Developing Secure Smart Cities: Overviews and Challenges

Purnima Ahirao
K J Somaiya College of Engineering
Vidyavihar, Mumbai

Priya Gadgil
ConnectWise LLC
Mumbai, India

ABSTRACT
Smart city, cloud, IoT are some buzzwords in recent times. Study shows that more than two billion connected things are deployed in the smart cities across the world. But such a vast number also exposes these systems to vulnerabilities that can be exploited by hackers and other malicious actors. The smart city offers technology where service providers use various ICT (Information and communication technologies) to create more effective urban organizations that can improve the quality of human life. The emerging IoT based architecture is the foundation of a smart city. IoT enabled sensors, networks, and interfaces also make vulnerability window wider. This paper explores current challenges considering the characteristics of smart city, threat vectors that can lead systems in the fatal situation and the security approach that can be considered while building smart cities.

General Terms
Smart City, IoT, ICT, Networks

Keywords
Cybersecurity, Security of smart city, IoT-cyber security, Data security

1. INTRODUCTION
A smart city is a combined framework of several information and communication technologies to develop, innovate and deploy urbanization practices. Smart city is an integrated technology environment where data is collected (usually via sensors), and the system is configured to make decisions based on the data collected. For example, data collected from various cars via smart sensors are used to decide the traffic conditions on the road. The very famous example is Google Map. So it is essentially a smart network of connected objects and machines that transfer/share the data using some wireless technology, which is stored on a cloud. Such storage applications then receive, analyses, store and manage data in real-time. All this combined environment is known as Smart-City ecosystem. Various surveys predicted that approximately 66 per cent of the world's population would live in an urban environment by 2050 [1]. This shall create an excessive burden on living conditions. This paper gives a detailed synopsis of smart city and security challenges regarding the smart city. [9] Urbanization is a global trend and India is not an exception. Many research shows that today nearly 40% of the population stays in the city. With this, the advancement of the smart city is growing at a fast pace. Smart city leverages technology and provides a higher quality of life.

The paper also describes possible security controls which can be implemented while developing a smart city or using IoT technologies.

2. IOT ARCHITECTURE OF SMART CITIES
From the starting phase of the smart city era, various architectures, frameworks have been proposed, developed and designed [2]. Though, there is no standard model for the smart city. As this work is about having an overview of security challenges of smart city, the architecture described is generally accepted layered architecture [3].

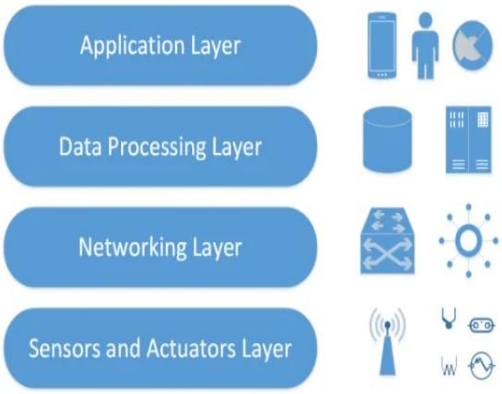

Fig 1: Smart City-Layered Architecture

A. Sensing Layer/Data Collection layer
As shown in figure 1, the IoT application development is distributed over different layers. The first layer is a sensing layer, which is the lowest layer of the architecture. Rather the work begins with data collection at this stage. This layer mainly considered as a data collection or data pool layer. Data gets collected from various heterogeneous devices, i.e. real-time sensors, actuators etc. After acquiring the required information, it is then sent to the next layer for analysis.

B. Network Layer
This is the key layer in the IoT architecture of a smart city. The main objective of this layer is to collect all the data through various devices and send it to the next layer and connecting smart devices, network devices, servers etc. This layer acts as a link between sensors (who collect the data from various devices) and the cloud bases applications which generally process all this data to make the decisions.

C. Support Layer
This layer works closely with the last layer, that is the application layer. It supports the requirement for the differentiated application using smart computing techniques that is cloud computing. Various compatibility technologies are used in this layer.

