International Journal of Computing and Network Technology
ISSN (2210-1519)
Int. J. Com. Net. Tech. 7, No. 1 (Jan-2019)

http://dx-doi.org/10.12785/ijcnt/070103

A Secure and Privacy-Aware Framework for Future Smart Cities

Kahkashan Tabassum[1] and Ahmed Ibrahim[2]

[1,2]*Dept. of Computer Sciences, CCIS, Princess Nourah Bint Abdulrahman University, Kingdom of Saudi Arabia*

Received: 3 Sept. 2018, Revised: 21 Dec. 2018, Accepted: 27 Dec. 2018, Published: (1 January 2019)

Abstract: Smart cities has developed in urban areas and are interconnecting every part of the city and offering enormous smart services to make the human life easier and convenient. The smart services are a result of data streams connecting the smart cities including citizen information, smart activities of the individual facilitate smart transportation, surroundings and also access to their information through local government portals for their own data. These huge amounts of data gathering and processing increases privacy preservation and security limitations and challenges at individual and social levels. Therefore it is required to ensure data security and privacy preservation to the stored citizens' data. But these issues are not only restricted to citizens' or stakeholders alone rather pervasive to service providers (SPs) and governments with their own databases. This research paper is an attempt to identify the issues and challenges of the privacy and security for ensuring that proper services are provided to the participants in smart city activities. This paper presents a secure and privacy-aware framework for offering efficient services in smart cities. The proposed model of smart cities ensures the stakeholders' privacy and integrity of services such as avoiding misuse of public data malicious SPs.

Keywords: Internet of Things, Cyber security, Smart Cities, Privacy and Security.

1. INTRODUCTION

Smart cities are developing rigorously due to the huge multiplication of Internet of Things (IoTs) or smart devices. These devices can be interconnected to provide solutions to many critical problems and include sensors, RFIDs, actuators, smart mobiles, wearable sensors, fog computing, cloud computing, etc. The smart city applications are gathering large scale data effectively to provide information awareness and planning, procedures and decision making for the smart city governance in order to manage data from local agencies and other departments. Cyber physical systems (CPS) [3] are required to maintain security of the systems in a society and comprises of the devices such as a number of Internet of Things (sensors, smart devices, smartphones, etc.), which work together to achieve a common objective[12] . CPS or IoT devices are very essential and are employed in different areas power grids, medical industry, smart forensics, drug discovery, commercial and business applications, healthcare systems, demand and supply management in markets and stock exchange, public safety, smart transport systems, smart homes, smart parking and more. All the smart devices are capable of elevating the quality of life and at the same time can reduce power consumption hence utilizing the resources effectively. Since the CPS are evolving rapidly, exceptionally new research applications are finding entry in this field due to the rise of IoT devices. But the critical side of this development is the growing privacy and security demands to successfully deploy, monitor, utilize, protect against the illegal attacks and manipulate these smart devices. This paper will focus on the protection and security issues of the IoT devices. The related research [13] states a factual scenario of denial-of-service attacks in distributed environment by smart devices. Smart city infrastructure is a diverse future application based on integrated highly smart IoT ,devices which is emerging and will have a tremendous success and great benefit in future if proper privacy and security could be implemented on these systems [14][15].

Cyber-technology is always developing and becoming more complex, and as new cyber-technology is invented security risks always follow. IoT is one such example of this case and as IoT is developing new cybersecurity has to be developed along with it. This article will explore IoT cybersecurity over a broad spectrum and then take more specific examples. It will also discuss IoT cybersecurity's greater implications and the security being developed to combat 3rd party attacks on IoT devices, such as hardware-assisted security, cyber-physical security, and virtualization. The article will explore different points of view on security and accountability, such as user accountability and IoT provider accountability. Section 2 discusses the perspectives of few articles about existing cyber secure systems. The remaining contents of this paper are arranged in the following manner: Section 3 deals with possible

E-mail: ktosman@pnu.edu.sa, azibrahim@pnu.edu.sa

stakeholders, how they can benefit from security solutions, briefly introduces smart cities and associated data security challenges. The Hybrid Smart Secure Service Framework is presented in Section 4. Section 5 concludes the paper along with future work.

