Exploration of Solutions for Smart Cities: Challenges in Privacy and Security

Adnan Jannat[1], Ahsan Ilyas[2], Tariq Saeed[3], Ahsan iftikhar[4], Anum Zahra[5], Dr. Atif Raza Jafri [6]
[1, 6]Cyber Reconninance and Combat (CRC) Lab, Bahria University, Islamabad, Pakistan
[1, 2, 3, 4,5, 6]Depertment of Electrical Engineering, Bahria University, Islamabad, Pakistan
[6]Dean Faculty of Engineering Sciences, Bahria University, Islamabad, Pakistan
Engr_adnan@yahoo.com[1], what.why.if@gmail.com[2], kk_tariq@hotmail.com[3], ahsaniftikhar9@gmail.com[4], anum140147@gmail.com[5], atifraza.buic@bahria.edu.pk[6]

***Abstract*— Smart cities are improving the urban quality of life. The cities are providing more and more facilities to enhance the living standards of city residents. Implementation of smart cities has improved the services provided by various urban systems. Out of the various challenges being faced by smart cities, most important are the privacy / security of its residents and sanctity of data systems. Traditional cyber security protection policies cannot be applied directly to smart city applications. Furthermore, it is important to identify these cyber threats so as to design and implement effective countermeasures. In this paper we will focus on current measures being taken to counter privacy and security threats to smart cities, identify limitations of these measures and also present future trends in this field. This research allows users of the domain to select an appropriate technology for relevant security threat and to design smart cities application according to their needs.**

Keywords– Smart Cities, Privacy and Security, Internet of Things (IoT).

I. INTRODUCTION

Current trends indicate massive informatization and urbanization across the globe. Due to industrial revolution, urbanization has increased manifolds and as of the year 2015, approximately 52% of the world papulation is living in urban areas [1]. According to the United Nation (UN) experts, it has been analyzed that in the year 2050, almost 6 billion people will be residing in the cities and 70% of energy resources will be consumed by the urban community [1]. World is witnessing a technological revolution where information is more important and prior then the material and energy resources. The Information Communication Technology (ICT) is a big breakthrough in ensuring efficient utilization of energy resources and digitalization of the world [2]. Consequently, the smart cities transfer information (Big data) by effective utilization of energy resources [3]. Additionally, it also provides efficient management system by integrating government and market to create business friendly and comfortable living environment. Many advantages are offered by smart cities, however, the key challenge that it faces is the privacy and security issue [4]. It thus requires countermeasure to mitigate this problem so as to ensure that user data is secure.

Among several others, Smart city is one of the emerging research areas as it drives efficient provisioning of connectivity with recently developed technologies and specially Internet of Things (IoT. Due to its requirement for the connectivity of several devices, processing big data in an efficient way is the core characteristic of smart city. In current modern world, many countries have developed intelligent strategies for functioning of smart cities. In year 2017, Cisco announced to invest one billion US dollars in smart cities. China, world's largest population, has around 200 projects of smart cities in progress [5]. Using IoT based infrastructures, various issues pertaining to smart cities applications such as building, home automation, transportation, health care, smart environment, waste management, traffic control, administration and many more have been addressed. However, with the advent of all these smart city applications, one of major challenge is the privacy and security issue due to vulnerabilities in every layer of smart system application. Intrusion attack is an unauthorized access to the system such as acquiring user personal data, launching Denial of Services (DoS) attacks and degrading the quality of intelligent services [6]. At present, cyber security is one of emerging challenges and has lots of research opportunities in IoT based smart applications [7]. Furthermore, IoT is the backbone and key source of information in smart city. The IoT based devices generate data specific to the application and also retrieve data from the source and destinations [8]-[9]. Summarizing, IoT based infrastructure is essential for the computations of required operations and thus also helps in various applications of smart cities development [10]. Additionally, it is also required to countermeasure for privacy and security problem to make efficient use of smart facilities.