D. Application Layer

This is the final layer which is responsible for delivering intelligent services, applications and facilities to users based on their data analysis and customized application configurations.

3. CHARACTERISTICS OF SMART CITY

A. Heterogeneity

There is no standard or universally accepted definition for smart city as it's a combination of different platforms and ICT technologies. IoT architecture varies from city to city. This is an important characteristic of a smart city, i.e. Heterogeneity, i.e. Combination of different technologies. But this can sometimes lead to undefined consequences. The absence of a common security structure/ standard and service is one of the challenges Smart city is facing these days.

B. Resource Limitations

Majority of IoT devices are resource constraint which means they have limited storage, memory, low battery life and processing capacity. This poses a challenge in the design and development of Smart city. Methods and solutions have to be worked upon before using these devices for development.

C. Connectivity and scalability

Connectivity enables one device to connect with the other, and this leads to form a network of a connected device. The smart city is nothing but systems which work based on synchronization between such networks. Smart cities are rapidly growing today; therefore, there is a considerable increase in both data as well as network traffic. Thus, for the successful implementation of smart city, it is crucial to building network keeping scalability in consideration.

D. Mobility

Mobility has been an important factor impacting the growth of modern cities. Mobility here does not refer to the movement of goods from one place to another. In the context of smart cities, it means technologies like city-wide wireless communication, real-time monitoring of traffic flow etc.

4. BROAD OVERVIEW ON SECURITY CHALLENGES IN SMART CITY

Many research article highlight different security challenges about smart city. Some researchers [4] present a comprehensive survey of security and privacy challenges. This paper also describes a classification of security and privacy issues of smart cities to highlight the need for designing a smart, secure city, identify the existing Security and privacy solutions. Authors [5] showcases the approach to detect data leakage caused intentionally or unintentionally considering the smart city architecture. This study helps us in gathering and highlighting the prominent issues and probable solution. This study also helps us in today's age, when any organization need to consider the data protection of any data they are collecting.

A. Infrastructure

A smart city uses different types of sensors to analyze and manage the data. There is a wide range of information these sensors carry for example rush hour statistics, air quality etc.

Complicated and sometimes economically not feasible infrastructure is involved in installing and maintaining these sensors. We have challenges ranges from wiring, steam pipes, installing high-speed internets. Managing and maintaining such embedded infrastructure creates a challenge.

B. Security and Hackers

This is one of the critical challenges smart city is facing these days. While developing any smart city, it has become necessary to take into consideration information security/cybersecurity challenges any smart city might face.

C. Privacy concerns

When we think about the smart city, there is always a tradeoff between smart life and privacy concerns. It means people want to live a healthy, connected and smart life, but at the same time, nobody wishes to continue being monitored. For example, cameras installed on the street can help in detecting the crime, but that can also probably put citizen's privacy in danger. Additionally, with rising compliance requirement (which usually gives individual rights to protect their personal information) it also becomes a challenge for smart city developers.

D. Convergence

Convergence is nothing but the integration of different environments. The smart city is typically integration of cyber and physical world where our physical devices are connected using cyber technologies like sensors, actuator, cloud computing etc. However, this convergence might also expose the system to ample of cyber threat vectors, malicious actors entering into the environment.

E. Interoperability

Many times, cities that make digital transformation needs to integrate new digital technologies with legacy systems. This can open significant security risks and challenges. For example, inconsistent security policies, different platforms can result in hidden Security gaps through smart city network.

F. Integration

As shown in figure 2, the city provides a large number of services that are mostly dependent on each other like power, water, and transportation, etc. In a smart city, these services are to be combined and connected through an organized web of digital technologies. The increasing integration and data exchange creates its own set of vulnerabilities.