2. LITERATURE SURVEY

This section provides the summary of the cyber physical systems and studies the aspects that are useful for providing security to heterogeneous systems from various point of view. The article in [1] explores IoT cybersecurity on a large spectrum. The authors define IoT and discuss what it is and its bigger implications. The researchers mention many algorithms, such as Advanced Encryption Standard (AES) and International Data Encryption Algorithm (IDEA), and they discuss how these algorithms can be used to secure ingoing and outgoing data. The authors discuss how Cryptography is an emerging science where IoT is concerned and they show how it is developing. They show how most the algorithms to secure IoT come under cryptography and how cryptography can be used to secure IoT Data.

The [2] explores how the most prominent smart home devices can be digitally attacked by personal and corporate users to acquire compromising information on the users of the IoT devices. It discusses several types of adversaries, forensic passive, forensic active, and real-time active. The researchers found that even the passive adversary had a variety of data available to the adversary. Data through which the adversary could pinpoint the actions or the location if the user targeted in the attack. The researchers explored how these data extraction techniques were used in real-life legal situations and the ramifications of their uses by mentioning some legal cases where passive adversaries were used as substantial evidence.

The [3] discusses the advancements made in Cyber Physical Systems (CPS), and how it has severe implications on user security. The researchers argue that privacy risks are a natural consequence of technological advancement, but these risks must be minimized as best as possible by developing new systems to combat security risks and adapting with the new ways invented to capitalize on privacy issues. The researchers show some ways to combat exploitation of the previously mentioned privacy issues. They also mention some devices that transmit data in CPS, the security issues with them (such as developing full system security instead of single-layer security), and ways to combat those issues.

The [4] aims to provide a categorization system for the different aspects of a smart city, their security risks, and proposed solutions to the security risks. The existing best practices regarding smart city security are discussed and analyzed with respect to their performance. The authors also analyze an IoT testbed for smart cities architecture and discuss their findings regarding the analysis. The authors also weigh how the conveniences and promises of a smart city may be undermined because of security risks. They also discuss how a smart city should keep the balance between security and people's rights to freedom and expression of thought. The researcher's point of view is to hold the government implementing smart cities accountable for any mishaps and they hold the government implementing the smart city responsible for its security.

Whereas [3] discusses how cyber security issues can be minimized from an aspect of combating security issues as a natural consequence of technological advancement, [5] argues that a part of the burden of security should fall on the shoulders of the government. It shows how neoliberalist governments shove the responsibility of this issue on the users, while merely giving said user's advice on how to combat this issue and leaving them to fend for themselves. The researchers discuss whether it is reasonable or judicious to do this, and they ultimately conclude that it is unreasonable and injudicious to do so. They base their conclusions on cases they have thoroughly studied. The researchers suggest a proposal for a risk regulation regime that would more effectively mitigate and ameliorate cyber risk.

While almost all the papers so far discussed security threats because of the actions of a government, a third party (hacker), or even the user, this article [6] explores if the devices themselves can be trusted. The authors say that in our daily lives all the "smart" devices we use may need to work together, yet if these devices are made by competing vendors or brands it could be hard to interoperate them, which could cause many issues. Third parties seeking a user's information could use these issues and errors to access the user's information. The researchers argue that wide-scale system updates could put devices in a vulnerable position, and these problems cannot be solved until everyone agrees on one system architecture and everyone agrees on what an IoT device constitutes. These problems are caused by heterogeneity, which is good for a country, but in respect to IoT it causes severe problems. The researchers conclude that, in their point of view, it may be impossible to solve these problems unless one IoT provider has a monopoly over IoT devices, but the problems of an IoT monopoly outweigh the benefits.

