IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 1 (January. 2019), ||V (III) || PP 63-71

Digital Security for Smart Cities in India: Challenges and Opportunities

Ashish Chandra Swami, Dr. Ritu Bhargava
Research Scholar, MJRP University Sophia Girls College, Autonomous, Ajmer
Corresponding Author: Ashish Chandra Swami

Abstract: Smart cities are need on an hour for the holistic development and growth of nation. Government is committed to provide basic services to the people living in urban areas with Intelligent Governance. Such governance in smart cities could be provided to its citizen through the use of Digital Gadgets and creating a network of Digital services. Digital network is a combination of interconnected digital devices creating Internet of Things, while communicating and exchanging services to each other producing voluminous data. This data produced is converted into knowledge and self-operated services using Big Data mechanism. IoT and BigData techniques are Digital services creating new cyber world. This Cyber world of Smart Cities will have all related information for Intelligent Governance. As Data is becoming more powerful than any other source of energy security mechanisms has to be adopted to keep them safe and secure for providing better governance to citizens of Smart City. This paper provides key components and pillars of smart city and mechanism that have to be kept in mind for securing Data and protecting it from Cyber criminals. This paper also proposes a Digital Security Task Force establishment for controlling and protection of Cyber network and digital data. It also suggests components for Governance and Management solutions for Cyber challenges.

Keywords: Smart Cities, Security, Digital Forensics, Cyber Security, Challenges of Smart City, Cryptography, Digital Network.

Date of Submission: 13-01-2019 Date of acceptance: 29-01-2019

I. INTRODUCTION

The Smart Cities initiative is a striking innovative activity by the Indian Government to provide momentum for financial development and enhance the personal satisfaction of individuals by empowering neighborhood improvement and outfitting innovation as a way to make keen results for natives. A brilliant city is a urbanized zone where various divisions collaborate to accomplish practical results through examination of logical continuous data shared among part explicit data and operational innovation frameworks. Keen Cities will use most recent computerized gadgets for the smooth working of the different administrations made accessible to the natives. Various activities will be taken by the Government too to give opportune and rapid administrations to its national in this manner making E-Governance to walking ahead towards Intelligent Governance.

With the expansion of Digital system and gadgets Cyber security will end up one of the key difficulties as a large portion of the information will be on the web. Today Cyberspace contacts pretty much all aspects of our day by day life. Be it through broadband systems, remote signs, neighborhood systems or the monstrous frameworks that control our country.

The risk from digital assaults and malware isn't just obvious yet in addition extremely troubling. There can't be a solitary answer for counter such dangers. A decent mix of Law, People, Process and Technology must be set up and after that an exertion be made to fit the laws of different nations remembering normal security measures.

