# Future Smart Communication Networks: A Survey of Security issues in Developing a Smart City

**Hussah N. AlEisa**
Department of Computer Sciences, CCIS Princess Nourah Bint Abdulrahman University, Riyadh,
KSA,haleisancaaa@gmail.com

**Abstract**
The smart cities are evolving constantly and are responsible for the current transformation of cities and countries into a completely connected network of information and technology This interconnected network of a huge number of smart devices is capable of exchanging complex information and provides tremendous support including enhanced quality of life within urban locations. Unfortunately this set-up is vulnerable to security attacks and requires the widespread ubiquitous network to authorize access through privacy and thus offer security in order to ensure civilian participation in a country. The smart network should benefit the individuals of the country by developing potential strategies to protect the smart cities and their participating entities from the unauthorized attacks. Trustworthy data sharing strategies based on the utilization of advanced technology features via smart communication network could solve some issues of privacy and security. This paper presents the challenges and issues related to protection and highlights the important aspects of securing the smart cities and its components. It also presents the role of cloud security for building a secure smart city.

***Keywords:*** *Internet of Things, Vehicular Adhoc networks, Smart City, Security and Privacy.*

## 1 INTRODUCTION

Smart City technology is growing rapidly and is emerging as potential strategy to provide solutions to the exceptional challenges faced by rigorous urbanization and proliferation of smart IoT devices, increasing density of population and provide better quality of services for the users(citizens/visitors/consumers) [1] at any time instant and circumstances. The necessary means for smart applications have been illustrated in Figure 1. It depicts few smart city components and domains, which are still expanding and they depend on smart applications that use digital objects such as sensors, mobile phones, actuators etc. and the necessary means of smartness in communication in any of smart city domains. In addition to using smart devices, the smart city domains should be effectively integrated and must offer information sharing among the related domains.

Smart Cities are a source for higher quality of service for a society. In recent times, there has been enormous development in technology and smart applications, which were non-existing few years ago, even though predicted by researchers. For instance a quick imagination of the scenario, where someone would like to place an order to pick up his/her sister from a karate class. Booking an autonomous car (Uber Taxi) with the help of smart phone seems to be the obvious solution. Within short time the vehicle would reach the requested location and hence the work would be accomplished via Global Positioning System of the smart device whether it be a Tablet or a smart phone. Not only this, we are surrounded by a number of smart systems at home, that help us to make our life easier that we can't ignore. For example, an air conditioner may be available everywhere by the use of smart technology that uses sensors to operate it. These actions convey the fact that there is seamless connectivity around us, which is facilitating us in our daily lives to solve many issues and provide easier solutions to the existing problems. As these methods become dominant in the routine activities, the structure surrounding our city may be vulnerable to threats related to privacy and security. Security is a critical issue that the Smart Cities have to face since it interconnects a wide range of networks, smart devices, sensors, service providers, smart hospitals, smart parking, smart transportation, smart users, etc.

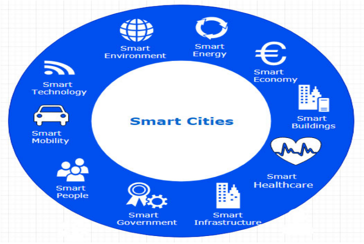

**Figure 1.** Smart City and Smart Applications

This research paper presents a survey of privacy and security issues and challenges with the available techniques applicable for the construction of Smart Cities. The survey

Manuscript received February 5, 2022
Manuscript revised February 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.2.18

papers studied also identify research areas that support smart cities and their effective existence in future.