Article [7] shows why normal security can't be applied to most IoT devices and also proposes a workaround for this problem. The authors introduce a middleware layer that connects IoT devices to the global Mobility First network. They propose an IoT name resolution service (IoT-NRS) as a core component of the middleware layer and develop a lightweight keying protocol that establishes trust between an IoT device and the IoT-NRS. This security system will remain lightweight and secure even though it may have to involve a third party. Therefore, the 3rd party must be verified and trusted to accomplish the goals of the security system.

Paper [8] discusses IoT security, assisted by hardware. The authors say that hardware-assisted techniques indeed offer an additional layer of protection with respect to traditional software-only cybersecurity. The researchers recognize that IoT requires a lightweight security system for flexibility and ease of use, and they come through by proposing some hardware-assisted security techniques that they believe meet security criteria. They show how these security techniques have stood up against multiclass security attacks, but they admit that it will take much more time and hard work to develop a lightweight hardware-assisted security system that meets security criteria.

Hardware itself can be used as a security device for IoT devices in specific fields. The [9] shows how Industrial IoT is vulnerable to cyber-physical attacks and how they might be secured. The authors investigate and compare two security technologies that provide isolation and a secured execution environment: ARM TrustZone and Security Controller. They find the TrustZone based approach promises greater flexibility and performance, but only the Security Controller strongly protects against physical attacks. However, the researchers propose the hybrid use of these two hardware security systems for the best industrial security against cyber-physical attacks.

The [10] discusses how hardware security's infrastructure might be flawed. It also shows how hardware-assisted security has been implemented in domicile systems, and even the automobile industry. To better serve security need the authors propose virtualization technology, which is an up and coming type of IoT security. The authors propose the adaptation of ASMI (Architectural Support for Memory Isolation—a general architecture available in the literature for the improvement of the performance and security of virtualization technology) on the popular MIPS (Microprocessor without Interlocked Pipeline Stages) embedded virtualization platform, which could be adopted in embedded virtualization architectures for IoT devices. The authors show the security enhancement by combining this with existing architectures.

3. Security Challenges in the context of Smart Cities

This section will explain the impact of Smart cities on consumers/stakeholders, different challenges associated with IoT deployment for the smart city development, identify the data generated while managing and controlling smart cities, identifies service challenges to set-up appropriate security measures and possible solutions

3.1 Stakeholders Roles:

To support the perspectives of various stakeholders at application level, the data security and privacy aspects are required to be framed with respect to their convenience. Eight major stakeholders' roles could be identified in the smart city information security repertoire depending on their direct or indirect involvement in smart city development. Although exhaustive, these roles use appropriate tools to define role-based policies for information access, the eXtensible Access Control Markup Language [18].

These roles are Service Consumers, Legitimate Service Providers, IT Experts, Data custodians (public security agencies), Untrusted Service providers, standard governing bodies and domain experts as shown in Onion Model [3] given below fig. 1.

3.2 Privacy and Security in Smart City

Due to the fast rise of Smart cities and Internet of Things (IoTs) or smart devices, the smart city applications are collecting large scale data effectively to provide sensitive information awareness and planning, policies and decision making for the smart city governance in order to control data of local agencies and other departments. Storing and processing large scale data by provisioning of cloud based virtual storage to improve quality of service requirements of end user. But these opportunities have open new challenges and threats to data protection. The urban governance models established due to the popularity of smart cities have created new decline in the device privacy and data confidentiality when the data communication occurs among different devices. In [15] the authors argued privacy issues for stakeholders and cloud security issues, which are propagated to contribute further intricacies and complexities in dealing with data security of Smart Cities. The report of Symantec Internet Security estimated an amount of 22% and 24%