1.1 Key Parameters of a Smart City

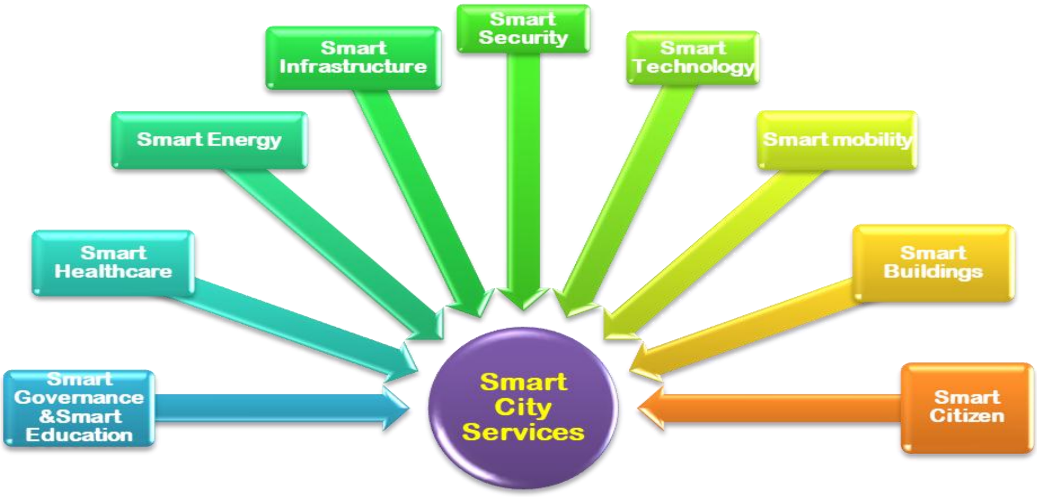

Fig: Key Issues / Parametrs of Smart City

- **Smart Governance and Smart Education:** Digital Government services; e-Government, e-Education, Digital school / education arrangements
- **Smart Healthcare:** Digital Healthcare; Distance Doctor Technology, Use of e-Health and m-Health frameworks Smart and associated medicinal gadgets
- **Smart Energy:** Smart Management of Energy; Digital frameworks, Digital meters, Intelligent vitality stockpiling
- **Smart Infrastructure:** Smart Administration of Infrastructure; Sensor systems, Smart control of clean and potable water and waste administration
- **Smart Security:** Threat Detection using Smart Bot; Digital Surveillance, Biometrics, Simulation displaying and wrongdoing insurance, Advanced proactive antivirus assurance
- **Smart Technology:** 5g & 4G availability, Uninterrupted Connectivity; Super optical fiber, Free Wi-Fi
- **Smart versatility:** Intelligent portability; Advanced traffic the board framework (ATBF), Parking the executives, ITS-empowered transportation evaluating framework
- **Smart Buildings:** Renewable Energy creation, Sustainable Buildings; Advanced Heating Ventilation and Air molding frameworks, Lighting Equipment
- **Smart Citizen:** Citizens of Smart City shall be trained to use the services and facilities available in the surroundings for better utilization and economic development.

Till 2020 worldwide Smart city marketplace is estimated to go beyond USD $1.5 trillion, with one-portion of smart urban communities from North America and Europe. E-Services to residents, for example, m-Payments, m-Exchange, m-Sharing, and so forth, will engage natives with continuous access to individual information and related administrations.

Essential to the formation of keen urban areas is the producing, investigating and sharing of expansive amounts of information. For sure the primary point of brilliant urban communities advancements is to make urban areas information driven; permitting city frameworks and administrations to be responsive and follow up on information progressively.

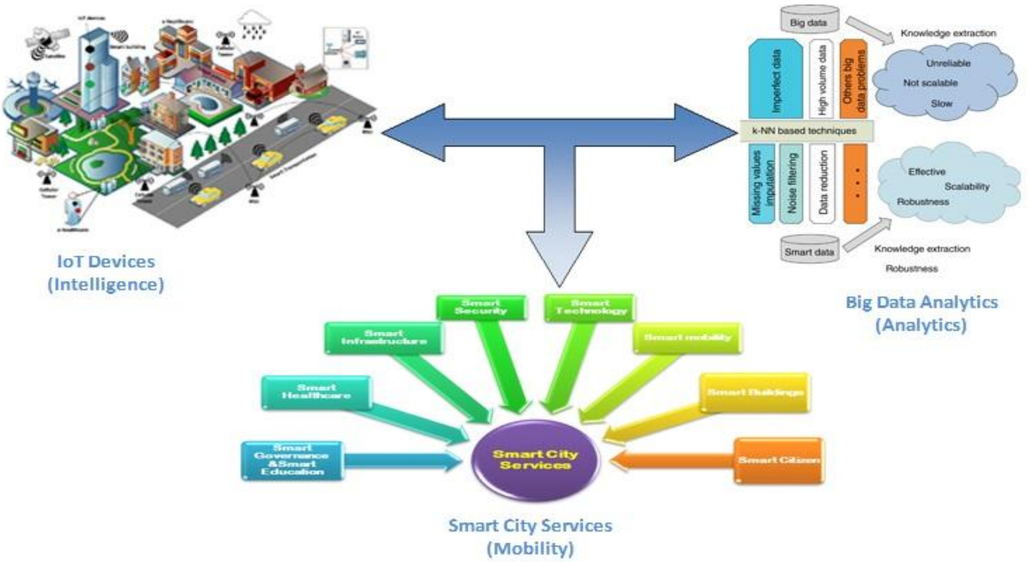

Fig: Utilization of Internet of Things (IoT) Devices & Big Data for Smart City Services

❖ **Intelligence:** Initial and most significant phase of security is deep observation and insight data congegation. This calls for gear, for example, CCTVs and Biometrics equipment and programming to gather the basics in its crude, natural shape. Anchored organize for transmission of information is vital to guarantee non-treating of information.

❖ **Analyzing Data gathered:** Analytics enable process, to translate and understand the terabytes of data and information gathered, by giving anchored stockpiling, investigation and measurable apparatuses. Transformation from byte-sized to chomp measured for powerful aversion against dangers or response to a disaster and give situational mindfulness.

