Impact of Privacy Issues on Smart City Services in a Model Smart City

Nasser H. Abosaq
Computer Science and Engineering Department
Yanbu University College, Royal Commission Yanbu, Kingdom of Saudi Arabia

***Abstract*—With the recent technological development, there is prevalent trend for smart infrastructure deployment with intention to provide smart services for inhabitants. City governments of current era are under huge pressure to facilitate their residents by offering state of the art services equipped with modern technology gadgets. To achieve this goal they have been forced for massive investment in IT infrastructure deployment, eventually they are collecting huge amount of data from users with intention of providing them better or improved services. These services are very exciting but on the other side they also pose a big threat to the privacy of individuals. This paper designed and simulated a smart city model. This model is connected with some mandatory communication devices which also produce data for different sensors, Based on simulation results and possible threats for alteration of this data, it suggests solution for privacy issues which are to be considered at top priority to ensure secrecy and privacy of smart city residents.**

***Keywords*—IOT; Public-Wi-Fi; Privacy; D2D; D2U; industrial 4.0; 5G; Secrecy; FIDO**

I. Introduction

With every passing day our cities are growing in population and on the other hand demand for increasing quality of services and latest smart services for city residents have been increasing, city residents expect from their governments to equip them with all latest technology gadgets which are helpful to do routine tasks. A Smart City considered to be the combination of variety of integrated small projects, which are initiatives and applications carried out as joint ventures by combination of public and private sector. These initiatives are rapid response to facilitate varied groups of community, therefore it not only results in un-planned selections by diverse background of participant according to their vested interests in any metropolitan area but keeping privacy as top priority, Thus these collections of projects may be similar or having heterogeneous nature of their operations and working. To address needs of general public in a smart city mega project is to address needs and interests of varied nature by facilitating in their daily life routine tasks without affecting their privacy and without any risks or threats in using these services. In this Section-I have discussed the topics as given below. In introduction section, technology background has been discussed. In Section-II describes IOT background and its architecture, Section-III describes smart city services in context of privacy. Section-IV describes about major privacy challenges. Section-V describe about related work of privacy. Section-VI shows simulation results of different sensors in smart city environment. Section-VII describes challenges and proposed solution for these challenges and the last Section-VIII discusses about future work in this particular area. Section-IX concludes this research based on all findings.

II. IOT Background

The steadily increasing density of sensing nodes and sophistication of the associated processing nodes will make significant qualitative change in how we work and live. Thanks to researchers of cutting-edge technologies and their contributions which made it possible to avail all these state of the art services just by a single click on their smart devices ranging from paying their utility bills to managing their kitchen appliances. Research in IoT [1] requires many directions as of massively scalable architectures and dependencies, creating knowledge from big data, robustness, openness, security, privacy and human factors in the loop [2].

How we can consider a particular city as smart city. A set of common multidimensional components when join together by considering core services, build a smart city [16]. Here is a list of basic building blocks which can play a vital role in reshaping an ordinary society into a smart society within a Smart City. Majority of connecting end user devices will be IoT devices which will provide connectivity and communicating services among different entities i.e. Device to Device (D2D) connectivity as well as Device to User Equipment (D2U) connectivity in order to use the IoT enabled services. Sensors are the main part of smart city infrastructure where all the communication among D2D either human controlled or self-directed is being done through sensors.

In a broader context, we can say that when different building blocks are connected together and integrated in such a way in which the input of one part is associated with the output of another part and in the same way the output one part contribute to an input of any other building block and in a broader picture, all these components are connected together to form one big network which host all these services as platform and provide them to inhabitants city government [3]. Smart cities can offer variety of community services ranging from smart signals, smart transportation, and smart houses till smart medical services which seamlessly monitoring medical conditions of patients and generate alerts and recommend for pre-emptive measures for any medical problem to any specific member based on his medical conditions. IoT works on layered architecture which is fully integrated and divided into layers, based on different functionalities and nature of job starting from perception layer till business layers as shown in Fig. 1.

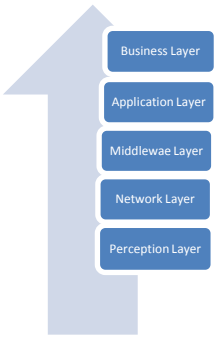

Fig. 1. IoT Basic Layered Architecture.

III. Smart City Services and Privacy

A smart city is interconnection of devices with heterogeneous computational and communication capabilities so there is always a need for smooth data communication. As far as usability of smart services is concerned, it is quite interesting and appealing to use smart services offered by smart cities but, on the other hand, we can see this as a graveyard of privacy of people and their personal data. Aggregated data and real-time data are two main sources of information in smart city environment where data about a specific thing or place is gathered in large quantities to spot trends for analysis. Many such examples are already available where aggregated data is utilized for analyzing traffic and add parking lots and provide appropriate street lights as per needs and size of crowds in parks. Because the data is aggregated, it is effectively anonymized; advantage for this is that it can't be used to track individuals with respect to their changing location. There is a model in some Cities which are gathering real-time data that does focus on individuals. In 2013, a company called Renew London piloted a program in which sensors installed in recycling bins tracked the Wi-Fi signals from passing phones [4]. Fig. 2 shows Location of recycling bins with only screens and recycling bins with function of tracking devices.

Fig. 3 shows location of screen bins and tracking bins which were mainly installed at different locations of city to track individuals for marketing purposes for advertisement of different promotions of products and offers available on nearby shopping malls or hotels/restaurants based on their pertinent interest which they extracted from internet browsing history and liking of different blogs and forums, The sensors could then be used the phone's unique media access control (MAC) address to target advertisements on that bin to the individual, based on their movement within the sensor network. But on the other side, if this information is hacked or misused by someone it could be a great threat to privacy of these persons.