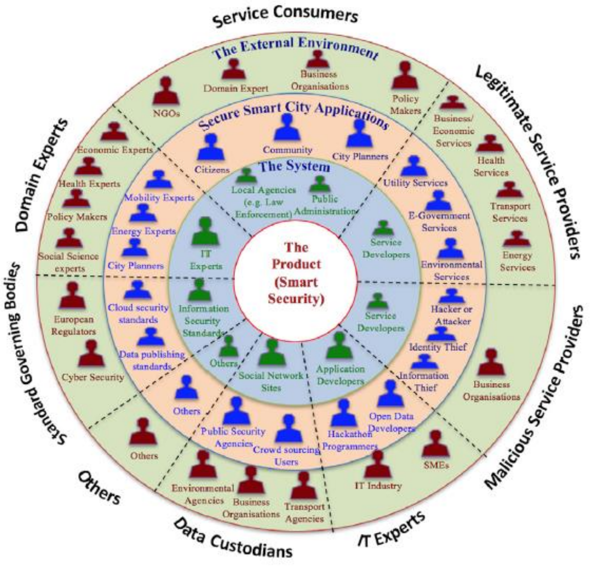

Figure 1. Onion Model for Smart City consumers

Attacks were targeted towards government utilities sector and government healthcare sector respectively. Thus the smart cities cannot compromise security and privacy of the its citizens/ habitants as their data will be at risk. Not only this service providers also have threats of cyber security, attackers gain illegal access to inhabitant services. The types of attacks could be more and dangerous ranging from attacker injecting malicious information or impersonating legitimate subscribers to access private as well as confidential data. Therefore it is recommended to have secure transition to a strong and robust smart city by forming a risk compliant, proactive, providing user authentication, secure services administrator based governance framework[16]. These concerns guides the governments towards creation of towards a useful maturity model of secure service provisioning in smart cities with rules and regulations. Also the research in [17] focused on trust challenges apart from privacy and security of smart cities when using ICT, instead it is identified that these are attributed due to the distribution of IoTs. Firewalls cannot protect the data since wireless channels can face attacks. IoT devices are wireless and can even be stolen by attackers, could be analyzed and hence more vulnerable to attacks. This situation gives rise to developing new strategies to avoid and overcome such issues. The interconnection of devices within smart cities, for instance traffic connections, energy grids, etc. may create mysterious vulnerabilities in the smart city systems. These require complex security solution s since they are initiated by complex distributed systems using complicated access control, encryption and authentication process. Finally, interoperability adds to all these vulnerabilities and makes privacy and security more challenging.

4. A Smart Secure Service Framework for Smart City

This paper proposes a hybrid strategy developed based on existing security frameworks in literature. To accomplish this approach we begin by analyzing the existing solutions that suffer with the vulnerabilities, challenges and limitations associated with smart cities data security. The approach will propose a solution to provide security in the smart cities. Although very complex, the solution can be attempted and can be made successful by developing a framework or model for data protection and security. The proposed provisional secure system under development will divide the security protection at macro level to separate and traceable protection based portions within the smart city systems. Therefore, the different security and protection processes of authentication and detecting data anonymity are applied on smart devices, at every service provider level. To verify the success of security architecture for selected components, a scenario based model verification technique is used[3].

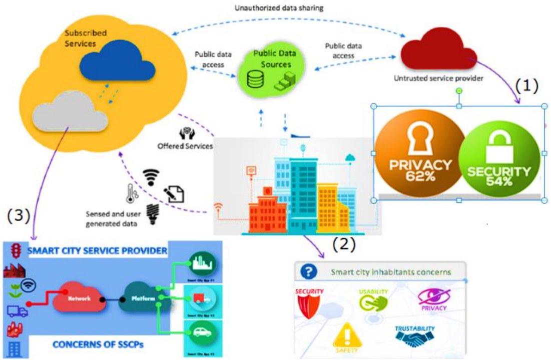

Figure 2. Security and Privacy Considerations in Smart City

The figure 2. Outlines the main concerns for developing a secure smart city. The hybrid model will consider to resolve the privacy and security issues by dividing problem into three parts. 1) Privacy and security of Stakeholders/ Consumers individually 2) The security issues related to the Smart City participants and 3) The privacy and security issues for Service Providers.