❖ **Channelizing the Resources:** There is human mediation in any security establishment with physical security contraption from edge insurance to specialized gadgets for work force progressing. The powerful assembly of individuals and gear is significant to the whole foundation of an immovable and anchored area. The interconnectivity of individuals, gadgets and associations in the present computerized world, opens up new susceptbilities — passages where the digital crooks can get in.

1.2 Key Challenges

The duplicating impact of the present cybersecurity challenges displays a dark universe of dangers that frequently originate from surprising or unexpected spaces which have a heightening impact.

- The pace of progress – can the Smart City's cybersecurity keep updated?
- New item dispatches, mergers, acquisitions, advertise extension, new innovation
- A system of systems has made information open all over the place, whenever
- One defenseless gadget can prompt other powerless gadgets
- Traditionally shut working frameworks can be gotten to remotely
- Cloud liabilities and Big information – capacity and server security challenges
- Bandwidth utilization from billions of gadgets will put a strain on the range of different remote interchanges.

1.3 Pillars of a Smart City

- **Institutional Infrastructure:** alludes to exercises identifying with administration, arranging and the executives of a city. ICT has given another feature to this framework making it national driven, proficient, responsible and straightforward.
- **Physical Infrastructure:** alludes to its load of cost-effective and savvy physical foundation, for example, the urban versatility framework, rapid broadband foundation, the lodging stock, the vitality framework, the water supply framework, sewerage framework, sanitation offices, strong waste administration framework, seepage framework, and so forth which are coordinated through utilization of innovation.
- **Social Infrastructure**: identifies with parts that empower advancement of human and social capital, for example, the training, medicinal services, stimulation, and so on. It additionally incorporates execution and innovative expressions, sports, the open spaces, youngsters' parks and gardens.
- **Economic Infrastructure**: relates to creating legitimate framework that produces business openings and pull in ventures.

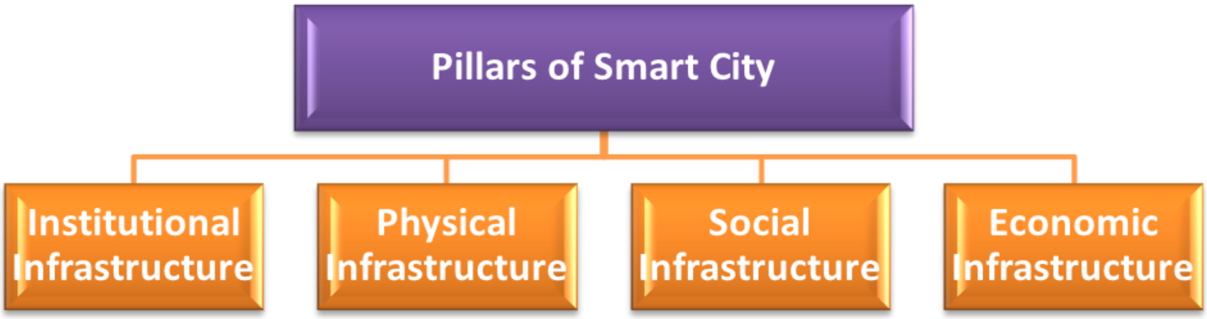

Fig: Pillars of Smart City

The development of smart urban areas and the expanding requirement for availability and interchanges will imply that more data is being accumulated and translated. This examination at that point gives knowledge on acceptable behavior and respond to basic circumstances. The transmission, examination and capacity of huge information will trigger the requirement for data security at all stages.

II. SECURITY IN SMART CITIES

Brilliant (astute) physical, social, institutional and monetary framework of Smart Cities guaranteeing quality life of residents in a maintainable domain. It is normal that such a Smart City will create alternatives for all occupants to seek after their occupations and interests definitively and with euphoria. (As indicated by the Indian Government Draft note on Smart City arrangements)

Keen reconnaissance innovation or investigation to deal with the group, traffic, digital safety, information protection, construction law to oversee characteristic/man-made fiascos and so on, are key aspects that could make a urban area safe and anchored for a national to flourish.

2.1 The ascent of digital danger

Viable cyber security is progressively mind boggling to convey. Digital crooks are taking a shot at new systems for traversing the security of built up associations, getting to everything from IP to singular client data — they are doing this with the goal that they can cause harm, upset touchy information and take protected innovation.