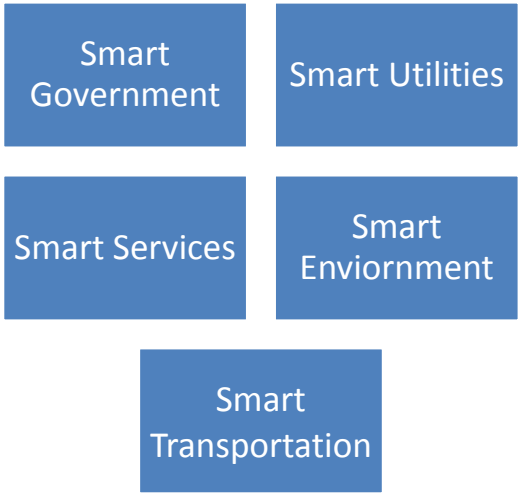

Fig 2: Typical Smart City-Components

Now let's have a look at some of the threat vectors of smart city and probable countermeasures that can help in making smart city secure.

5. POSSIBLE MEASURES FOR SECURED SMART CITY DEVELOPMENT

Table 1. Security Threat vs possible measures

Threat	Probable Countermeasures
Privacy, Identity (data) theft	Authentication, Encryption and Access control.
Device Hijacking	Device Identification and access control, Security lifecycle management
DDoS attack	Authentication, encryption, access controls, Security monitoring and log analysis, Application-level DDoS protection
Application-level DDoS attacks	Security monitoring and log analysis
Man in Middle attacks	Authentication, encryption, Security lifecycle management

As shown in Table 1, let's have a look at some of the threat vectors of smart city and its possible measures.

The developing smart city always brings the essential factor that is big data. The ample data gathered in the smart city is a stable factor, including multiple records, logs and different type of data [6]. Such data can create vital information and provide more intelligent life. However, such data can also cause various challenges of Security and Privacy. Although the progress of smart cities has improved the quality of human life, the smart and intelligent applications within the smart city make the environment more dynamic, which in turn leads the entire ecosystem more vulnerable to different kind of attacks. Research has already done on how privacy and other security aspects can be in a fatal situation and can cause a security breach [6] [7]. The study has also demonstrated the security threat to smart city considering various types of attack scenarios. All these aspects make it necessary to design a unique system that can be used in creating a Secured Smart Environment. An approach which focuses on building strong basic security measures while deploying various technologies in the smart city and provide a secure, intelligent system is an important step towards smart city development. Few such aspects are described in the section below.

A. Firmware integrity and secure boot

Firmware security is securing hardware devices at the kernel level. It lets cryptographic sign techniques which ensure that the device performs only code by OEM (Original Equipment Manufacturer) or the other trusted party.

B. Mutual Authentication

In a smart city, whenever the device connects to the network should be authenticated before sending the data. This helps in ensuring data originates from the legitimate source. With mutual authentication, two communicating agents (device and service) should prove their identity to avoid any unauthorized entry.

C. Security analysis and log monitoring

The smart city generates lots of data. It is important to collect data and the overall status of the system, including endpoint systems and generated traffic. This data then can be analyzed to detect the possible security incident. A smart city collects a lot of data. This data typically gets collected and transferred on the internet, such as any sort of cloud services/applications. The tool/solution can be developed, which shall make sure the integrity of data while transit or in rest. Which means with the help of a single comprehensive tool, we will secure data flow within the smart city.

For example, when data is collected from IoT devices and when it gets transferred within the network or when it gets transferred on the internet via the network, we will apply relevant security measures at each step like mutual authentication and data encryption.

Consider the flow of Data in a Typical Smart City.

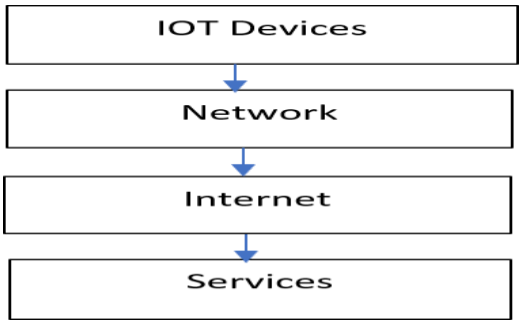

Fig 3: Data flow within Smart City Ecosystem

As shown in figure 3, between each step-in above cycle, strong mutual authentication, data encryption, and relevant security technologies shall be integrated to make the data flow more secure.

