International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/CSEIT241061239

Cyber Security in Smart Cities: Role of 5G Technologies the Indian Perspective

Putarjunam R[1], Kala N[2]

[1]Research Scholar, Centre for Cyber Forensics and Information Security, University of Madras, Chennai – 600005, Tamil Nadu, India

[2]Assistant Professor, Centre for Cyber Forensics and Information Security, University of Madras, Chennai - 600005, Tamil Nadu, India

ARTICLEINFO

Article History:

Accepted : 25 Nov 2024

Published: 15 Dec 2024

Publication Issue

Volume 10, Issue 6

November-December-2024

Page Number

1919-1931

ABSTRACT

The UN-Habitat World Cities Report 2022 published in June 2022 states that, population in urban areas of India is estimated to reach at 675 million and will be 43.2 percent of its total population by 2035. It will be the second highest figure, behind China's one billion. In last two decades, India and China experienced rapid urbanization and economic growth. As a result, number of people living in poverty reduced [1]. The Government of India launched "The Smart Cities Mission (SCM)" on 25 June 2015[2]. The aim is to spearhead development and quality of life in urban areas with the help of IT and IT enabled services.

The smart cities in India though growing in numbers are more of an up-gradation of the old legacy township where the basic amenities and infrastructure are being given a fresh look with implementation of the modern tools and development techniques. Presently many legacy manual systems for essential services like power, water, communication, transport and many public distribution systems lack the resources and capacity to meet the growing demand and aspirations of people. Most smart cities are seeing uncontrolled and uncoordinated developments with various agencies working in their comfort zones and SILOS have failed to adequately address the role of cyber security that comes as potential risk with such modern IT enabled services. Adherence to standards and protocols for cyber security in the smart city sector are mostly missing or being adopted in an adhocmanner.Since the concept of changing urban life style in the Smart Cities is in a very nascent stage, it throws lot of challenges for the administration to deal with issues of cyber attacks.

This research is aimed at identification and analysisof potential cyber security risks and challenges of smart cities. The focus will be to understand the entire

ecosystem of smart city challenges and desired security standards, various security regulatory frameworks in world &India and how they can be adopted to the Indian scenario. Further the latent capabilities and advantages of using 5G technology has been touched upon in conjunction with how its adoption id developing the Smart Cities can help.

This research finally proposes a way ahead to an integrated approach to smart city development, exploiting the available technologies.

Keywords: Smart City, Ecosystem, Urbanization, Challenges, Information and Communications Technology, Internet of Things, Cyber Security, Threat, Connectivity, 5G

Introduction

The *2018 edition of "Revision of World Urbanization Prospects"* produced by the Population Division of the UN Department of Economic and Social Affairs (UN DESA) notes that future increases in the size of the world's urban population in India, China and Nigeria will account for 35% of the projected growth of the world's urban population between 2018 and 2050. The report notes that by the year 2050, India will have 416 million urban dwellersadded to its Human Terrain Map[3].Migration of population from rural to urban areas is increasing numerically world over and India is no exception. With this rate of migration of human population there will be a need of approximately 500 to 600 new cities to accommodate this influx which may be termed as "Urbanisation". Smart Cities offer a conceptual solution to deal with such unprecedented migration of people and urbanization. It is often said that Urbanization in India is directly related to poor planning of infra development in the rural region and increasing aspirational needs of the rural population. A detailed analysis of the issues reveal that this inevitable phenomenon of migration to urban land requires to be dealt with differently and must be looked as an opportunity to growth.

Urban Governance- Inevitable Need for Transformation

As per info available on the official website of the NITI Ayog, Government of India, the urbanisation trends in India are a direct reflection of the structural changes that are taking place in the economy [4].It is imperative that we understand the contours of this rapid urban growth phenomenon in India.Huge employment generation in cities is creating influx of people from rural areas to urban cities in search of better life and economic development. This bringshuge opportunities for people to look for greener pastures predominantly driven by economic compulsions and better job opportunities.*India's rapid economic development, in a way is directly linked to this fast urbanisation. Two aspects driving this phenomenon of urbanisation are economy and poverty. This has generated jobs for people, improved India's gross domestic product.*

SMART Cities

A dynamic change was needed in the mind set of policy makers and project implementation core groups to have an integrated approach focusing on urban governance to make Indian cities future ready.In 2016, the first list of 20 cities was announced by the Government of India as part of the Smart City Mission (SCM) and the plan was to complete the

development of these 20 cities by 2022. The list has been updated by the Government to 100 plus cities as of date [5].

