Privacy and Security Technologies for Smart City Development

Chapter · October 2020

DOI: 10.1007/978-3-030-53149-2_1

4 authors:

Gauri Vaidya
University of Limerick Ireland
15 PUBLICATIONS **58** CITATIONS
SEE PROFILE

Prabhleen Bindra
Government College Of Engineering Aurangabad
5 PUBLICATIONS **175** CITATIONS
SEE PROFILE

Meghana Kshirsagar
University of Limerick
72 PUBLICATIONS **572** CITATIONS
SEE PROFILE

Sharvari Chandrashekhar Tamane
Jawaharlal Nehru Engineering College
26 PUBLICATIONS **191** CITATIONS
SEE PROFILE

Privacy and Security Technologies for Smart City Development

Gauri Vaidya, Prabhleen Bindra, Meghana Kshirsagar, and Sharvari Chandrashekhar Tamane

Abstract The ever-increasing rate of urban population and latest technological advances including the IoT, sensors, big data, cloud computing and data analytics has replaced the standard methods of service delivery to the citizens. The IoT devices collect real-time and integrated data by monitoring an individual's daily activities with the aim of providing efficient services including but not restricted to smart transportation, waste management, personalized healthcare and recommendations. As personal and sensitive information is being collected by these devices, security and privacy challenges are crucial paradigms for concern. While safety and privacy have always been significant study areas, there is a need for a broader perspective to protect personal data with evolving technological challenges. This chapter introduces the security and privacy issues faced by the existing infrastructure. Some case studies are discussed with the measures undertaken for data privacy and security. The chapter concludes with open research challenges grounded on security and privacy.

Keywords Privacy · Security · Internet of things · Big data · Cloud computing · Smart city

G. Vaidya (✉) · P. Bindra
Graduate Student, Computer Science and Engineering Department, Government College of Engineering, Aurangabad, India
e-mail: gsvaidya2608@gmail.com

P. Bindra
e-mail: prabhleenbindra13@gmail.com

M. Kshirsagar
Postdoctoral Researcher, Biocomputing and Development Systems Lab, Lero, The Irish Software Research Centre, University of Limerick, Limerick, Ireland
e-mail: meghana.kshirsagar@ul.ie

S. C. Tamane
Department of Information Technology, Jawaharlal Nehru Engineering College, MGM University, Aurangabad, India
e-mail: sharvaree73@yahoo.com

S. C. Tamane et al. (eds.), *Security and Privacy Applications for Smart City Development*, Studies in Systems, Decision and Control 308,
https://doi.org/10.1007/978-3-030-53149-2_1

1 Introduction

The way smart cities are defined globally differs in the context of what the citizens of a country may seek. For developing and underdeveloped countries the citizens may aspire for a smarter infrastructure whereas the western countries may look at more digitization and automation [1]. With IoT being the driving force for sensing, and collecting data these days, every minute detail of an individual is monitored. Integrated data collected through different smart services can prompt unsafe bits of knowledge about a person. For example, the behavior of a person can be analyzed from a person's transaction timings or from his/her medical data.

Smart infrastructure [2] forms the basis of a smart city and is essential to pace up the growth of urbanization in a city. It includes smart homes, smart mobility, smart governance, smart environment and smart economy. *Smart homes* [3, 4] are furnished with numerous sensors and various smart technologies such as smart meters, smart televisions, smart speakers equipped with virtual personal assistants, etc. to name a few. These devices not only track consumption patterns of users, but also record security passwords, sleep patterns, and child behavior. *Smart healthcare* [5] crucially records patient sensitive data, such as a patient's medical history which is critically very personal and cannot be shared without a person's consent. Various social networks can access a person's health records thereby compromising with sensitive data [6]. *Smart mobility* [7] aims at developing advanced and sustainable ways to improve travel experience along with environment-friendly fuels for efficient management of public and private transport. Due to ineffective and inappropriate management of vehicles, various ill-effects such as increased pollution and traffic congestion have signaled the demanding need to come up with appropriate smart mobility solutions. *Smart transportation* [8] helps pace up with the fast-growing urban population and encourages in effectively managing the city traffic, automatic street-lights, automatic pothole detection, etc. being the new addition to the system. An extension to smart transportation includes location-based services like navigation. Many organizations sell sensitive information such as a user's place and time for minting cash from a business perspective. There is a strong need to protect such data from being leaked [9, 10].

Intelligent manufacturing [11] too has been a key feature in development. The manufacturing sectors have been on par excellence and achievement with the least human interference. From handling raw materials to producing finished products, data analytics is used for the analysis of machinery to know about which parts may fail and thus taking necessary measures in advance, running various simulation processes for finding better ways of doing things has enhanced manufacturing and effectiveness in recent years. *Smart governance* [12] has also been a significant development since the advent of smart cities. By facilitating better choices and planning, making transparent and trustworthy transactions, the effectiveness in the delivery system of public services has increased. *Smart economy* [13] drives the economic development of a city by experimenting and promoting strategies through tourism, local assets, and resource management. Internal and external threats, data proliferation, strong

Table 1 Security and privacy challenges in smart city

Dimension	Challenges
Smart homes	Data tampering, data and identity thefts, eavesdropping, denial of service (DoS), software exploitation [14]
Smart healthcare	Physical attacks, DoS, trust, data manipulation [15]
Smart mobility	Sybil attacks, DoS, DDoS, flash events, security of software platform [16]
Smart transportation	Broadcast and message tampering, jamming, man in the middle, eavesdropping, device hijacking, sybil [17]
Smart governance	Accessibility, DoS, transparency, trust [18]
Intelligent manufacturing	DoS, cloud security, botnets, data tampering, malware [19]
Smart economy	Internal and external threats, data proliferation, strong regulation at national and international level [20]

regulation at the national and international levels can be regarded as a few threats posed due to the wide domains economy plays a role in. There is an observed pattern among the challenges faced by each of the domains mentioned above. Table 1 depicts these challenges in terms of privacy and security threats. Domains which involve data transfer have a threat of data theft and data tempering whereas those which involve data storage are affected by trust and software attacks threats. This study of patterns of threats is useful while implementing digital technologies in determining which technology covers most of the threats for that domain.

With advancement of technology and countries shifting towards the digital world, it is important to study and review the security and privacy threats for developing sustainable smart city architectures. It is equally important to study the approaches of certain cities which have excelled in overcoming the challenges faced by them with upcoming digital technologies. In this study, we bring upon the potential threats possessed while storing, accessing and retrieving data collected using IoT devices, stored on various cloud platforms or processed using big data techniques. Through the course of this study, we present forthcoming technologies which shall play a vital role in the coming future to overcome these challenges. We present a machine learning based approach which can identify the probabilistic chances of identifying a threat that could be faced in a specific domain. This could help in identifying the revenue losses caused due to lack of security to this information.