Consistently, their assaults turn out to be increasingly advanced and harder to overcome. In light of this continuous improvement, we can't tell precisely what sort of dangers will rise one year from now, or in coming few years' time; we can just guess upcoming dangers that will be considerably more unsafe. We can likewise be sure that as old wellsprings of this danger blur, latest techniques will develop for their rectification. In spite of this vulnerability — truth be told, as a result of it — we should be clear about the kind of security controls required

2.2 Cyber-assaults have changed the hazard scene

City-wide issue of cybersecurity is not only an innovation hazard. Since numerous open doors for IoT will emerge through mechanical joining and joint effort, which will keep on expanding in multifaceted nature — this unpredictability breeds chance.

A standard way to deal with hazard the executives accept that the trust limit is as of now characterized. What is absent in the hazard centered and techno-driven methodology is everything identified with the administration of trust, i.e., the new capacities and forms, and the new arrangements and structures required to extend the hazard limit.

Hazard Landscape

To successfully deal with the dangers in a Smart City, it is vital to obviously characterize the cutoff points of that biological community. We likewise needs to choose what we will oversee inside those points of confinement: is it simply the dangers looked by gatherings of individuals that are in the city itself, or should we additionally attempt to impact the moderation of dangers looked by individuals/information outside the breaking points characterized.

III. SMART CITIES SAFETY ISSUES

Information Confidentiality and security threats: confidentiality and protection is considered as a fundamental human right and is ensured by Indian Constitution in various ways. Protection worries incorporate the worthy practices with respect to getting to and uncovering individual and touchy data about an individual.

Touchy data can identify with a number of individual aspects, for example, any data that can be utilized without anyone else or with other data to recognize, contact, or find a solitary individual, or to distinguish a person in setting.

Smart city advancements catch information identifying with all types of protection and definitely grow the volume, range and granularity of the information being created about individuals and spots. Security can be compromised and ruptured by various practices which are typically treated as unsatisfactory, anyway are a piece of tasks in a keen city eco framework.

- **Surveillance:** Viewing, following, tuning in to or recording an individual's exercises
- **Accumulation:** Blending of different parts of information about an individual to recognize a pattern or example of exercises.
- **Data spillage:** absence of information assurance arrangements can prompt spillage or inappropriate access of touchy data
- **Extended utilization:** utilization of information collected for duration longer than expressed or for purposes other than the expressed reason without the subject's assent

Unreliable Hardware: Other than known, significant worries about savvy urban communities sensors in the gear; structures and so on are uncertain and not tried altogether. Attributable to absence of institutionalization of IoT gadgets, the sensors are inclined to hacking. Infamous people can trap the sensors and feed counterfeit information, causing signal disappointments, framework shutdowns and so on.

Bigger Attack surface: Smart city tasks use complex, arranged get together of ICT framework to oversee different administrations. Any gadget that is associated with the system is helpless against being hacked; the quantity of potential passage focuses is increased in Smart Cities. By trading off a solitary gadget, it is conceivable to assault the whole framework or system. The powerlessness of frameworks is exacerbated by various issues including frail security and encryption; the utilization of shaky inheritance frameworks and poor support; course impacts; and human mistake.

Transmission capacity utilization: Large portion of the sensors utilize a decoded connection to convey, and subsequently, there are conceivable outcomes of security slips. The transfer speed utilization from lakhs of gadgets will put a challange on the range of different remote interchanges, which additionally work on other frequencies like radio, TV, crisis administrations, and so forth.

Application hazard: Apps have quickened the reconciliation of cell phones inside our day by day lives. From mapping applications, to long range informal communication, to profitability devices, to diversions, applications have to a great extent driven the cell phone upset and have made it as critical and as sweeping as it is today. While applications exhibit utility that is apparently bound just by engineer creative energy, it likewise expands the danger of supporting stakeholder own gadgets in a professional workplace.

As the association empowers representatives to use their very own gadgets, the requirement for utilizing similar gadgets to get to business related information definitely introduces itself. This presents for the most part two security dangers:

- **Malicious applications (malware):** the expansion in the quantity of applications on the gadget improves the probability that some may contain malevolent code or security gaps
- **App Susceptibilities:** applications created or conveyed by the association to empower access to corporate information may contain safety shortcomings

IV. GETTING IN FRONT OF DIGITAL WRONGDOING

Early cautioning and identification of ruptures are conclusive to being in a condition of availability, implying that the accentuation of cybersecurity has changed to danger insight. A condition of preparation to manage digital assaults requires practices that are insightful, considered and communitarian. No association or government can ever anticipate or keep all (or even most) assaults; yet they can decrease their engaging quality as an objective, increment their flexibility and limit harm from some random assault.