## 2 BACKGROUND AND RELATED WORK

A high percentage of world's population is urbanized and this is drastically rising, therefore, smart cities are seeking a lot of attention. Smart cities are a well-maintained, networked collection of entities in a city to enable convenient and enhanced living of the population within a country. To facilitate the emergence of smart cities worldwide, a number of initiatives have been adopted to address the commercial and institutional needs of the nation and its citizens, through efficient service provisioning. As described in [2], smart cities is a promising technology that provides a connecting environment for all its citizens. This research also presents a comprehensive analysis of the threats and the associated vulnerabilities of every component. It has identified four smart city components - Building Automation Systems, Smart grids, Smart Vehicles, Unmanned Aerial Vehicles, with empowering IoT sensor technology and the cloud. The researchers found that the security of the data stored in the cloud is effective only if data integrity is maintained and is kept confidential. The researchers in [3] examined the aspects of security and privacy and according suggested that the data could be secured at the time of production and distribution hence giving rise to smart production and smart distribution. They presented a model indicating the interactions among users (humans), computer servers and things (smart devices), that are constitute the major elements in the Smart City and therefore are needed to be protected against any type of vulnerabilities. In [4], the researchers have explained the factors that affect information and data security in a smart city, also they provided an overview of the major security issues related to smart elements involved in the network and presented effective solutions against the privacy and security attacks in the context of Smart Cities. The research in [5] has adopted all possible efforts to make Smart City a Safe City. They provided the readers with the insight of privacy and security modelling and simulations that can be applied to design a Safe City. According to the research work in [6] smart cities have a complex architecture and any vulnerability could affect all the population and hence any individual present in the city. Further, it states that upcoming challenges in the smart city are also due to the high-energy consumption apart from just security and privacy. The focus of many challenges is robust and scalable smart city extension and implementation. The local governments in urban areas are nowadays shifting their fossil fuel energy consumption techniques towards the use two important renewable sources of energy namely solar and wind energy for fueling the smart cities [6]. Most smart cities use intelligent energy systems to supply power in remote areas. As far as local places are concerned, they use decentralised production and storage of electricity in areas such as local buildings, university and college campuses, local ports and hospitals. In [8], [9], [10] the authors investigated the cyber-security in smart grid systems and outlined the significant cyberattacks intimidating the smart grid infrastructure, its applications and protocols. The authors also proposed a strategy [11] to identify the vulnerabilities of potential elements by detecting malicious actions thus helped to protect customer privacy and improve data transmission security over the network. The researchers in [12], [13], and [14] have studied the cybersecurity from the perspective of IoT security and information security. The researchers have discussed about the overlap of the term cyber security with information security. They stated that even though they are used inter changeably they are not similar beyond a limit. Information security refers to role of individuals in the security process whereas in cyber security there are other dimensions to this factor. In [13] authors describes the three layers of IoT-perception layer, transportation layer and application layer and they have investigated the security problems at every layer distinctly. They contrasted the traditional network issues with security issues of IoT. In [16] the authors have presented a survey about the research challenges along with few solutions to solve the IoT security. In [18], [19], [20] the authors studied the big data and cloud computing security issues. In [18], a system consisting of integrated Cloud Computing and IoT was used to explain the security issues corresponding to Big Data to enhance security issues on the network.

## 3. SECURITY AND PRIVACY THREATS IN DATA SHARING IN SMART CITIES

The security issue in a smart city is mainly dependent on methods and requirements of the data sharing, data transmission and Internet Architecture. Firstly, it is required to protect/encrypt the data using encryption techniques meant for protocols or information transfer followed by protecting the transmission (containing interaction among public/ private /business parties. The Internet architecture is not inherently secure but it is dependent on its protocols and these protocols may be secure but the whole architecture is generally not protected against the massive malicious attacks. Hence, the smart cities have to be protected against these cyber security attacks. Smart cities also pose challenges to the citizens as well as public/government in a similar manner. In this scenario smart cities may also be confronted by spoofing attacks, eaves dropping, lack of service availability, data tampering and other security issues associated with the information structured within a smart city for its citizens and their safety. Few challenges may be as follows: scalability that can expand the span of smart cities, mobility required to support accessing in different locations, deployment, interoperability needed to include several heterogeneous technologies, latency, legality and other resources. The smart cities network thus constitutes a critical infrastructure may suffer severe damage in case of critical applications deployed such as essential services such as electricity, water and gas access needed for industrial plants and control systems based on Supervisory Control and Data Acquisition (SCADA) and Vehicular Ad hoc networks (VANETs) requiring pseudo authentication for protecting vehicles' privacy. SCADA is used to control and manage Smart electrical GRID systems remotely, it detects the efficiency of the Smart GRID by detecting anomalies, disconnections and interruptions in services.

