Security Threats and Challenges in Smart Cities

[1]Dharmendra Kumar Kanchan, [2]Dharamdas Kumhar

[1]Assistant Professor, [2]Assistant Professor
[1]Department of Computer Science & Information Technology,
Bundelkhand University, Jhansi, India

Abstract: *With the advancement in the field of computer science and information technology, the world is changing very fast. Peoples are migrating from small towns to major cities. Now a day the majority of the inhabitants living in urban environments so it has become necessary to increase all kinds of advanced facilities in the cities. This concept leads to build Smart Cities using the latest information technologies. ICT technologies are the building blocks for Smart cities. The Internet is a globally accepted phenomenon that can play a very important role in developing Smart Cities. With the growing Internet usage, every human being is connected to the whole world via Internet connections. These connections include smart mobile phones, electronic gadgets like Tablets, laptops, Desktops and PCs, each other via wireless or wired Internet connections. Apart from these connections, cities also have bank ATMs, kiosks etc. and almost every office building like banks, railways and different govt. and private organization are connected through the Internet for deploying their services. Given that these systems will greatly impact human lives and leads to a higher risk of cybercrime related issues. This paper summarizes the key challenges, emerging ICT technology standards and issues related to the cybercrime and cyber security in smart cities. A key observation is to study the potential opportunities in cyber security space to build safe and secure smart cities free from the risk of cyber crime.*

Keywords — Cyber crime; Cyber security; Internet; Information technologies; ICT technologies

I. Introduction

The world is changing very fast in every area of life. Small villages are turning into towns and towns are turning into cities. The person migrates from small towns/cities to big/metro cities for various reasons such as in search of a career, Job, business opportunities and/or good sustainable life. In this changing scenario the world’s political and economic significance of cities are growing rapidly. Now a day, most of the world’s population resides in the cities, and peoples are continuously migrating from rural areas to urban areas. Therefore, cities are a central part to solve major social, environmental, and economic challenges. One of the biggest challenges is to ensure that these cities are resourceful connected and sustainable is a major challenge but also an opportunity to improve the lives of millions of people along with the health services and future opportunities of the planet itself. The Internet and information technology has a great impact on the life of city dwellers. Everybody in the big cities is highly dependent on the Internet and Communication Technologies (ICT) in daily life routine such as using the Internet for online transaction, accessing E-commerce sites, Net banking, offices and buildings are well connected through computer and networking devices so we observe that ICT technologies can play the role of game changer in the development and expansion of smart cities and have great potential to encourage sustainable growth.

There is no globally accepted definition for smart cities. We can state that it is an urban development mission to incorporate multiple of information and communication technology (ICT) and the Internet of Things to provide a solution in a secure manner to manage resources in the city. These resources include, but are not limited to, computerized government and private organizations’ with MIS, Schools/colleges with smart class rooms and libraries equipped with RFID (Radio frequency identification) systems, smart and efficient transportation system, well equipped hospitals, power generation and supply chain, water supply networks, solid waste management system, law enforcement, and different community services. The objective of building a smart city is to enhance the quality of living standards using ICT technologies to improve the effectiveness of services to meet citizens’ needs. This requires monitoring activities and recording of what is happening in the city. Data collection, processing and analysis are also necessary for the future planning of city resources. We can apply data mining techniques to predict future trends. The information and knowledge gathered are the keys to tackling inefficiency [1]. Information and Communication Technology (ICT) is used to reform the quality, high performance and activity of urban area services, to bring down costs and resources utilization and to improve communication between citizens and the government [2]. Smart city applications are developed with the goal to improve the management of urban streams and permitting for actual time responses to challenges [3]. A smart city may, therefore, be more prepared to respond to challenges than one with a simple 'transactional' relationship with its citizens [4]. Yet, the term itself remains unclear to its specifics and therefore, opens to many interpretations and subject [5].