The structure of the Smart City Security Layer consists of the Consumer/Stakeholder (2 or 3) requesting a particular service, this is followed by generation of a secure code to access the service requested. The generated code is then used to access the service. The security code creation uses advance Hashing method (double hashing) and is supported by Universal Hash functions.

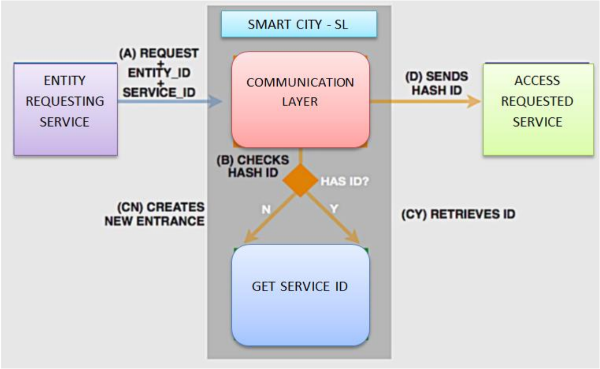

Figure 3. Secure Smart City Layer

The Secure Smart City Layer in figure 3 is the concept involved that allow changing identifiers to perform communication within the system relation. The layer has an entity requesting a service, could be a citizen/any stakeholder/consumer/ sensor. It has a service representing service requested from the entity. A Communication Layer, which is a link from entity to service, exchanges identifier between entity and the services within the service. The figure 3 represents four data main communications as follows:

A. Represents the access to information/service from various applications. In this situation, the attacker can also send ID along with legitimate senders and it has to be resolved by applying encoding and comparison of ID.

B. Information/Service Tracking, although its difficult to isolate the actual service ID from the many received due to attacks.

C. The inhabitant/citizen tracking through Smart City – SL is difficult, therefore the citizen tracking is challenging to the attacker.

D. Inhabitant/citizen Data loss: The strength of OAuth, OpenID, and SAML standars section for

Authentication and interoperability, the (D) is not so much affected.

The hash-code generated during this process of request of service and access of service will be used to maintain end-to-end security for the Smart City-SL.

CONCLUSION

This paper have highlighted security and privacy issues for smart cities, including the smart city participants, stakeholders. The security and privacy threats with the service providers' perspective, impact on government bodies, IoT devices interconnectivity and interoperability have been presented. Based on the analysis of these risks of threats a hybrid service framework for secure smart city is proposed.

It implements end-to-end security and privacy for the provision of secure services in smart cities.

The rise of IoT devices that are being deployed in Smart Cities is rising enormously. In the future work we will identify other smart devices which can aid in smart business, smart health, smart homes, smart forensics, smart transport, and those used in battlefields and Military, determine the privacy and security related issues in their respective domains. The advance work will integrate the hybrid model of privacy and security provisioning with a potential extended component to automate the determination, utilization and manipulation of vulnerabilities in a extensive range of smart policies for deploying smart devices.

REFERENCES

[1] Shivaji Kulkarni, Shrihari Durg, Nalini Iyer, "Internet of Things (IoT) security" IEEE, pp. 821-824, 2016.

[2] Quang Doa, Ben Martinia, Kim-Kwang Raymond Choo, "Cyber-physical systems information gathering: A smart home case study", ELSEVIER Computer Networks, vol. 138, pp. 1–12, 2018.

[3] Yosef Ashibani, Qusay H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions", ELSEVIER computers & security, vol. 68, pp. 81–97, 2017.

[4] Sidra Ijaz, Munam Ali Shah, Abid Khan, Mansoor Ahmed, "Smart Cities: A Survey on Security Concerns", IJACSA, vol. 7, pp. 612-625, 2016.

[5] Karen Renaud, Stephen Flowerday, Merrill Warkentin, Paul Cockshott, Craig Orgeron, "Is the responsibilization of the cyber security risk reasonable and judicious?", ELSEVIER computers & security, vol. 78, pp. 198–211, 2018.