Henceforth with the growth in Smart Cities architecture, huge number of Cyber security threats arise and consequently threats are converted to vulnerability, these vulnerabilities are propagated to other components and also may affect and risk the infrastructure of the smart city as a whole. To estimate the magnitude of this affect and risk associated with smart city infrastructure is quite challenging in this complex environment, that invariably depend on the data created by each component in the smart city as shown in Figure 2.

This figure depicts several important interconnected components of a Smart City. (1) Smart Homes (2) Smart grids (3) Cloud computing IoT sensors (4) Unmanned Aerial Vehicles (UAV) (5) Building Automation Systems, (6) Uplink Station (7) Gateway (8) Smart Services (9) Smart Vehicles and (10) Citizens It is obvious that all data in Smart City are collected from data vulnerable environments and is needed to be stored in Cloud, which offers the support as a reliable backend. It is necessary that the data transmission and storage onto the Cloud and the Cloud Services used must be secure; it is in turn dependent on the reliable security and privacy techniques being used to ensure that data transfer through the Smart City infrastructure is secure. By detecting and preventing cyber occurrence in privacy and security threats, the associated vulnerabilities landscape for each component in the smart city security can be determined, tracked and solved. The security and privacy issues related to every layer corresponding to the Smart City architecture are highlighted in [19],[20].

Due to the significance of data storage on the Cloud, we discuss the privacy and security issues of Cloud Computing in the next section that could have impact on Smart City security issues.

## 3.2 Challenges in Cyber security for making secure Smart Cities

Various protocols are applied at the different layers such as each layer could cover many protocols to maintain security. This section surveys the susceptibilities with the OSI and Cybersecurity.

**Layer 1 (Physical Layer):** The Physical layer comprises of the machines and the way these machines are connected with channels of communications consisting of connectors and cables (fibre optics). A hacker may steal sensitive data in many ways such as modifying configuration settings and calibration or damaging the device (computer).

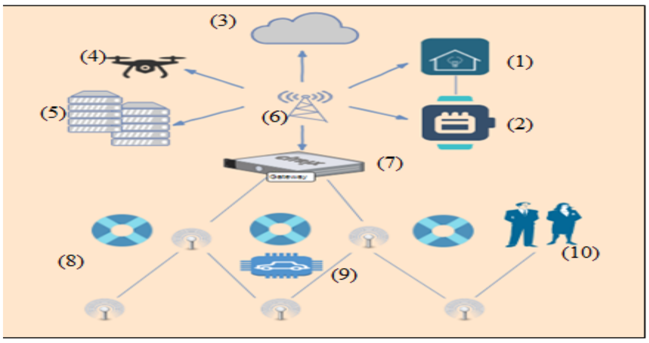

**Figure 2**. Interconnectivity of Smart City Components

Similar problems arise even in cybersecurity preservation at physical layer level [27] where the type of attacks may range from damaging connections between two computers by unplugging or removing cables and then even unauthenticated and illegitimate use of computers.

The hacker is likely to get the access to the network through common methods of wiretapping and by gaining authentication details. The network could be exploited with the man-in-the-middle attack that is easily implemented by gaining the access points of the network by some attackers and turning them into malicious access points.

Even humans like dissatisfied employees of an organization are a threat to cybersecurity who can remotely connect to the organizational systems and gain access to critical information, manipulate or damage it through wireless networks like Bluetooth or Wi-Fi.

Apart from the reasons mentioned above, the network is also vulnerable to natural vulnerabilities as if exposure to harsh weather caused due to thunder lightning and storms.