II. INFRASTRUCTURE ELEMENTS IN SMART CITIES

The necessary components to build smart city could include:

1. Sufficient and purified water supply.
2. 24x7 electric power supplies.
3. Installation of CCTV cameras and monitoring centre with image processing facilities.
4. Proper sanitation, hygiene and the solid waste management system.
5. Smart Public transportation system with GPS Navigation to track vehicles and its locations.
6. Smart Housing societies equipped with all modern amities and Internet technologies.
7. ICT technologies and Internet connectivity to all individuals, buildings and organizations (Govt. and private) in the city using optical fiber cable (OFC), Wi-Fi, or WiMax facility.
8. E-Governance and citizen participation & feedback.
9. Sustainable and conducive living environment.
10. Safety, protection and security of people against crime; including cyber crime.
11. Modern hospitals and health management system.

12. Modern schools, colleges and institutions with smart class rooms and compulsory education for all citizens.
13. Opportunities for economic growth & development.

The purpose of smart cities is to improve the quality of living of the peoples living in the smart cities with the help of ICT technologies. Also, provide opportunities for economic growth with Job opportunities and Business developments to enhance income for all. All these points discussed are the building blocks that heavily depend on the use of ICT technologies and the Internet to provide connectivity to integrate operations and information. Therefore ICT technology plays a vital role in communication, information sharing, and data analysis to build smart cities' multifaceted and cross-domain challenges, and provide optimized solutions to ensure the sustainability of the city, citizen well-being and economic development [6]. With the inter-connectivity of everything, it increases the ICT technology complexity and security issues in the Internet of Things (IoT) environments [7].

III. CYBER SECURITY THREATS IN SMART CITIES

Since, in smart cities, everything is connected to each other through the Internet and ICT technologies so there is a great chance of cyber crime or cyber attacks.

A. Cyber Crime

There is no universally accepted definition of cyber crime. We can define cyber crime as "a crime conducted in which a computer was directly and significantly instrumental". We can suggest the following definitions of cybercrime [8]:

1. An unlawful activity where a particularly knowledge of ICT technologies is necessary for its crime, examination or prosecution.
2. Any traditional crime that has acquired a new dimension or order of magnitude through the aid of a computer, and abuses that have come into being the use of a computer.
3. The Financial fraud that takes place in a computer and networking environment.
4. Any threats to the computer itself, such as theft of hardware or software or information stored in a computer system.

The other terms that are synonyms to the cyber crime are computer-related crime, computer crime, Internet crime, E-crime, High-tech crime etc. We can say crimes completed either on or with a computer. Crime committed using the computer and the Internet to steal a person's identity (identity theft), crime completed either on or with computer, any illegal activity done through the Internet or on the computer, and all criminal activities done using the medium of computers, the Internet, cyberspace or world wide web are comes under the category of cyber crime.

Table 1 Table Cyber crime percentage wise report years (1999 – 2008)

Crime	**2004**	**2005**	**2006**	**2007**	**2008**
Denial of service	39	32	25	25	21
Laptop theft	49	48	47	50	42
Telecom fraud	10	10	8	5	5
Unauthorized access	37	32	32	25	29
Viruses	78	74	65	52	50
Financial fraud	8	7	9	12	12
Insider abuse	59	48	42	59	44
System penetration	17	14	15	13	13
Sabotage	5	2	3	4	2
Theft/loss from proprietary information : - *From mobile device:* *From all other sources :*	10	9	9	8	9 4 5
Website defacement	7	5	6	10	6
Abuse of wireless network	15	16	14	17	14
Misuse of web application	10	5	6	9	11
Bots				21	20
DoS attacks				6	8
Instant message abuse				25	21
Password sniffing				10	9
Theft/loss of customer data *From mobile device:* *From all other sources:*				17	17 8 8

