SMART SECURITY AND SMART PRIVACY: BACKBONE OF SMART CITIES

Neeraj Rathore[1], Alka Verma[2], Amit Agarwal[3]
[1]DIT UNIVERSITY, Dehradun, [2]Research Scholar, [3]UPES, Dehradun

Abstract

The development and functionality of a smart city is always subjected to the pivotal role of the security architecture. In order to address an array of apparent challenges of urbanization smart cities must infuse smart transformations like smart healthcare, smart governance, smart environment, smart transportation, smart energy, waste and water management applications. However these applications can confront various socioeconomic, political and technical hurdles as these smart applications gathers huge volume of personal and Impersonal data which arise the concern of security and privacy of the data. Thus, there is a need of secured smart architecture which ensures pervasive security and privacy of the data associated with these smart applications. Smart cities should be able to handle the data usage and policy challenges which can reach to the local government. Also, which can restraint city prerequisite and can affect people's lives.

Keywords: Smart City; Smart City Architecture; Security Concerns; Security Issues

1. Introduction

A smart city mean to be an urbanized town, by embedding Information and Communication Technology in its infrastructure which serves various innovative and advance services to its citizens, in order to improvise the quality of their life. A smart city must encompass all the forthcoming and highly advance integrated technology, the core of which is "Internet of things" (IOT) [1]. Smart technologies like smart governance, smart communications, smart environment, smart transportation, smart energy, waste and water management applications promises the smart growth of the city, but at the same time needs to enforce pervasive security and privacy of the large volume of data associated with these smart applications. Special smart security measures are needed to cover urbanization trends in advanced, innovative administration of urban transference and various smart services to the residents, visitors and the local government to meet the ever expanding and manifolds demands [2].when the city grows urban, its residents may suffer from various privacy and security issues due to smart city applications vulnerabilities [3].

Conceptually smart cities entirely depend upon internet of things, embedded systems and smart technologies [4]. It will be a misapprehension that long established technologies, in terms of network, could be used in city's architecture to turn it into smarter [5]. Smart architecture is needed to build-up a smart city along with the smart security and smart privacy applications. In section II we suggest a hypothetical smart secure architecture. The security is indispensible in the architecture of a smart city as the network is prone to a large domain of malicious attacks and the third party is not always trusted so security is a paramount [6].

Smart innovation in Information and Communication technology brings into scope many technical, social and political issues, which should be taken into consideration and possible solutions should be implemented and guaranteed. In technical issues, along with some other problems like cost-effective technology and interoperability, the security and privacy is prime concern [7].Information security pertains

to the security and privacy issues. Primarily the main objective of information and security is to guard the data or the information from malicious attacks, viruses, frauds and various others malicious activities which may harm either to the information or the requirement of the information for the embedded technologies used in smart city [8]. The impact of information security is not restricted to the technical side only, but also influence the economic issues as well[9] Moreover, the smart technologies integrated in smart cities must need to understand the security concerns of the people over the information gathered. The people are mainly concerned about the usage of the data collected i.e the purpose for which the data is collected and its accessibility. Though it's not explicit when it comes to what they take as personal data but mainly the information collected as gender ,age ,nationality ,etc. is consider to be less sensitive where as other information regarding the salary, accounts ,contacts, etc. involves the more privacy and security concerns[10].

2. Smart City Architecture

In order to gain collective sensing as well as refined management of city , the information is manipulated via smart city which is sensed from the substantial world, the information which is transmitted in the communication world, in addition to the information processed in the information world for clever services. The sensing components, mixed network infrastructure, processing units, and control along with operating components are integrated in it as shown in the Figure 1. While the data or information is being transferred from Substantial World to Communication World and henceforth from Communication World to Information World it should be secured in all ways because in Smart City a lot smart transformations like smart healthcare, smart governance, smart environment, smart transportation, smart energy, waste and water management applications are being used therefore a proper authentication mechanism as well as encryption algorithm should be used while transmission of information.