**Layer 2 (Data Link Layer)** some protocols in this layer uses predominantly Ethernet for communications as compared with others. To join the network through Ethernet an attacker may acquire some port on a switch using any device. The host disconnection is also used by few attackers to expand the network in an unauthorized manner by adding new users of their own, by installing their own access points (AP) within the network. [29]

**Layer 3 (Network Layer)** The communications infrastructure is laid down by network layer and it defines many protocols for this purpose which define a number of ways to en-route the packets of information through intermediate devices (nodes) to its destination (destination node) initiating at a device usually referred to source node. This layer encompasses primary network protocols namely IPv4/IPv6 [14] [28]. Other important ones are ICMP, ARP and IGMP. Since the network, exchanges packets of information between the nodes may it be computers, APs, routers or switches these are susceptible to poor authentication and are likely to be misused by the attacker. The other attacks that are associated with the network protocols are flooding, spoofing and manipulating data through other means poisoning messages by manipulating them. Section 3.3 discusses the details of Cloud security, which is an integral part of Network security.

**Layer 4 (Transport Layer)** This layer is responsible to maintain end-to-end connectivity using the following two types of connections: a) TCP Transport b) User Datagram Protocol (UDP). TCP is a reliable protocol since it is based on connection establishment and acknowledgement whereas UDP is an unreliable and connectionless protocol. The internet protocol (IP) usually establishes network connection by defining type of connection in the port field. The attacker can insert fabricated segments in the message sequence by reassembling the message and cause errors. In addition, the attacker can scan the network ports to get the information about the IP address along with applications used by the systems those have been connected to the ports.

### 3.3 Cloud Security

Data transfer and storage in the Cloud is an essential aspect, which is related to smart cities. So there are more effective ways to detect and prevent cybersecurity threats before they cause widespread harm [2] [7]. Cloud Computing is prone to many security threats and challenges that are common with organizations that are managing in-house infrastructure and those involved in traditional outsourcing models. Cloud computing attackers can be divided into internal and external attackers that can be clearly differentiated. Their capabilities to execute successful attacks is what differentiates them as a threat to users and vendors alike [20-23]. The following section discusses how clouds can manage data confidentiality, integrity and availability that are critical to cloud environment.

Data Confidentiality in Cloud: Cloud storages have security built into its platform allows unauthorized access and data protection. This is necessary to manage online services for worldwide business. Cloud providers may create certain rules and regulations, the customers should comply with and thus sign an agreement to validate the breaches, and data losses would be avoided and secure measures be followed.

The data Integrity of cloud means protection from unauthorized data update or deletion. If permissions and logs system is used then inappropriate access to customer data could be avoided. Also a cloud containing huge amounts of data which is a result of accessing many sources can define a means of access and impose crucial authorization methods of interaction with data with the proof without any data loss.

A cloud infrastructure is vulnerable and inevitable to network failures therefore one should ensure that cloud data is highly available even in such a situation. The storage service providers are responsible to maintain several storage and redundant components, thus increasing data availability across various geographic regions and manage the failures effectively and efficiently.

### 3.3.1 Categories of Cloud Security

According to the research in [24][25][26] related to the Cloud Security issues with Smart City perspectives found in sections 3.2.1 and 3.2.2, the various attacks and risks can be classified as follows:

*Cloud Infrastructure*: It covers attacks that are specific to the cloud infrastructure (IaaS, PaaS and SaaS) such as tampered binaries and privileged insiders

*Network*: It involves network attacks such as Connection Availability, Denial of Service (DOS), DDOS, flooding attack, internet protocol vulnerabilities, etc.

*Security Standards:* These describe the standards that are essential to take precautionary measures in cloud computing in order to prevent attacks. It governs the policies of cloud computing for security without compromising reliability and performance

*Access Control:* It includes authentication and access control. It captures the issues that affect the privacy of user information and data storage.

*Data:* It is the data related security issues including data migration, integrity, and confidentiality and data warehousing.

### 3.3.2 Cloud Computing Security Risks

*Data Leakage:* this occurs when the cloud computing begins to run out; two changes may be occurred in users data. First, data is stored in a location other than the computer, and

Second, data from one run to multiple run. With these changes in the user data, there is the risk of leakage or loss of information.

*Insecure Interface:* all software and applied interfaces are showed by cloud computing providers where these are used for interaction of cloud with users, Sorting information, personality administration, and observing, service, occurs in the cloud and authentication and access control are also monitored by these interfaces.