A Smart City is built driven by the benefaction and activities of forward looking, self-decisive, intellectually aligned and aware citizens meeting the requirements of good governance, environment, health conditions and basic amenities like water, electricity, education and social security.Investments in improvement of human and social capital, efficient transport system,development & management of reliable communication, a good quality of life, efficient management of natural resources and good governance are key to developing a 'Smart City".

real time, accurate and authentic information and data mobility at all levels. **A Smart City encompasses** IT enabled solutions for management of Water, Waste, Electricity and other Citizen Services.

Figure 1: Smart Solutions for Smart Cities-Illustrative List; Source: http://www.gudcltd.com/smart-cities

Smart City Enablers

The primary objectives of building Smart Cities are creating state of the art infrastructure & supporting services, growing economy and maintainable dwellings by consolidation of financial resources and implementable development activities. Technology must be looked as a support for speedy execution and sustenance of the terminal objective of creating the best and state of the art Smart City.The Institute of Electrical and Electronics Engineers (IEEE) envisions a smart city as one that brings together technology, government and society. Following are the characteristics(key enablers) for Smart City [6].

- Developing**Economy**
- Good**Governance**
- Improved standard of **Living**
- Happy and contended**People**
- Fast**Mobility**
- Healthy**Environment**
- Reliable**Technologies**
- Efficient **Services**

Smart City development incudes innovative digital technology application in every aspect utilizing and leveraging Information and Communications Technology (ICT) to the fullest extent possible,shaping the urban landscape into a dynamic and continuously evolving system. This demands, fast,

Digital technology is a common enabler employed across projects to solve urban challenges, enable efficient city managementand foster transparent and accountable governance. Use of video evidence to help reduce the crime rate, environment sensors for automatic weather and air quality monitoring & lightening detection, flood sensors for timely warning and response, Wi-Fi on BRTS corridors to improve ridership, CCTVs and GPS are few areas that can be immediately implemented.

Need for Robust & Reliable Connectivity

A robust network can provide reliable connectivity across the length and breadth of a city opening excellent opportunities for individuals, households, businesses, institutes and government bodies who can be benefitted from information, communication, banking, ecommerce, location tracking, collaboration, entertainment, internet of things, cloud computing and storage, e-governance, security, education & training among others. A robust network of connectivity provides an information superhighway and helps create a product and services economy that rides over-the-top of the connectivity network.

The availability of strong connectivity network can provide an impetus to the local business environment

and strong governance which are inherent to any successful model. Some of the benefits of a robust and reliable connectivity are:-

- **Economy -** Fast and secure internet connectivity, digitization and effective ICT regulations will always bring positive impacts on the economy and GDP. A strong IT system avoids revenue loss. Downtime could mean economic loss, so it's crucial to have a reliable network to reap the benefits.
- **Reduced Processing Time -**Centralized data and an automated Decision Support System (DSS) will significantly reduce the processing and decision making time.
- **Secure data –** A strong data protection and a secure network will help to keep confidential information secure.

Smart City Complexity

Smart city development initiatives have brought about considerable change in the people, processes, policies and technology to achieve the set goals. Long-term objectives of a smart city is to improve the efficiency of services provided to citizens and bring perceptible change in their quality of life. A smart cityintegrates technology to achieve these objectives.

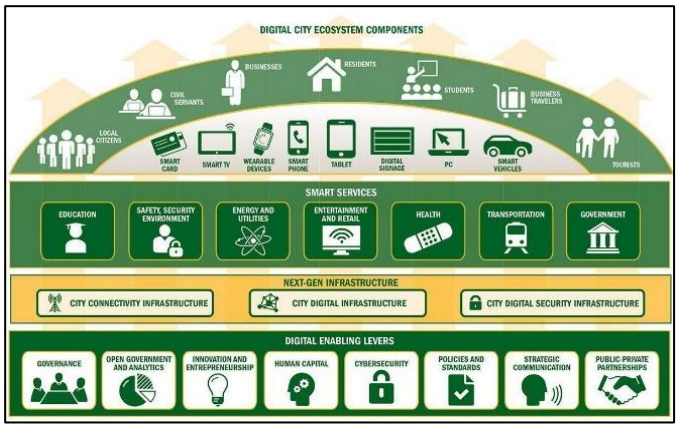

Figure 2: Digital City Ecosystem Components;Source: https://www.pinterest.com/pin/574209021232033302/

Smart cities epitomise the concept of an ecosystem that aims to drive digital innovation. The complexity in this type of ecosystem arises because of high stakes and reliance on the third party and private players for various services and integration. Asmall disruption of any of the components of this complex interlinked ecosystem will have a terrible consequence on the interoperability, reliability and success of the whole system.