Sensing Components:

The sensing components basically consists of the devices which are wearable , industrialized sensors, along with smart devices (e.g., smart watches, smart phones, smart ACs, and video observation cameras [11]) to evaluate information from the substantial world and send out this information to the processing unit for further decision making or we can also call the sensing components as the link which connects the substantial and information worlds. The Confidentiality , Authenticity and Integrity of data should be maintained while transmission of data. The authorities which basically deploy the sensing devices are either the government departments as well as companies, or are carried out by users. In addition, the real-time and granular data is sometimes preprocessed or compressed by the resource- constrained sensing devices before transmitting it to the network because of the restrictions of device size, battery, and processing capabilities .

Heterogeneous Networks:

The sensing information is gathered in diversified ways such that the heterogeneous network infrastructure acts as an influential job in supporting the smart city , with the coexistence of immense sensing devices and various applications [12]. The Heterogeneous networks majorly consists of wide area networks (WAN), device-to-device (D2D) communications, mobile networks , Wireless local area network (WLAN) , sensor networks, and so on, and enable seamless switching among different types of networks. While the communication of information is being done whether it's device-to-device communication or WLAN communication etc. it should be a properly secured communication with the help of proper encryption algorithm being used such as IDEA , DES etc. so that sensitive information of the users/clients should be secured. The communication world is represented by Heterogeneous World in a smart city in order to join the substantial and information worlds.

Processing Unit:

The prevailing cloud computing servers, rich databases, as well as committed control systems are majorly constituted by the Processing Unit in order to examine and process the gathered sensing information from the substantial world for decision making. The data

or information which is kept in the cloud servers or databases should be kept very secured by using suitable firewalls and the data should be properly encrypted by using highly secured encryption algorithm so that the cloud servers or databases should not accessed by an unauthorized user or intruder. The information world is controlled by the Processing Unit in a smart city. The government hospitals, industries, users, and so on are the authorized entities which have few rights along with authorizations in order to use the gathered information. The necessities or rules can also be determined by them for effective decision making and control in a smart city.

Control and Operating Components:

The information is fed back by the smart city in order to manipulate the substantial world with the help of the control and operating components, such as smart phones , smart watches etc. in order to leverage the optimization along with decisions of the processing unit. For offering a superior quality of life in a smart city the control and operating components optimize and make adjustments to the substantial world. The two-way flow of the smart city (i.e., sensing and control) is also implemented by them. This two-way flow can not only gain the information about the substantial world but it can furthermore supervise as well as control each gadget or component in a smart city to make it work correctly and"smart"