Although people have benefited a lot from the above applications, ensuring that personal data of an individual is retained, not used without his prior consent, and not vulnerable to cyber-attacks is a must. In the coming sections we learn about the recent developments in the diverse domains of smart cities. We also touch upon the privacy and security threats faced. We then study about the issues, threats and problems faced in smart city developments for data security. We propose a few emerging technological solutions to overcome the barriers faced and build secure smart city networks. In the final sections of the chapter we highlight a few smart cities which have excelled in certain domains and have emerged as models to be followed. Discussions, future scope and research opportunities available are presented to conclude the chapter.

In this chapter, we introduce security and privacy issues existing in the current scenario and discuss the steps taken towards the privacy of the data and the laws for data usage. Existing system infrastructure for the collection of digital information, it's components along with security measures at each layer of the infrastructure are presented. The analysis of integrating traditional methodologies with emerging technologies is discussed. The chapter concludes with possible solutions to overcome the threats in smart city architecture.

2 Background

There are many factors that have led the notion of smart cities to be the buzzword of the moment. The percentage of people residing in urban areas has drastically increased in the last decades and anticipated to develop more in the future as seen in Fig. 1. Sustainability, quality of life, education, income source, transport, etc. are the services that attract people to migrate to urban regions. About 68% of the total

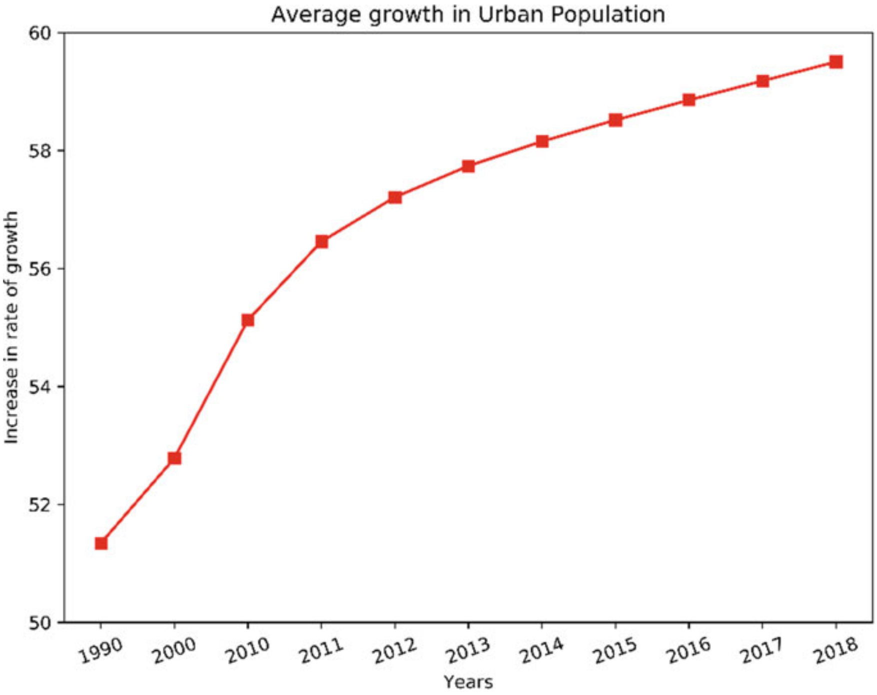

Fig. 1 World population growth in urban areas. *Data Source* World Data Bank (2019) [23]

world's population is expected to live in urban areas by 2050, particularly in Asia and Africa [21].

Developments and urbanization have become so crucial that the capital city of the state sometimes contributes to half of the country's GDP, for example, the capital city of South Korea. According to Forbes's recent study, London stands to be the smartest city in the globe with the use of the latest technologies across more than one dimension. In addition to advancing technological developments, there are other elements that add to the city's top ranking. The Cross rail project, which is Europe's largest project is being carried out in London i.e. smart cities also have the potential to earn global resources and exports for the country in which they reside. This has led to the trend of the use of the latest technologies to a large extent where every physical thing is connected to the Internet. The smart cities are characterized by the following characteristics in terms of digitalization: Internet of Things (IoT), Big Data and Cloud Services to integrate and draw significant insights from them. Most cities are developing rapidly in terms of intelligence using these digital technologies. Louisville is the smart city in the U.S. that is now on the track of becoming smarter through the IFTTT platform (if this is then that) and community-wide applets. For example, the home color can be changed if there is an emergency in their area which helps in taking immediate actions. Songdo has a very strong network of cameras and sensors that helps people to find everything from home. For example, a hair stylist may advise them from home as well as plan a trip with their travel agency by being at home via video conferencing. Similarly, Copenhagen is known for its free data exchange, as they have achieved great heights through proper management of waste, lights, energy and buildings. They may be carbon neutral by 2025 through this. These best smart city examples prove that our future is already here. However, this great future also brings with it, two major issues: security and privacy of the data, which has the potential to destroy the whole system infrastructure [22].

2.1 Security

The increasingly complex network structure of the smart city systems due to digital communication, connected devices and network systems is often less secured. 80% of the data is heterogeneous owing to the modifications in the device status as per the activities of an individual like sleeping, eating, location, etc. [23]. These devices are interconnected through a wireless network and follow open network protocols or APIs which can readily be attacked with a tiny piece of code. Man-in-the-middle, Distributed Denial of Service (DDoS), Device Hijacking and Permanent Denial of Service (PDoS) are some commonly caused threats to smart devices. For example, the smart houses' keypad can be locked by an attacker initiating with control over the thermostat, or the un-protectable wears could cause identity threat by obtaining information, or the device could be completely damaged with control over the thermostat, transmitting the data to the cloud and then feeding inappropriate information for its operation [24].

Security is the prime concern for data; various tools for securing data have come up. Cui et al. have put forth the security threats and issues faced within a smart city like botnet attacks on IoT sensors, possible artificial intelligence (AI) threats, autonomous vehicles (AV) if once hacked can pose a threat to driverless vehicles. Unencrypted healthcare data can also create privacy threats. Security requirements include privacy protection, authentication, confidentiality and availability of data. Technologies like blockchain, cryptography, biometrics, machine learning and data mining, game theory, and ontology can be used to maintain security and privacy of the system [25].