*Malicious Insiders:* This risk arises due to the misuse of data by employees of specific organization

*Shared Technology:* The *C*omponents that work under cloud do not support strong isolation until creating space for cloud computing, such as virtual memory and virtual processing unit.

## 4. CONCLUSION

This paper have discussed possible challenges and concerns on maintenance of security and privacy issues for the development and deployment of Smart Cities in urban areas. We have also described the energy and cloud aspects that may be beneficial for the deployment of different Smart City components. The related security issues, the role of Cloud Security with Smart City perspective have also been a focus of discussion in this paper. The Smart Cities construction is developing rapidly, with a huge rise of opportunities for future research on privacy preservation and security challenges. Many areas of future including firewalls and micro-firewalls and smart cards are still in the state of launch for utilization. Internet of Things (IoT) security measures are a crucial concern that is urgent requirement of the secure smart city. Further researchers and business executives are inclined towards working on the creation of rules for unauthorized access leading to cyber-crimes that would offer consumers a protection the senor based IoT devices could provide. Smart cities make the future vision of interconnected cities come true through their viability and ability to increase secure and quality life.

### References

[1] Allan A. Friedman and Darrell M. West, “Privacy and Security in Cloud Computing”, Issues in Technology Innovation, No 3, pp24-29, November 2010

[2]Zubair A. Baig, Patryk Szewczyk, Craig Valli, Priya Rabadia, Peter Hannay, Maxim Chernyshev, Mike Johnstone, Paresh Kerai, Ahmed Ibrahim, Krishnun Sansurooah, Naeem Syed, Matthew Peacock, “Future challenges for smart cities: Cyber-security and digital forensics”, Journal of Digital Investigation, pp3-13, (2017).

[3]Adel S. Elmaghraby and Michael M. Losavio, “Cyber security challenges in Smart Cities: Safety, security and privacy”, Journal of Advanced Research, Volume 5, pp. 491–497, 2014.

[4]Anwaar AlDairi and Lo’ai Tawalbeh, “Cyber Security Attacks on Smart Cities and Associated Mobile Technologies”, The International Workshop on Smart Cities Systems Engineering (SCE 2017) Procedia Computer Science, Volume 109C, pp. 1086–1091, 2017.

[5]Maro Lacinak and Jozef Ristvej, “Smart city, Safety and Security“, TRANSCOM 2017: International scientific conference on sustainable, modern and safe transport, Procedia Engineering, Volume 192, pp. 522 – 527, 2017. .

[6]Rida Khatoun and Sherali Zeadally. “Smart cities: concepts, architectures, research opportunities”. Magazine of Communications of the ACM, Volume 59, Issue 8, pp. 46-57 August 2016.

[7]Terence K.L. Huia, R. Simon Sherratt, Daniel Díaz Sánchez, Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies”, Future Generation Computer Systems, Volume 76, 2017, pp. 358–369.

[8]Zakaria El Mrabet, Naima Kaabouch , Hassan El Ghazi, Hamid El Ghazi, “Cyber-security in smart grid: Survey and challenges “, Computers and Electrical Engineering, Volume 67, 2018, pp. 469–482.

[9]Rossouw von Solms and Johan van Niekerk,” From information security to cyber security”, computers and security, Volume 38, 2013, pp. 97-102

[10]Carol Hawk and Akhlesh Kaushiva, “Cybersecurity and the Smarter Grid”, The Electricity Journal, Vol. 27, Issue 8, pp. 84-95, October 2014.

[11]Rafał Leszczyna, “A review of standards with cybersecurity requirements for smart grid”, Computers and Security Volume 77, pp. 262-276, 2018.

[12] Ilhami Colak, Seref Sagiroglu, Gianluca Fulli, Mehmet Yesilbudak, Catalin Felix Covrig, “A survey on the critical issues in smart grid technologies”, Renewable and Sustainable Energy Reviews, Volume 54, pp. 396-405, February 2016.