D. Security lifecycle management

Security lifecycle management allows service providers and manufacturers to control the security aspects of the devices. With the help of security lifecycle management, we can even maintain the minimum service disruptions.

6. STATISTICS AND DISCUSSIONS

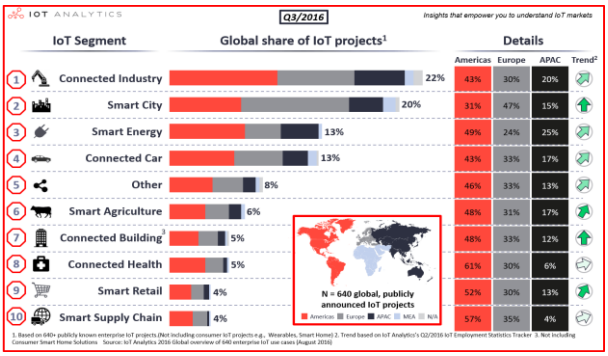

Fig. 4 Global share of IoT projects

As shown in figure 4 [14], Smart city development using IoT remains second in the list of IoT projects around the globe. Other applications like smart agriculture or smart retail can be seen securing lower positions as compared to a smart city. The report clearly states that Smart city developers are looking for IoT based solutions for their projects.

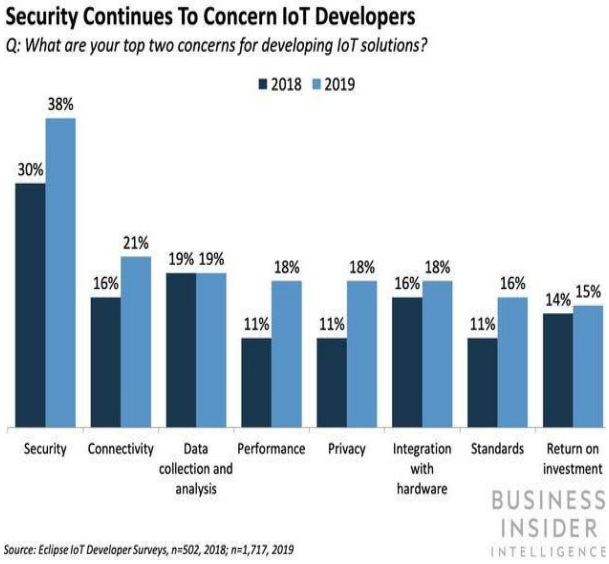

Fig 5. Security concerns of IoT developers

As shown in fig 5 [15], though the developers are expanding their horizons to fit in the benefits of IoT for smart city, the challenges and concerns they face are making it difficult to unfold all the benefits of IoT. The topmost security concern being the Security concern as the report suggests.

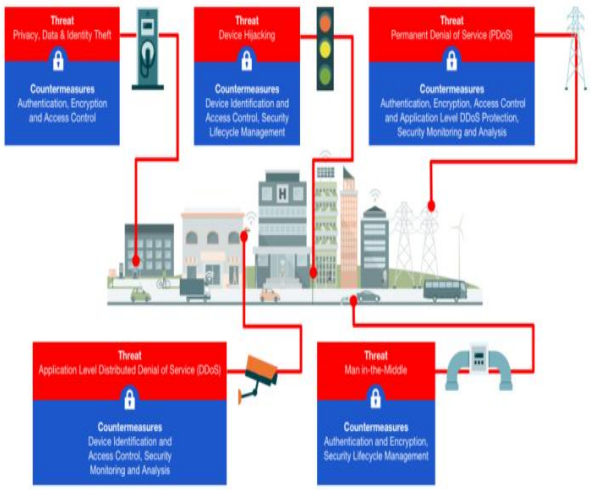

Fig 6. Countermeasures for Secured Smart city

As shown in figure 6 [16], there are some possible countermeasures such as Authentication, Encryption, Access control, packet monitoring for various potential threats to the smart city implementation. Using these suggested and essential Security features, the developers can go ahead to provide improved quality of life to the urban citizens.