A condition of preparation incorporates:

- Designing and actualizing a digital risk insight technique to help key choices and use the estimation of security
- Defining and enveloping the associations broadened cybersecurity biological community, including accomplices, providers, administrations and business systems

- Taking a digital monetary methodology — understanding your crucial resources and their esteem, and putting explicitly in their assurance
- Using legal information examination and digital risk knowledge to dissect and envision where the probable dangers are originating from and while, expanding availability
- Ensuring that every one of the partners comprehend the requirement for solid administration, client controls and responsibility

Governments will be unable to control when data security episodes happen, however they can control how they react to them — extending location capacities is a decent place to begin. A well-working Cyber security Task Force (CSTF) can frame the core of compelling location. Overseeing digital dangers as per key needs should be the focal point of the CSTF. By relating important data against a safe pattern, the CSTF can deliver significant announcing, empowering better basic leadership, chance administration and business coherence. A CSTF can empower data security capacities to react quicker, work all the more cooperatively and offer learning all the more viably.

4.1 Cyber Security Components of a Safe Smart City

❖ **Surveillance framework and hardware:** The point of keen city is to give shared security nearness and ongoing reconnaissance with the utilization of camcorders. The cameras gather information in picture or video organize which might be checked from a focal area, and enable specialists on call for act immediately in a crisis circumstance.

❖ **Video investigation:** Video examination is the capacity of consequently dissecting recordings to identify certain items, conduct, spatial and worldly occasions. This is utilized in a wide scope of spaces, including excitement, Health care, observation, home computerization and so forth. These Video examination apparatuses can be utilized with a wide scope of modules for different purposes and can function as a proactive observing device, activating cautions to flag prompt consideration of concerned groups.

❖ **Data focus:** The server farm is the unified storage room for every one of the information gathered from the numerous sensors in the system. The server farm gives constant information to checking habitats for powerful activities. The server farm has applications for the activity of video the board, examination and traffic control and so on. The structure of server farm relies upon the sort of uses that are kept running in the brilliant city.

❖ **Command Center:** The war room gives a framework that can evaluate the coordinated data given by the server farm, for example, live video for occurrence reaction. It helps in faster examination of information for better basic leadership.

❖ **Knowledge Transfer:** It is critical to scatter the required learning and abilities for the smooth task and execution of the smart city activities. The concerned staff should be prepared in working the new and overhauled administrations and productively convey the yields.

4.2 Possible Solutions to Challenges

As referenced already, keen city advances have expansive assault surfaces that have various vulnerabilities, particularly in frameworks that contain inheritance segments utilizing old programming which has not been routinely fixed. Innovation arrangements expect to utilize best practices to relieve these dangers

This incorporates:

► End-to-end encryption
► Strong secret key arrangement
► Up-to date firewalls, hostile to infection
► Audit logs
► Isolation of confided in assets from open assets (DMZ)
► Implement manual supersedes on all frameworks

The point is to diminish the assault surface however much as could be expected and to make the surface that is unmistakable as strong and flexible as would be prudent.

Security as an Expense, to security as an Income

Security is typically situated as a compulsory expense — an expense to pay to be agreeable, or an expense to pay to lessen chance. In any case, moving to a model of security as hazard and trust the executives infers viewing security as an empowering influence; for instance, overseeing open information get to use the money related estimation of the information as opposed to concentrating on the insurance of the information itself. Actually, this change implies empowering the advancement of significantly increasingly expanded systems of systems, of more and new types of joint effort and portability, and of new plans of action. "Security as an Income" ought to be a backbone of the business.

Ceaselessly Learn and Develop

Nothing is static — not the lawbreakers, not the eco framework or any piece of its working condition — along these lines the cycle of consistent enhancement remains. Turn into a learning association: consider information (counting crime scene investigation), keep up and investigate new community oriented connections, invigorate the technique consistently and develop cybersecurity abilities.

