Framework for Managing Smart Cities Security and Privacy Applications

Modafar Ati
College of Engineering
Abu Dhabi University
Abu Dhabi, United Arab Emirates
Modafar.ati@adu.ac.ae

Tasnim Basmaji
College of Engineering
Abu Dhabi University
Abu Dhabi, United Arab Emirates
1052846@students.adu.ac.ae

Abstract— **The enormously growing population in urban areas and the impact it has on the urban environment escalates the need of sophisticated management approaches that acquire the latest advancements of ICT, IoT and AI to enhance every city offered service. A smart city is capable of monitoring the physical world in real time and gathering city and citizens related data, then processing and analyzing this data in order to control city facilities and influence the life of citizens. The emerging of such technologies in cities raises multiple security and privacy concerns and challenges at individual and community levels. Several attempts have been introduced to guarantee the security and privacy of sensed data. In this paper we examine the security and privacy of smart city applications, the challenges faced and the solutions proposed. We first introduce smart cities and we provide an overview of major security problems and current solutions in some categories of smart cities. We then investigate the security challenges related to both city infrastructure and data, and we propose a framework to overcome these challenges.**

Keywords—ICT; IoT; AI; security; privacy; smart city; SCSMS

I. Introduction

Cities can be defined as complex and highly organized human settlements that have extensive servicing systems for housing, power and water supplement, transportation, sanitation, land use, utilities and communication. These systems are responsible for facilitating interaction between people, government, organizations and business owners. Historically, cities were inhabited by a small proportion of humanity overall. Statistics showed that about 30 percent of the world's population lived in cites in 1950. However, half of the world's population is said to live in cities nowadays where the number shot up to nearly 55 percent in 2016. By 2030, 60 percent of the world's population is expected to live in cities[1]. The rapid growth in size of residents generates a wide range of challenges including air pollution, traffic congestion, waste-disposal problems, high energy consumption and high crime rate. These problems can be difficult to tackle if cities were not prepared nor properly managed to accept the incoming population. As cities grow in population, citizens' demands and needs must be met in ways that carry less harm to the environment.

A. Definition of smart cities

A smart city is a sustainable and innovative city that uses Information and Communication Technology (ICT) along with other means to optimize the efficiency of urban services and the quality of life, while ensuring that it covers the necessities of present and future generations with respect to environmental, economic and social aspects [2]. Smart cities aim to reduce resource consumption and to increase communication between citizens and governments. They are equipped with basic infrastructure and networks of sensors to collect information regarding the operational status of the various systems and urban services for real time analysis by information processing systems so as to improve their management and performance. The developed systems and applications in smart cities are designed to connect all devices and services within a city in order to facilitate the interaction of city representatives with both community and city infrastructure and to monitor the changes in the city and the way it evolves. The integration of sensor networks and computer systems across city infrastructure will reveal their exact operational status through measuring the flow of vehicles and people, waste disposal and levels of consumption. Hence, smart cities are crucial to face urbanization challenges effectively and to achieve more efficient and sustainable cities that drive economic growth and improve the quality of life for urban citizens [3].

B. History of smart cities

Smart cities term was first used in the 1990s and the concentration was on the importance of new ICT with regard to infrastructures within cities. Specifically, the examination of the relationship between ICT and urban areas began in 1992. The California Institute for Smart Communities was among the first to research and work on the topics of how communities could become smart and how a city should be designed in order to implement ICT. Researches in smart city have grown sharply over the years as it became the icon of ICT-driven urban innovation and attracted an escalating attention of global researchers, governments and businesses[4][3]. By analyzing Google scholar's data, it has been found that within 26 years of researches, the annual production of publications on smart cities has tremendously increased from 16 in 1992 to reach 22,800 publications in

978-1-5386-3527-8/18/$31.00 ©2018 IEEE

2017 with a total production of 544,000 publications these years.

C. Security and privacy in smart cities

Security, privacy and reliability of smart cities are the main challenges and vital prerequisites to the acceptance of citizens and governments. Due to the vulnerabilities of smart cities applications, people may suffer from a series of security and privacy threats when cities become smarter. Illegal access to information can get complicated when cities adopt the IoT. Malicious attackers may launch Distributed Denial of Service (DDoS) attacks causing physical disruptions and affecting sensing, transmission and control abilities of the systems to degrade the quality of services in smart cities. They may also generate false data to manipulate sensing results and to demean the reliability of services and decisions in smart cities. Never the less, the pervasive video surveillance in a smart city and the information collected and managed by smart home applications may be illegally utilized to invade residents' privacy and disclose their sensitive information.

