchain by aggregating and analysing the raw data from IoT devices. The blockchain technique is used to address some of the challenges in the IoT platform such as reliability, scalability and availability of services. This framework can help to ensure integrity, increase security and enhance performance. In this section, we overview the structure of the proposed framework and describe its components. The framework is built on three layers: secret sharing, fog computing and blockchain, as shown in Fig.2.

1. Secret sharing layer
   This layer is responsible for monitoring the physical environment, which consists of numerous sensor nodes Fig.2(a). Those sensors are capable of sensing and gathering information about the surroundings. Consequently, they can cover several domains and critical applications in smart cities, such as health,

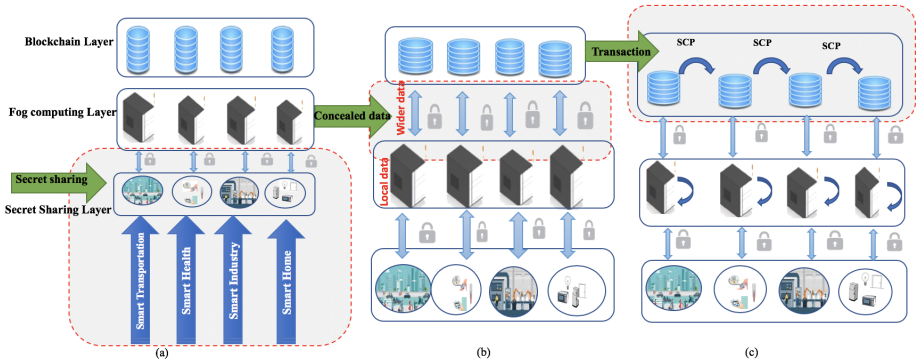

Fig. 2. Smart City Framework.

transportation, home, and government. Raw data collected from IoT devices may have different formats, such as plain text, sounds, and images, while the devices themselves can have limited resources in terms of processing power, storage, and battery life. As explained above, data privacy and integrity are critical challenges that need to be addressed. To this end, we introduce a concealed data filtering technique that allows the data to be filtered by the fog layer without the need for it to understand the content of the messages and with no complex pre-processing that would require the devices to rapidly consume battery power. The sign share approach for secret sharing introduced in secret sharing part can be used here to provide concealed data filtering. The main idea is that each node (device) is loaded with the required parameters at the initial stage by applying the first phase of the sign share approach. Then the sensor node senses the physical environment and, before producing its data, applies the second phase of the sign share approach as mentioned above. Finally, the data are sent to the next layer (fog layer) for processing. As the sensors can produce sensitive data, they encode and split the collected data into number of chunks. Modern cryptology can ensure that only the desired destination can understand the content, without the need for the fog layer, which filtered the data, to understand it. When the final destination nodes have received all the chunks, the received data are reconstructed and formatted into transactions. Note that the secret sharing steps apply only in the case of sensitive data; other data are sent directly to the next layer without going through these steps.

2. Fog computing layer
   As mentioned earlier, the fog computing layer plays an essential role in reducing the overload of the top layer by filtering the data received from the previous layer. Each fog node in this layer is connected to a group of sensors; when these nodes receive the data of the previous layer, they apply

the following steps, as shown in Fig.2(b). First, concealed data filtering is used to analyse the received data without understanding the content of the messages by using the aggregation phase of sign share. Then the data are sorted into sensitive data and normal data. Normal data are stored separately to be accessed by local services. The sensitive concealed data are fed into wider services in the next layer,and that is Blockchain. This has two significant benefits. First, fog computing deals with the sensitive data without understanding the content, thus ensuring data integrity and privacy. Second, filtering the data and sending only the sensitive data reduces overload of the top layer and improves the latency performance of the system.

3. Blockchain layer
   The highest layer is blockchain. As illustrated in Fig. 2(c), this layer receives and processes data and information from nodes from the second layer. Blockchain also acts as a base station which receives data from the previous layer, verifies it and converts it into the transaction using the verification decoding phase of sign share. To manage transactions among blockchain, we adapted the Stellar Consensus Protocol (SCP) consensus mechanism[32], which has the following key features:
   - Decentralisation: Each node in blockchain can participate and eliminate the third-party authority.
   - Low latency: SCP helps nodes to investigate consensus in relatively shorter time[33].
   - Flexibility: Blockchain nodes can trust any group of nodes that have sufficient consensus.
   - Security: The use of digital signatures and hashes that consider critical parameters can protect against adversaries with unimaginably vast computing power.