2.2 Privacy

Data analytics is prominent in every sector in today's world for decision-making processes, and thus data is a significant factor. However, as stated previously, as each activity of an individual is being tracked, this data is an important asset of an individual, right from his personal health habits to his thoughts on social media. From the embedded information acquired, the analytics could easily find out the social habits and status of the individual. This information becomes even more vulnerable when integrated with health information. However, while discussing social media, there is at least an indirect consent an individual agrees before sharing or using the service. While discussing IoT devices, there is no such input media for the device to ask for approval nor can the individual grant consent themselves. This has resulted in important research: The government and private bodies, which are consistently aiming at a better quality of life for people or the people who are the generators of the data; this challenging research has opened a wide horizon of alternatives and further discussions about the extent they assert the privacy of the data [26]. According to He, the IoT network, the clients and the application communicate in a wireless environment, which is susceptible to attacks of an individual's personal data. The following seven requirements must be taken into account while designing any application for maintaining security or privacy of the data: mutual authentication, non-traceability, no verification table, session key agreement, perfect forward secrecy, and attack resistance. He evaluated the Liu et al.'s methodology to secure the network through public and private keys by claiming that if the public key is forged, there is no way to verify the legality of the public key, making it insecure. He proposes a framework that first verifies whether the public key is legal or not by introducing a new key called session key that will never be disclosed even if the public key is forged [27].

Kuan Zeng et al. [28] proposed smart city architecture based on which security measures have been recommended. Security and privacy issues existing in the system have been described. Storing data directly over the cloud may endanger data over hacking. A probable solution suggested is encrypting and storing data over the cloud using cipher text. This ensures that the cloud servers cannot directly access stored data. Smart cities require a trustworthy and dependable control of data. Social network data can be used to analyze and diagnose certain medical diseases as follows. Speaking specifically for healthcare and social data privacy and security [29], proposes a Mobile Healthcare Social Network (MHSN) data privacy scheme. An encryption algorithm for storing health and social data on the respective cloud by generating cipher text has been proposed. As known, data is collected using sensors. This data is stored over the cloud after consent by the data owner, in a cipher text format thereby making sure of the privacy aspect. It works on the public key and master key concepts, using which attribute and secret keys are generated. To further maintain privacy, health data is not completely de-encrypted. It is first partially decrypted at the cloud level followed by user-level decryption. Another privacy-preserving application specified is to prevent tampering of smart meters [30].

The Global Positioning System (GPS) details may reveal personal details of a vehicle such as its location, speed, etc. With AdSense and e-advertisements gaining popularity, public agencies sell this sensitive data which requires confidentiality to private agencies for commercial profits. Various techniques mentioned in [30, 31] include dummy-based methods (wherein a dummy location along with the actual location is forwarded creating anonymity), k-anonymity (which hides confidential details of users and service providers using third-parties called anonymizers) [31, 32], cryptography, and differential privacy. The authors mainly focus on differential privacy for preserving GPS data. Continuing further, Zhang also suggests, smart navigation for intelligent transport wherein the threat for data leak to the road service unit (RSUs) from querying vehicles can be resolved by encrypting source and destination locations using AES and Elgamal schemes. A group signature is created using credentials disseminated by trusted authorities. Group signatures also help authorities trace malicious activity if any. Location privacy is thus maintained using distributed RSUs.

To summarize, we may conclude that it is necessary to come up with new security measures on a daily basis in order to tackle mundane and trivial issues in a smart infrastructure.

3 Issues, Controversies, Problems Towards Smart City Development

As emphasized above, we realize how important it is to maintain security and privacy in a smart city. However, while addressing any issue, it is important to study the trends of it in detail. These trends give an exact idea about what issue needs to be addressed. We have analyzed the data available from standard reports and studied them from the perspective of data threats. In this chapter, a predictive survey over a dataset has been performed to highlight the same. The dataset included various data thefts and breaches with their details on smart cities over the past few years. Based on this data, specific data analytics has been performed to understand the trends of data threats in smart cities with respective technologies.

The number of IoT devices is increasing at a regular pace in the infrastructure of smart cities. There has been a regular growth of around 10% every year. However, the statistics of the increase in the data threats are quite surprising. Only in the single year 2016–17, the data threats have increased by 600%, which is more than the total number of IoT devices in the world. In order to study the threats pattern, it is important to know the environments where organizations prefer to store private and sensitive information of the users. The Thales Report by International Data Corporation (IDC) states that cloud services, mobile payments, social media, and IoT devices are the top-rated environments where sensitive data is stored. The traditional ways of storing sensitive data in encryption mode in databases have been replaced by digital transformation and using technologies like cloud, IoT, Big Data and Blockchain [32, 33]. This emphasizes the need for service providers to ensure the following (Fig. 2):

1. Data protection technologies like tokenization, encryption and data anonymity techniques for data safety have been applied before sending the data to the center before storing data over the cloud.
2. Data from various infrastructures when integrated needs to be encrypted before sending further for any process.

As cloud, IoT and Big Data [33–35]have sensitive data stored and these technologies are also significant in smart cities point of view, we study the trends of each one of them in detail.

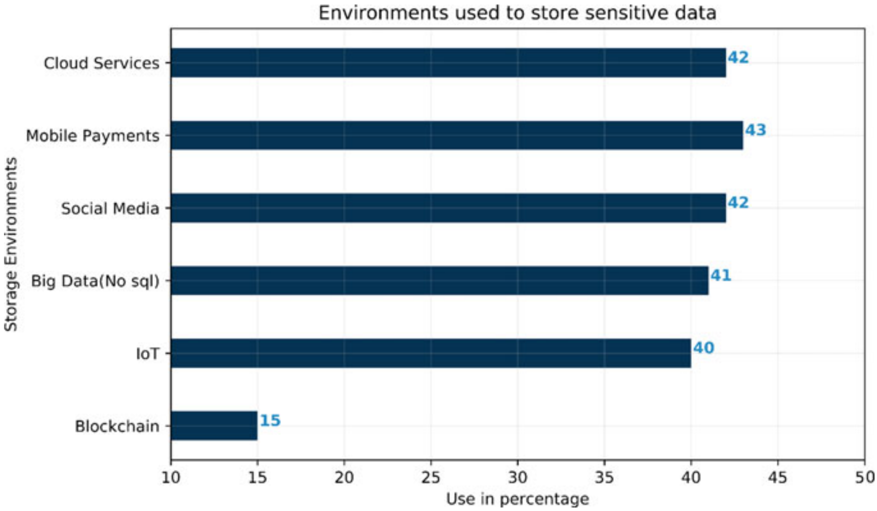

Fig. 2 Analysis of platforms used to store personal information. *Data Source* International Data Corporation (2019) [33]

3.1 Cloud Services

Cloud services including Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) are being used these days for data storage purpose due to their efficient properties like better technology management, scalability, interoperability, data mobility, remote control, and effective cost. Though the use is ever increasing due to their advantages, there is an increasing concern for growing data threats over cloud services. A recent study has proved that most of the data breaches have occurred due to a lack of data privacy policy, cloud services fail to ensure the privacy of the data and others. The operational structure of cloud services need to be stronger in terms of access controls over the data like who can access the data, and up to what level of privacy can data access be granted [35, 36]. A detailed analysis of frequent data threats in smart cities is as follows (Fig. 3):

- Security of customers' data is at stake if the cloud provider fails to protect the data due to poor security practices, application vulnerabilities, and others. This leads to data breaches like insider attacks, data theft, etc.
- Security breach/attacks at the service provider rank as a top concern for data threat vulnerabilities.
- Lack of a data privacy policy or privacy service level agreement is the comprehensive cause of data attacks which puts even public cloud's data at stake.
- Lack of visibility into security practices at the end of the service creates an invisible entry for attackers.