The foremost objective of smart cities is to provide benefit to its resident. Smart cities have many sub applications; however, we will target eight applications in this paper as shown in fig.1 [4]. Smart government refers to provisioning of government services in best possible manner to the community [11]. Second is smart environment that ensures sustainable society with the capability to monitor energy consumption, quality of air and structural integrity of buildings [12]. Smart health care provides health care facilities at doorsteps of city residents [13]. Smart transportation gives intelligent traffic network thus

2020 IEEE 23rd International Multitopic Conference (INMIC) | 978-1-7281-9893-4/20/$31.00 ©2020 IEEE | DOI: 10.1109/INMIC50486.2020.9318070

enhancing secure, faster and efficient transportation system. Smart homes have helped integrate all sorts of home appliances like air conditioners, lights bulbs, home security and many more things for efficient management. Smart villages concept is also surfacing to mitigate the rural urban divide. Smart traffic control is used to monitor and control the flow of automobiles on roads junction. Smart management ensures energy, water management, smart energy metering [14] and also smart grid management to monitor the distribution of energy resources [15]. Consequently, all these applications help in provision of comfortable living to their users.

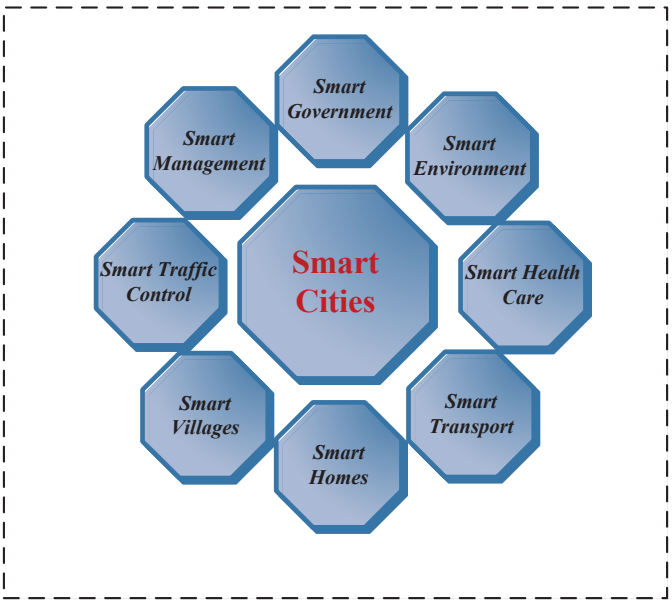

Fig. 1. Application of Smart Cities

All these applications are prone to various malicious attacks, such as DoS, probing, DDoS etc. [4]. With rapid development of information and communication technology, the hacker's community is also becoming smarter and is also developing the strategies to evade the existing detection apparatuses. Therefore, these privacy and security challenges encourage researchers to develop technologies for protection of important data of smart cities [6]. Additionally, to mitigate the privacy and security challenges in functioning of smart cities, we need to comprehend the identified problems and current available solutions. The main purpose of executing this study is to answer following two research questions.

Research Question 1 (RQ1): In terms of the applications of smart cities, what are the identified threats pertaining to privacy and security? Study will focus research undertaken between 2017 to 2019.

Research Question 2 (RQ2): What are the flaws in currently available solutions to address these privacy and security threats to smart cities?

The paper covers background along with relevant literature review in Section II. The current challenges of smart cities and proposed solutions are given in Section III. Discussions and answers to the research questions are provided in Section IV. Finally, conclusion of the paper will be presented in Section V.

II. BACKGROUND LITERATURE ANALYSIS

Smart city is one of the subsets of Information and Communication Technology. It can be employed in various applications i.e., home appliances, transportation, environment systems, security development systems, health cares and several others. In order to operate these applications in practical environment, IoTs are commonly involved [9]. In implementation of smart cities, data security is one of the key problems and to overcome these security issues, many protection methods have bene proposed. Consequently, the present hi-tech solutions, for the development of smart cities, are described in [1]–[3], [5], [16] & [17] whereas privacy and security concerns are covered in [4], [6], [7] & [18].

From different geographical locations, several continents such as Asian, American and Europeans implemented the concept of smart cities to moderate their cities. Among Asian countries, China has implemented smart city concept in two distinct phases, as provided in [3]. Out of these two, the first one is 1.0 that is constructed by increasing the network bandwidth and operate on new generation of information technology i.e., broadband and 4G. In the second phase 2.0, they have operated smart city on the big data. In both the phases, cloud computing and IoTs are used to control the operational functionalities of deployed smart cities. Additionally, the concept of machine learning is also used in their second phase. One of the deployments by U.S Society of Heating, Refrigerating and Air Conditioning based on Building Automation and Control Network (BACnet) is presented in [16]. They deployed their solution based on the concept of pentagon and also tested advance methods in research labs to prevent the building from earthquake and also detect harmful chemical substance in air duct.