[13]Aakanksha Tewari, B.B. Gupta, “Security, privacy and trust of different layers in Internet of Things (IoTs) framework”, Future Generation Computer Systems, May 2018. Available at https://doi.org/10.1016/j.future.2018.04.027

[14]Zhihong Yang, Yingzhao Yue, Yu Yang, Yufeng Peng, Xiaobo Wang, Wenji Liu, “Study and application on the architecture and key technologies for IoT”, in: Proceeding of 2011 International Conference on Multimedia Technology, pp. 747-751, ( ICMT), 2011.

[15]Rishika Mehtaa , Jyoti Sahnib, Kavita Khannac, “Internet of Things: Vision, Applications and Challenges”, International

Conference on Computational Intelligence and Data Science (ICCIDS 2018), Procedia Computer Science, Vol. 132, pp. 1263-1269, 2018.

[16]S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead”, Computer Networks Journal, Vol. 76, pp. 146–164, 2015.

[17]Mahmoud Ammar, Giovanni Russello, Bruno Crispo, “Internet of Things: A survey on the security of IoT frameworks”, Journal of Information Security and Applications, Vol. 38, pp. 8–27, 2018.

[18]Christos Stergioua, Kostas E. Psannisa, Brij B. Guptab, Yutaka Ishibashic, “Security, privacy & efficiency of sustainable Cloud Computing for Big Data & IoT”, Sustainable Computing: Informatics and Systems, Vol. 19, pp. 174–184, 2018.

[19]Jianwei Hou, Leilei Qu, Wenchang Shi, “A survey on internet of things security from data perspectives”, Computer Networks Journal, in press, Dec 2018.

[20]Zhifeng Xiao ; Yang Xiao, “Security and Privacy in Cloud Computing”, IEEE Communications Surveys & Tutorials, Volume 15 , Issue 2 , pp. 843 – 859, Second Quarter 2013.

[21]Jeevitha B. K., Thriveni J., Venugopal K. R, “Data Storage Security and Privacy in Cloud Computing: A Comprehensive Survey”, International Journal of Computer Applications (0975 – 8887) Volume 156 – No 12, December 2016, pp. 16-27.

[22]Sumitra Binu and Mohammed Misbahuddin, "A Survey of Traditional and Cloud Specific Security Issue" International Symposium on Security in computing and Communication, SSCC 2013: Security in Computing and Communications, Sabu M. Thampi et al. (Eds.): SSCC 2013, pp. 110–129, 2013.

[23]Saeed Shafieian, Mohammad Zulkernine, Anwar Haque, "Attacks in Public Clouds: Can They Hinder the Rise of the Cloud", n: Mahmood Z. (eds) Cloud Computing. Computer Communications and Networks. Springer, Vol 6, pp. 3-22. 2014.

[24]Issa M. Khalil, Abdallah Khreishah, Muhammad Azeem, “Cloud Computing Security: A Survey”, Journal of Computers, Volume 3, pp. 1-35, 2014.

[25]“Top Threats to Cloud Computing + Industry Insights”, CLOUD SECURITY ALLIANCE The Treacherous 12, 2017.

[26]Hassan Takabi, James B.D. Joshi, Gail-Joon Ahn, " Security and Privacy Challenges in Cloud Computing Environments", IEEE Security & Privacy, Vol. 8, No. 6, pp. 24–31, 2010.

[27] Ramnath, Deepak , Krishnakumar, Vijayaraghavan, S., Ramanathan, R. “An improved secret key update for multiple intersymbol obfuscation in physical layer security” in Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI), India, 13–16 September 2017.

[28] Lu Z.; Shakeri., Razo M, Tacca, M.; Fumagalli, A., Galimberti, Martinelli,, Swallow, G. “Orchestration of reliable three-layer networks”, in Proceedings of the 19th International Conference on Transparent Optical Networks (ICTON), Spain, 2–6 July 2017.

[29] Al-Salloum, Wolthusen, “A link-layer-based self-replicating vulnerability discovery agent” in Proceedings of the IEEE symposium on Computers and Communications, Italy, 22–25 June 2010.