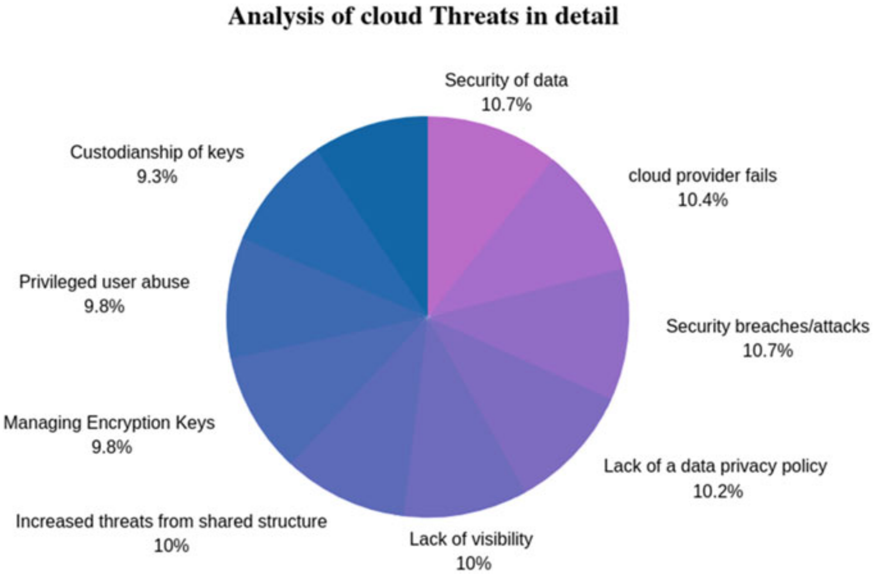

Fig. 3 Category wise cloud threats. *Data Source* International Data Corporation (2019) [33]

- There has been an increase in vulnerabilities from shared infrastructure as a cloud is the central storage for data from all resources.
- Managing encryption keys across multiple cloud environments is a significant challenge for ensuring data privacy.
- Privileged user abuse at the cloud or SaaS vendor managing, monitoring and deploying multiple cloud-native security tools.
- Lack of control over the location of data/data residency concerns meet.

3.2 *Internet of Things*

The infrastructure of smart cities is at its pace of betterment due to the increasing benefits of connected devices over networks which have made it possible to connect every device and person with each other with its own pros and cons. As already mentioned, the benefits of IoT devices have been proved by their increasing demands and smart applications in the industry from homes to offices, traffic to health, covering every aspect of an individual's life. Factors like weak web interface for asking consent of private information, lack of security structures in the devices and others leads to data threats like misuse of data, Denial of Service (DoS), man-in-the-middle attacks to name a few [36, 37]. A detailed study of security concerns of IoT devices is as follows (Fig. 4):

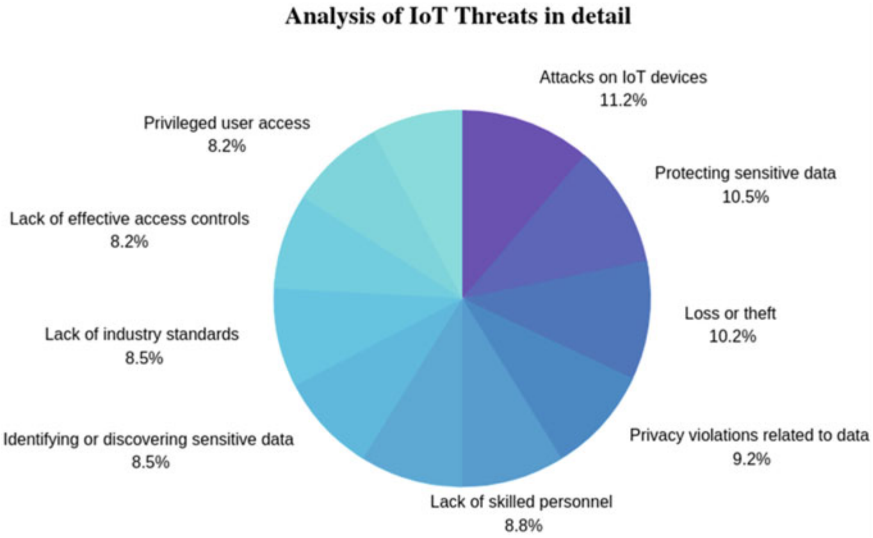

Fig. 4 Category wise IoT devices' threats. *Data Source* International Data Corporation (2019) [33]

- There are increased chances of attacks on IoT devices due to insecure interfaces of these devices which may further lead to malfunctioning of the devices and cause damage at a higher scale.
- The sensitive information generated by these devices is a rising issue of concern. The data obtained from various sensors and devices are in different formats and there needs to be standard policy and communication protocol for the interoperability of this data in the security ecosystem.
- Easily available data if combined with additional information through social media and IoT devices, all the private information about a person revealing his identity can be obtained. There is a need for validation of the integrated data before being used for any analytical purpose.
- Lack of improvised privacy policies according to rising trends in the industry regarding access control of the data, use of the data, the extent of the use of the data often attract attackers to easily penetrate into systems.
- The operational system of managing IoT devices is not as efficient as needed by the current industry. Any information that can reveal any identity-related data of an individual when identified must be protected and encrypted. The infrastructure needs to be compatible with such management of data. For this technical expertise is the need of the hour.

3.3 Big Data

The IoT devices generate a plethora of data that needs to be processed and analyzed for the implementation of public services and better management. Big data is also promoting open data initiatives for the betterment of the human community and a better future [37–39]. While big data has many business-related opportunities and applications, it proves to be a menace when data security is taken for granted. Distributed frameworks, real-time security, access controls and lack of management of a large amount of data generated often risk the data to attacks. Following are the data threats in terms of big data that need to be contemplated (Fig. 5):

- As big data processing frameworks are non-SQL, they lack security constraints like encryption of passwords and personal information before transferring among systems and are prone to attacks.
- Data anonymization techniques are not applied before performing analysis which can lead to personal identity insights after processing the data. The data which was not sensitive while entering into the system proves harmful after performing analysis over it.
- Often data anonymization techniques are weakly implemented leading to data leakages and identity thefts.
- Lack of privacy violations from data originating in multiple countries often leads to cyber-attacks from remote parts of the world.

