International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 11 | Nov 2018 www.irjet.net p-ISSN: 2395-0072

Smart City: Overview and Security Challenges

A. K. Pradhan

IEEE Member

Abstract - *Technologies (ICTs) is inextricably linked with the urban development. In last decades, smart cities have become a hope for many of decision makers and people as well to overcome the cumulated urban problems. Internet of Things (IoT) is a paradigm that involves a network of physical objects containing embedded technologies to collect, communicate, sense, and interact with their internal states or the external environment through wireless or wired connections. The nature of IoT information exchange among the connected objects "Things" and remote locations for data storage and data processing gives the ability to collect numerous amounts of data about individuals, and other things in the smart city.*

Key Words: smart cities, Internet of things, authentication, security issues, Radio frequency identification.

1. INTRODUCTION

Smart City has become an umbrella term for numerous technologies with the goal of improving the efficiency of future cities and the quality of life for their inhabitants, not just by introducing new applications but also by making existing processes smarter. It has become fashionable to call cities smart and there are political efforts intended to encourage the development of smart cities [1]. There exist a number of formal definitions of what makes a city smart: Caragliu et al. define "a city to be smart when investments in human and social capital and traditional (transport) and modern (ICT) communication infrastructure fuel sustainable economic growth and a high quality of life, with a wise management of natural resources, through participatory governance." [2]. While others argue that there cannot be an absolute definition as the term smart city does not describe a static concept but rather a process towards more liveable and resilient cities [3], there seems to be agreement that certain novel technologies and applications amount to making cities smarter [4].

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 products.

Fig -1: Generation of Smart City

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 [5]. 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[6].

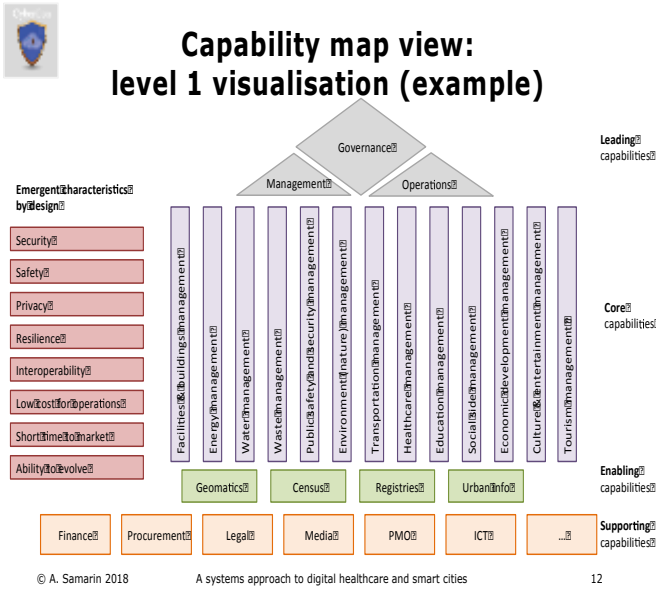

Fig -2: Application of Smart City

3. SMART CARDS

The main privacy issue in smart cards is the logging of transactions. For example, transactions in public transport can disclose spatio-temporal information about the card holder. These mobility patterns can include locations, habits, and visits to sensitive places or events. When data from different users is correlated, possible links between them can also be revealed. Information collected by smart cards can contribute to optimizing public transport schedules, however, it can also be repurposed for advertising, profiling, and

tracking. Separation of authentication and service. Separating user authentication from the service accessed by the user is a step towards providing unlinkability between users and transactions [7]. In some cases, this separation can be achieved by not including identifying information on the smart card, i.e., by using anonymous, pre-paid smart cards. In other cases, for example when the smart card is used to access buildings or to buy discounted bus tickets, the user needs to be authenticated to ensure that they are allowed to access the service. Even in cases where authentication is required, it is not necessary to create a link between user and transaction. Instead, attribute-based credentials allow the system to cryptographically verify certain of the user's attributes (for example, a student or discounted fares attribute would indicate that the user is entitled to discounted bus fares) without revealing the user identity [8].