Renew [6] through this scheme in the beginning of experiment they installed 100 recycling bins with very attractive HD digital screens on various locations in entire London before the 2012 Olympics. It was a great opportunity for advertisement companies to buy space on these internet-connected bins, and the city administration gets 5% of the airtime to display public information. For further experiment, Renew installed new bins with gadgets that track smartphones. The idea is to bring internet tracking cookies to the real world. The bins record a unique identification number, known as a MAC address, for any nearby phones and other devices that have Wi-Fi turned on. That allows Renew to identify if the person walking by is the same one from yesterday, even the specific route down the street and how fast the person is walking.

Sensor installation is no more a big deal with any urban area. Existing infrastructure is sufficient for housing these smart sensors, the only modification might require some extra space on streetlight polls or on sign boards as shown in Fig. 4. In a smart city environment a single installed device can house variety of sensors based on specific needs of that particular area or community, for example environmental sensors might be having prime role in an industrial area to get latest info about environment and to control pollution while on the other hand pedestrian sensors might be having more importance on roadside walkways and school areas.

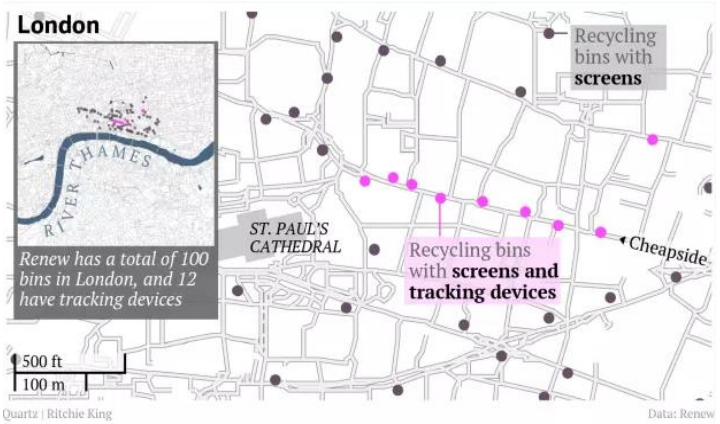

Fig. 2. Map of Smart Recycling Tracking Bins in London [4].

Fig. 3. A Screenshot of Marketing Materials Issued [4].

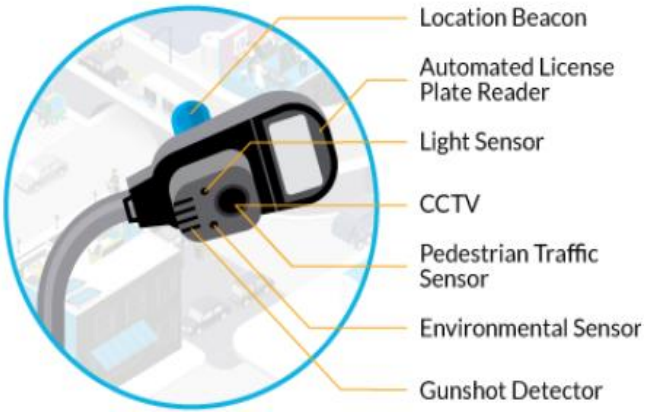

Fig. 4. Sensors Housing in Smart Street Light Poles [6].

IV. Major Privacy Challenges

In context of smart city services deployment following are major privacy challenges related to Communication of IoT devices, which need to be addressed for gaining confidence and trust of citizens. These challenges are Authentication, Access control, Confidentiality, Trust, data secrecy, policy implementation, and secure middle-ware. A lot of research have been carried out to address these challenges. Here we are discussing in detail of those contributions made by different researchers. There are different areas of interests for hackers through which they can inject some unauthorized connectivity and start reading all communication among different entities including sensors or actuators which are involved for device to device (D2D) connection establishment and data transmission.

V. Major Privacy Challenges and Related Work

Based on popularity of smart cities and infrastructure deployment many researchers have done a great job related to privacy and security for IoT devices in smart city environments to protect the data of individuals and companies. Privacy of user's data in smart city environment is very important issue. Many projects have been started with regard to this perspective. Butler's project is one of them which is European Union FP7 projects [5]. In this context, it is pertinent to mention that in some countries privacy of individuals' data is very important and governments have given these rights in many countries of Europe regarding their privacy and if someone wants to use their data including pictures, videos or even their visited places, they need to get permission from them.

There is huge pressure on all kinds of administration who are directly or indirectly involved for city planning and management to provide viable services to its increasing population of metropolitan with required services which should be helpful to complete their day to day routine tasks with ease while using application on their smart phones, tablets or computers. In a standard smart city, any user may have access to six basic services starting from smart people, smart economy, smart governance, smart industries, smart environment and smart houses. IOT is the backbone to achieve this smart city goal for its users to get benefit of these services which mainly relies on cloud services for data manipulation and management. Major research work is going on to protect data on transit at the time of connection establishment for device to device data communication. Researcher are working on finding optimal way to protect data from unauthorized injection during this session by external players which might be using this private information for some hidden intensions including selling of those data to criminals or even some government agencies of some other countries which might process that data and get some required results for their own intensions. On the other side, researchers are also trying to embed some encryption techniques for data privacy which require minimal processing to encode data and its protection on these IOT enabled devices.

As far as user data is concerned, there is always a challenge to keep it private and way from unauthorized access after putting it on public or community network, same is the IoT devices and the data they are transferring by using a public infrastructure in community or metropolitan environment. It covers vast range of challenges from technical sophistication, absence of mature standard, and considering IoT services as commodity and challenges for manufacturers to design state of the art products.

"Sensor communication model" is need of hour for following layered approach for data collection in a systematic order right from various attached sensors according to different needs of communication at different times.

Since no direct processing is required so this collection of data can be done by low end computing handheld devices without compromising privacy of this data.