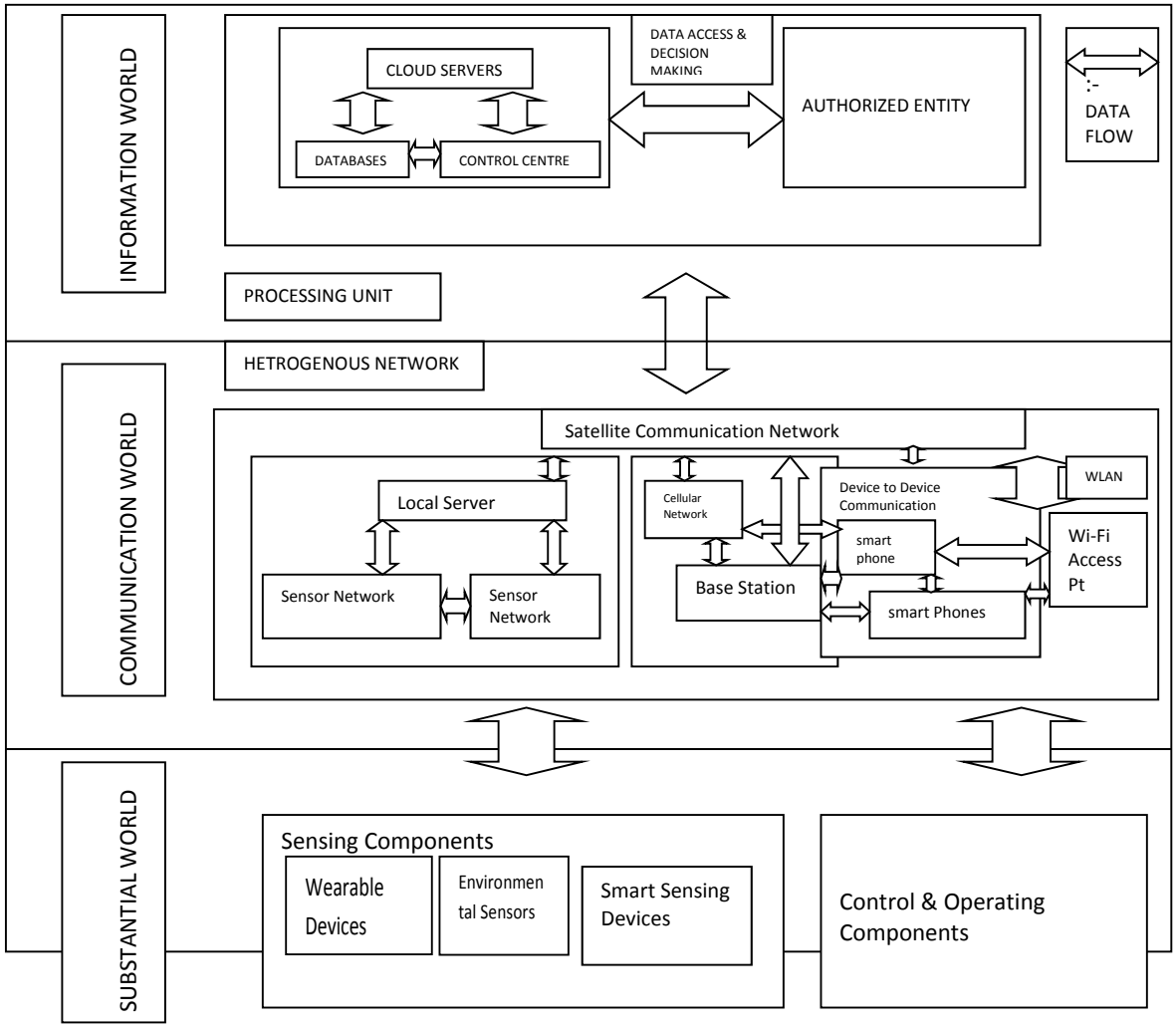

Figure 1:- Architecture for Smart City:- Substantial World , Communication World and Information World

3. Smart City Security Concerns

The data or information should be protected in the following different aspects to ensure security of data: Confidentiality, Authenticity , Integrity and Availability.

These concepts are in study as of quite a few years [13] , latest studies have pointed out that these concepts should be taken into consideration for a wide range of areas [14][15]. Those four concepts are defined as follows:

1. Confidentiality :

The confidentiality concept basically specifies that only the sending user and the intended receiver should be able to access the contents of message. If an unauthorized user is able to access the information, the confidentiality gets compromised which is called the interception attack.

For e.g:- If a user A wants to send some message to user B and some other unauthorized user C is able to access the message then the purpose of confidentiality is defeated.

2. Authenticity:

The authenticity concept basically helps to set up the evidence of identities. This concept ensures that the origin of message is correctly identified.

For e.g- Suppose that user A is sending a message to user B over the internet. However , the problem is that an unauthorized user C is pretending to be user A and is sending the message to B . How would B be able to identify that A is the legitimate user?

3. Integrity:

The concept of Integrity ensures that the contents of the message are not modified even if the message is accessed by the unauthorized user. If the unauthorized user is able to modify the message which is being sent from user A to B then the integrity of the message is lost and this type of attack is called modification.

For e.g- Suppose that user A sends Rs. 100 to user B but an unauthorized user C gets an access to the message and modifies it to Rs 10,000.

4. Availability:

The concept of availability states that the resources (i.e. information) should be available to the authorized user Twenty Four cross Seven.

For e.g- Because of the intentional actions of an unauthorized user C , the legitimate user A is not able to contact server B.