Various research that highlight security and privacy issues were proposed by other researchers. Zhang et al. [5], discussed some of smart city applications with emphasis on healthcare, transportation, and smart energy. The authors proposed an off-the-shelf techniques including encryption and authentication to protect data as well applications. Gubbi et al. [11], on the other hand, proposed a framework that aims to solely protect data confidentiality via encrypting data prior to transmission to cloud servers for the purpose of storage and processing.

Frameworks that implement encryption, authentication and other anonymity techniques would not be sufficient to prevent all security and privacy issues associated with smart cities. Hence, it is vital to implement a framework that takes all issues into consideration in order to provide an appropriate solution to prevent attacks to both infrastructure and data of smart cities. In section III of this paper we describe the challenges that are facing smart cities and a solution framework is presented.

II. RELATED WORK

A. *Securit*y challenges in smart cities

Future challenges for smart cities article gives a holistic view of security vulnerabilities in smart cities and provide the solution to help develop better cities. The report covers the security vulnerabilities of four categories including smart grids, Unmanned Aerial Vehicles (UAVs) and Smart Vehicles.

Smart grids are electric grids that allow two way communication between the utility and its customers. Due to the fact that the interconnected communication channels of smart grids often lay in insecure locations, attackers target customers by launching DDoS attacks into the interconnected communication channels of smart grids. This attack generates traffic delay and jams smart grid components protocol stacks of IPv4, IPv6, 6lowPan, and TCP/IP.

UAVs or drones uses unsecured network to connect to smart devices and to microprocessor/embedded systems. Each drone uses unsecured root privileges of a user account with open access to File transfer protocol and cellular services. Drones are prone to hijacks, control takeover, and connection denial thus require to adopt encryption services. Also, to avoid compromising smart security system, encryption locks need to change frequently, for example, tampering data, eavesdropping, data confidentiality and sensor failures.

Reckless driving in smart cities gets detected through roadside traffic sensors that reports for exceeding speed limits. Sensory data is then transmitted to central network to alert authorized stations such as police to tackle incidents. In case motorists are speeding through a smart vehicle; sensors attached to it alarm data centre and send information related to the vehicle including location coordinates, speed and passengers. The received information allows law enforcement agencies to take the necessary actions [6].

B. Security and pivacy of road traffic in smart cities

According to the article published in the Personal and Ubiquitous Computing journal, in order to build smart cities, the country needs to manage different sectors of infrastructure. Of all the services provided for the betterment of citizens, road traffic is a significant area of development. Therefore, Vehicular ad hoc networks (VANETs) are set up to continuously share traffic data with motorists, road traffic managers and various service providers for an improved travelling experience. End to end traffic data sharing exposes the information of both data and vehicles for attackers (e.g. popular trip location, route access, preferences)[7].

Several proposals including public key cryptography, ID-based cryptography and pseudonyms, were put forward in order to find an end to this privacy concern but were insufficient. Lately, Attribute-Based Credentials (ABCs), particularly, Idemix, U-Prove and Persiano, were used in VANETs application. Since ABCs only acquire a subset of the driver's information, the application may show the location of the driver without disclosing their identity information [6][7].

C. Security issues of waste management system in smart cities

Trend Micro, a global information security company, has put up some security considerations for different smart city sectors. It gives an insight that hacking of smart automated waste management system such as trash can and sewage systems can risk people health. Like, releasing untreated sewage water in fresh water, smart valve blockage resulting in overflows and falsified sensor results registering air quality. Therefore, environmental systems need secure configurations with interface access controls and restrictions[6].

D. *Security and privacy issues of internet hostspots in smart cities*

Communication sector provides public WIFI on various hotspot locations. These hotspots draw privacy concerns through the disclosure of users' private information when registering a mobile phone on an open network with little or no encryption. A signal jammer, set up by a cyber attacker can drain cell phone batteries by repeatedly demanding to reconnect to an available network. The attacker can then track down users IP address, contact details and access data transmitted to and from cloud services [6].