Fiasco recuperation and back-up administrations

Server farms, either on location or off site, are at the core of savvy urban areas. Fiasco recuperation is a basic piece of the server farm's design. On the off chance that servers go down, is it vital that frameworks are brought back online as quickly as time permits and, when those frameworks are back going, need all their past outstanding tasks at hand operational. It is critical to distinguish the correct dimension of back-up required for different administrations.

Information back-ups ought to be done frequently, and as indicated by the accepted procedures, ought to be done off site. This aides in information insurance if there should be an occurrence of physical security rupture at the server farm.

4.3 Prominent Norms at Global Level

- **Data Protection Directives**: Recently the European Parliament embraced The EU General Data Protection Regulation (GDPR) which intends to reinforce and bind together information insurance inside the European Union. At the point when GDPR becomes effective in May 2018, the EU inhabitants will acquire control of their own information, all associations will have similar guidelines and will answer to one regulating expert. There are stringent limitations on profiling, and meaning of "assent" to gather/process information.

- **Digital get to Control Frameworks**: DACs must be worked to guarantee just the approved authorities approach smart city information and the systems. DACs are essential to shield the city's administrations from digital dangers, hacking or modifications to information. In these DACS, diverse dimensions of section can be allotted to various gatherings so as to guarantee that the opportune individuals see precisely the required measure of data. Isolation of obligations and refreshed database of who approaches the information and systems will help recognize causes when a rupture happens.

- **Privacy Enhancing Technologies**: PETs give people instruments, applications and components to secure their by and by recognizable data (PII) and direct how PII ought to be dealt with by various administrations. PETs have been characterized by the European Commission as 'a cognizant arrangement of data and correspondence innovation estimates that ensure security by disposing of or diminishing individual information or by avoiding superfluous and additionally undesired handling of individual information without losing the usefulness of the data framework. PETs incorporate moderately basic apparatuses, for example, advertisement blockers, treat blockers and removers, malware identification and capture attempt, site blocking, encryption devices, and administrations to quit databases held by information merchants. When all is said in done, these sorts of PETs are gone for ensuring PII on sites and cell phones and overseeing how information are taken care of by information agents.

4.4 Management and Recommended Solutions

A basic part of well-run smart city is its administration and the board structure and procedures. Administration gives the structure through which vital bearing is thought and set, and control and oversight managed. Then again the board comprises of driving and driving forward activities and managing the day-today running of administrations.

Setting up solid rule drove administration and the board is accordingly an essential for making a savvy city that tries to amplify benefits while limiting damages. Anyway to date, there are not very many reported instances of such administration and the board structures being established. Rather, savvy city activities have been acquired and created with minimal composed thought of protection and security hurts and opened into existing city the executives in an impromptu mold with insignificant vital oversight.

Given the potential damages and the related costs that can emerge, this piecemeal methodology should be stopped to be supplanted with a progressively key, facilitated approach that comprises of mediations at three dimensions: vision and technique (savvy city warning board); oversight of conveyance and consistence (keen city administration, morals and security oversight council); and everyday conveyance (center protection/security group and PC crisis reaction group). This methodology perceives that there is a requirement for coordinated effort between specialists in various areas to guarantee sharing of information and shared learning.

a) **Smart City Corporation**: in light of the security ramifications of smart city advancements and various reactions of the city's information rehearses, Government should establish up a Smart City Corporation Advisory Committee (SCCAC) to survey the manners by which the city specialists create, store and use information, and to consider issues, for example, classification, secrecy, recorded methods, cancellation, sharing and distributing as open information, and the capacity to direct legal inside reviews. The SCCAC shall distribute a lot of essential protection standards. Generally, these standards basically affirm that the city is following FIPPs (reasonable data practice standards) and its effectively existing legitimate commitments. They are supplemented by a significantly more nitty gritty security articulation that sets out the city strategy on protection issues.

b) **Transparent Information Arrangement:** A neighborhood government body in charge of open transport in Europe and organizing travel for many travelers day by day creates and deals with a huge measure of information from a various arrangement of sources. The association has received a straightforward way to deal with information security and information assurance arrangements, which are distributed on their site.
For each sort of information detail: what individual data they hold, why they gather that data, how they utilize the data; the period of time they keep it before erasing differs from 24 hours to 7 years, contingent upon sort and reason, how they secure it, how they share it, if any of the information are prepared abroad, how somebody can get to the information held about them, any pertinent protection takes note.

c) **City Computer Emergency Response Teams (CERTs)**: CERTs comprise of a group of key work force, drawn from the center protection/security group, IT administrations, smart city activities and crisis benefits, that spring vigorously when a brilliant city innovation encounters a cybersecurity occurrence and is hacked and records stolen or the framework disturbed or terminated.* CERT is like other crisis reaction groups that handle other city occasions. CERTs get ready nitty gritty plans of activity and responsibility/obligation on account of various sorts of episodes.