4 Smart Healthcare Use Case

This section considers the potential use case of our framework. The paradigm is not limited to this example, but it demonstrates the benefits of the framework. It can be generalised to a wider range of application domains, such as smart homes, to enhance the deployment of privacy-preserving IoT services [34, 35].

Alice is an elderly woman who experienced a heart attack last month and who lives alone. Our system allows authorised persons to monitor her health status, and the information can be made available to all hospitals in the city Fig.3. It will also ensure that Alice receives a timely medical response in the case of a critical health issue. Her house will be equipped with passive RFID tags and medical sensors to keep an eye on her activities and movements. Biometric sensors will also be in place to monitor cardiac activity, glucose levels, temperature, CO2 levels, brain activity, blood pressure, GSR stress levels, and oxygen blood levels. Such vital data can be collected and analysed in realtime and stored for future access.

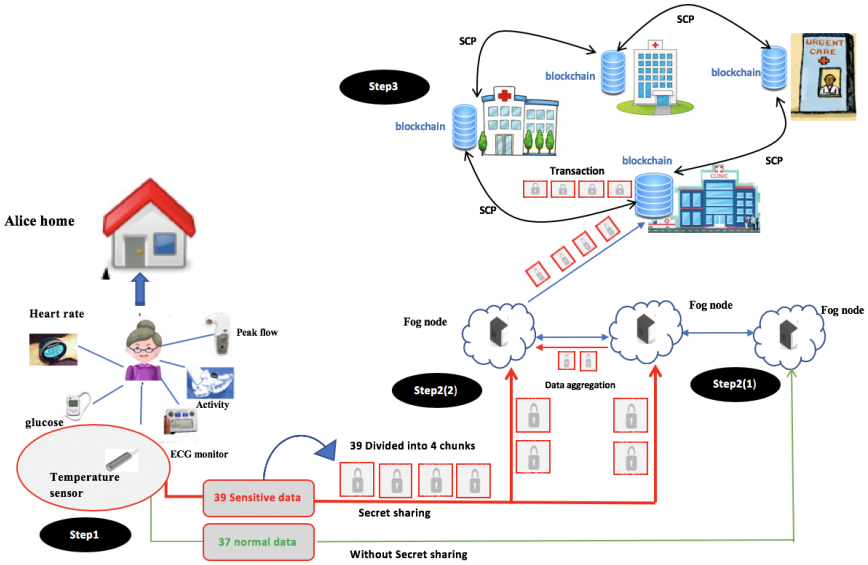

Fig. 3. Comprehensive Example for Smart healthcare.

Medical Sensors. At step 1 in Fig.3, medical sensors are used to monitor Alices health at home. These sensors are capable of sensing and gathering sensitive information about her. The sensor nodes sense Alices situation and produce data that are sent to the fog layer. Every sensor needs to classify its data into two types: sensitive or normal. For example, when a body temperature sensor yields a reading above 39 degrees Celsius, this value will be classified as sensitive data as it contains personal health information about Alice. The body temperature sensor will apply the second phase of secret sharing, where data are decoded and split into four chunks, each of which is decoded. These steps would only be applied on sensitive data (the data that need to be sent to the hospital for additional processing). Normal data will be sent directly to the next layer. The main feature of this layer is that sensitive data will be protected from any modification or alteration until the next layer receives it.

Data Flirting and Features Extracting. Fog node is connected to all medical sensors at Alices home. When this node receives the medical sensory data, it will apply the following procedures. First, the data chunks are collected and concealed data filtering is used to categorise these received data as sensitive or normal. Normal data will be stored in this node as step 2(1) in Fig.3 and sensitive data will be sent to the upper layer as step 2(2) in Fig.3. In our example, the data will be sent to the next layer for further processing. This layer has the following features:

- The integrity of the sensitive data will be intact because this layer deals with sensitive data without knowing the content.
- The performance of the system is enhanced by filtering the data into two types.