III. Challenges and Solutions

Components that are required to build smart cities can be categorized into four areas; Hardware, Software (utilities and services), data, and the communication components that enable data exchange between the different services. The communication components disseminated across the hardware (routers, switches, Firewalls, IPS, etc) and service (routing protocols, policies implementations, ACLs, VPNs, etc). Therefore it is essential that each of these areas need to be protected based on their importance to the delivery of services to end users. The implementation of ICT, IoT and the usage of artificial intelligence (AI) presents a variety of security challenges that are threatening the functionality of smart cities. As such, it is vital that we incorporate security measures into the design of developed and utilized systems. The following sections highlight the security challenges and threats related to both system infrastructure and data of smart cities. Solutions framework to overcome such challenges is also proposed.

A. *Infrastructure Security*

Smart cities infrastructure includes traffic, transportation, communication, water, electricity systems and other services. These services need to communicate with each other in order to provide an optimum service. Identifying components that are vulnerable to the functionality of the city can form the basis of targeted attacks, such as DDoS, spoofing, malicious data injection and theft attacks. The aim of such attacks is to disrupt the sensing functionality as well as the functionality of transmission of data and their control, which consequently leads to degrading the Quality of Services (QoS) offered. End points as well as end user devices represent the control and feedback systems in the physical world. This, in turn, makes them greatly exposed to threats and to be attractive targets for attackers. Thus, security policies are required to be in place in order to ensure the protection of the overall infrastructure [8][9].

In order to ensure the protection of smart cities infrastructure, there is an essential need to develop a security framework that guarantees the protection of the overall system. This is done via adding a new Smart City Security Management System (SCSMS), which provides an extra protection layer and ensures validity, integrity and availability of all individual components to the rest of the system that form the core of smart cities. SCSMS must be able to handle all types of malware, bots, loggers, rootkits and attacks using prevention tools such as firewalls, antivirus software, intrusion detection systems and intrusion prevention systems. In addition, the proposed system continuously monitors and analyzes network traffic and ensures protection through access control authentication and logging mechanisms, encryption methods, decentralizing storage system and auditing. The system must have the ability to monitor and control the entire infrastructure systems and endpoints in real-time. SCSMS should have the ability to continuously search for unidentified devices and sensors added to the network without proper inspection and permission. Machine learning algorithms, however, need to be developed and tested in order to detect intelligent threats in smart cities though scouring the web for vulnerabilities ahead of time.

B. *Data Security*

Smart city applications are tightly coupled with data and connectivity. Services provided by smart cities rely on accumulating, transmitting and processing data streams collected from all over the city i.e, citizens' location and digital engagement information, transportation and local government information. The collected streams of data raise a sequence of concerns and challenges in terms of data security and privacy. Gathered data must be protected from unauthorized access, disclosure, disruption, modification and inspection. However, the ultimate goal of providing a plug and play strategy, where equipment can be plugged in the system from different vendors, would raise a major problem. This is due to the fact that most of the devices and systems not tested thoroughly and ultimately would be prone to attacks. The possibilities of security lapses are quite high due to the lack of cryptographic security and authentication factors. For instance, sensors communicate with each other using unencrypted link; hence, attackers can penetrate these sensors which might lead to injecting fake data to cause signal failures and system shutdowns [10]. Supervisory control and data acquisition systems (SCADA), used in smart cities to collect and process data then control multiple operations, are susceptible to frequent attacks as well as the poor security protocols that are usually sacrificed for a lowering the latency of data exchanged among this type of equipments. Consequently, a targeted attack could threaten the privacy of the data and shut down multiple city services from a single entry point. Simple computer bug is another example as it could grant the attacker an access to invade the control systems of the smart city and send manipulated data to servers in order to exploit and crash data centers [9]. Data breaches can be costly to remedy as they disrupt daily operations and services of smart cities and invade the privacy of citizens. Therefore, solutions must be found to maintain user privacy, preserve integrity and confidentiality of data and secure services provision.