The deployment described by the Europeans, presented in [2], discusses two different scenarios i.e. one for smart airport and another is for smart homes. For smart airport, an Italian Linate Airport in Milan city, has been modernized by using the IoTs infrastructure to manage the water and energy usage. For smart home-based solution, the authors of [2], marked Greece for metering the different water and energy consuming devices. All these applications of smart cities attract cyber hackers, such as in year 2015 about 230K citizens of Ukraine suffered a long electricity outage due to hacking of power grid system [18].

The top five cyber security hacks in smart cities systems during 2002 -2015 are describe in [19]. In year 2015, systems of USA Office of Personnel Management were hacked as hackers breached more than 5.6 million fingerprint images of people seeking security clearances. During the year 2006 group of hackers targeted the Church of Scientology and even hacked US President's website. The attack named as Gary McKinnon which was executed in year 2002 gain unprecedented access to US military computers and NASA. Hacker posted a massage on a military website "your security is crap" [19]. So, it can be stated that ICT equipment are prone

to various privacy and security threats. Resultantly, smart city users need trustful and secure systems to ensure that privacy and security is not compromise.

III. The Current Challenges of Smart Cities

A. Architecture for IoT Based Smart City

For continuous advancement in system's infrastructure of smart cities, various architectures have been proposed [4]. Fig. 2. Shows basic architecture for smart city applications based on IoTs. The architecture is based on four layers which are described below:

Application layer: The first layer of IoT based architecture which directly belongs to the user-based application of smart cities like smart government, smart environment and smart heath care etc.

Support layer: The Second layer after application layer is support layer which is closed to application layer. This layer provide support to the applications for intelligence computing technique like edge and cloud computing.

Network layer: This layer acts as core of the IoT based architecture for smart cities. Which is provide network interface to IoT device over the internet or Wireless local area network (WAN). This layer is responsible to connect the smart objects, devices and various servers.

Recognition layer: This is the last layer which is also called sensing or perception layer. which is directly communicate with smart city infrastructure and collect data from real world applications through sensors.

Additionally, all these above mention layers for IoT based architecture is used in all kind of smart city applications. However, privacy and security issues vary application to application which is unsecure the user personal data and also damage confidentiality and integrity of smart system.

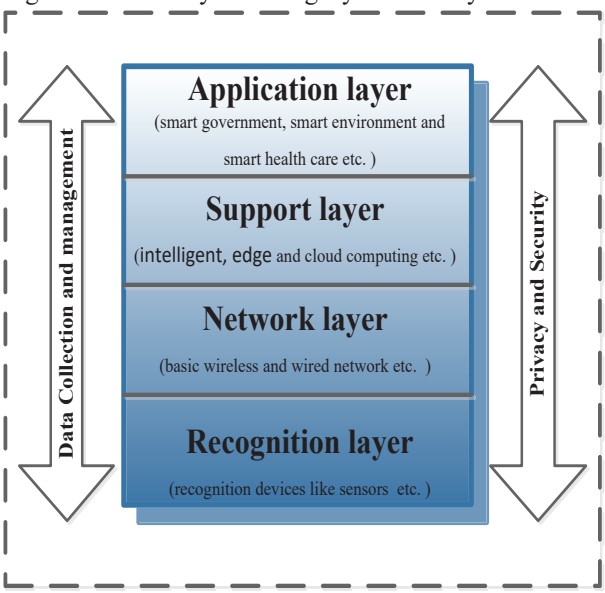

Fig. 2. Architecture for IoT Based Smart City

B. Privacy and Security Problems and Solutions

Various privacy and security threats have been identified such as collusion attacks, spam attacks launched on smart cities infrastructures. Security countermeasures are taken by encryption, intrusion detection and prevention techniques etc. Targeted applications, problems and relevant solutions for privacy and security threats are as shown in Table 1. Column 2 of Table 1 describes specifically the targeted smart city applications such as smart heath, vehicles, transportation and cards etc. referred from [4]-[7], [20]-[32]. Column 3 of Table 1 provides data on privacy and security threats to different applications. Threats vary according to applications. Column 4 of Table 1 gives detail on new technological solution against the mentioned privacy and security threat. Study identifies that machine leaning, intrusion detection system, cryptographic algorithms and blockchain technologies are the recent solutions to the privacy and security threats mentioned in [4]-[7], [20]-[32]. Consequently, cryptographic algorithms are identified as back bone for protection against malicious attacks. Most frequently utilized security and privacy protection is blockchain technology which provides decentralized features and enables the application to operate in distributed manner.