A. Smart Services in Urban Area

In urban area, there is a huge scope of smart services. Fig. 5 below is showing use of smart technologies in utilities, transportation, telecom sector, government services, and Environment control services. Smart cities generate massive data through enormous and increasing network of connected devices equipped with latest cutting-edge technologies that power new and innovative services ranging from mobile applications that can help drivers find route and different parking spots as per their interests. The modern sensors are also popular for testing water quality against different set standards. In addition, these services can improve individual's efficiency resulting their lives with comforts. On the other hand, massive use of these technologies can increase privacy issues for city administration, which can be minimized by the use of sophisticated data privacy programs to mitigate these concerns.

B. Smart Transportation

Traffic controls react automatically to pedestrians in case someone wants to cross a busy road, shared public bikes can be managed by RFID tags, smart cars communicate with city management system and with other cars [19]. Location beacons can be used to support navigation for the blind people, automated license plate reader cameras can be used to capture images for passing license plates, through smart buses routes can be managed based on demand from different regions of city . Sensors measure traffic to optimize urban planning, drone cameras can also be used to monitor traffic, rider can plan

ahead with transportation through mobile apps for busses, through smart rail network that can transmit data on usage and breakdown.

C. Telecom

For inhabitants urban smart cards provide universal access to city services, Cloud Services hold and process data, public broadband connects services seamlessly and efficiently, public Wi-Fi Kiosks provide free Wi-Fi to the residents of smart city with public private partnership.

D. Smart Governance

Experimental studies show that the Smart cities governance model initiatives follow the same principles of the governance model preconized by e-government research area [7][8][9][10][11], that is accountable, collaborative, involved and open for all the residents.

Privacy mechanisms are divided into two categories which are known as flexibility and limited access. Discretionary access prevents cloning of data and limited access prevents malicious attacks on user's data. Secured domain name system for smart devices which authenticate the authorized users and prevent illegal attacks. Furthermore, the decentralized anonymous privacy protection mechanism for IOT applications defines the roles of nodes as data originators and data collectors. Nodes authenticate themselves to the data collectors through anonymous authentication credentials which encodes the particular attributes.

VI. Simulation Results of Data for Various Sensors

In current era, it has been observed that residents of smart cities start comparing their smart city services with the offered services by some other smart cities. Eventually they are more demanding in terms of smart services regardless of their different circumstances as compared to other cities. Therefore, it is very important for city administration to decide which services should be provided to them without compromising on security and privacy of individual's data.

There is a great need to propose an IOT communication model which follows the layered approach and get data in a systematic way from different sensors according to communication requirements. This data can be collected by using different low computing devices, including smart phones, tablets or handheld devices. Below figures (depict data collected from different devices by variety of sensors and on next step this data is plotted against diverse range of values which smart city residents might be using to monitor different day to day activities of their concerned tasks at work place or at home. These simulation figures show data results of smart environment from different sensors.

To monitor data of different sensors and how they will be working and responding in real world environment we have created a simulation model in cisco packet tracer software [12]. For this simulation design, we used cisco packet tracer version 7.2 and created a prototype network design with some of routine readings of sensors connected to a smart city environment for end user services. Users will be using this data for monitoring of different personal activities ranging from their room temperature management to atmospheric pressure in their vicinity. This data should be generated by Customer Premises Equipment (CPE) Sensors and only concerned authenticated users or administration of smart city should be having access to this data and accordingly they must be having rights to modify input or generate some alarms in case of any special situation for different sensors.

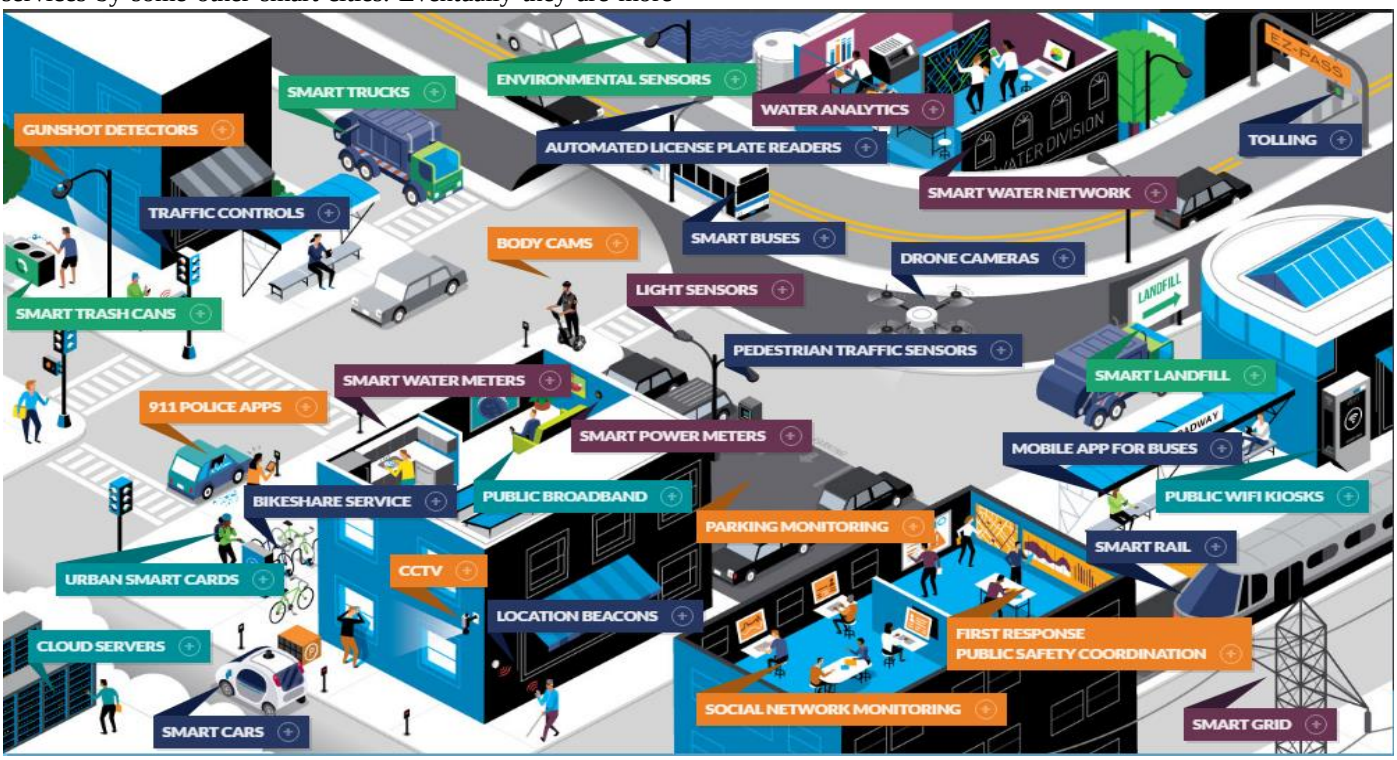

Fig. 5. Urban Sector being Served by Smart Technologies [6].