Source: 2008 CSI Computer Crime and Security Survey

B. Cyber crime and Information security

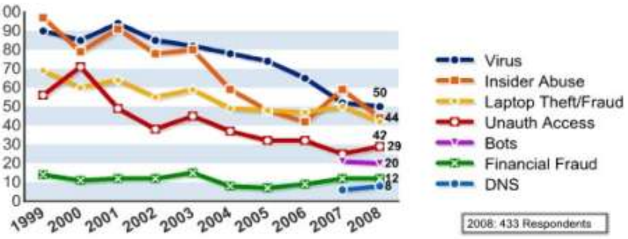
Lack of information security gives rise to the cyber crime [12]. Cyber security means protection of information, electronic gadgets, devices, computer software and hardware, computer peripherals and communication devices and information and data stored therein from unauthorized access, usage, discovery, disruption, modification or destruction.. This means providing both the physical security of devices as well as the information stored therein.

C. Cyber crime and financial losses

Cyber crime leads to great financial losses to the organization or individuals so cyber security is an important factor to be considered in the development of smart cities since everything and every individual is connected through ICT technologies or the Internet to each other. The 2008 CSI Survey on computer crime and security support this indicated in Table-1 [9].

Cyber crime has a great impact on cyber security. There are a number of challenges to fight against cyber crime to build smart cities. Figure-1 indicates several categories wise cyber crime incidences like denial of service attack, financial frauds, viruses, insider abuse, laptop theft and unauthorized access to the system [14].

Figure-1: Percentage wise different types of incidents



Source: 2008 CSI Computer Crime and Security Survey

D. Cyber crime and criminals

A person who commits a crime with the help of ICT technologies is called cyber criminal. Since smart cities are hi-tech cities, there are a lot more chances that smart cities may be targeted by cyber criminals due to the Internet connectivity. Now, the question arises, why some peoples (or cyber criminals) are involved in this kind of act? There are some reasons shown in the Table-2.

Table-2: Types of cyber criminals

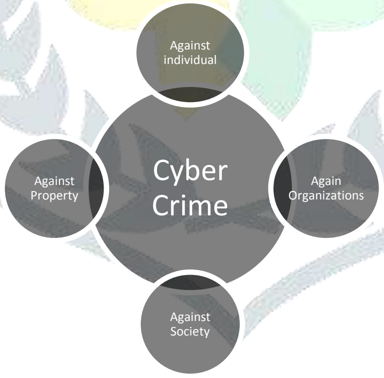
Type	Criminals
Person want recognition	Students' hacker, software engineers, politically motivated hackers, terrorist groups
Do not want recognition	Person hacking for money (corporate espionage), mentally distorts peoples, state-sponsored hackers, organized criminals
Insiders or Employees	Employees seeking revenge; competing organizations using employees to gain financial advantages through damage and/or theft

Thus, the motive behind cyber criminals seems to be greediness, desire to gain power and/or publicity, desire for revenge, a sense of adventure, looking for a thrill to access forbidden information, destructive mindsets, to steal and sell network services. So, the safety of smart cities is the great challenge.

IV. CLASSIFICATION OF CYBER CRIME

We can classify crime roughly into four categories as represented in Figure-2. This classification is necessary because the risk of cyber crime is higher in smart cities than that of other cities since most of the peoples, organizations, buildings and offices are connected through a network and using ICT technologies, so it is better to organize smart cities cyber security category wise to combat cyber crime efficiently.

Figure-2: Classification of cyber crime



The table Table-3, Table-4, Table-5 and Table-6 describes cyber crime against individuals, against property, against the organization and against society.