Most of the security incidents in such a complex intertwined ecosystem of a Smart City emerge from poorly managed critical organisational assets because third parties are being made responsible for operating and maintaining critical infrastructures like Internet of Things (IoT) and Cloud without any security clearance and review. Availability of trusted and reliable data is the backbone of successful operations in a Smart City, but a potential cyberattack could corrupt data on the grid and controls of the systems leading to far reaching implications and total breakdown of the system.

Cyber Threats in Smart Cities

Smart cities, while providing unprecedented economic opportunities will also give excellent opportunities to cyberattack because of the large number of interconnected devices. Smart cities are dependent on robust machine-to-machine (M2M) connectivity and a reliable decision-support system. But these are also the greatest risks. Theinterconnected devices are the easy targets of cyber attacks because most of these devices are deployed without changing their default and generic settings. This directly affects the security and privacy issues for the people living in these Smart Cities.

Attacks on infrastructure and smart cities cannot be compared with attacks on industries for they are of a larger magnitude and impact. Smart city and infrastructure attacks can create utter chaos even at regional or national level. Interconnected devices without standard protocols being used by various stake holders in a Smart City environment are the best targets for Cybercriminals. This happens more often because every third party involved in the development of a smart city works in a SILO and

follows own protocols. Smart Cities provide cyber opportunists a large canvas for attack and exploit into broader campaigns:

- Self-propagating malware and worms, DDoS attacks, Ransomwareetc.could sabotage the entire ecosystem by compromising information related to Healthcare, Social Security and Banking Credentials, Electrical Grids, CCTV Network, Fire Alarm Systems and many more.
- Cyber vandalism and physical damage to critical infrastructure by the Cyber Activists can lead to breakdowns and financial loss that may be difficult to sustain.
- Man-in-the-middle attack can create breach and interruptions in the communication and other networks including water supply and expose them to biological hazards
- Unprotected infrastructure such as EV charging stations and CCTV surveillance feeds, Access Control Systems are easy targets that can be exploited for fraudulent transactions and data & identity theft.
- Device hijacking can help any attacker take control of a device and alter their basic functioning protocols. Ransomware attacks on Energy Management Systems (EMS) can help in theft of power and electricity which in turn can result in revenue losses to the exchequer.
- RFID and Wireless Sensor Network(WSN) which are extensively used for surveillance & monitoring and collection of data related to physical and environmental conditions like temperature, humidity etc. in a Smart City environment are vulnerable to snooping, spoofing, tampering, alteration and gaining unauthorized use & access that can compromise integrity, availability and confidentiality of data.
- Smart phones and smart grids (connected to embedded systems) which use WiFi, Bluetooth and GPS can be subjected to DoS attack, malwares, Botnets thus resulting in privacy issues, data theft, altering messages, intercepts, interruptions and economic loss.
- Smart communication, smart mobility, e-commerce and banking which are integral to Smart City plans are vulnerable to being targeted for software errors, malfunctioning, jamming, Supply chain attacks etc. bringing loss of reputation.

Security objectives for smart cities

All stakeholders - governments, software providers, device manufacturers, network integrators, service providers and above all the policy makers and implementersneed to integrate solutions that abide by four cardinal objectives:

- **Availability:** Actionable, real-time, and reliable data being made available is important for any smart city to thrive. Security systems need to facilitate and not impede availability. Collection, moderation, and sharing of data and information are critical.
- **Integrity:** Reliable and accurate data are very important for building a Smart City.
- **Confidentiality:** Adequate security measures must be taken to prevent unauthorized access to sensitive information.
- **Accountability:** User interactions with various systems must be logged and audited periodically to ensure accountability. Strong authentication is necessary to achieve security objectives and prevent intrusion and hacking.

Countermeasures - Can smart cities be secured and trusted?