4. Smart City Security Issues

This sections basically depicts the set of certain security issues that needs to be considered in urban systems and city may be under risk of.

In this section the main focus will be on the scenarios and situations that could appear as a threat to Smart Cities. The various security issues for this Urban System environment are as follows:-

1. Access to information through various applications:

To implement efforts for adding security in order to enhance the confidentiality along with integrity of data the packet transmit is ought to be explored[15][16][17][18]. The packet should be accessed by various devices in diversified ways as well as locations, from network point of view. Therefore ,in order to decrease latencies while data transmit, the local copies of those packets may possibly be formed [19].

The traffic of Packets commencing from local devices (that is anything through a physical sensor to the smart phone) to the network and from the network to the devices is a major issue in our study.

2. Tracking of Information:

For a Smart City to be interactive, it is essential to have an atmosphere in favor of the systems which is interrelated as well as interoperable [17],[20], [21], [22]–[25]. It is also utmost important that the information which is being used by System B and is sent to System B through A should never be traced back to the original one in order to implement confidentiality.

Hence it is utmost important to guarantee that this communication should be secured, furthermore in order to ensure the data exchange in a safe mode a secured medium should be presented, also the source of original information should not be revealed [17], [16].

For example suppose that system A shares an information with a solution B.

Let us assume that A is a system that provides criminal reports; B is one more system that provides the solution which uses these criminal reports for defining the safest location for opening a fresh commercial building; The information which is being provided by System A to System B, as well as B's information should not be revealed. Such kind of condition can demolish the secrecy in A.

3. Tracking of Citizens:

It is very much feasible for urban systems to have an enhanced city management with the help of various different sensors(physical & social) that are being used since these sensors are used to gather the data from various different city scenarios.

These sensors should be under the supervision of a reliable authority so as to safeguard its functionality and data which is being generated, in order to avoid further troubles.

The major reason for ensuring sensors accurate implementation is straightforwardly linked with the assurance to facilitate that not an iota of the sensors information could be used to track citizens, their steps as well as decisions along with the other things [26], [27], [18],[28].

From the various problems discussed in this section, the following issues should be resolved: Unauthorized access of citizen data, movement patterns discovery should be avoided etc.

4. Losing Citizen's Data:

In Smart Cities , the Smart Systems will be implemented, with the help of which the access to Smart Devices such as Smart Phones , Smart Watches , other smart gadgets etc. will be very easy. An extensive range of data and information will be provided by these Smart Devices. It is likely to include personal information, such as Messages, pictures, Appointments, Bank Account, Contacts etc. , depending on the type of data being handled by these devices,.

This issue majorly deals with the concern that the various applications being used by the smart gadgets are saving a lot of valuable data of the user and if not treated well then this valuable data can be lost which can create major problems to the users .

The applications which are accountable for maintaining this valuable data, in most of the cases, use local storage tools or APIs in order to maintain these data in the device itself. It is very much required to avoid a dissimilar application, system or service, to have an access to the data in the client side, until and unless it is authorized to do so.

This may perhaps be gained by adding a proper mechanism which is related to client cryptographic storage [29] or system isolation. [16], [14], [26], [18].

5. Inter-access to information in data centre:

In this issue, we majorly deal with scenarios which are linked to the undesired right to use of information by exploiting security breaches on the server side.

The entire system can be compromised , if by any means the data security is sullied such as while storing , analyzing or managing the data.

This section majorly deals with the problem which goes beyond authentication and authorization of a particular entity. The major focus lies on the accurate limitations along with precincts definitions in an interoperable atmosphere [16],[30].

6. Inter-access in Client Side:

Issue #5 majorly dealt with unauthorized access in server side. Unlike issue #5 this issue majorly deals with unauthorized access in client side.

Unlike issue #4 which majorly focused upon the users/clients data or information which is not properly stored on devices having local storage with proper safety mechanisms is likely prone to unauthorized access , this issue majorly deals with the information security which is breached while transmitting of information from system A to system B.