Below series of Figures (6-13) show a detailed model with interconnected devices where some of the links are connected with wired network while others are connected wirelessly (through IR, Sensor, WIFI, Bluetooth) and data is being transferred through IOT enabled sensors. Strict security policy has been implemented on this model network given in Fig. 6. This network permits only authorized users with different level of access to get into the system for data monitoring, data alteration and data management which is generated by different devices either through wired links or generated through actuators which are part of complete smart city infrastructure. Considering the situation, if this whole network data is manipulated by some unauthorized person who manage to get access to central database of smart city and start modifying it as according his particular intensions. How it would be affecting the life of smart city inhabitants. We have discussed various including sudden or gradual increase and decrease in data values and then its affects after manipulation of data for different sensors.

This simulation is showing communication between different smart devices and generation of data retrieved from different sensors and its expected results in any particular situation based on manipulated value of single sensor, multiple sensors or all sensors.

Above Fig. 6 shows model network city model with connected actuators to show readings of data on different output at various levels this data is further calibrated in Cisco Packet Tracer version 7.2, sensors can be added or removed as per particular needs of environment before building a physical topology for its deployment. Fig. 7 shows values which have been taken in normal situation at different time intervals for different levels of atmospheric pressure. In case if some intruder breaks security wall of system and launch access attack [26] by sniffing network traffic and then through modification attack [27] try to modify this data for specific goals. The results of such activities could be catastrophic since they get some wrong results at some critical time which might generate a great loss as City Central System and individuals might be relying on information provided be these sensors.

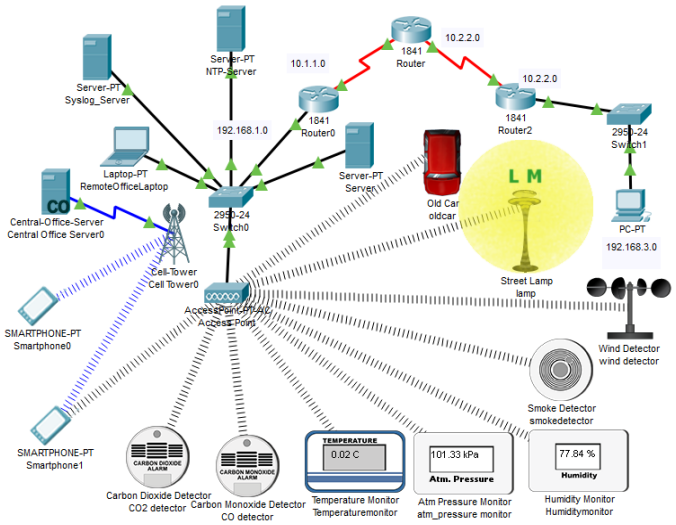

Fig. 6. Model Simulation Design for Different Sensors.

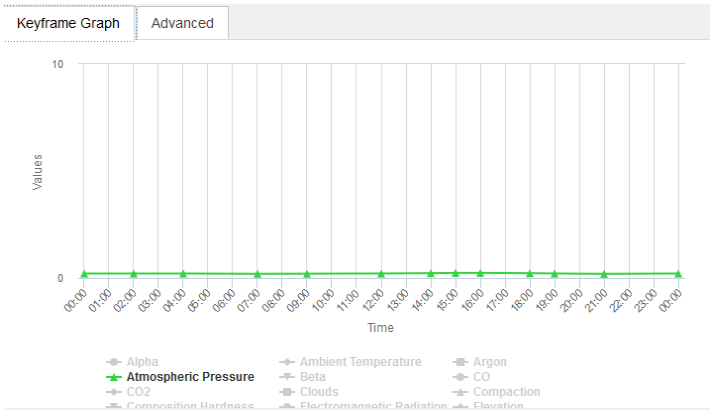

Fig. 7. Atmospheric Pressure.

Atmospheric pressure at some particular location in normal conditions where Max=1.46, Min=1.35

Fig. 8 shows different levels of Carbon Dioxide at different intervals of time, these values have been taken in normal situation, In case if some intruder breaks security wall of system and launch access attack by sniffing network traffic and then through modification attack and try to modify this data for specific goals. The results of such activities could be catastrophic as people and Central system might be relying on output values provided by these sensors. In case they get some wrong results at some critical time which might generate great loss if there is extra ordinary increase in CO2.

Fig. 9 shows different levels of ambient temperature variation at different intervals of time throughout the whole day, these values have been taken in normal situation, In case if some intruder breaks security wall of system and launch access attack by sniffing network traffic and then through modification attack try to modify this data for specific goals. The results of such activities could be catastrophic as people might be relying on output values provided by these sensors. If there is extra ordinary change in environmental temperature and it might further make is critical for industry especial in the presence of industrial 4.0 if it goes unnoticed due to fake readings presented through any compromised IoT monitoring system.