Cyber security in Smart City environment is the biggest challenges. Therefore Cyber security must remain a prerequisite for development plans of Smart Cities. The cyber security plan must adjust and adapt to the requirements and complexities of the new digital landscape. There are highly efficient and reliable solutions available to address these issues. Therefore putting in place a reliable cyber security

apparatus to defend the infrastructure will need a concerted and joint effort involving both the local administration and private sector organizations. Some of the important points that need attention are: -

- Identification and prioritization of critical assets.
- Segregation of critical private assets from the public network.
- Establishbenchmark for operation of critical assets and ensureadherence.
- Immediate replacement of components in case of compromise or forced shutdown.
- Quick reaction plans, backup facility, cloud management and manual overrides.
- Access Control, Authentication and Encryption.
- Monitoring and Analysis of logs and feeds.

Challenges

The challenges to put in place a workable solution to deal with the emergingcyber security issues of Smart Cities are equally complex as this ecosystem itself. A single solution to deal with all the threats and vulnerabilities is a hard reality. Since the entire ecosystem of Smart City is practically built not as an integrated solution but in SILOS of independent systems, the compulsions are going to be difficult to be dealt with. "One solution fits for all" cannot work but the need is put in place a framework that can be used as a guideline to plan and execute such mega projects. Therefore it is imperative that an in-depth understanding of the underlying challenges to be dealt with is listed.

Smart City Issues	Challenges
Complex ecosystem	• Maintaining scalability of infrastructure • Strategic Management of assets • Deployment & integration of subsystems • Patch updates & Log analysis • Maintaining Operational synergy between agencies/third parties • System interdependencies & Cascade effects
Cyber Attacks	• Hardware capabilities & configurations • Use of insecure legacy systems • Large and complex attack surfaces • Poor maintenance • Virtualization, Crypt & Data analysis
Software vulnerabilities	• Insecure isolation techniques • Configuration errors • Software design and vulnerabilities/bugs • Weak software security and data encryption
Legislation and Policies	• Gaps in Policy frameworks • Interoperability between local & policies • Leadership & responsibility Management

Table 1: Smart City: Issues and Challenges

Global Initiatives: Policies, Standards and Frameworks

Implementation of "SMART" concept in a smart city will heavily depend on the exploitation of technologies and concepts like **IoT, ICT solutions, Wireless Access Network, Integration of devices and services, Quality and speed of delivery of services, Disaster Recovery Mechanism** all of which are essential to guaranteed availability of various services in the ecosystem. Future implementation of Smart City projects will highly depend on the availability of high speed connectivity - anytime, anywhere and with anything. This will require the following: -

- Better speed to upload and download data.
- Low Latency (negligible delays).
- Larger device density and big data capabilities.
- More efficient implementation of virtual networks.
- Better support for simultaneous connections.
- Excellent quality of service.
- Highly secure and encrypted subscriber identity.

- Authentication confirmation for roaming subscribers.
- Secure identity management.

Across the world communities have become more and more dependent on emerging technologies like IoT, Cloud, which forms the backbone of successful Smart City projects. In order to ensure effective cyber security in this race for urbanization various initiatives have been taken by many governments, non-governmental organisations, global think tanks, corporate houses and cyber security forums. All these initiatives are based on the fundamental pillars of **Knowledge & ExperienceSharing**, **Effective Regulations**, **Strong Framework and Standards**, **Capacity Building**, **Compliance & Continuity**, **Legal Policies& Measures** and **Asset Management**Some of the global initiatives on policies, standards and frameworks [7]in this area of concern over the years are given below:-

Policy/Standards/Framework	Salient Points
Government of India, Ministry of Housing and Urban Affairs (MoHUA): Cyber Security Framework for Smart Cities (2016)	Advisory to all smart cities on conformity to Cyber Security Framework for Smart Cities
Data Security Council of India (DSCI) and PWC: Report on Creating cyber secure Smart Cities.	• Guidelines for stakeholders. • Importance of the need to enhance cyber security of smart cities.
Tata Communications: How to secure the smart cities of the future: A smart approach to city-wide data security- (2019)	• Guidelines to keep smart cities safe. • Security framework covering all the technology layers
USA Government Internet of Things Cyber Security Improvement Act, 2017	Cyber Security standards for IoT devices.
European Union (EU) Network and Information Security (NIS) Directive for Sectorial Supervision	Directive on supervision of Cyber Security of critical market operators.
European Union Agency for Network and Information Security (ENISA) Guidelines for Cyber Security of Smart Cities	• Guidelines for security. • Suggestive model for public transport, health services and infrastructure.
Smart Cities Council Australia and New Zealand: Guidelines & Best Practices in Smart Cities (2018)	Best practices for cyber security standards.
NEC Corporation Japanese	Security Requirements and Technologies for Smart City IoT.
Government of UK, Department for Digital, Culture, Media & Sport: Guidance collection on Secure connected places (smart cities)	A comprehensive collection of government guidance on the security of connected places.