The security and privacy of data gathered in smart cities must be guaranteed throughout each step of data management from collecting and aggregating data to analyzing and exchanging it among applications. Hence, in order to minimize the risk on exposing data to attacks, the SCSMS need to include the following components to ensure security and privacy of data:

- **Policy decision point component:** Deals with a collection of policies to ensure that the required measures were taken before approving the access to private and confidential information. Polices are cautiously selected based on the sensitivity of the gathered information. They specify and determine whether all or specific data require encryption.
- **Authentication component:** Enforces appropriate access control polices and preserves an access control log to keep track of the access activity and the involved entities. Digital Access Control systems (DACs) can be built in smart cities to ensure that only authorized officials have access to confidential data and networks. They are used to protect the provided services from cyber threats and hacking as they protect data from alterations. In these DACS, different views and levels of access can be assigned to different parties based on their requirements.
- **Data confidentiality component:** Deals with data security and ensures that malicious service providers or users can not access private and confidential data. Some of the services provided in smart cities require accessing private data and storing it on unreliable domains. In order to ensure the security and privacy in such cases, data must be encrypted or anonymized before leaving the user controlled domain. Data confidentiality component provides the required cryptographic algorithms to grant authorized users and service provides the ability to process and analyze data using unreliable domains such as public cloud services. It is used to conceal sensitive data based on the security policy selected by policy decision point.
- **Services Management Component:** Growing population would lead to an extensive usage of smart devices that pose different threats to residents' privacy, intelligence, and data. This component is to prevent these silent attacks and to provide traceability, monitoring and auditing. Frequent update of privacy policies, rules and regulations are approved by this component prior to implementation.

IV. Future work

The regular security solutions currently offered do not fulfill all the insecure loopholes present in a smart city. In order to fill these gaps, extensive research is conducted to propose additional security solutions. The next step in this research is to design the blue print and to partially implement the Smart City Security Management System (SCSMS) proposed in this research. Validity and robustness of the SCSMS need to be tested to increase confidence in such management system and ultimately to move a step further into the protection of smart cities.

V. Conclusion

Smart cities employ the latest advancements of ICT, IoT and AI to enhance the offered services and to improve the life of citizens. Cyber security in smart city is a significant issue that takes into account several security challenges related to the technology employed, infrastructure developed and data gathered. The emerging of technology raises privacy and security issues at individual and community levels that must be addressed and resolved. Worldwide security experts have provided several solutions to overcome some of the security challenges. In this research paper, we have discussed some of the current security challenges and the previously introduced solutions to protect different services. In addition, we proposed the SCSMS framework to ensure the privacy and security of both infrastructure and data.

REFERENCES

[1] T. Becker. "Smart cities.", Georgia Tech Research Horizon, issue 1, 2017 [Online]. Available: http://www.rh.gatech.edu/features/smart-cities

[2] R. Lea, "Smart cities: An overview of the technology trends driving smart cities",2017.https://www.ieee.org/publications-standards/publications/periodicals/ieee-smart-cities-trend-paper2017.pdf

[3] V.Albino, U. Berardi, RM. Dangelico. "Smart cities: Definitions, dimensions, performance, and initiatives," Journal of Urban Technology, 2015.

[4] L. Mora, R. Bolici, M. Deakin, "The first two decades of smart-city research: A bibliometric analysis," Journal of Urban Technology, 2017.

[5] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. Shen, "Security and privacy in smart city applications: Challenges and solutions," IEEEXplore, 2017.

[6] Z. A. Baig et al., "Future challenges for smart cities: Cyber-security and digital forensics," Elsevier Digital Investigation, volume 22, September 2017, Pages 3-13

[7] L. S.-O. J. De Fuentes, J. M.; Gonzalez-Manzano, "Assessment of attribute-based credentials for privacy-preserving road traffic services in smart cities," Personal and Ubiquitous Computing, 2017.

[8] P. Nielsen. "Optimal partition of QoS requirements on unicast paths and multicast trees" 2016 Available: http://www.informationsecuritybuzz.com/articles/smart-city-security-and-cyber-attacks/

[9] A. AlDairi and L. Tawalbeh, "Cyber security attacks on smart cities and associated mobile technologies," ScienceDirect, 2017.

[10] E. . Y. LLP, "Cyber security a necessary pillar of smart cities", India Security Conference, 12-13 September 2016, Mumbai, India

[11] J. Gubbi *et al.*, "Internet of Things (IoT): A Vision, Architectural Elements, And Future Directions," Elsevier Future Generations Computer Systems, vol. 29, no. 7, 2013, pp. 1645–60