7. CONCLUSION

The issues of information security in a smart city are continuously increasing, including social, economic and governance factor. As discussed above to absorb IoT potential to its full extent, the various constraints are to be handled efficiently. One of the major constraints being Security threats over the cyber landscape, the IoT stack needs to be added with a layer of Security at the top. This paper provides an overview of smart city with the context of its characteristics, challenges and possible threat vectors. The technological factors are crucial in the implementation of a smart city. Studying smart city keeping in mind the associated cybersecurity threats will help in developing a robust solution, which can benefit the society to a large extent.

8. REFERENCES

[1] Department of Economic and Social Affairs, World Urbanization Prospects: The 2014 Revision, Highlights. New York, NY, USA: United Nations Population Division, 2014.

[2] I. Yaqoob et al., ‘‘Internet of Things architecture: Recent advances, taxonomy, requirements, and open challenges,’’ IEEE Wireless Commun., vol. 24, no. 3, pp. 10–16, Jun. 2017.

[3] L. Tan and N. Wang, ``Future Internet: The Internet of Things," in Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE), vol. 5, Aug. 2010, pp. V5-376_V5-380.

[4] R. Kitchin, “The real-time city? Big data and smart urbanism,” GeoJournal, vol. 79, no. 1, pp. 1–14, 2014.

[5] Zhang, Kuan, Jianbing Ni, Kan Yang, Xiaohui Liang, Ju Ren, and Xuemin Sherman Shen. "Security and privacy in smart city applications: Challenges and solutions." IEEE Communications Magazine 55, no. 1 (2017): 122-129.

[6] R. Kitchin, ``Getting smarter about smart cities: Improving data privacy and data security," Dept. Taoiseach, Data Protection Unit, Dublin, Ireland, Tech. Rep., 2016.

[7] S. Finster and I. Baumgart, ``Privacy- aware smart metering: A survey," IEEE Commun. Surveys Tuts., vol. 16, no. 3, pp. 1732_1745, 3rd Quart., 2014.

[8] Dattana, Vishal, Kishu Gupta, and Ashwani Kush. "A Probability based Model for Big Data Security in Smart City." In 2019 4th MEC International Conference on Big Data and Smart City (ICBDSC), pp. 1-6. IEEE, 2019.

[9] Qiu, Jinglin, Xueping Liang, Sachin Shetty, and Daniel Bowden. "Towards secure and smart healthcare in smart cities using blockchain." In 2018 IEEE International Smart Cities Conference (ISC2), pp.

[10] https://gcn.com/articles/2019/12/17/sase- smart-city-security.aspx

[11] Sookhak, Mehdi, Helen Tang, and F. Richard Yu. "Security and Privacy of Smart Cities: Issues and Challenge." In 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pp. 1350-1357. IEEE, 2018.

[12] Dattana, Vishal, Kishu Gupta, and Ashwani Kush. "A Probability based Model for Big Data Security in Smart City." In 2019 4th MEC International Conference on Big Data and Smart City (ICBDSC), pp. 1-6. IEEE, 2019.

[13] Qiu, Jinglin, Xueping Liang, Sachin Shetty, and Daniel Bowden. "Towards secure and smart healthcare in smart cities using blockchain." In 2018 IEEE International Smart Cities Conference (ISC2), pp.

[14] https://iot-analytics.com/wp/wp-content/uploads/2016/08/List-of-640-IoT-projects-min.png

[15] https://discoperi.com/wp-Content/uploads/2018/11/0_gE2zniOBV4dVY-u_.png

[16] https://42xtjqm0qj0382ac91ye9exr-wpengine.netdna-ssl.com/wp-content/uploads/2017/12/Smart-City-Threats-and-Countermeasures-1024x576.png.

[17] https://www.marketsandmarkets.com/Market-Reports/iot-smart-cities-market-215714954.html

[18] https://www.visualcapitalist.com/anatomy-smart-city/