Table 2: Policies, Standards and Frameworks

Global Smart City Cyber Attacks

Most of the smart cities in the world have faced cyber attacks some time or the other which have only become more severe and sophisticated. Some of the known instances are listed below.

Global Smart City	Cyber Attack Effect
Atlanta, Georgia March 2018	• Encrypted files. • Target - Police records and video footage. • Affected functioning of services and payment systems. • Recovery cost - Approx $17 million.
Baltimore, Maryland 7 May 2019	• Ransomware attack. • Target - government computers. • Essential citizen services affected.
Greenville, North Carolina, April 2019	• Ransomware attack. • Approx 800 computers affected. • Target - Police department computers.
Ukraine 23 December 2015	• Compromised information systems • Target - Energy distribution companies • Affected electricity supply.
Istanbul, Turkey July 2013	• Target - Istanbul Ataturk International Airport. • Affected passport control system.
Pune, India February 2021	• Ransomware attack. • Target - Pimpri-Chinchwad Municipal Corporation (PCMC), Pune • Affected approx 25 servers of PCMC Smart City project.

Table 3: Global Smart City Cyber Attacks

Prevention and Mitigation

As we strive to put in place areliable mechanism to deal with this increasing cyber threats in the smart city environment, it must be understood that given that there are multiple stakeholders in this ecosystem the need is to develop a holistic plan that meets the requirement of all stakeholders. The aim should be to create “Cyber Secure Smart Cities”. Many countries have deployed technologies and controls to mitigate cyber attacks, prevent breaches and data theft, maintain network without any breakdowns and avoid disruption of essential services that can completely shut down a Smart City’s functioning.

Smart cities function on the basic foundation of advanced technologies such as Internet of Things (IoT), Information Technology (IT), and Operational Technology (OT), Systems and Devices which work in an integrated environment. Therefore, the prevention and mitigation technique to deal with cyber security challenges also need to be based on a solid integrated technological approach that can provide authentic and actionable information to help maintain services without any breakdown.Cyber threats are always dynamic and associated with an element of surprise henceno single approach can stop these attacks. Professional and seasoned criminals will always find ways to remove any roadblocks and attack all vulnerable assets. Following are important:-

- Develop an effective cyber security organization.
- Periodic security audits, reviews and assessments.
- Implementstrong defensive measures.
- Solicit top management support to ensure timely & correct implementation of policies and frameworks for dealing with cyber security issues of Smart City projects.
- Despite growing incidents many managers feel investments in general security arrangements will also protect their infrastructure from cyber security breaches and attacks, which is not true. Educating all about cyber risks and securityby conducting awareness and outreach programs is an essential part of the overall security framework in any Smart City environment.Organizations seldom give this the required importance.
- Providing resources to developers will help them understand potential security issues and implement best practices.
- Include vulnerability assessment and penetration testing as part of policies for implementing IoT solutions.
- Implementing identification, authentication and strong passwords policies to avoid phishing attacks.
- Timely software updates to mitigate potential vulnerabilities.

Implementation of 5Gin Smart Cities

The scope for improving quality of living in Smart Cities is phenomenal and has not been exploited to the fullest. The components and indicators of Quality of Life are no longer restricted to the classical aspects of health, education, governance, and economic conditions. The 4th Generation Long Term Evolution (4G LTE) system has many limitations. To name a few: -

- Unencrypted data transmission
- Limited variety of applications
- High power consumption
- High cost of bits of data
- Poor authentication confirmation
- High latency (transmission delays)
- Poor simultaneous connections

A comparison between 4G and 5G capability is given below.

