Assessing Vulnerabilities and Security Strategies in Smart Urban Areas

Sofia Petrova
Assistant Professor, Department of Computer Systems, Sofia University, Bulgaria

ABSTRACT

The smart city is a new phenomenon that has emerged in the recent times. It has evolved from innovations in ICT that, while they create new socio-economic opportunities, there are challenges to our security and expectation of privacy. Hence the cities will need to be smart. Though city life provides basic amenities to its residents, but smart city technology can bring development to businesses, environment, and houses and enhance agriculture, save energy. People are already communicating through smart phones & gadgets. The security and privacy of these automated systems within a city will play a leading role in smart cities. The security of these smart devices and systems & privacy of their data has become an important point of research in today's scenario. This paper mainly focuses on various issues and challenges related to smart city security and also suggest solutions that are helpful in making a city smart and secure in a more advanced manner.

KEYWORDS: Smart City; ICT; Information Security; Issues; Challenges

I. INTRODUCTION

The concept of a "Smart City" has attracted substantial attention in the context of urban development policies. The Internet and broadband network technologies as enablers of e-services becoming more and more essential for development of the urban areas while cities are increasingly assuming a critical role as drivers of innovation in areas such as health, government, environment and business [1].

A smart city is the recent development in city life that makes use of ICT and provides services that makes the city become more aware, efficient, and interactive. When IT meets the real world, it gives birth to something called Internet of Things (IoT). Implementing this new concept of IoT, the working of people has become more refined. We can attain better life quality by combining the society people and real world systems through the use of smart technology and IoT worldwide. It is forecasted that by 2050, 70% of the world's population—more than 6 billion people—will live in cities and their suburbs [2]. A smart city is a city which functions in a sustainable and intelligent way, by integrating all its infrastructures and services into a cohesive whole and using smart devices for monitoring and controlling, for ensuring sustainability and efficiency.

The data security and its privacy issues with respect to smart city is the most crucial part that interests the scientists and researchers. As information is the prime factor in case of basic day to day services being used in urban life, it needs to be secured. There are various issues that create hindrance to smart city security but the most important issues are related to government, social and economic factors. The researchers are trying to identify every issue concerned and propose solutions related to them. This paper mainly focuses on various issues and challenges related to smart city security and also suggest solutions that are helpful in making a city secure and smart in a more advanced manner.

II. ISSUES AND CHALLENGES

In the early 1990s the term "smart city" was proposed to signify how urban development was turning towards technological innovation and globalisation. Creating smart cities are subject to various problems during their development phase which are social, economic and political in nature. But the most important challenge is related to technology. Various issues and challenges faced while implementing smart city and making it secure are discussed here in subsequent part of the paper.

Technical Issues

As we are aware that technology plays a vital role in fulfilling all the commitments of a smart city. A smart city is depending on technology to provide better services to the government, citizens. But implementing technology has its own various issues in order to make smart city more secure. The major security issues related to smart city are seen in education sector, business sector, healthcare sector, transport sector, etc. The biggest challenge is not only to provide e-services and their management, but also to protect the data from illegal frauds, attacks. Thus these attacks can be a major problem in implementing the smart city services in a city. [3]. The data

security within smart city can be improved by incorporating various technical changes like RFID tags, smart grids, smart phones, machine to machine communication, biometrics to name a few. They have their own technological issues that need to be sorted for a secure smart city.

Various sectors of smart city like environment, industry ,transportation, etc. use radio frequency identification (RFID) tags enormously but it is also open to many security threats which leads to problems like denial of Service, jamming, communication threats, privacy issues, signal interference tag cloning, etc. Usage of these tags tends to leak sensitive data through unauthorized access.

In the Smart Cities, nowadays smartphone apps are quite popular on which major smart city services depend. But using these apps has their own risk factors. Every smartphone has unique identifiers that can be accessed and shared by apps, some of which can be captured externally via Wi-Fi or Bluetooth signal. Using these identifiers by hackers, phones can be easily traced and further become more vulnerable to malicious attacks [4].

The Machine to machine communication is making smart city real time in terms of applications and services offered to citizens [5]. These M2M protocols are being used for communicating at least two nodes of a network. Data privacy is a basic human right of every smart city resident. But maintaining data privacy can be very difficult in case of M2M communications. The major issues mostly seen in case of M2M communication are eavesdropping, privacy breaches, malicious software updates, DoS, network security threats like traffic tunneling etc.

In order to implement and manage energy, smart grids are created in a smart city. When we require communicating data in real time smart grid gadgets are used which are mainly the communicating sensors. Data is more prone to attacks and threats, which can be the major cause of the system failure when communicated in real time between power generators and service providers.

Governance Issues

There are various issues in sectors like health care, transportation, education, business, etc. When government implements technology in a smart city, they face major issue that government authorities mainly focus on testing the functionality rather than concerning about privacy and security of the data. We should take care of various threats related to IoT and smart grids technologies. Also there is big data related to critical systems that can create big problems in terms of data integrity and resilience Hence it is the responsibility of these critical systems to preserve the data integrity, resilience and security in a smart city. Services in smart city are more dependent on smart phones and data in mobile is more prone to attacks and threats as they can be hacked by the hackers easily.