Suppose normal day temperature:T, Max=42C, Min=30

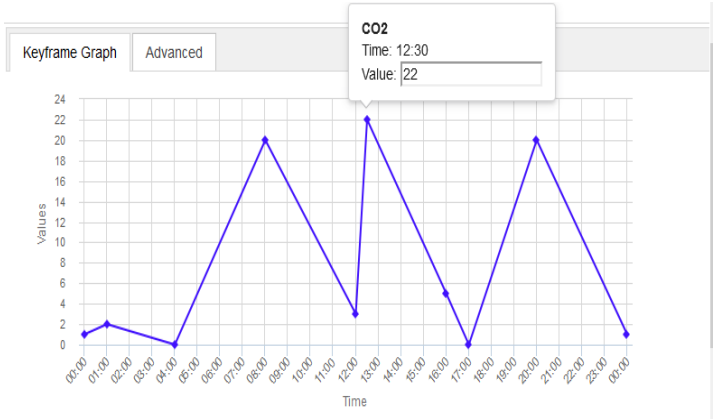

Fig. 8. Carbon Dioxide Levels.

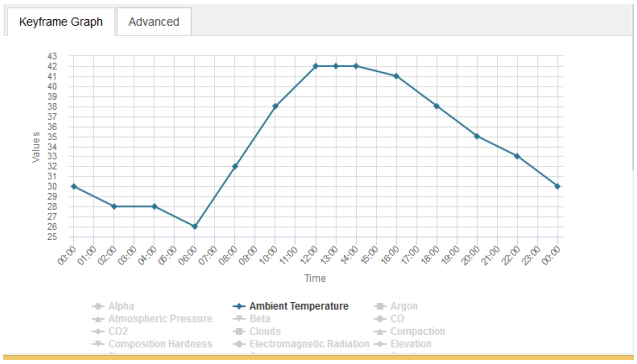

Fig. 9. Ambient Temperature Variations throughout a Day.

Following Fig. 10 shows different levels of humidity at different intervals of time, these values have been taken in normal situation, In case if some intruder breaks security wall of system and launch access attack by sniffing network traffic and then through modification attack and try to modify this data for specific goals. The results of such activities could be catastrophic as people and Central system might be relying on output values provided by these sensors. In case they get some wrong results at some critical time which might generate great loss if there is some extra ordinary change in humidity.

Putting all these together and plotting them all in one graph for all different readings of simulation model of smart city Fig. 11 showing overall trends for varied data collected from different sensors. In case they get manipulated data which ultimately produce totally different results pole a part from actual situation at some critical time. Decisions made after getting manipulated data might generate great loss e.g. if there is extra ordinary change in environmental temperature, atmospheric pressure, CO2, Smoke detection and humidity level. It might further make it very critical and catastrophic for industry especially in the presence of industrial 4.0 where in place of human being some cyborgs will be working at different power plants, industry units or even in some weather forecasting systems. If this kind of situation goes unnoticed for a longer period due to fake readings presented through any compromised IoT monitoring system.

Let's consider scenario of modification for data on one of the above sensors. Fig. 12 and 13 show data at different modifications of sensors. We have considered data for sensor associated with Ambient Temperature after Modification, where T=2T & T=T/256 respectively, Look at the graph how the values are changing and how it can affect the real life in a smart city environment.

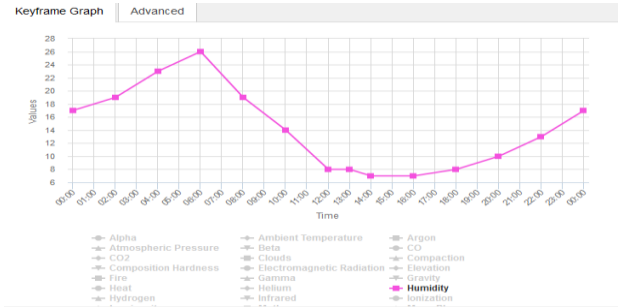

Fig. 10. Normal Humidity Level throughout a Day.

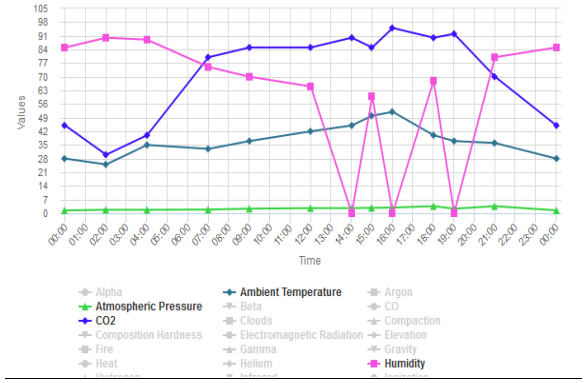

Fig. 11. Combined Graph for Multiple Sensor's Data.

After modification of Temperature T=2T & T=T/256.

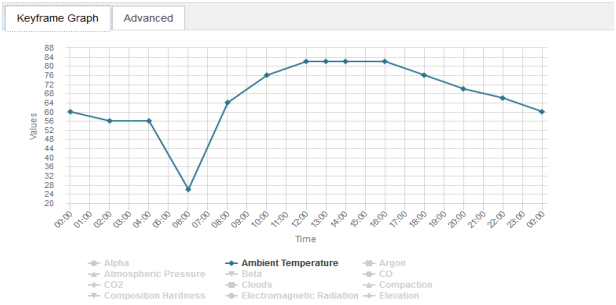

Fig. 12. Ambient Temperature for T=2T.

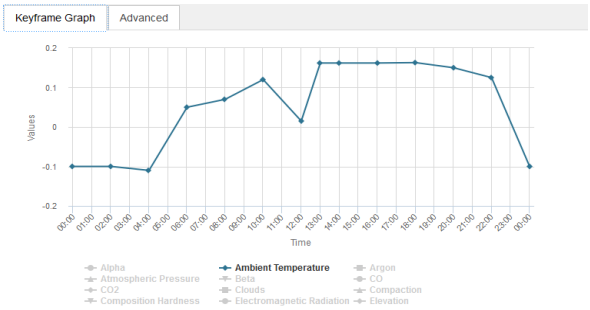

Fig. 13. Ambient Temperature for T=T/256.

