# Issues of Cyber Security in Integrated Modern Technologies

Dr.Dileep Singh, HOD, Assistant Professor JLU School of Engineering & Technology

JagranLakecityUiversity, Bhopal

jagraneip@gmail.com

***ABSTRACT:Smart City alludes to the city which incorporates modern technologies for efficient and automated service giving to improve the lifestyle of citizens. Most recent studies represent that as the 62 present of the entire population of the world would be living in the urban areas in 2040. This greatly developing population in the urban areas prompts the importance of approaches of advanced management which utilize the most recent techniques and IT platforms for smartening each city related to the service. Such a new reconciliation of technologies faces few security related to the challenges because not considering the security tests of latest conveyed technologies, notwithstanding not connecting with other framework parties with the security incidents because of the immense communication. On the opposite side, high complexity, intensive communication and large inter dependency prompt cryptography related and unbounded attack surface issues. In this paper, its intention to give briefed overview dependent on the literature of significant security problems and the latest solutions of smart cities. Besides, it depicts a few impacting factors that affect the security of information and data in smart cities.***

***KEYWORDS: Cyber security, Impacting factor, Smart cities technologies, Security problems.***

## INTRODUCTION

There is no universal and particular definition for smart city concept as nations and its governments decide how far it goes for smartening as per its eagerness for changing, financial status and resource limitations. Be that as it may, it, for the most part, utilize the smart city concept for the incorporation between most recent technologies of communication and data and traditional infrastructureto make a whole framework for service related to the real-time city and resource-efficient giving in the urban areas. There are five principal segments that are basically required to be for a smart city such as modern communication and information technologies, infrastructure and utilities, traffic management and transportation, buildings and city itself[1].

In fact, a smart city is a cooperation between private and public foundations and governance institutes for implementing and deploy long haul computerized platforms that enforce utilizing present-day technologies including electronic objects, intelligent decision-making strategies, mobile cloud computing and network strategies. Smart cities across the world objective, for the most part, deal with the principle challenges that as of now face the globe, for example, growth of high population, atmosphere changes, and urbanization and limited resources. In addition, the objective of smart cities for securing the economic competitiveness in the urban environments and let the residents of urban experience more classy lifestyles. Ideas for becoming smart are different from the urban communities themselves[2]. Generally, there are six areas or measurements where the cities can get smarter such as smart governance, smart environment, smart economy, smart living, smart people and smart mobility as shown in Fig. 1.

The smart city wasn't just about deploying the smart platforms for performing services related to the city efficiently, yet it is a broad idea that contains a few electronic and physical objects that communicate and interact through the wireless and wired networks. Utilizing these insecure items may cause a few hacks prompting filling the framework with fraud information, which causes service termination and shutting down the systems. To quantify how smart city is, it checks the level of computer systems and automation it utilizes, notwithstanding the integration between the frameworks[3]. This high integration prompts operational interdependencies from most typical systems to the easiest ones causing immense cascade attack which can harm the communication and entire infrastructure. On the other hand, smart cities face the issues in recovering plans, vulnerabilities assessment and response. At last, dealing with security is expensive and obtaining enough budget needs a long procedure in the public sectors. To summarize, problems in smart cities related to security are genuine and current and require immediate consideration and analysis [4].

Hence, issues related to privacy and security are interesting topics particularly that technologies of smart city and the frameworks are getting essential for optimizing cities and improve personal satisfaction. In this paper, it considered a few concerns related to privacy and security in smart cities. Through information security, it means information tendency to be unintentionally or purposefully influenced by the technical disappointments caused by malicious activities or attacks; and through information privacy, it meant the capacity to protect information from reusing or unauthorized accessing notwithstanding for protecting its collection procedures and all tasks being run over them[5].