V. CONCLUSION

Smart Cities construction and establishment are an enormous market chance of 2.0$ trillion, with in huge number of urban communities projected to be set up by 2025. Smart Cities intend to give global scope of advantages, for example, better transportation, squander the board, vitality the executives, which will extensively enhance the expectations for everyday comforts for the residents. The test is to recognize that there are a lot of issues and worries that should be tended to, and to discover and receive answers for these that likewise empower the advantages of brilliant city advances to be picked up.

Keen city models should support improvement while not trading off on information protection and security. Brilliant city arrangements include multi-faceted improvements, completed by a differing biological community of suppliers including front line innovation including basic and complex ICT executions.

Notwithstanding, expanding ICT unpredictability infers expanding powerlessness, both to malignant assaults and accidental occurrences. By having hearty security and data insurance system and strategies set up, wellbeing for the two nationals and endeavors can be guaranteed. It is presently imperative to build up the great practices distinguished up until this point, to expand on and thoughtfully improve the recommended arrangements. When the arrangements are sent by and by, these should be assessed thusly and continuous learning mechanism should be connected.

Public Private Partnership associations should be established for succesfull implementation of Smart City utilities, technologies and administration, to utilize the skill of the private segment so as to convey the advantages of brilliant urban areas proficiently.

REFERENCES

[1]. Internet-of-Things Based Smart Cities: Recent Advances and Challenges, Yasir Mehmood, Farhan Ahmad, Ibrar Yaqoob, Asma Adnane, Muhammad Imran, and Sghaier Guizani, IEEE Communication Magazine 55(9) · September 2017

[2]. A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of Things for Smart Cities,” *Internet of Things Journal, IEEE,* vol. 1, no. 1, pp. 22–32, 2014.

[3]. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “In- ternet of Things (IoT): A Vision, Architectural Elements, and Future Directions,” *Future Generation Computer Sys- tems,* vol. 29, no. 7, pp. 1645–1660, 2013.

[4]. A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo, “A Survey on Facilities for Ex- perimental Internet of Things Research,” *Communications Magazine, IEEE,* vol. 49, no. 11, pp. 58–67, 2011.

[5]. J. Jin, J. Gubbi, S. Marusic, and M. Palaniswami, “An Information Framework for Creating a Smart City through Internet of Things,” *Internet of Things Journal*, *IEEE*, vol. 1, no. 2, pp. 112–121, 2014.

[6]. Source: Cerrudo, C. (2015) An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks.

[7]. https://www.ey.com/Publication/vwLUAssets/ey-cyber-security-a-necessary-pillar-of-smartcities/%

[8]. 24FILE/ey-cyber-security-a-necessary-pillar-of-smart-cities.pdf

[9]. http://www.sersc.org/journals/IJSH/vol10_no11_2016/18.pdf

[10]. Terence Eden, ‘‘Car Hacking – With Bluetooth OBD’’ June 12, 2012, <http://shkspr.mobi/blog/2012/12/car-hacking-with-bluetooth-obd/> (accessed 24.04.13).

[11]. Patrick R. Mueller. Comment: Every Time You Brake, Every Turn You Make–I’ll Be Watching You: Protecting Driver Privacy In Event Data Recorder Information, 2006 Wis. L. Rev.135.

[12]. The Town Talk, Technology: Only you – and your care – know where you’ve been.’’ May 24, 2013, <http://lobby.la.psu.edu/_107th/093_OBD_Service_Info/Organizational_Statements/SEMA/SEMA_OBD_frequent_questions.htm> (accessed 25.04.13)

[13]. *Cyber Security Challenges in Smart Cities: Safety, security and privacy*. Adel S. Elmaghraby *, Michael M. Losavio, Journal of Advance Research(2014)5, 491-497 Available from: https://www.researchgate.net/publication/26055929

Ashish Chandra Swami. “Digital Security for Smart Cities in India: Challenges and pportunities .” IOSR Journal of Engineering (IOSRJEN), vol. 09, no. 01, 2019, pp. 63-71.