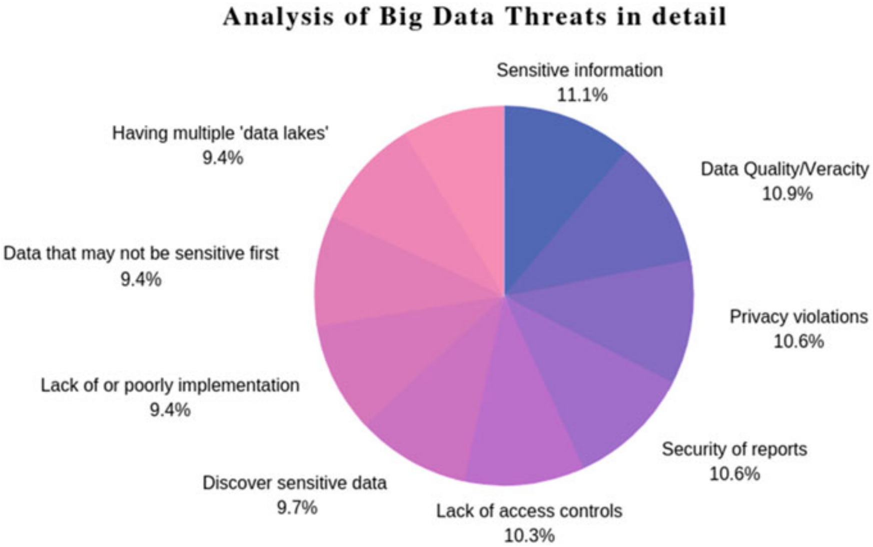

Fig. 5 Category wise big data threats. *Data Source* International Data Corporation (2019) [33]

- Security frameworks within the big data ecosystem must be compatible with the growing data risks in the industry. The system needs to be updated on a regular basis for data security concerns.
- Granular auditing is needed on a regular basis to determine the parts of the system where private information can be located.

4 Proposed Solution

Having discussed the threats faced in building a smart city architecture, in this section we shall discuss upcoming technologies which prove to be potential solutions to overcome the aforementioned issues. All these techniques can be applied on every level of the architecture in order to enhance security. These techniques help secure the data and prevent attacks like tampering, DoS, and other network threats. We can implement the below mentioned solution at every level of network security in order to prevent data thefts and secure the system. A combination of multiple solutions can provide even better security and preserve privacy of trusted user data. We propose a Naive Bayes approach to predict the possibility of threats in a specific domain given the past record of attacks.

4.1 Cryptography

Cryptography and encryption have always been the most frequently employed security technique. Encryption techniques can be deployed at each layer of infrastructure in order to build a secure environment. Cryptographic methodologies ensure confidentiality, authenticity, integrity, trust, and key management in any system [39, 40]. Popular techniques and algorithms include symmetric cryptographic encryption protocols and asymmetric cryptographic encryption protocols. Blockchain, as we shall discuss further, is an advanced technology that uses this technique for storing and securing records in blocks. With the coming of these fast-paced technologies, cryptographic solutions have gradually started declining and are deployed less in use.

4.2 Blockchain

A blockchain is a shared, distributed ledger that records transactions, agreements, and contracts. It provides a transparent and secure platform for storing and managing data. In a smart city framework, we can integrate the blockchain platform at network and database levels as blockchain itself is a distributed database. For every block that is inserted in the chain, a unique hash is assigned, making it difficult to hack and intrude the chain. Blockchain thus provides a reliable, trustworthy, efficient and scalable environment for preventing any security attack [40, 41]. Blockchains can protect the privacy within the block as every individual user has their own unique digital signature. Also, information can only be exchanged when permitted by the owner, thereby highly securing personal data. We can prevent various threats, and identification thefts using the technology.

Speaking specifically regarding the various facilities provided in a smart city, blockchain can be implemented in each individual unit. For example, in the healthcare sector, blockchain can be implemented to provide a unified platform for storing records, data authorization as well as managing data identity. In smart governance, blockchain provides efficiency, accountability, trust, and transparency [41, 42].

Blockchain is, therefore, emerging as a transitional solution to overcome security and privacy issues of the digital world.

4.3 Game Theory

Game theory provides a mathematical, reliable, distributed and defensible mechanism with a responsive action mechanism. Game theory can effectively prevent DoS, eavesdropping, and cyber-physical security attacks using static techniques such as a static zero-sum game, Stackleberg game, Bayesian game, etc. The classic privacy protection algorithms have as well incorporated game theory. With the growing pace of smart cities, it can be rightly concluded that game theory will play a significant role in protecting data privacy in the near future [42, 43].

4.4 Machine Learning and Data Science

Structured and unstructured data has always been a driving force in a smart city. However, data is processed and filtered, i.e. converted into smart data before drawing insights from them. But even with the growing smart data, the risk of data attacks has grown exponentially as compared to the last few decades. Machine learning and data science work hand-in-hand with big data and can be used as tools to protect and secure our system. Various machine learning algorithms can be used in order to train models that can predict future threats encountered in a smart city [43–46].

To understand the concept in detail, let's consider a simple scenario. Within a smart city, hundreds of breaches are attempted each day which may harm the data integrity of the system. The cyber security cell of each smart city can record every detail of the breach in terms of the type of attack, the domain (home, transport, business, etc.) along with the losses incurred. Through a thorough investigation, we can also identify the particular attack that has occurred. This database can be fed to a probabilistic model to predict the future chances of any such attack. We refer to Naïve Bayes Classifier (a probabilistic machine learning model) in this example. Explaining it mathematically, in the Naïve Bayes classifier, we calculate the posterior probability, given the likelihood, prior probability, and evidence.

$$posterior = \frac{prior \times likelihood}{evidence} \tag{1}$$

If A and B are two events, posterior represents the probability of occurrence of A given event B has occurred (P (A|B)). Prior probability represents an occurrence of B given event A has already occurred (P (B|A)). Likelihood and evidence represent P (A) and P (B) respectively. Thus,

$$P(B) = \frac{P(B|A) \times P(A)}{P(B)} \tag{2}$$

Coming back to smart city, if we're given the following dataset, we can determine the probability of threat using the above-mentioned technique. From the data represented in Table 2, we can calculate the probability of a data tampering theft on a smart transportation environment as:

Table 2 Sample dataset of threats in a smart home

Domain	Attack type
Transportation	• DDoS • Data tampering • Device hijacking • Sibil • Data tampering
Home	• Data tampering
Governance	• Cloud theft • Identity theft
Healthcare	• Data tampering • Data manipulation

$$P(Data\,Tampering|Transportation) = \frac{P(Transportation|Data\,Tampering) \times P(Data\,Tampering)}{P(Transportation)} \tag{3}$$

$$= \frac{P(Transportation\ Data\,Tampering) \times P(Data\,Tampering)}{P(Transportation)}$$
$$= \frac{0.2 \times 0.4}{0.5} \tag{4}$$

$$P(Data\,Tampering|Transportation) = 0.16 \tag{5}$$

Thus, we may conclude that there could be a 16% chance within this small dataset itself for a possibility of data tampering in smart transportation. If we scale the dataset we can come up with more such insights.