**Fig. 1: Meseurments of Smart Cities**

## RELATED WORK

Privacy and security are always hotly debated issues to talk about. For smart city, privacy and security issues are more significant than these are for any type of technological phenomena since smart cities are expanding quickly around the world. Accordingly, researchers must give more consideration so issues related to privacy and security in smart cities so as to improve the literature with more studies and researches in such manner[6]. For this paper, it checked on a few important types of research that the challenges of privacy and security and its related issues.The researchers depict smart cities like the state of art collecting of communication and information technologies and it talked about the latest urban modern technologies and urban issues. Notwithstanding that, it explained uncertainties and the latest risks in smart cities by describing the situations of cities that are expressed smart[6]. The work gives data about challenges, necessities and advantages in the research area of smart city inquire about the region. It additionally discusses the latest view of "Cloud of Things (COT)" that is the integration among the cloud computing science and technology IOT; and it also talked about how services of smart cities can be given dependent on the Cloud of Things[7].

The researchers inspected the concerns of privacy and security by giving a model which shows the significant components of the smart cities such as servers, things and people and interaction among them. The researchers talk about the guidelines on the violations of privacy and security and it expresses that these guidelines sometimes fall short for the criticality and importance of privacy and security issues. It was well known that huge benefits were provided by smart cities to the users, however, at the equivalent the users worry about its privacy of information which is transferred over the non-secure channels. So as to provide secure media, it is an absolute necessity for securing the communication channels for transferring the data uniquely over the wireless networks[8].

The researchers talk about privacy exchange off with the smart city. It talk the drawbacks that smart cities may bring into its lives in regards to the infringement of privacy that may happen. Users must give immense consideration to what it share and should know that once it share any bit of individual information, it won't fade. It is very important to alarm analysts and organizers for the need of thinking about the protection against the vulnerabilities of security during the plan of the smart city. During the planning process, cyberinfrastructure technologies should be defined during the configuration procedure for predicting the response of a smart city[9].

## SMART CITY RELATED TO SECURITY

It referenced that it is a challenging and very tricky security-wise process to develop a particular city from being associated with being smart as it involves a high level of connectivity and dependency over its layers such as technology, infrastructure, information/data, and application. In this area, it depicts the major challenges of security and its related infringements that may happen in each layer of the smart city.

- *Infrastructure Security:*

A few risks and vulnerabilities face the cyber-physical infrastructure which utilized in the city smartening. Anyway these latest systems of cyber-physical infrastructure are hugely utilized, there is no fantastic knowledge for its threats and vulnerabilities. Mostly incidental and purposeful dangers on the security of smart city infrastructure cause various serious consequences as per the smartness and maturity of the city[10].

In this manner, it shows the major challenges and threats related to the security of the encountered infrastructure. Urban infrastructure, for example, streets, power supply, buildings, water distribution and others face a few security dangers in its particular cyber-physical systems and components are as follows:

- *Communication Networks:*

By utilizing a few communication technologies, cyber-physical components are associated together by the smart city for example, 4G, GSM, Wi-Fi, RFID, and others. Every one of these has particular concerns about security that should be seen during the arrangement and utilization of communication technologies.

- *Transport Management System:*

These frameworks face the most typical hacks as it causes catastrophes particularly when it occurs to train control systems or air traffic systems[11]. In addition, it causes gigantic traffic

roads that may keep going for many hours by hacking the traffic lights control systems and its speed limit signs, sequencing, and road signs.

- *Cameras:*

Urban areas are loaded with public and private cameras that both are secured dynamically utilizing password protection and encryption protection[12]. Arriving at public or private cameras and approaching on them cause infringement to the privacy of people and keeping an eye on the governmental concerns.

Essentially, the infrastructure of the city is a mixture of cyber-physical frameworks that are incorporated with the physical independent segments. Cyber-physical systems involve interconnected physical components for example, sensors, networking objects, computing elements and so forth. Cyber-physical systems must achieve fundamental three tasks in smart cities which are as collecting information, choosing which proficient procedures must be run and control the physical parts. It depicts the major threats briefly that intimidate the integrity of urban infrastructure are as follows:

- *Eavesdropping:*

Embed tools of eavesdropping in a particular network for eavesdropping on the channels of communication, catching the behavior of network traffic and obtaining the map of the network[13]. Eavesdropping is a hazardous threat that prompts break down confidentiality and integrity which causes personal and financial failures.

- *Denial of Service:*

DOS is to excess connections until devices and services are blocked which are relying on them. Attacks of DOS affect systems availability or connections.