Table-3: Cyber crime against individuals

S.No.	Crime Type
1.	E-Mail spoofing and online fraud
2.	Phishing, Spear phishing and various forms
3.	Spamming
4.	Cyber defamation
5.	Cyber stalking and harassment
6.	Computer sabotage
7.	Pornographic offences
8.	Password sniffing (can be done anywhere)
9.	Identity theft

Table-4: Cyber crime against property

S.No.	Crime Type
1.	Credit/Debit Card frauds
2.	Intellectual property crime includes: s/w piracy, copyright

	violation, trademarks violations, program source code theft
3.	Internet time theft

Table-5: Cyber crime against the organization

S.No.	Crime Type
1.	Unauthorized access to a computer system
2.	Password sniffing
3.	Email bombing
4.	Salami Attack/Salami Techniques
5.	Trojan Horse
6.	Logic bomb
7.	Data diddling
8.	Denial of service attacks
9.	Virus attack/dissemination of viruses
10.	Industrial spying/espionage
11.	Software piracy
12.	Computer network intrusions
13.	Crime emanating from Usenet newsgroups

Table-6: Cyber crime against Society

S.No.	Crime Type
1.	Forgery
2.	Cyber Terrorism
3.	Web jacking

V. CYBER SECURITY CHALLENGES IN SMART CITIES

Information or Data security is the protection of data against incidental or intentional, destruction, revelation or moderation [11].Cyber security can be defined as the protection of computer systems, networks and data from cyber attacks. In smart cities with continuous network connectivity, the possibilities of cyber crime or cyber attacks are higher. Cyber attacks can originate from any sources that are local, remote, domestic or foreign [13]. These attacks could be launched by an individual or a group of cyber criminals. These cyber attacks could be casual probes from hackers using personal computers from their homes, handheld devices like mobile, tablet PC, any electronic gadgets or intense scans from cyber criminals. Providing cyber security is one of the biggest challenges in smart cities and is a critical issue to be considered in the development of smart cities. Cyber security will only become more important as more devices, 'the Internet of things' (IoT), become connected to the internet. In order to provide cyber security in smart cities, we have to focus on following four major areas while planning & developing smart city's networks**:**

A) Application System Security

For Application system security, all security measures are taken into consideration at the time of system development life cycle to protect applications from threats that are observed during the system design, system development, deployment, system up-gradation and maintenance. Following are some basic techniques to deal with application system security issues are: **-**

a. Validation of input parameters.
b. Administrator/End-user Authentication & Authorization.
c. Session management, parameter manipulation and Exception handling.
d. Application system audit trail and logging

B) Information Security

Information security means protecting information from unauthorized access, use; disruption and modification to avoid identity theft and to ensure privacy protection. Techniques used to provide information security are: -

a. Identification of end-user
b. Authentication of end-user
c. Authorization of end-user
d. Cryptography & encryption techniques
e. Privacy policy

C) Recovery from a system crash

Crash recovery planning is a process that includes performing risk measurement, maintaining priorities, developing recovery strategies in case of a system crash. An organization should prepare a solid plan in advance to recover from system crash for both hardware and software so that normal operations can be resumed as quickly as possible after a system crash.

a. Maintain backups.
b. Develop a procedure to restore after system crash: including hardware, software, and data.

D) Traffic management and control

Since most of the functionality in Smart cities is based on the Internet and network communication technologies, it required a high-speed communication network which is free from network congestion in order to perform network operations smoothly. The different algorithms which are used for congestion control are suggested in [16]. This can be used to enhance the performance of the different type of communication networks used in smart cities.

E) Network Security

Network security means establishing a secure network connection to protect the unauthorized access of network. This includes activities to protect the usability, reliability, integrity and safety of computer and data [10]. Many network security threats like viruses, worms, malware, Trojan horses, spyware, Hacker attacks, data theft and identity theft etc. are spreading over the network. Implementing robust security strategies are essential to prevent the network from intrusion and also stop threats from spreading over the network. Network security is implanted through hardware and software. A network security system usually consists of many components. These components include:

a. Installation of Anti-virus, anti-malware and anti-spyware Software and updating software and virus definitions regularly.
b. Installing Firewall to block unauthorized access to network system from hackers.
c. Intrusion prevention systems (IPS) to identify fast-spreading threats, such as zero-day or zero-hour attacks [15].
d. Virtual Private Networks (VPNs) to provide secure remote access and/or remote login.