Taking this a step ahead, we can also calculate approximate revenue losses that could incur and take steps well in advance. A possible solution could be implementing a blockchain that will secure the data and prevent the attack so as to minimize revenue as well as other losses.

Machine learning and data science can find many more such applications in order to provide a safe and secure environment (Fig. 6).

5 Review of Smart Cities

As mentioned above, smart buildings, smart mobility, smart energy infrastructure, and smart water meters form the basis of the people in the city to live efficiently. Smart city initiatives are being taken by many of the advanced cities in the world to cope with the challenges faced by their respective citizens with the best use of

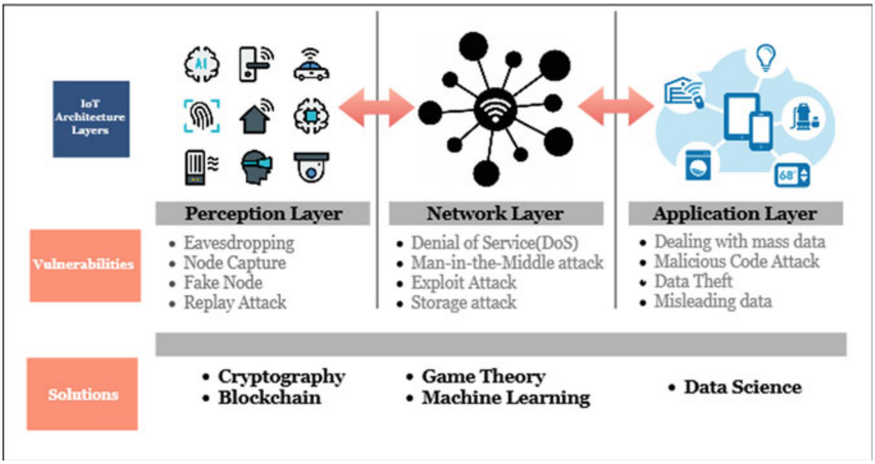

Fig. 6 The landscape of vulnerabilities and solutions. *Data Source* [10, 24]

digital technologies. Following is the review of the example smart cities which are renowned for their best solutions:

- **Smart Buildings**

A smart building refers to a block that is built with innovative ways by taking into account energy and material efficiency, comfort and well being of people thus maximizing productivity with minimizing resource requirements [46, 47]. One of the examples of such smart buildings is Software Development Block 1 (SDB 1), Infosys campus at Pocharam in Hyderabad, India. The key characteristics of this building are water efficiency, energy efficiency, and day lighting management. The building consists of 18% recycled material. 100% water recycling strategies and 90% natural day-light arrangements are used to reduce the overall maintenance cost. This building has also adopted radiant cooling technologies, thus, reducing 50% of its total energy requirements. Several data mining and machine learning algorithms are used to study the temperature and patterns of air conditions in the building to predict the needs in the future. This helps in efficient energy management of the building. SDB has proved the importance of merging towards innovative ways to build infrastructure than the traditional ways to achieve sustainability.

- **Smart Mobility**

Mobility is a wide term including all the means of the mobility of an individual including but not restricted to private cars, bikes, and public buses. Mobility has been an issue of concern for many of the smart cities and there are a few examples of it in terms of pacing technologies. The efficiency and quality of public buses have been improved through Bus Rapid Transit (BRT) and is being used successfully in 197 countries across the world. Argentina, Chile, Columbia, Brazil, Ecuador, Mexico and Uruguay have adopted bicycle-sharing transport systems with a vast lane network for bicycles. Mobile applications have proven themselves very important in the successful implementation of this information. Mobile applications for bike sharing systems, efficient parking and electric charging stations are the next targets for these cities [47, 48]. This has contributed to saving 232 tons of carbon dioxide emissions in its few years of beginning. Car sharing, popularly known as ZipCar is another concept that is gaining importance nowadays in Europe and the USA. Each ZipCar reduces around 15 cars in a city which ultimately leads towards environment sustenance [48, 49].

- **Smart Water Meters**

Water meters are the need of the hour for planning controlled use of water. Smart meters aim at scalable and low-cost water management solutions. With a smart meter for water, a user can keep a track of water consumption, water loss and water leakage in order to efficiently predict the need of water in his/her house in a day [50]. The most recent and live example of smart water meters is in Mumbai, India, which are controlled remotely. With smart water meters, 50% of water leakage losses have been reduced which accounts for 16% more water savings as compared to the global average of reduced water loss [49, 51].

- **Smart Waste Management**

Smart waste management helps to efficiently manage waste disposal, its reuse and recycling, thereby contributing to the nation’s economy. Santander, a smart city in Spain is well known for its smart waste collection strategies. GPS connected vans are used for the collection of waste bins and are optimized using optimal routing networks. This has covered the issue of visiting empty bins and overflowing bins. This leads to reduced emission of carbon dioxide and transport loads for the collection of waste [50, 52].

- **Smart Healthcare**

Every country tries to improve the quality of its healthcare services as the citizens are the country’s biggest asset. India has initiated the “Smart Health India” campaign to reach out to every corner of the country for quality health services at low prices for general chronic diseases. In Singapore, digital technologies are widely used for such monitoring. The technologies are developed with a patient-centered approach ensuring the ease and services required by the people. The daily lives of people are monitored by sensors in the environment and sent automatically to service providers which record and update the status of a person’s health. Basic details like pulse rate, blood pressure, etc. are forwarded to providers and can be visible over smart devices such as phones, and fit bands. The healthcare network is planned to be centralized to avoid duplication of services and for immediate actions depending upon the nature of the disease [51, 53].