After getting all above information with readings from different sensors, which are clearly showing normal situation of any community or even normal situation of a model smart home which is quite usual and its showing normal routine life activities are going on without any extra ordinary situation. In case if someone leave home for a couple of days or weeks and at the mean time someone have access to sensor's data for of their home this could turn into following results.

- By eavesdropping someone can easily figure out activities of residence by looking into sensor's data related to use of home appliances (e.g. air conditioners, room heaters, water sensors or use of coffee machine with timings).
- This will be a clear invitation for the thieves to visit the visit for stealing of their valuables.
- They can also easily figure out the presence of some particular members of family at home at some

particular time by going deep into data processing after viewing reading for past few days or months and can easily see normal trends of data from sensors.

- In case if intruders get further access to system by altering data of sensors or even in case change sensitivity level of sensors and adjust them to some specific values for fulfilling their particular goals this can result in to catastrophic situation, based on readings given in following diagrams which are clearly showing sudden rise or fall of graph for different sensors e.g. increase/decrease in temperature, increase/decrease in CO2, or even increase/decrease in atmospheric pressure.
- In case intruders manage to get access to central databases and from the main system if they alter sensors for different city services the result of this act might be a massive destruction with a huge loss to property or even threat to lives of smart cities residents.
- At Governments level countries can misuse this opportunity to destroy valuable properties or even military installations of their opponents or their enemies.

If privacy of smart city is breached it can result in tracking of any particular personality or group of peoples.

VII. Challenges and Proposed Solution

There are quite a number of challenges related to privacy in smart city environment which are affecting privacy of individuals. Following are major privacy challenges which need to be addressed to win the confidence of inhabitants and to provide them with better services and peace of mind.

A. Confidentiality

Different authors have various findings related to confidentiality of devices and data. Custom encapsulation mechanism which includes encryption with signature is one of the proposed and very popular method used by different researchers. There is also two-way security authentication scheme which is also popular but is not that much strong in terms of attack-resistance. These methods provide better security with respect to confidentiality & authentication. However, there is no authentic clue for implementers to take concrete decisions regarding which layer need to be applied for security mechanism.

B. Privacy

To enforce privacy data, tagging technique is considered very effective. Data tagging is helpful in the information flow and preserve the identity of individuals but this technique contains lots of overhead to manipulate so it is not very helpful in IOT because of their low processing capabilities. User controlled privacy preserved protocol mechanism is also very effective and popular where user define what kind of information to deliver and what to hide from which person. Another technique known as CASTLE i.e. continuously anonymizing streaming data via adoptive clustering. It ensures anonymity, freshness and delay constraints on data stream.

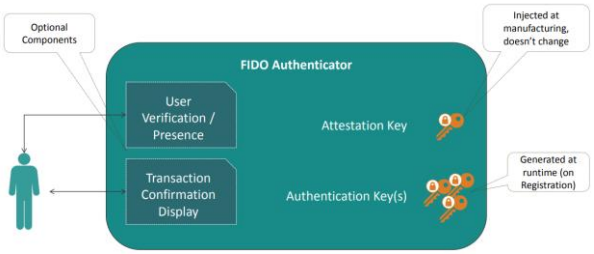

Fig. 14. FIDO Authentication Process [24].

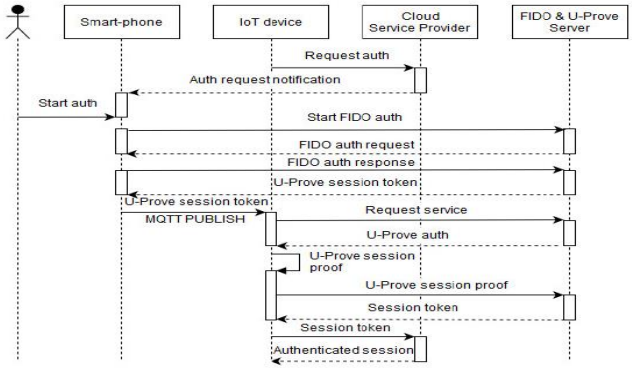

Fig. 15. Sequence Diagram for IoT Privacy-Preserving FIDO Authentication Process.

To ensure privacy there must be step by step to ensure authenticity of any user device which connect to network for performing any tasks or to get data of any sensor. Below Fig. 15 describes IOT privacy preserving by using a sequence diagram to indicate occurrence of events sequentially with interactive interfaces and communication among different components which participate throughout this process. As shown in Fig. 14, we recommend FIDO authentication Process for device to network or device to cloud authentication.

C. Policy Enforcement in IOT

Enforcement means to apply the rules to maintain security, privacy, order and consistency. First paper describes the network security, security policy and policy enforcement and firewall management. It uses services like encryption, authentication, antivirus and firewall to secure data confidentiality, trust and security. Second paper describes two types of languages. One language describes policy enforcement while the other describe the policy analysis. Policy enforcement has several advantages, it reduces the gap between different policies and development. Third paper describes different type of languages like Web Service Policy and extensible access control markup language (eXACML). Fourth paper describes semantic based model for policy enforcement cross domain boundaries. For example in hospitals, pharmacy and medical schools there must be cooperation and interoperability among different domains. Sometimes their policies are different so there must be common policy enforcement to maintain order. Fifth paper describes the hierarchical policy languages for distributed systems. It is used for policy enforcement in distributed systems. Policy monitors control the information data and control the decision engines. The decision engine can add and remove the signature from metadata, encrypt or decrypt the confidential information.

Sixth paper describes the security enforcement in e-commerce. It uses two aspects like trustworthiness and customer anonymity. Seventh paper describes the policy enforcement via software defined approach. It is conservative approach so Eighth paper describes liberal approach for security enforcement of software defined system. Ninth paper describes algebra for communication process (ACP) for concurrent process and basic process algebra (BPA) for security policies are described. Tenth paper describes the Policy machine which is access control framework. It consists of authorized users, objects, system operations and processes. Policies are grouped under classes so one policy may belong to different classes controlled by objects. It is further believed that Metropolitan administration should involve citizens in the planning and designing phase of Smart City which will eventually increase the rate of return on investment on finance and political levels. City administration in collaboration with business units, universities, research institutes, nonprofit organizations and residents can also share their expertise and findings to allow maximum benefits delivery to everybody. Smart City is considered as a complete set of many tiny blocks which might consist of more virtual gadgets than physical building blocks of any normal city.