In order to manage distributed energy efficiently by the users, it is more dependent on smart grids which use bidirectional communication. Data security and privacy are by far the topmost concerns for the users while adopting smart grid method. Proper methods should be taken to prevent energy and utilities from malicious attacks and threats.

Socio-Economic Issues

Assistance and personal management provided to people in smart cities are taken care by means of technology which is a basis of urban planning and resource management [3]; hence the smart cities are changed into a system of single stop service. With this service, the city is assured of more efficient services and offers smart city citizens with smarter economic growth, improved banking, business, and finance activities. The various issues in making a city smart are banking, personal identity, communication and finance. All of these mentioned issues are also vulnerable to privacy and protection of data of a smart city.

Telecommunication division is subset of smart city services set which is more susceptible to malevolent attacks, viruses, frauds and privacy issues. The need to have a more secured and authentic channel increases even more as various governmental activities use telecommunication sector and wireless networks. Besides, Machine to machine communications also helps to provide services to smart city people. Hence the protection issues related to machine to machine communications has to be considered. With the utility of smart gadgets as an upgraded communication media among the people of a smart city, these results in more new protection issues in a smart city. As more and more people are getting attached with technology, they are more vulnerable to malicious threats. As we see all ICT technologies are being required in smart data communication but the protection issues must be take care while giving smart solutions to these threats.

Every individual person has the fundamental right to privacy in a smart city. Every individual person of a smart city uses variety of services & latest technology to for communication with each other. These latest technologies that form of heterogeneous systems are the major target areas for hackers who wish to intervene into the people's data and personal area, depriving them from their personal right. The social networking websites and its related data play an important role and should be considered with respect to information security and data privacy. The privacy issues related to social networking depends upon the individual. These social networking providers and apps who promise to keep user's identities safely at times tend to provide sufficient data to identify the individual's profile.

The sectors that become the main pillars of smart economy in a smart city are finance; banking & business. Although smart cities helps to expedite the economic growth, and provides better banking, better business opportunities and services, yet this sector of smart city is most susceptible to security threats and could be attacked for personal financial use. The target of hackers is to damage the city or an organization's economy.

III. SOLUTION FOR SECURE SMART CITY

In order to provide enhanced security services in a smart city that it is main to discuss different methods that can be incorporated. Each and every citizen has the need and the right for more secured city which needs to be catered seriously for building an effective smart city. Following general solutions are suggested here related to governance, socio-economic and technological issues related to smart city:

- In case of security testing requirements, awareness among the authorities is required so that they understand the need of checking the security issues.
- The critical infrastructure in a smart city needs to be protected from various threats and attacks that may cause major harm to the promised services. Critical smart city infrastructure should have secure encrypted systems for proper storage, management and protection of the data from frauds and threats.
- The optimized utilization of ICT technologies is the best solution for the problems in smart mobility security & privacy domain.
- To resolve security issues in smart grids we generally use public key infrastructure (PKI) or managed PKI.
- Various techniques that may provide enhanced security services of RFID in a smart city are relabeling, re-encryption and minimalist cryptography. Other techniques include tag sleeping, tag blocking and selective blocking [3].
- Methods that can be used to omit interference issue in the RFID system are data integrity check, multiple re-transmission and data coding.
- By ensuring the integrity of meter data and maintaining meter securely in smart grid can be the possible solution to ensure security of devices.
- Anti-viruses, firewalls, secure API, Authentication and access control and SPAM filters can be major solutions to threats and attacks to smart phones.
- The solution suggested for M2M communication is the use of IEEE Standards Solutions that talks about characteristics like creating time slots in real time quality using; CSMA-CD technology, secure communication with merged assistance.

IV. CONCLUSION

A smart city comprises of various security issues related to governance, economic, technical, or social factors. This paper gives a complete overview on the smart security related threats, vulnerabilities and suggests some valuable solutions that simplify the problem areas of smart city security. It is quite clear that security has always been the weakest link in smart city implementation. The features and services assured by a smart city will be destroyed because of flawed security. If there is ambiguity in the security system, it will disrupt the functionality of the smart solutions. Hence in order to resolve the security issues related to smart city, various solutions have been suggested which if implemented, will lead to a secure smart city.

V. REFERENCES

[1] Schaffers H., Komninos N., Pallot M., Trousse B., Nilsson M., Oliveira A. "Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation." In: Domingue J. et al. (eds) The Future Internet. FIA 2011. Lecture Notes in Computer Science, vol 6656. Springer, Berlin, Heidelberg.

[2] C. Chang, C. Cheng Lo, "Planning and Implementing a Smart City in Taiwan", IEEE Computer Society, August 2016.

[3] S. Ijaz, M. A. Shah, A. Khan, M. Ahmed, “Smart Cities: A Survey on Security Concerns”, International Journal of Advanced Computer Science and Applications, Vol. 7, No. 2, 2016.
[4] http://www.govtech.com/Security-Privacy-Governance-Concerns-About-Smart-City-Technologies-Grow.html
[5] J. Wan, D. Li, C. Zou, and K. Zhou, “M2m communications for smart city: An event-based architecture,” in Computer and Information Technology (CIT), 2012 IEEE 12th International Conference on. IEEE, 2012, pp. 895–900.