[6] Jeffrey Voas (NIST), Richard Kuhn (NIST), C. Kolias (GMU), A. Stavrou (GMU), Georgios Kambourakis (University of the Aegean), "Cybertrust in the IoT Age", IEEE Computer, vol.51, pp. 12-15, 2018.

[7] Xiruo Liu, Meiyuan Zhao, Sugang Li, Feixiong Zhang, Wade Trappe, "A Security Framework for the Internet of Things in the Future Internet Architecture", future internet (MDPI), vol. .9, pp. 2-28, 2017.

[8] FahimRahman, Mohammad Farmani Mark Tehranipoor, Yier Jin, "Hardware-Assisted Cybersecurity for IoT Devices", IEEE, vol.10, pp. 51-56, 2017.

[9] Christian Lesjak, Daniel Hein, Johannes Winter, "Hardware-security technologies for industrial IoT: TrustZone and security controller", IEEE, pp. 002589-002595, 2015.

[10] Jithin R., Priya Chandran, "Secure and Dynamic Memory Management Architecture for Virtualization Technologies in IoT Devices", future internet (MDPI), vol. 10(12), pp. 2-16, 2018.

[11] RBAC, Core and hierarchical role based access control (RBAC) profile of XACML v20, OASIS Standard, 1 February 2005.

[12] L. Atzori, A. Iera , G. Morabito , The internet of things: a survey, Comput. Netw. vol. 54 (15), pp. 2787–2805, 2010.

[13] Z. Whittaker. After massive cyber-attack, shoddy smart device security comes back to haunt, 2016 (Accessed: 22 October 2016)

[14] T. Nam, T.A. Pardo, Conceptualizing smart city with dimensions of technology, people, and institutions, in: Proceedings of the 12th Annual International Dig- ital Government Research Conference: Digital Government Innovation in Chal- lenging Times, College Park, Maryland, USA, pp. 282–291, 2011.

[15] Bajramovic, K. Waedt, A. Ciriello, D. Gupta, Forensic readiness of smart buildings: preconditions for subsequent cybersecurity tests, in: Proceedings of the 2016 IEEE International Smart Cities Conference, pp. 1–6, 2016.

[16] World Economic Forum, Risk and Responsibility in a Hyperconnected World Pathways to Global Cyber Resilience, 2012 (Accessed: 9 Nov. 2015).

[17] J.-M. Bohli, P. Langendorfer, A. Skarmeta, Security and privacy challenge in data aggregation for the IoT in smart cities, in: O. Vermesan, P. Friess (Eds.), Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, River Publishers, pp. 225–244, 2013.

[18] Zaheer Khan, Zeeshan Pervez b, Abdul Ghafoor Abbasi, "Towards a secure service provisioning framework in a Smart city environment", Future Generation Computer Systems vol. 77(C), pp. 112–135, 2017.

Dr. Kahkashan Tabassum Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Kingdom of Saudi Arabia.

She is currently working as a computer sciences faculty in college of Computer and Information Sciences in PNU. She received her Ph.D. (Computer Science Engineering) and her M. Tech (Computer Science and Engineering) from Jawaharlal Nehru Technological University, Hyderabad, India. Her area of interests are Database Management Systems, Mobile Computing, Cloud Computing, Network Security and Data Mining. She has published more than 50 technical papers in National, International conferences and journals. She is an active researcher and her current research projects are based on the areas, Internet of Things and Health Informatics, Cyber Security, etc.

Dr. Ahmed Z. Ibrahim Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Kingdom of Saudi Arabia. He is an assistant professor in the department of computer sciences in the college of computer and information sciences at Princess Nourah Bint Abdulrahman University where he has been a faculty member since 2009. He completed his Ph.D. at Belarusian State University of Informatics and Radio-electronics. His research interests included data processing and cryptography. He has collaborated actively with researchers in several other disciplines of computer science, particularly in algorithms and networks. He has already published 11 articles. He was the former Head of Graphic Design Department, Director of Communication, Consultation and Continuous Learning Office, and the Administrator of IT (Network) and Hardware Assembly at Irbid national University, Jordan.