Table 4: Comparison - 4G and 5G Technology

Capability	4G	5G
Data rate (Peak)	1Gbps	>=20Gbps
Latency (minimum round-trip time)	10ms	<1ms
Bandwidth (Data)	2Mbps to 1Gbps	More than 1 Gbps
Max carrier aggregation	5	16
Carrier bandwidth	20MHz	20Mhz to >1GHz
Frequency	Under 6GHz	600Mhz to 100GHz
Use	• High speed applications • Mobile &wearable devices	• High resolution video streaming. • Remote control of vehicles • Robotic medical procedures

Need for better connectivity has been felt because of following:-

- Growth in number of connected devices
- Growth in variety of services & applications
- Global appetite for data analytics
- Universal desire for data visualization
- Corporate yearning for business intelligence for policy makers
- Growth in connected devices and Apps
- Appetite for data analytics
- Urban-Rural dichotomy
- Dropping cost of connectivity
- Varying consumer expectations
- COVID-induced changes
- Emergence of new technologies

It is envisaged that efforts required to change our systems and make it compliant with 5G communication network standards will be herculean task. However, this will be an inescapable requirement and vital in the future development of smart cities.Introduction of 5G will be able to exploit best use of vehicle to infrastructure technologies, navigation systems and automatically connect vehicles. The inherent advantages of 5G like greater transmission speed, capacity to handle higher network traffic and reduced latency will bring revolution in the services of sectors such as **Healthcare, IoT, Education, Autonomous Driving and Smart Cities**.

5G will increase the capabilities of technology, bring greater scope for the future Smart City applications and facilitate seamless integration of different applications. But the real challenge will be adopting the technology for various applications and services. Added to this will be the emerging requirements of the "**Seven Vs of Big Data"**namely – Variety, Variability, Veracity, Visualization and Value [8].

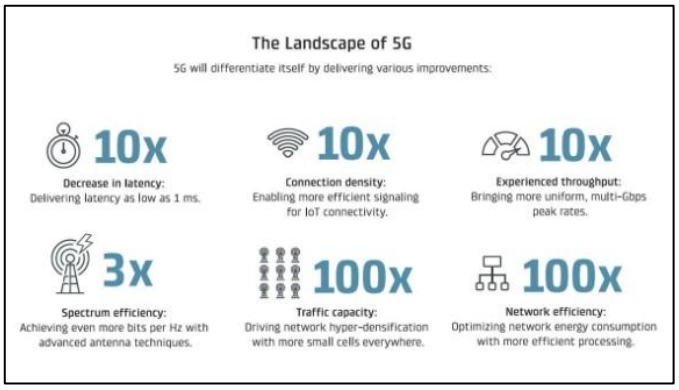

Figure 3: Landscape of 5G; Source: www.visualcapitalist.com

5G's will be able to easily transmitHD contents and overcome bandwidth limitations making mobile VR and AR main stream [9].

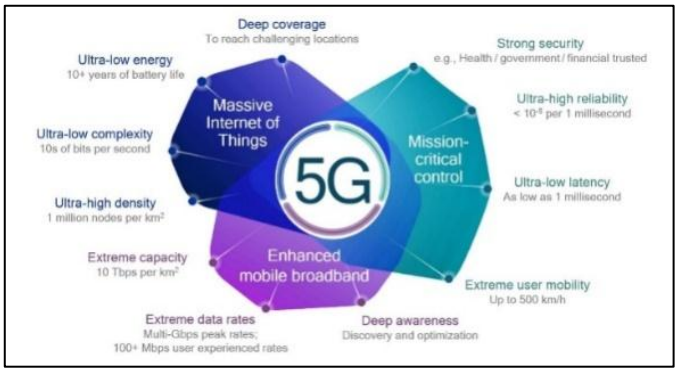

Figure 4: Everything about -5G; Source: https://www.itworldcanada.com

An efficient 5G enabled automatic transit management system is integral to Smart Cities with an aim to offer a seamless, cohesive, interoperable transport & travel machinerygenerally referred to as"Intelligent Transport System (ITS)". Implementing ITS will help solving issues like, traffic congestion, road safety, air pollution, economy of fuel etc. The major components of ITScan be summarized as:-

- Advanced traffic management system.
- Automatic vehicle location and fleet management system.
- Automatic vehicle detection system.
- Travel information system.
- Traffic control system.

- Toll collection system.
- Quick response to traffic congestion, pollution, and accidents.
- Improved navigation, fuel and time resource efficiency.

5G will be a game changer for **autonomous vehicle**technology. It will enable vehicle-to-vehicle communication and pave the way for development and deployment of new applications.

Indian Perspective on Smart Cities

Smart Cities Mission in India is still in the nascent stage and only about seven years have passed since launch of the mission in the year 2015. Close to two years of COVID-19 related lockdown in in the year 2019 and 2020 has put the pace of workmuch behind schedule and thrown new challenges related to finance, availability of equipment & technology or other policy and management issues. Considering that India's developing smart cities will always remain a potential target of cyber attack, the solution needs to be holistic and addressed in the correct perspective. Key factors to be borne in mind while framing any policy will be convergence of IoT, IT and OT related issues, interoperability of various systems & subsystems and their seamless integration.