Suppose, for example, Smartphone values which are associated with student grade are saved in System A, furthermore the similar mechanism is used by System B to store the user information concerning the users/ clients bank account. If the proper security mechanism is not provided while transmitting the data from System A to System B , it is quite likely that

through A an intruder have an access to information in B, moreover , it is also possible that an access to both the systems data or information can be gained by introducing a malicious program [16], [13], [29].

7. Viral outcome in Urban Atmosphere:

For a Smart City to be interactive, it is essential to have an atmosphere in favor of the systems which is interrelated as well as interoperable [17],[20], [21], [22]–[25].

If the boundaries of these associations are not clear, then the systems can face a situation where a value is modified in system A moreover when system B will use this modified value, it can corrupt the value or information produced or stored in system B.

The major outcome of such conduct is a viral effect. The system will infect system, which will further infect other systems that keeps on infecting the other parts of other systems resulting in compromising the entire network.

For example, let us suppose that if this environment is made of a sequence of systems (systems A, B, C ... Z), we may face circumstances where A gives B, an infected value while B may gives C ... Z systems. It is very easy for an attacker to infect the entire system environment by just infecting a small segment of the system and wait for the infectivity to be spread [18], [31], [32].

5. Conclusion

In this paper we have majorly discussed about the Smart City Architecture and various privacy and security concerns and issues related to the Smart City. We have firstly introduced the importance of Smart City & its benefits for the users/ clients living in it. In the next section we have discussed the Smart City Architecture. After that we have presented various privacy and security concerns related to the Smart City. In addition to it we have also taken into consideration various privacy and security issues. We hope that this article sheds more light to the Smart City Security Architecture and the security concerns and issues related to it.

References

[1] J. Liu *et al*., "Software-Defined Internet of Things for Smart Urban Sensing," *IEEE Commun. Mag*., vol. 53, no. 9, Sept. 2015, pp. 55–63.

[2] X. Li *et al*., "Smart Community: An Internet of Things Application," *IEEE Commun. Mag*., vol. 49, no. 11, Nov. 2011 pp. 68–75

[3] A. Martinez-Balleste, P. Perez-Martinez, and A. Solanas, "The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City Is Possible," *IEEE Commun. Mag*., vol. 51, no. 6, June 2013, pp. 136--41.

[4] International Journal of Advanced Computer Science and Applications Vol. 7, no. 2 , 2016.

[5] Felipe Silva Ferraz , Carlos Andre Guimarass Ferraz, "Smart City Security Issues: Depecting Information Security in the role of an urban environment.

[6] A. Baroli, J. Hernandez- Serrano, M. Soriano , M. Dower , A. Kuontouris and D. Barther, " Security and Privacyin your Smart City" , Proceeding of the Barcelona Smart Cities Congress , 2011.

[7] M. Naphade *et al*., "Smarter Cities and Their Innovation Challenges," *IEEE Computer*, vol. 44, no. 6, 2011, pp. 32–39.

[8] International Journal of Advanced Computer Science and Applications Vol. 7, no. 2 , 2016.

[9] R. Anderson , " Why Information Security is hard- an economic perspective," in Computer Science Applications Conference , 2001. ACSAC 2001, Proceedings 17th Annual IEEE, 2001 pp. 358-365.

[10] Government Information Quarterly 33(2016) , 472-480.

[11] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," IEEE Internet of Things J., vol. 1, no. 1, 2014, pp. 22--32.

[12] K. Zhang et al., "Security and Privacy for Mobile Healthcare Networks — From Quality-of-Protection Perspective," IEEE Wireless Commun., vol. 22, no. 4, Aug. 2015, pp. 104–12.

[13] R. Turn and W. H. Ware, "Privacy and Security Issues in Information Systems," IEEE Trans. Comput., vol. C–25, no. 12, pp. 1353–1361, Dec. 1976.

[14] W. Li, J. Chao, and Z. Ping, "Security Structure Study of City Management Platform Based on Cloud Computing under the Conception of Smart City," in 2012 Fourth International Conference on Multimedia Information Networking and Security, 2012, pp. 91–94.