Top Layer The hospital receives the data then constructs it again as transactions using the verification decoding phase of sign share as step 3 in Fig.3. Because of the decentralisation feature in the blockchain, the data are available to all hospitals in this city to ensure the highest quality of of health services provision. In our case, this layer provides the following features:

- The integrity of the sensitive data is ensured by using blockchain.
- All of Alices health records will be available in all hospitals in her city.

5 Discussion and Conclusion

Since IoT data are dynamic in nature and vast in quantity, data integrity is a significant concern in the context of the smart city. Our proposed framework helps to address the data integrity issue. Generally, the entire smart system involves validating data integrity, from data aggregation until destination. Some studies focus on providing secure data for specific aspects in their frameworks [11],[12] ,[17],[31]. The primary goal of our framework, in contrast, is to ensure life-cycle data integrity. As part of our future work, we intend to explore how to leverage this framework in the context of IoT recommendation systems, which impose harsher constraints on data/device security and privacy[36].

In summary, the service framework we propose has the following advantages:

- It ensures that data can be transferred among nodes that are unaware of data content until the destination is reached.
- It deals with critical challenges in coordinating large IoT devices and generating data simultaneously.
- It provides resiliency against many threats by using blockchain and has several unique features to deal with sensitive data.

Our case study shows how the framework could be useful in some domains of smart cities, such as smart healthcare . However, this work also poses some challenges that have not been addressed in this paper, such as latency and energy consumption issues, which will be the subject of future work. We also intend to evaluate this framework for use as a platform for different applications for the smart city.

References

1. C. Ferreira, R. Walsh, and A. Ferreira, "Degradation in urban areas," *Current Opinion in Environmental Science & Health*, 2018.
2. M. Sheng, Y. Qin, L. Yao, and B. Benatallah, *Managing the web of things: linking the real world to the web.* Morgan Kaufmann, 2017.

3. T. Bakıcı, E. Almirall, and J. Wareham, "A smart city initiative: the case of barcelona," *Journal of the Knowledge Economy*, vol. 4, no. 2, pp. 135–148, 2013.
4. K. Su, J. Li, and H. Fu, "Smart city and the applications," in *Electronics, Communications and Control (ICECC), 2011 International Conference on*, pp. 1028–1031, IEEE, 2011.
5. X. Chang, Y.-L. Yu, Y. Yang, and E. P. Xing, "Semantic pooling for complex event analysis in untrimmed videos," *IEEE transactions on pattern analysis and machine intelligence*, vol. 39, no. 8, pp. 1617–1632, 2017.
6. Z. Zeng, Z. Li, D. Cheng, H. Zhang, K. Zhan, and Y. Yang, "Two-stream multirate recurrent neural network for video-based pedestrian reidentification," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 3179–3186, 2018.
7. M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of internet of things (iot)," *International Journal of Computer Applications*, vol. 111, no. 7, 2015.
8. R. S. Sandhu, "On five definitions of data integrity.," in *DBSec*, pp. 257–267, 1993.
9. G. Sivathanu, C. P. Wright, and E. Zadok, "Ensuring data integrity in storage: Techniques and applications," in *Proceedings of the 2005 ACM workshop on Storage security and survivability*, pp. 26–36, ACM, 2005.
10. B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for iot data," in *Web Services (ICWS), 2017 IEEE International Conference on*, pp. 468–475, IEEE, 2017.
11. K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016 IEEE 18th International Conference on*, pp. 1392–1393, IEEE, 2016.
12. S. Chakrabarty and D. W. Engels, "A secure iot architecture for smart cities," in *Consumer Communications & Networking Conference (CCNC), 2016 13th IEEE Annual*, pp. 812–813, IEEE, 2016.
13. Y. Jararweh, M. Al-Ayyoub, E. Benkhelifa, *et al.*, "An experimental framework for future smart cities using data fusion and software defined systems: The case of environmental monitoring for smart healthcare," *Future Generation Computer Systems*, 2018.
14. T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A privacy preserving communication protocol for iot applications in smart homes," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1844–1852, 2017.
15. P. Gope and T. Hwang, "Bsn-care: A secure iot-based modern healthcare system using body sensor network," *IEEE Sensors Journal*, vol. 16, no. 5, pp. 1368–1376, 2016.
16. C. Liu, C. Yang, X. Zhang, and J. Chen, "External integrity verification for outsourced big data in cloud and iot: A big picture," *Future generation computer systems*, vol. 49, pp. 58–67, 2015.
17. N. Rifi, E. Rachkidi, N. Agoulmine, and N. C. Taher, "Towards using blockchain technology for iot data access protection," in *Ubiquitous Wireless Broadband (ICUWB), 2017 IEEE 17th International Conference on*, pp. 1–5, IEEE, 2017.
18. P. K. Sharma, S. Y. Moon, and J. H. Park, "Block-vn: A distributed blockchain based vehicular network architecture in smart city," *Journal of Information Processing Systems*, vol. 13, no. 1, p. 84, 2017.
19. G. Sagirlar, B. Carminati, E. Ferrari, J. D. Sheehan, and E. Ragnoli, "Hybrid-iot: Hybrid blockchain architecture for internet of things-pow sub-blockchains," *arXiv preprint arXiv:1804.03903*, 2018.