6 Discussions

The issues, solutions and review of a few smart cities opens up many opportunities and scopes for open research. We arrive at opportunities to overcome the barrier and threats posed over the privacy and security of user sensitive data. We arrive at a few important questions as to what causes such threats to the data. Is it companies minting money, or the carelessness for security by agencies which lead to the breach in data. With advancements in technology, the world is even advancing in building techniques to break into the system and mishandle data. We aim towards creating systems in the city which make it hard to access data where-so-ever it is being accessed from. We are ourselves responsible for our data security and privacy. We should agree and allow use of the data which we feel would not harm our identity, personal security, and monetary benefits. Open research opportunities to overcome these challenges are discussed in the next section.

7 Future Research Directions

The above-reviewed analysis of the smart cultures adopted in a city prompts every emerging smart city to adopt technologically advanced and up-to-date solutions. Sharma and Park [52, 54] propose a smart city architecture based on the blockchain through which we can decentralize various domains at a city level wherein each domain forms a new block. Smart homes, hospitals, offices, and buildings can altogether form independent entities but on a larger scale are integrated into the smart city chain. At the bottommost level, we can aim to centralize and create a database that can store details of every minute activity within the framework. For example, say, data from smart meters can analyze and calculate both water as well as energy consumption patterns, smart televisions, smart plugs, smart geysers, sensors, and various smart appliances can be collected over regular intervals over a single platform which later forms a single entity, that is, a smart home. Similar cases can be followed and implemented for other domains. Using this architecture, users can identify a single platform through which they can make bill payments, monitor and record all the expenses and pay taxes as well. Such a smart city based architecture will benefit the citizens and government agencies.

With the aim to minimize security and privacy threats in a smart environment, we can emerge with custom solutions that merge multiple proposed solutions such as applying different cryptographic techniques along with game theory in order to enhance privacy. Wide machine learning models can be trained which can on an early basis identify breaches and threat possibilities so as to take preventive measures in advance.

8 Conclusions

Through the course of this chapter, we bring across the concept of a smart city, the features it inhibits and the vulnerabilities it is exposed to. From IoT, through cloud computing, big data, we have touched on various security threats that could possibly be faced in a smart city. Knowing all the threats, we elaborate on possible solutions using which we can eliminate and overcome them. We have demonstrated a simple machine learning algorithm that can possibly determine the probability of future threats in order to reduce revenue losses. Review studies of a few smart cities have been elaborated and touched upon which is followed by future research directions. We end the chapter by proposing a layered architecture solution with attack and prevention schemes.

References

1. Solanki, V.K., Katiyar, S., Bhashkar Semwal, V., Dewan, P., Venkatasen, M., Dey, N.: Advanced automated module for smart and secure city. Procedia Comput. Sci. **78**(C), 367–374 (2016)
2. Al-Hader, M., Rodzi, A.: The smart city infrastructure development & monitoring. Theoret. Empir. Res. Urban Manag. **4**(11), 87–94 (2009)
3. Poland, M.P., Nugent, C.D., Wang, H., Chen, L.: Smart home research: projects and issues. Int. J. Ambient Comput. Intell. **1**(4), 32–45 (2009)
4. Belgith, A., Obaidat, M.S.: Wireless sensor networks applications to smart homes and cities. In: Smart Cities and Homes. Key Enabling Technologies, pp. 17–40 (2016). https://doi.org/10.1016/B978-0-12-803454-5.00002-X
5. Al-Azzam, M.K., Alazzam, M.B.: Smart city and smart-health framework, challenges and opportunities. Int. J. Adv. Comput. Sci. Appl. **10**(2), 171–176 (2019). https://doi.org/10.14569/IJACSA.2019.0100223
6. Eken, C., Eken, H.: Security threats and recommendation in IoT healthcare. In: Proceedings of the 9th EUROSIM & the 57th SIMS 374 (2016). https://doi.org/10.3384/ecp17142369
7. Arce-Ruiz, R., Baucells, N., Moreno, A.C.: Smart mobility in smart cities. In: XII Congreso de Ingeniería del Transporte (2016). https://doi.org/10.4995/CIT2016.2016.3485
8. Lytras, M.D., Visvizi, A.: Who uses smart city services and what to make of it: toward interdisciplinary smart cities research. Sustainability **2018**(10), 1998 (2018). https://doi.org/10.3390/su10061998
9. Noura, H., Znaidi, W.: Security of cooperative intelligent transport systems: standards, threats analysis and cryptographic countermeasures. Electronics **4** (2015). https://doi.org/10.3390/electronics4030380
10. Delcroix, G.: Smart cities and innovative uses for personal data: scenarios for using data to restore the balance between public and private spheres. In: Special Issue 17 | 2017: Artificial Intelligence and Robotics in the City, pp. 75–79 (2017)
11. Lom, M., Přibyl, O., Svítek, M.: Industry 4.0 as a part of smart cities (2016). https://doi.org/10.1109/SCSP.2016.7501015
12. Pereira, G., Parycek, P., Falco, E., Kleinhans, R.: Smart governance in the context of smart cities: a literature review. Inf. Polity **23**, 1–20 (2018). https://doi.org/10.3233/IP-170067
13. Kumar, T.M.V., Dahiya, B.: Smart economy in smart cities (2017). https://doi.org/10.1007/978-981-10-1610-3_1
14. Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., Baldini, G.: Security and privacy issues for an IoT based smart home. In: 40th International Convention on Information

and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1292–1297 (2017)