Smart Applications, Internet of Things, Cloud Computing, Big Data, Wireless Mesh Networks, Wireless Sensor Networks and many other cutting-edge technologies would be the major entities that will play their vital role in creating an optimized Smart City.

D. Respecting Privacy by Creating a Secure Environment

Talking about privacy for end user data, privacy of information is considered to be a major task in Smart City services. This research intends to introduce a secure framework of Smart City infrastructure, where user data could be taken by network model which will be extracted by deep learning algorithm [22]. On the other hand, this deep learning algorithm might get information from hacker's data sheet from history of DoS attacks [23] or DDOS attacks [30], then by applying matching algorithm if such thing is there or they find some matching information it should not forward to community cloud.

VIII. Discussion and Future Work

This paper discusses different privacy issues related to smart city infrastructure deployed for city residents to gain end user services rights from their handheld devices. Future work related to privacy of data for sensor to sensor communication is also addressed [13]. We should also consider industry 4.0 standards where most of the communication will be from machine to machine [18]. In a nutshell, we can consider the following key future tasks which need to be completed to avoid all the mentioned issues. [15] It also describes monitoring of progress for smart cities offered services and their quality and privacy by joining together cutting-edge research and the findings from technical development projects from prominent consultants to capture the transition to smart cities and also paying subsidizes to the sustainability of metropolitan development. A context aware framework based on information based smart services can also be used [20].

A. Policy Up-Gradation

There should be training and awareness campaign for inhabitants through printed material, sign boards, billboards, and through video tutorials about privacy setting of mobile and all communication devices that they are accessing by using internet. There should be well written and precise terms and conditions for users and prominent points should be clearly indicating consent of the users. Educational material should be user friendly and unambiguous which should indicate data gathering techniques and pertinent risks for that data, there should be enough material for privacy setting, data selection and analysis processes and the potential outcomes from user-generated data and sufficient information on responsible data management authorities of citizen's data.

B. User Data Encryption

These risks can be minimized by implementing adequate data encryption techniques [28] which are already very popular and are used for privacy of medical data, genetic, and insurance data. Private data of users can be protected against decryption of data to expose their identity. There should be default settings on every application which should encrypt end users data and keep it in encrypted format.

C. Use of Elliptic Curve Cryptography (ECC)

Since IOT devices designed for light weight data communication with low processing power and small antennas are used with less battery consumption, there are possibilities for communication bottlenecks. To optimize the consumption of bandwidth and computational resources it is recommended to use Elliptic Curve Cryptography (ECC). The main advantages of using ECC are the greater computational complexity of problems and the smaller key length required for a particular security level at time of authentication [25].

D. The Right to be Forgotten

This right to be forgotten was instigated when there were reports regarding publicizing private life events of inhabitants which eventually is violation of citizen's rights to privacy [29]. In 2012, the European Union expanded the right to be forgotten to the internet data, which require the search engines to erase personal data documents which was endorsed by European Parliament and Council of the European Union in 2016. This right to be forgotten is not available in most part of the world but still it can be introduced at least in countries where city governments are providing smart city services to their citizens which is very important tool for privacy protection of users. Better protection could be extended by making right to be forgotten explicit for every smart city governments and non-governments agencies [17]. In various countries still privacy rules have not been implemented to address latest challenges of privacy for inhabitants [21]. In conclusion, we can say that the privacy of users' data should be a main concern and it should not be compromised while planning and designing the infrastructure of smart cities. Both government and corporate sectors should work together to protect users' data from exploitation, otherwise, trust on privacy of end users data would only be a dream. More realistic research needs to be conducted to develop an ideal infrastructure of a smart city while keeping in mind different city governments, their data

policies, ethics, and other cultural norms with consideration of environment friendly green technology [14] for smart devices.

IX. Conclusion

Based on all above scenarios related to breach of privacy, even there could be much worst scenarios which smart city administration should seriously consider at the time of planning, designing and at the time of infrastructure deployment and at the time of activation of different services. In conclusion we can say using state of the art services offered by smart city infrastructure is fascinating but at the same time we should also ensure secrecy of our private data. One should not forget this while running in greed of some comfortable and pleasant technology gadgets. Privacy should be considered as integral part of smart city infrastructure. Both government and corporate sectors should work together to protect user data from exploitation otherwise faith for privacy of end user's data would considered only be a dream. Strict regulations should be implemented from governments to punish the violators of privacy either from administration side or from outsiders. Still realistic research is needed to ensure user's privacy. It can be done by carefully examining smart city security and privacy mechanism with implemented policies in according to specific circumstances.

References

[1]. Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., Jubert, I., Mazura, M., Harrison, M., Eisenhauer10, M., et al.: Internet of things strategic research roadmap. In: Internet of Things: Global Technological and Societal Trends, p. 9 (2009).

[2]. Shahbaz Pervez, Faheem Babar, Gasim Alandjani, "An Efficient Cloud Model with integrated Services by addressing Major Security Challenges., Journal of World Scientific Engineering Assembly and Society Transactions on Computers Print ISSN: 1109-2750, E-ISSN: 2224-2872.

[3]. Nasser H. Abosaq, Gasim Alandjani, Shahbaz Pervez. "IoT Services Impact as a Driving Force on Future Technologies by Addressing Missing Dots". International Journal of Internet of Things and Web Services, 1, 31-37, April-2016.