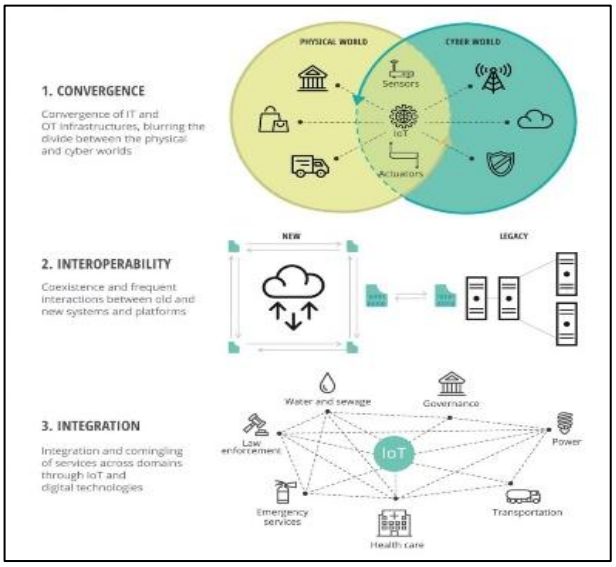

Figure 5: Key factors Influencing Cyber Risk in Smart City; Source: Deloitte Analysis

Initiatives by Indian Government

A. Smart City Governance

The Smart City Mission of Government of India is the responsibility of Ministry of Housing and Urban Affairs (MoHUA) [7]. Stake holders at the execution level includes:-

- Smart City Special Purpose Vehicle (SPV)
- Project Management Consultant (PMC)
- Master System Integrator (MSI)
- Original Equipment Manufacturer (OEM) and third-party vendors

A number of policies and regulations have been designed by the Government of India and many independent agencies aimed at addressing the cyber security issues of smart city infrastructure. Government of India, MoHUA released a model framework for cyber security in smart cities on 20 May 2016 covering the security of smart cities across different layers, namely sensor layer, communication layer, data layer and application layer [7]. The major guidelines include:-

- Using National Institute of Standards & Technology (NIST) reference for IT architecture for secured network.
- Recommendations for security related to storage and transmission of data in a Smart City environment. This includes systems, devices and services.
- Compliance with various international standards.
- Reporting of security incidents to Computer Emergency Response Team – India (CERT-In) and National Critical Information Infrastructure Protection Centre (NCIIPC).
- Dealing with biometric information in compliance with "The Aadhaar Act, 2016".
- Policy on storage, exchange, privacy and security of data related to health records in compliance with proposed "Digital Information Security in Healthcare Act (DISHA)"and "National Health Authority in India".

- Compliance with"The Personal Data Protection Bill (Draft)" for storage and processing of personal and sensitive data in Smart Cities.

B. Major challenges in India

Major challenges in addressing cyber security issues of Smart City projects of India have been identified as under; -

- A comprehensive Cyber Security policy is yet to be put in place in India.
- No nodal agency identified and made responsible for cyber security within Smart Cities.
- Initial planning of projects lack holistic cyber security considerations. Cyber security risk profiling of Smart Cities is missing as part of the plan.
- Absence of any formalised mechanism and policy to perform regular security audit and assessments of the smart city projects.
- Budget allocation for cyber security infrastructure never matches the actual requirements thus bringing inadequacies. Stakeholders involved in these projects have no or minimum awareness of cyber security issues.

C. The 5G initiatives in India

The roll-out of 5G services is expected to startfrom 01 October 2022. The trials will soon commence for achieving 3 Gbpsthroughput. Many Indian telecom companies have signed MoUsfor launch of 5G network in the country [10]. It is only a matter of time that the technology reaches the urban and rural area of the country. There is ample scope therefore to leverage this capability to ensure that the Smart Cities of India quickly grab the opportunity and take full advantage of it. High cost of infrastructure and spectrum will be an area of concern as to how the 5G proliferation takes shape in the country. According to Ericsson's research, 5G will enable Indian telecom companies to generate $17bn in incremental revenue from enterprises by 2030 [11].