VI. CONCLUSION

The concept behind Smart cities is to provide better living condition and quality of life to the citizens. Everything in smart cities is supposed to be controlled by the computer system, electronic devices, networking and the Internet technologies. A television set that is connected to the Internet and used for browsing is called smart TV similarly almost all electronic devices and gadgets like Smart mobile phones; Tablets PCs, etc. are enabled with smart features and the internet connections. All buildings, offices, schools/colleges, hospitals and organizations are supposed to use ICT technologies for improving the quality and efficiency of the service provided to smart city dwellers.

As internet technology advances so do the threat of cyber crime. Since the risk of cyber attacks is inherent, providing securities to IT-enabled services have is a big concern in smart cities. Domain specific knowledge is required to provide cyber security in a particular domain. While developing smart cities, a comprehensive architecture with security measures is to be considered in beginning. Our overall research challenges can be classified into the following aspects: Application security, Information security, Network security and System recovery. These security issues should require attention while planning smart cities. In times like these, we must protect ourselves from cyber crime and cyber attacks. Using antivirus Software's, Inserting Firewalls, uninstalling unnecessary software, maintaining backups, checking security settings, never give your full name or address to unknown, learning more about Internet privacy policies, use virtual keyboard for online transactions, use Private Browsing and Security patches. Never open suspicious e-mails and only navigate trusted sites are common techniques that can be used to prevent cyber crime are important ingredients for smart cities securities.

REFERENCES

[1] Sam Musa. "Smart City Roadmap". http://www.academia.edu/21181336/Smart_City_Roadmap

[2] "Building a Smart City, Equitable City - NYC Forward". http://www1.nyc.gov./site/forward/innovations/Smartnyc.page

[3] Deakin, Mark, ed. Smart cities: governing, modelling and analysing the transition. Routledge, 2013.

[4] Dept Business(2013) Page 7 https://en.wikipedia.org/wiki/Smart_city#Biz2013

[5] Cavada, Marianna, D. V. Hunt, and C. D. Rogers. "Smart cities: Contradicting definitions and unclear measures." In *World Sustainability Forum*, pp. 1-12. 2014. http://sciforum.net/conference/wsf-4/paper/2454

[6] Celino, Irene, and Spyros Kotoulas. "Smart Cities [Guest editors' introduction]." *IEEE Internet Computing* 17, no. 6 (2013): 8-11.

[7] Thing, Vrizlynn LL. "Cyber security for a smart nation." In *Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on*, pp. 1-3. IEEE, 2014. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7238277

[8] Belapure, Sunit, and Nina Godbole. "Cyber Security: Understanding Cyber Crimes." *Computer Forensics and Legal Perspectives, ISBN* 978, no. 812: 6521791.

[9] Richardson, Robert, and C. S. I. Director. "CSI computer crime and security survey." *Computer security institute* 1 (2008): 1-30.

[10] http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/what_is_network_security/index.html?referring_site=smartnavRD

[11] Laxmikant Vishwamitra, B.P. Singh, (2004), Cryptography and Network Security.

[12] Nanni, Giampiero. "Transformational 'smart cities': cyber security and resilience." *Symantec Corporation* (2013).

[13] Urban Analysis and Modeling. (n.d.). *Massachusetts Institute of Technology (MIT)*, 2014.

[14] Celino, Irene, and Spyros Kotoulas. "Smart Cities [Guest editors' introduction]." *IEEE Internet Computing* 17, no. 6 (2013): 8-11.

[15] Thing, Vrizlynn LL. "Cyber security for a smart nation." In *Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on*, pp. 1-3. IEEE, 2014.

[16] Dharamdas Kumhar and Avanish kumar, "QRED: An Enhancement Approach for Congestion Control in Communication Networks", INDIACom-2018; IEEE 5th International Conference on Computing for Sustainable Global Development, Proceedings. IEEE, vol. 12, pp. 634-647, 2018.