4. INTERNET OF THINGS

Irjet Template sample paragraph .Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

4.1 RFID tags

Radio frequency identification (RFID) tags are being used immensely in the various components of smart city including smart environment , industry and mobility , etc. It has brought significant benefits in many other areas as well through improving real-time information visibility and traceability. This widespread technology is also prone to many threats and attacks thus making it vulnerable to security . According to the RFID tag is prone to give away sensitive information through unauthorized access, creating problem of data confidentiality and privacy. The problems to data integrity may also occur due to information leakage

4.2 Biometrics

Biometrics is an automated recognition of a person through unique behavioral and biological characteristics. There are two main types of biometric characteristics: physiological and behavioral. Both are acquired by applying proper sensors and distinctive features are taken in use to get a biometric template in authentication process . In fact, it is generally thought that any other substitute to biometrics for identification in integrated security applications does not exists. Biometrics is said to play a key role in information security issues [9], [10], [11] in a smart city. According to Bill Maheu, who is senior director for Qualcomm Government Technologies, every year 3.7 trillion dollars are lost to global frauds, which can be solved sufficiently by implementing biometrics . Biometrics in fact can make various components of a smart city secure with respect to frauds and malicious attacks

Health

_ Education

_ Institution

_ Utility

_ Patrol and security

5. LACK OF FOCUS ON CYBER SECURITY IN SMART CITIES

Even though the fact that cyber security is important has been established; that cyber security is crucial in information heavy environment, cyber security is not one of the primary concerns and considered as a non-challenge in a smart city sphere (Washburn and Sindhu, 2010; Wenge et al., 2014; Pierce and Andersson, 2017). The following section will discuss different reasons for lack of cyber security focus into the category of factors; knowledge and aware- ness, organizational, financial, outsourcing. The reasons for these categories were that there were common identifiable themes throughout the literature that have plausible effects on the consideration of cyber security. Knowledge and awareness category pertains to a more per- sonal level, the perception of individuals, as it is hard to gauge the knowledge and awareness of a complete organisation. The organisational category is then used to catch the non-per- sonal factors and pertains to organisation wide decisions, structure and strategy. The financial category includes factors related to factors more economical in nature, which could potentially lead to a lack of decisions taken regarding cyber security [12], [13]. Finally, the outsourcing category highlights different factors connected with suppliers and contractors.

6. CHALLENGES

Despite its various applications specified in this paper, there are some issues which need attention for its viability. The challenges are presented in Perera etal. and briefly headlined here only for a quick reading.
(a) Architectural Designs, Sensor Configuration, Data Fusing / Filtering, Processing /Storage,Infrastructure, Energy Consumption

(b) Standardization, Accuracy Security and Privacy,

(c) Innovation, Entrepreneurship, Entry Barriers [14], [15].

(d) Sustainability, Licensing, Business Practices, Credibility

(e) Trust, Social Acceptance, Change Management, Awareness

(f) Security and Privacy [13], Safety, Accessibility, Usability, Legal Terms

● *Enable strong encryption*: All communications should be properly protected against unauthorized eavesdropping, interception, and modification. Encryption keys must be well protected and kept in a safe place [16], [17], [18].

● *Secure system administration*: Avoid using a single administrator system user to perform all actions on all systems. Use different administrator users and passwords and grant granular permissions

● *Set strong passwords*: All access to administration interfaces, functionality, etc. should require a user account with a strong password. Passwords policy must be defined for password strength and duration validity. To enhance authentication capabilities, use strong authentication mechanisms (one-time password, certificate- or biometric-based authentication, multifactor authentication, etc.) especially any technology that can impact public safety[19], [20].

● *Remove unnecessary user accounts*: Some solutions come with test/default accounts and passwords that could be used by unauthorized parties to access the systems, if these accounts are not removed. Specific accounts can be created for the implementation process, but these accounts must be removed after the solution is installed and not used for operation purposes. These accounts should be identified in the product and implementation documentations for easy identification and removal.

● *Disable unused functionality and services*: Some solutions have all functionality and services enabled by default. Disabling unused functionality and services reduces the attack surface and prevents possible attacks that abuse weaknesses in those functions and services.

● *Enable auditing of security events*: Constantly monitoring audit logs will help to identify ongoing attacks and breaches.

● *Add anti-tampering, anti-vandalism mechanisms*: Devices should be protected against unauthorized physical access for modification, vandalism, or device stealing.

Malicious Insider threats: Many Cloud service providers do not reveal the clearance and screening procedures of their personnel and how they grant access to the resources of the client organization (Behl, 2011).

Denial of Service Attacks (DoS): Since an outside party is hosting the services on the Cloud, it is often easy for an adversary to extract information about the smart city infrastructure, as its hosted publicly making data publicly accessible [18].

7. CONCLUSION AND FUTURE SCOPE

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] Tarun Dhar Diwan, Durga Chandrakar, Implementation Of Android Based Mobile Phone Search Engine And Live Image Sender, International Research Journal Of Engineering And Technology, Volume: 02 Issue: 03, ISSN: 2395- 0056, June-2015

[2] A. Wood, L. Fang, J. Stankovic, and T. He, SIGF: A Family of Configurable Secure Routing Protocols for Wireless Sensor Networks, ACM Security of Ad Hoc and Sensor Networks, Best Paper Award, October 31, 2006.

[3] S. Munir, J. Stankovic, C. Liang, and S. Lin, New Cyber Physical System Challenges for Human-in-the-Loop Control, 8th International Workshop on Feedback Computing, June 2013.