IV. Discussion and Emerging Trends

Study highlights various security and privacy concerns in employment of smart cities. It also identifies various countermeasures being taken to ensure sanctity of important data and also to ensure consumers privacy.

Answer of RQ1: Research reveals that cyber threats to smart cities vary from application to application. However, main focus remains in ensuring the sanctity of consumer's data. Hacker's threats cannot be overlooked. New advancements in cyber security measures, such as machine learning and cryptographic algorithms, are being employed to counter these threats, however, at the same time the hacker's community is also gaining new potentials to exploit the vulnerabilities. Providing optimal security against such threats is thus a continuous process.

Answer of RQ2: Research focused on various solutions proposed to counter the cyber threats and identified various flaws in their employment for smart cities applications. Research proposes new emerging technologies like cryptography algorithms, blockchains and biometric solutions to overcome new privacy and security concerns. These solutions provide secure data handling and ensures sustained integrity of smart service users.

TABLE I. TARGETED APPLICATIONS, PROBLEMS AND RELEVANT SOLUTION FOR PRIVACY AND SECURITY THREATS

Sr. No	Targeted Smart City Application	Privacy and Security Threats	Technological Solution	Ref. No
1.	General Smart city application	Data mining	Encryption-based technologies	[4]
2.	General Smart city application	Public security	IoT based solution	[5]
3.	Intelligent healthcare, transportation, and smart energy.	Leakage of patient data	Homomorphic encryption	[6]
4.	Network based applications	Cyberspace security problem	Intrusion detection, and threat intelligence sensing.	[7]
5.	Smart vehicles	Security of communications (devices / mediums that support message exchange)	Multi-layered security encryption	[20]
6.	Smart card	Leakage of sensitive data	Blockchain technology	[21]
7.	Blockchain-based business applications	Leakage of sensitive data	Blockchain technology	[22]
8.	Cyberinfrastructures	Cyberspace security problem	Blockchain technology	[23]
9.	Smart homes, personal monitoring devices	Attack threats in IoT	Firewalls and intrusion detection systems	[24]
10.	Smart Homes	Data acquisition and information processing security	Hash-based and MAC-based authentication	[25]
11.	Smart vehicles	Cloud services, security issues	Machine Learning based Intrusion Detection System	[26]
12.	General Smart application	Malicious smart applications	Artificial intelligence	[27]
13.	Cryptocurrency applications	User data leakage	Blockchain technologies	[28]
14.	Smart environments	Security threats	IoT based Intrusion detection systems (IDSs)	[29]
15.	Cryptocurrency applications	Threats of hackers	Blockchain technologies	[30]
16.	General Smart city application	Security threat from theft,	-	[31]
17.	Smart health	User data security concern	Cryptographic primitive	[32]

V. Conclusion

Smart cities promise provision of many facilities to its resident. One of the major challenges in smart city is to secure the user data from unauthorized access. So, researchers are focused on privacy and security of smart city applications. To counter ever growing threats to smart cities systems, three major technological solutions are cryptographic algorithms, biometric and blockchain technology. In recent years, these technologies have provided the efficient solution for privacy and security threats to smart services. Out of these technologies, cryptographic algorithms provided the best solution. Whereas, blockchain has been employed most frequently to address these concerns. The concept of smart cities is the emerging trend for future technology. This paper helps the researcher to quickly understand the current state of the art privacy and security issues and trends in smart cities implementation.

References

[1] S.Musa, "Smart cities A road map for development," IEEE Potentials, 2018, pp. 18-23.

[2] M. Guo, Y. Liu, H. Yu, B.Hu, Z. Sang, "An Overview of Smart City in China," China Communications, 2016, pp. 203-211.

[3] E.Curry, et-al., "Internet of Things Enhanced User Experience for Smart Water and Energy Management," IEEE Computer Society, 2018, pp. 18-28.

[4] Jones and Lawrie "Securing the smart city," Engineering & Technology. vol.11, pp.30-33, 2016.

[5] Golias et al., "Challenges, Risks and Opportunities for Connected Vehicle Services in Smart Cities and Communities," IFAC-PapersOnLine, vol. 51, pp. 139-144, 2019.