- *Privacy of Data in Smart Cities:*

Smart Cities manage enormous amounts of real-time information and its related technologies i.e. information driven technologies that follow up on, create, procedure, run and produce information.Smart Cities have numerous resources that producing various kinds of information. Among these resources are frameworks that persistently produce exclusive data and fine-scaled. These frameworks are across the board in smart cities and data it produces are called the big data. Many frameworks are the systems machine learning that develops data analytics and the latest data[14].

All these urban information are utilized to implement the smart city technologies, now then it is required to maintain these huge amounts of information and data secure. Additionally, it is important to keep up the privacy of personal data and locked data and to ensure that these are not purposefully or unintentionally accessed or arrived. The issues related to privacy can be ordered in to three classes of privacy such as communication, business privacy and individual shown in Table 1.

**Table 1: Challenges and violations related to privacy**

| Category | Challenges related to privacy | Violations |
|---|---|---|
| Business privacy | • Banking<br>• E-commerce | • Phishing<br>• Attacks for integrity of data<br>• Spoofing |
| Communication privacy | • Communication from M to M<br>• Communication from resident to smart city | • Eavesdropping<br>• Side channel attacks<br>• Secondary use<br>• Denial of service<br>• Identification<br>• Attack of man in Middle |
| | | |

## CONCLUSION

Privacy and security are always hotly debated issues to talk about. For smart city, privacy and security issues are more significant than these are for any type of technological phenomena since smart cities are expanding quickly around the world. Accordingly, researchers must give more consideration so issues related to privacy and security in smart cities so as to improve the literature with more studies and researches in such manner. For this paper, it checked on a few important types of research that the challenges of privacy and security and its related issues.

Cybersecurity of smart cities is a significant issue that includes considering a few concerns of security about technology, infrastructure, data/information and applications. Chiefly cybersecurity is influenced by the exigent technologies integration and resulted in serious communication, high interdependency and high complexity, which prompts cryptography and unbounded attack surface related issues. Cybersecurity of smart urban areas is a significant issue that requires international collaboration, that involves specialists from everywhere throughout the world.

**REFERENCES**

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet Things J.*, 2017.

[2] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Commun. Surv. Tutorials*, 2012.

[3] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, "The internet of things for health care: A comprehensive survey," *IEEE Access*, 2015.

[4] A. Aldairi and L. Tawalbeh, "Cyber Security Attacks on Smart Cities and Associated Mobile Technologies," in *Procedia Computer Science*, 2017.

[5] Z. Drias, A. Serhrouchni, and O. Vogel, "Analysis of cyber security for industrial control systems," in *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications, SSIC 2015 - Proceedings*, 2015.

[6] C. Hennebert and J. Dos Santos, "Security protocols and privacy issues into 6LoWPAN stack: A synthesis," *IEEE Internet Things J.*, 2014.

[7] T. Limba, K. Agafonov, L. Paukštė, M. Damkus, and T. Plėta, "Peculiarities of cyber security management in the process of internet voting implementation," *Entrep. Sustain. Issues*, 2017.

[8] M. Wu, Z. Song, and Y. B. Moon, "Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods," *J. Intell. Manuf.*, 2019.

[9] L. Jóźwiak, "Advanced mobile and wearable systems," *Microprocess. Microsyst.*, 2017.

[10] D. Solak and M. Topaloglu, "The Perception Analysis of Cyber Crimes in View of Computer Science Students," *Procedia - Soc. Behav. Sci.*, 2015.

[11] B. Zheng, W. Li, P. Deng, L. Gérardy, Q. Zhu, and N. Shankar, "Design and verification for transportation system security," in *Proceedings - Design Automation Conference*, 2015.

[12] X. Zhou, A. Y. Zomaya, W. Li, and I. Ruchkin, "Cybermatics: Advanced Strategy and Technology for Cyber-Enabled Systems and Applications," *Future Generation Computer Systems*, 2018.

[13] P. Sharma, D. Doshi, and M. M. Prajapati, "Cybercrime: Internal security threat," in *Proceedings of 2016 International Conference on ICT in Business, Industry, and Government, ICTBIG 2016*, 2017.

[14] C. H. Wu and J. D. Irwin, *Introduction to Computer Networks and Cybersecurity*. 2016.