[15] M. Okuhara, "Security Architectures for Cloud Computing," pp. 397–402.
[16] M. Sen, A. Dutt, S. Agarwal, and A. Nath, "Issues of Privacy and Security in the Role of Software in Smart Cities," in 2013 International Conference on Communication Systems and Network Technologies, 2013, pp. 518–523.
[17] F. Ferraz, C. Sampaio, and C. Ferraz, "Towards a Smart City Security Model Exploring Smart Cities Elements Based on Nowadays Solutions," ICSEA 2013, …, no. c, pp. 546–550, 2013.
[18] G. Loukides, A. Gkoulalas-Divanis, and J. Shao, "Efficient and flexible anonymization of transaction data," Knowl. Inf. Syst., vol. 36, no. 1, pp. 153–210, Sep. 2012.
[19] G. Suciu, A. Vulpe, S. Halunga, O. Fratu, G. Todoran, and V. Suciu, "Smart Cities Built on Resilient Cloud Computing and Secure Internet of Things," 2013 19th Int. Conf. Control Syst. Comput. Sci., pp. 513–518, May 2013.
[20] N. Mitton, S. Papavassiliou, A. Puliafito, and K. S. Trivedi, "Combining Cloud and sensors in a smart city environment," EURASIP J. Wirel. Commun. Netw., vol. 2012, no. 1, p. 247, 2012.
[21] T. T. A. Dinh, W. Wenqiang, and A. Datta, "City on the Sky: Extending XACML for Flexible, Secure Data Sharing on the Cloud," J. Grid Comput., vol. 10, no. 1, pp. 151–172, Mar. 2012.
[22] I. B. M. Global, B. Services, and E. Report, "A vision of smarter cities."
[23] F. Gil-Castineira, E. Costa-Montenegro, F. Gonzalez-Castano, C. López-Bravo, T. Ojala, and R. Bose, "Experiences inside the Ubiquitous Oulu Smart City," Computer (Long. Beach. Calif)., vol. 44, no. 6, pp. 48–55, Jun. 2011.
[24] M. Al-Hader, A. Rodzi, A. R. Sharif, and N. Ahmad, "SOA of Smart City Geospatial Management," 2009 Third KSim Eur. Symp. Comput. Model. Simul., pp. 6–10, 2009.
[25] A. Aldama-Nalda, H. Chourabi, T. a. Pardo, J. R. Gil-Garcia, S. Mellouli, H. J. Scholl, S. Alawadhi, T. Nam, and S. Walker, "Smart cities and service integration initiatives in North American cities," Proc. 13th Annu. Int. Conf. Digit. Gov. Res. - dg.o '12, p. 289, 2012.
[26] A. Martinez-Balleste, "The pursuit of citizens' privacy: a privacy-aware smart city is possible," Commun. …, no. June, pp. 136– 141, 2013.
[27] J. Veijalainen, D. Kozlov, and Y. Ali, "Security and Privacy Threats in IoT Architectures," Proc. 7th Int. Conf. Body Area Networks, 2012.
[28] H. Chourabi, T. Nam, S. Walker, J. R. Gil-Garcia, S. Mellouli, K. Nahon, T. a. Pardo, and H. J. Scholl, "Understanding Smart Cities: An Integrative Framework," in 2012 45th Hawaii International Conference on System Sciences, 2012, pp. 2289– 2297.
[29] M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F. Buschmann, and P. Sommerlad, Security Patterns : Integrating Security and Systems Engineering (Wiley Software Patterns Series). John Wiley & Sons, 2006.
[30] A. Bartoli, J. Hernández-Serrano, and M. Soriano, "Security and Privacy in your Smart City," cttc.cat, pp. 1–6.
[31] IBM, "IBM Smarter Healthcare."
[32] A. Ukil, "Connect with Your Friends and Share Private Information Safely," 2012 Ninth Int. Conf. Inf. Technol. - New Gener., pp. 367–372, Apr. 2012.