[6] L.Purohit and S. Kumar, "Web Services in the Internet of Things and Smart Cities," IEEE Consumer Electronics Magazine, 2019, pp. 39-43.

[7] D. Snoonian, "Smart Buildings," IEEE Spectrum, 2003, pp. 18-23.

[8] Eckhoff et al., "Privacy in the smart city—Applications, technologies, challenges, and solutions," IEEE Communications Surveys \& Tutorials, vol. 20, 2017.

[9] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," IEEE Commun. Mag., vol. 55, pp. 122-129, Jan. 2017.

[10] Cui, Lei and Xie, et al, "Security and privacy in smart cities: Challenges and opportunities," IEEE access.vol. 6, pp. 46134-46145,2018.

[11] J. R. Gil-Garcia, "Towards a smart state inter-agency collaboration, information integration, and beyond," Inf. Polity, vol. 17, pp. 269-280, 2012.

[12] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," IEEE Internet Things, vol. 1, pp. 22-32, Feb. 2014.

[13] M. J. Mudumbe and A. M. Abu-Mahfouz, "Smart water meter system for user-centric consumption measurement," in Proc. IEEE 13th Int. Conf. Ind. Inform. (INDIN), Jul. 2015, pp. 993-998.

[14] N. Khan et al., "Wireless controlled smart digital energy meter and theft control using GSM with GUI," International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), 2018,pp.1-6.

[15] L. Catarinucci et al., "An IoT-aware architecture for smart healthcare systems," IEEE Internet Things J., vol. 2, pp. 515-526, Dec. 2015.

[16] Xie et al., "A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges," IEEE Communications Surveys \& Tutorials, vol. 21, pp.2794-2829, 2019.

[17] Mora et al., "A Use Case in Cybersecurity based in Blockchain to deal with the security and privacy of citizens and Smart Cities Cyberinfrastructures," IEEE International Smart Cities Conference (ISC2),2018, pp.1-4.

[18] Celik et al., "Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities," ACM Computing Surveys, vol. 52, pp. 1-30, 2018.

[19] Batalla et al., "Secure smart homes: Opportunities and challenges," ACM Computing Surveys (CSUR), vol. 50, pp.75, 2017.

[20] Aloqaily et al., "An intrusion detection system for connected vehicles in smart cities," Ad Hoc Networks, vol. 90, pp. 1-25, 2019.

[21] Braun et al., "Security and privacy challenges in smart cities," Sustainable cities and society, vol.39, pp. 499-507, 2018.

[22] Ehrenberg et al., "Blockchain in Context," Information Systems Frontiers J., pp.1-7, 2019.

[23] Elrawy et al., "Intrusion detection systems for IoT-based smart environments: a survey," Journal of Cloud Computing, vol. 07, pp.21, 2018.

[24] M.Niranjanamurthy et al, "Analysis of Blockchain technology: pros, cons and SWOT," Cluster Computing, pp.1-15, 2018.

[25] Rao et al., "Impact of 5G technologies on smart city implementation," Wireless Personal Communications, vol. 100, pp.161-176, 2018.

[26] Zhang et al., "Towards privacy protection and malicious behavior traceability in smart health," Personal and Ubiquitous Computing, vol.21, pp.815-830, 2017.

[27] Razzaq MA, Gill SH, Qureshi MA, Ullah S., "Security issues in the Internet of Things (IoT): a comprehensive study," International Journal of Advanced Computer Science and Applications. vol. 8, pp.383, 2017.

[28] Razzaq, "Internet of Things (Iot) Applications An Overview," International Journal of Computer Science and Emerging Technologies. vol. 1, pp. 43-48, 2017.

[29] Razzaq MA, Mahar JA, Qureshi MA, Abidin Z., "Smart campus system using internet of things: simulation and assessment of vertical scalability," Indian Journal of Science and Technology. vol.13, pp. 2902-2910, 2019.

[30] K. Zetter, "Inside the cunning, unprecedented hack of ukraine's power grid," Wired, Mar. 2016. [Online]. Available: http://www.wired.com/ 2016/03/inside-cunning-unprecedentedhack-ukraines-power-grid.

[31] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," IEEE Commun. Mag., vol. 55, pp. 122-129, Jan. 2017.

[32] Wu, Jiang-xing,et al., "Security for cyberspace: challenges and opportunities," Springer, 2018.