[4] Somayya Madakam , R. Ramaswamy , Siddharth Tripathi, 'Internet of Things (IoT): A Literature Review' , Journal of Computer and Communications , 2015, 3, 164 -173 Published Online May 201 5 in Sci Res .

[5] http://www.scirp.org/journal/jcc

[6] Alok Kulkar et al, / (IJCSIT), Healthcare applications of the Internet of Things: A Review , International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6229-6232

[7] Andrea Zanella, Internet of Things for Smart Cities, IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 1, FEBRUARY 2014, pp 22-32

[8] J. P. Lynch and J. L. Kenneth, "A summary review of wireless sensors and sensor networks f or structural health monitoring," Shock and Vibration Digest, vol. 38, no. 2, pp. 91– 130, 2006

[9] T. Nuortio, J. Kytöjoki, H. Niska, and O. Bräysy, "Improved route planning and scheduling of waste collection andtransport," Expert Syst. Appl., vol. 30, no. 2, pp. 223– 232, Feb. 2006.

[10] B. Jana and J. Poray, "A performance analysis on elliptic curve cryptography in network security," 2016 International Conference on Computer, Electrical & Communication Engineering (ICCECE), Kolkata, 2016, pp. 1-7.doi: 10.1109/ICCECE.2016.8009587

[11] S. Mitra, B. Jana and J. Poray, "A novel scheme to detect and remove black hole attack in cognitive radio vehicular ad hoc networks(CR-VANETs)," 2016 International Conference on Computer, Electrical & Communication Engineering (ICCECE), Kolkata, 2016, pp. 1-5. doi: 10.1109/ICCECE.2016.8009589

[12] B. Jana, S. Mitra and J. Poray, "An analysis of security threats and countermeasures in VANET," 2016 International Conference on Computer, Electrical & Communication Engineering (ICCECE), Kolkata, 2016, pp. 1-6. doi: 10.1109/ICCECE.2016.8009588

[13] S. Mitra, B. Jana, S. Bhattacharya, P. Pal and J. Poray, "Quantum cryptography: Overview, security issues and future challenges," 2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix), Kolkata, 2017, pp. 1-7. doi: 10.1109/OPTRONIX.2017.8350006

[14] B. Jana, J. Poray, T. Mandal and M. Kule, "A multilevel encryption technique in cloud security," 2017 7th International Conference on Communication Systems and Network Technologies (CSNT), Nagpur, 2017, pp. 220-224.doi: 10.1109/CSNT.2017.8418541

[15] Jana B., Poray J. (2018) A Hybrid Task Scheduling Approach Based on Genetic Algorithm and Particle Swarm Optimization Technique in Cloud Environment. In: Bhateja V., Coello Coello C., Satapathy S., Pattnaik P. (eds) Intelligent Engineering Informatics. Advances in Intelligent Systems and Computing, vol 695. Springer, Singapore

[16] Jana B., Chakraborty M., Mandal T. (2019) A Task Scheduling Technique Based on Particle Swarm Optimization Algorithm in Cloud Environment. In: Ray K., Sharma T., Rawat S., Saini R., Bandyopadhyay A. (eds) Soft Computing: Theories and Applications. Advances in Intelligent Systems and Computing, vol 742. Springer, Singapore

[17] Jana, Bappaditya and Chakraborty, Moumita and Mandal, Tamoghna and Kule, Malay, An Overview on Security Issues in Modern Cryptographic Techniques (May 4, 2018). Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2018 held at Malaviya National Institute of Technology, Jaipur (India) on March 26-27, 2018. Available at SSRN: https://ssrn.com/abstract=3173527 or http://dx.doi.org/10.2139/ssrn.3173527

[18] Jana B., Poray J. (2016) VANET: OVERVIEW, SECURITY ISSUES AND CHALLENGES, International Journal of Engineering Research-Online, Vol-4, Issue-2, Pages-451-459, http://www.ijoer.in

[19] M Chakraborty B. Jana, T. Mandal and M. Kule, " An Performance Analysis of RSA Scheme Using Artificial Neural Network " 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)), Bengaluru, 2018, dOI: 10.1109/ICCCNT.2018.8494032

[20] Mandal, Tamoghna & Jana, Bappaditya. (2018). A Study on Risk Assessment in Information Security. SSRN Electronic Journal. 10.2139/ssrn.3261593.

[21] S. Mitra, B. Jana and J. Poray, "Implementation of a Novel Security Technique Using Triple DES in Cashless Transaction," 2017 International Conference on Computer, Electrical & Communication Engineering (ICCECE), Kolkata, India, 2017, pp. 1-6. doi: 10.1109/ICCECE.2017.8526233