[4]. https://qz.com/112873/this-recycling-bin-is-following-you

[5]. FP7 in Brief, How to get involved in the Europe, 7th Framework Programme for Research, ISBN 92-79-04805-0, © European Communities, 2007. https://www.iotone.com/organization/butler

[6]. http://www.renewlondon.com/

[7]. Future of Privacy Forum "Shedding Lighton Smart City Privacy", https://fpf.org/2017/03/30/smart-cities/

[8]. Raj Jain, "Smart Cities: Technological Challenges and Issues," IEEE CS Keynote at 21st Annual International Conference on Advanced Computing and Communications (ADCOM) 2015, Chennai, India, September 19, 2015, Chennai, India, September 18, 2015.

[9]. S. Alawadhi and H. J. Scholl, "Smart Governance: A Cross-Case Analysis of Smart City Initiatives," in 49th Hawaii International Conference on System Sciences (HICSS 2016), 2016, pp. 2953–2963.

[10]. S. Alawadhi, A. Aldama-Nalda, H. Chourabi, R. J. Gil-Garcia, S. Leung, S. Mellouli, T. Nam, T. Pardo, H. J. Scholl, and S. Walker, "Building Understanding of Smart City Initiatives," in Electronic Government: Proceedings of the 11th IFIP WG 8.5 International Conference, EGOV 2012, 2012, vol. 7443, pp. 40–53.

[11]. S. AlAwadhi and H. J. Scholl, "Aspirations and Realizations: The Smart City of Seattle," in Proceedings of the 46th Hawaii International Conference on System Sciences (HICSS-46),2013, vol. 0, pp.1695–1703

[12]. Cisco Networking Academy http://cisco.netacad.com/group/packet-tracer

[13]. Vakali, A., Angelis, L., & Giatsoglou, M. (2013). Sensors talk and humans sense towards a reciprocal collective awareness smart city framework. IEEE International Conference on Communications Workshops (ICC).

[14]. Shahbaz Pervez, Faheem Babar, Nasser Abosaq, "Optimal Power Management & Regeneration Schema to Support Green Technology in Mobile Computing Devices for Better Battery Backup", 4th International Conference on Energy and Environment Technologies and Equipment September 20-22,2015. Michigan State University,MI, USA.

[15]. Kourtit, K., Deakin, M., Caragliu, A., Del Bo, C., Nijkamp, P., Lombardi, P., & Giordano, S. (2013). An Advanced Triple-Helix Network Framework for Smart Cities Performance. In M. Deakin (Ed.), Smart Cities: Governing, Modelling and Analysing the Transition (pp. 196-216). New York: Routledge.

[16]. Pardo, T., Taewoo, N. (2011). Conceptualizing smart city with dimensions of technology, people, and institutions. Proceedings of the 12th Annual International Conference on Digital Government Research (pp. 282–291). ACM, New York.

[17]. Shahbaz Pervez, Nasser Abosaq, Gasim Alandjani, "IoT Services Impact as a Driving Force on Future Technologies by Addressing Missing Dots" , 16th International Conference on Applied Computer Science (ACS '16), Istanbul, Turkey, 15-17 April 2016.

[18]. Industry 4.0: the fourth industrial revolution – guide to industry 4.0 http://www.i-scoop.eu/industry-4-0/

[19]. M Handte et. Al (2016), "An Internet-of-Things Enabled Connected Navigation System for Urban Bus Riders", IEEE Internet of Things Journal, Volume 3, Issue 5

[20]. Z. Khan, S. Kiani, K. Soomro, "A Framework for Cloud-based Context-Aware Information Services for Citizens in Smart Cities", Journal of Cloud Computing: Advances, Systems and Applications, vol. 3, No. 1, pp. 14, 2014.

[21]. Yang F, Xu J. "Privacy concerns in China's smart city campaign: The deficit of China's Cybersecurity Law. Asia Pac Policy Study. 2018;1–11.

[22]. Kim, Sangwook, Lee, Minho, Shen, Jixiang, "A novel deep learning by combining discriminative model with generative model", IEEE 2015 International Joint Conference on Neural Networks (IJCNN) - Killarney, Ireland (12-17 July, 2015)

[23]. Ning Zhu, , Yongfu Zhang, , Chen, Xinyuan, "A new method to construct DoS attack oriented to Attack Resistance Test", IEEE International Conference on Information Theory and Information Security (ICITIS) - Beijing, China, Dec, 2010.

[24]. FIDO Alliance forum 2017 (https://fidoalliance.org/wp-content/uploads/The_Future_of_Authentication_for_IoT_Webinar_170328_v10.pdf)

[25]. Hankerson, D., Menezes, A.J., Vanstone, S.: Guide to Elliptic Curve Cryptography. Springer-Verlag New York, Inc., Secaucus (2003).

[26]. P. Anu ; S. Vimala, "A survey on sniffing attacks on computer networks", IEEE International Conference on Intelligent Computing and Control (I2C2), Coimbatore, India june-2017.

[27]. Yimeng Dong, Nirupam Gupta, Nikhil, "Chopra On content modification attacks in bilateral teleoperation systems", IEEE American Control Conference (ACC), Boston USA, 6-8 July 2016.

[28]. H. R. Nagesh, L Thejaswini, "Study on encryption methods to secure the privacy of the data and computation on encrypted data present at cloud", IEEE International Conference on Big Data Analytics and Computational Intelligence (ICBDAC), 23-25 March 2017.

[29]. Nathalie Devillier, "Aging, Well-Being, and Technology: From Quality of Life Improvement to Digital Rights Management- A French and European Perspective", IEEE Communications Standards Magazine (Volume: 1 , Issue: 3 , SEPTEMBER 2017).

[30]. Kseniya Yu. Nikolskaya ; Sergey A. Ivanov ; Valentin A. Golodov ; Aleksey V. Minbaleev ; Gregory D. Asyaev, "Review of modern DDoS-attacks, methods and means of counteraction", IEEE International Conference "Quality Management,Transport and Information Security, Information Technologies" (IT&QM&IS) St. Petersburg, Russia, 24-30 Sept. 2017.