20. A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for iot," in *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, pp. 173–178, ACM, 2017.
21. M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for internet-of-things security: a position paper," *Digital Communications and Networks*, 2017.
22. Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," *Work Pap.–2016*, 2016.
23. X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, 2017.
24. C. Perera, Y. Qin, J. C. Estrella, S. Reiff-Marganiec, and A. V. Vasilakos, "Fog computing for sustainable smart cities: A survey," *ACM Computing Surveys (CSUR)*, vol. 50, no. 3, p. 32, 2017.
25. S. Yi, C. Li, and Q. Li, "A survey of fog computing: concepts, applications and issues," in *Proceedings of the 2015 workshop on mobile big data*, pp. 37–42, ACM, 2015.
26. N. S. Patil and P. Patil, "Data aggregation in wireless sensor network," in *IEEE international conference on computational intelligence and computing research*, vol. 6, 2010.
27. J. Jose, J. Jose, and M. Princy, "A survey on privacy preserving data aggregation protocols forwireless sensor networks," *Journal of computing and information technology*, vol. 22, no. 1, pp. 1–20, 2014.
28. Y. Yang, X. Wang, S. Zhu, and G. Cao, "Sdap: A secure hop-by-hop data aggregation protocol for sensor networks," *ACM Transactions on Information and System Security (TISSEC)*, vol. 11, no. 4, p. 18, 2008.
29. M. Rezvani, A. Ignjatovic, E. Bertino, and S. Jha, "Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks," *IEEE transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 98–110, 2015.
30. W. Y. Alghamdi, H. Wu, and S. S. Kanhere, "Reliable and secure end-to-end data aggregation using secret sharing in wsns," in *Wireless Communications and Networking Conference (WCNC), 2017 IEEE*, pp. 1–6, IEEE, 2017.
31. P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for iot," *IEEE Access*, vol. 6, pp. 115–124, 2018.
32. D. Mazieres, "The stellar consensus protocol: A federated model for internet-level consensus," *Stellar Development Foundation*, 2015.
33. A. Baliga, "Understanding blockchain consensus models," *Persistent*, 2017.
34. L. Yao, Q. Z. Sheng, and S. Dustdar, "Web-based management of the internet of things," *IEEE Internet Computing*, vol. 19, no. 4, pp. 60–67, 2015.
35. U. Salama, L. Yao, X. Wang, H.-y. Paik, and A. Beheshti, "Multi-level privacy-preserving access control as a service for personal healthcare monitoring," in *Web Services (ICWS), 2017 IEEE International Conference on*, pp. 878–881, IEEE, 2017.
36. L. Yao, Q. Z. Sheng, A. H. Ngu, and X. Li, "Things of interest recommendation by leveraging heterogeneous relations in the internet of things," *ACM Transactions on Internet Technology (TOIT)*, vol. 16, no. 2, p. 9, 2016.