15. Ragupathy, S., Thirugnanam, M.: IoT in Healthcare: Breaching Security Issues. IGI Global (2017)
16. Hussein, S.M., Donahoo, M.J., Cerny, T.: Security challenges in smart city applications. In: International Conference Security and Management SAM'18, pp. 306–310 (2018)
17. Kumar, B.: Data security and privacy management; addressing meticulous crime strategies in smart cities. Int. J. Adv. Technol. **10**(1) (2019). https://doi.org/10.4172/0976-4860.1000223
18. Ijaz, S., Shah, M.A., Khan, A., Ahmed, M.: Smart cities: a survey on security concerns. Int. J. Adv. Comput. Sci. Appl. (IJACSA) **7**(2), 612–625 (2016)
19. Tuptuk, N., Hailes, S.: Security of smart manufacturing systems. J. Manuf. Syst. **47**, 93–106 (2018). https://doi.org/10.1016/j.jmsy.2018.04.007
20. Spremić, M.: Cyber security challenges in digital economy. In: Proceedings of the World Congress on Engineering 2018, vol. I (2018)
21. Sethi, M.: Smart cities in India: challenges and possibilities to attain sustainable urbanisation. Nagarlok—J. Indian Inst. Public Adm. (2015)
22. Edwards, L.: Privacy, security and data protection in smart cities: a critical EU law perspective (2015). https://doi.org/10.5281/zenodo.34501
23. World Bank staff estimates using the World Bank's total population and age/sex distributions of the United Nations Population Division' Vs World Population Prospects: 2019 Revision. https://data.worldbank.org
24. Walia, N., Grover, A.: Big data in smart cities (2015)
25. Cui, L., Xie, G., Qu, Y., Gao, L., Yang, Y.: Security and privacy in smart cities: challenges and opportunities. In: IEEE Access: Practical Applications, Open Solutions, vol. 6, pp. 46134–591 46145 (2018). https://doi.org/10.1109/ACCESS.2018.2853985
26. Fuster, G.G., Scherrer, A.: Big data and smart devices and their impact on privacy (2015)
27. Wu, L., Wang, J., Kumar, N., He, D.: Secure public data auditing scheme for cloud storage in smart city. Pers. Ubiquitous Comput. **21** (2017). https://doi.org/10.1007/s00779-017-1048-7
28. Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., Shen, X.: Security and privacy in smart city applications: challenges and solutions. IEEE Commun. Mag. **55**, 122–129 (2017). https://doi.org/10.1109/MCOM.2017.1600267CM
29. Huang, Q., Wang, L., Yang, Y.: Secure and privacy-preserving data sharing and collaboration in mobile healthcare social networks of smart cities. Secur. Commun. Netw. **2017**, 1–12 (2017). https://doi.org/10.1155/2017/6426495
30. Hashem, I., Chang, V., Anuar, N.S.A., Yaqoob, I., Gani, A., Ahmed, E., Chiroma, H.: The role of big data in smart city. Int. J. Inf.Manag. **36** (2016). https://doi.org/10.1016/j.ijinfomgt.2016.05.002
31. Kido, H., Yanagisawa, Y., Satoh, T.: An anonymous communication technique using dummies for location-based services. In: Proceedings of the International Conference on Pervasive Services 2005, ICPS'05, pp. 88–97 (2005)
32. Qu, Y., Nosouhi, M.R., Cui, L., Yu, S.: Privacy preservation in smart cities. In: Smart Cities Cybersecurity and Privacy, 1st edn., pp. 75–88 (2019). https://doi.org/10.1016/B978-0-12-815032-0.00006-8
33. Thales Data Threat Report Survey (2019) IDC. https://go.thalesesecurity.com/rs/480-LWA-970/images/2019-Thales-Data-Threat-Report-European-Edition-A4-ar.pdf
34. Dey, N., Hassanien, A.E., Bhatt, C., Ashour, A., Satapathy, S.C. (eds.): Internet of things and big data analytics toward next-generation intelligence, pp. 3–549. Springer, Berlin (2018)
35. Sarkar, M., Banerjee, S., Badr, Y., Sangaiah, A.K.: Configuring a trusted cloud service model for smart city exploration using hybrid intelligence. Int. J. Ambient Comput. Intell. **8**(3), 1–21 (2017)
36. Aldairi, A., Tawalbeh, L.: Cyber security attacks on smart cities and associated mobile technologies. Procedia Comput. Sci. **109**, 1086–1091 (2017). https://doi.org/10.1016/j.procs.2017.05.391

37. Mohammed, H., Qayyum, M.: Internet of things: a study on security and privacy threats (2017). https://doi.org/10.1109/Anti-Cybercrime.2017.7905270
38. Dey, N., Tamane, S. (eds.): Big data analytics for smart and connected cities. IGI Global (2018)
39. Pal, D., Triyason, T., Padungweang, P.:Big data in smart-cities: current research and challenges. **6**, 351-360. https://doi.org/10.11591/ijeei.v6i1.543
40. Zeadally, S., Das, A.K., Sklavos, N.: Cryptographic technologies and protocol standards for internet of things. Internet of Things 100075 (2019). https://doi.org/10.1016/j.iot.2019.100075
41. Biswas, K., Muthukkumarasamy, V.: Securing smart cities using blockchain technology. In: 2016 IEEE 18th International Conference on 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). https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198
42. Theodorou, S., Sklavos, N.: Blockchain-based security and privacy in smart cities. In: Smart Cities Cybersecurity and Privacy, 1st edn., pp. 21–37 (2019)
43. Cuong, D., Tran, N., Hong, C.S., Kamhoua, C., Kwiat, K., Blasch, E., Ren, S., Pissinou, N., Iyengar, S.: Game theory for cyber security and privacy. ACM Comput. Surv. 50, 1–37 (2017). https://doi.org/10.1145/3057268
44. Mohapatra, B.: Machine learning applications to smart city. ACCENTS Trans. Image Process. Comput. Vis. 5, 1–6 (2019). https://doi.org/10.19101/TIPCV.2018.412004
45. Fong, S., Li, J., Song, W., Tian, Y., Wong, R.K., Dey, N.: Predicting unusual energy consumption events from smart home sensor network by data stream mining with misclassified recall. J. Ambient Intell. Humaniz. Comput. **9**(4), 1197–1221 (2018)
46. Dey, N., Fong, S., Song, W., Cho, K.: Forecasting energy consumption from smart home sensor network by deep learning. In: International Conference on Smart Trends for Information Technology and Computer Communications, Aug 2017, pp. 255–265. Springer, Singapore (2017)
47. Stamatescu, G., Stamatescu, I., Arghira, N., Fagarasan, I.: Data-driven modelling of smart building ventilation subsystem. J. Sens. **2019** (2019). https://doi.org/10.1155/2019/3572019
48. Jirón, P.: Sustainable urban mobility in Latin America and the Caribbean (2013)
49. Pop,M., Proștean,O.: A comparison between smart city approaches in road traffic management. Procedia Soc. Behav. Sci. **238**, 29–36 (2018). https://doi.org/10.1016/j.sbspro.2018.03.004
50. Mudumbe, M., Abu-Mahfouz, A.: Smart water meter system for user-centric consumption measurement. In: The IEEE 13th International Conference on Industrial Informatics (INDIN) (2015). https://doi.org/10.1109/INDIN.2015.7281870
51. Bayo, J.G.: International Case Studies of Smart Cities Santander, Spain. IDB-Inter-American Development Bank (2016)
52. Chidepatil, A., Bindra, P., Kulkarni, D., Qazi, M., Kshirsagar, M, Sankaran, K.: From trash to cash: how blockchain and multi-sensor-driven artificial intelligence can transform circular economy of plastic waste? Adm. Sci. **10**(2), 23 (2020) https://doi.org/10.3390/admsci10020023. https://www.mdpi.com/2076-3387/10/2/23
53. How, C.H., Fock, K.M.: Healthcare in Singapore: the present and future. Singapore Med. J. **55**(3), 126–127 (2014 Mar). https://doi.org/10.11622/smedj.2014027
54. Sharma, P.K., Park, J.H.: Blockchain based hybrid network architecture for the smart city. Future Gener. Comput. Syst. **2018** (2018). https://doi.org/10.1016/j.future.2018.04.060