Suggested Way Forward for INDIA

A. Smart City Mission

a) Ministry of Housing and Urban

1) Affairs (MoHUA)

MoHUAisresponsible to formulate rules, regulations and laws for urban development [7]. Some of the suggested way forward for MoHUA is:

- Develop and implement a comprehensive guideline for cyber security in smart cities. Such a guideline must include reference security architecture for smart cities.
- All stake holders connected with Smart City projects to explicitly follow security guidelines.
- Ensure information sharing and knowledge transfer for cyber security amongst stake holders of smart cities and other agencies.
- Define structure, role and responsibilities of security organisation for Smart City Mission.
- Cyber security enforcement mechanism be linked to budgetary sanctions.

2) Special Purpose Vehicle (SPV)

The smart city SPV being responsible for execution of project remains the most important stakeholder in the scheme of things. The entire success of the project rests on the SPVs ability to drive the project which requires creating synergy between various agencies, periodic monitoring and time bound implementation [7]. Suggested issues to be addressed at the level of SPVs specific to cyber security issues of Smart City projects are: -

- Budget allocation to meet requirements of cyber security.
- Monitor progress on decisions taken in the meetings of various stake holders.
- Ensure cyber security requirements are stated as prerequisites in tender documents and considered a must in the process of evaluation of technical and commercial offers by participating firms and contractors.
- Appoint and define the role and responsibilities of Chief Information Security Officer (CISO).

- Accreditation of skills, qualifications and experience of people being made responsible for various job roles in the project. Where required, complete background checks be done. Sensitive job roles must include non-disclosure agreements.

3) Project Management Consultant (PMC)

The PMC will be responsible to manage the design, implementation and operations of the smart city [7]. Following issues are important for consideration:-

- Cyber security experts must be part of the PMC team and made responsible for planning and implementation of the cyber security architecture.
- Be responsible for periodic audit &assessment of risks and security in respect of systems and devices, operating system, databases and network.
- Review of privacy policy to meet global standards.
- Periodic review and update of business continuity and disaster recovery plans.

4) Master System Integrator (MSI) and Original Equipment Manufacturer (OEM)

The MSI and OEM are responsible to ensure that all systems,services &components are implemented as per the standards laid down for development of the smart city. Since they form an important pillar of the Smart City Mission, following are suggested for implementation: -

- Prepare the parameters for development and testing of various systems.
- Develop plans for troubleshooting and conflict resolution.
- Prepare plans for directing processes.
- Prepare periodic business reviews like QBRs.
- Define and implement strategies for integration of devices and systems.
- Be updated and Research on latest technological developments in various fields of interest with a view to implement them as part of the project.
- Ensure systems and devices are updated with the latest patches regularly.

b) Roll out of 5G in India and Adoption to Smart Cities

The roll out of 5G and adoption to Smart Cities is inevitable, but given the federated governing system of the country, the technology may take a while to get fully implemented. [12]. Recommended way forward is:-

- **Structural changes:** Structural changes to existing core infrastructure need to be made to implement 5G. This will require a large investments and refinement of procedures and operations [13].
- **Level playing field:** Every OEM needs to be given a level playing field to adapt to the changes that 5G will bring in processing and handling of information. Operators have to be given sufficient time and resources to embrace new technology [13].
- **FDI and subsidies:** Foreign Direct Investments in telecom sector will bring in faster reforms. Subsidies to the initial players need to be considered by the government so that their tax burden is reduced and the benefits are transferred to the end customers.
- **Assigning 5G spectrum for private enterprise business:** Allotment of 5G spectrums directly to private enterprises may not be happening initially. Therefore they will have to source it from the telecom service providers. This has been done to protect the interest of telecom companies who are expected make huge initial investments in getting the spectrum and roll out the services. However this policy needs to change at the earliest to exploit the full potential of 5G capabilities.

Conclusion

Smart Cities were a distant dream just a few years ago. Though it is still early days, it is evident that the concept is going to drastically improve efficiency of services and change the lives of the people. All this

will come at a cost of making us more vulnerable to cyber attacks. It is imperative India cannot afford to be left behind in adapting to the changing technology and have insecure smart cities. Therefore implementing cyber security standards for Smart City will be important to ensure that they are secure and ready to defend any misadventure of cyber criminals. 5G technology and its ability to provide massive device connectivity and a massive speed and ability to compute data need to be exploited.

Challenges of cyber security issues in Smart Cities will become more and more complex to be handled therefore it must form part of the overall plan and architectural design of the Smart City ecosystem. Cyber security plan must adapt to the requirements and complexities of the new digital landscape. There are highly efficient and reliable solutions available to address these issues. Therefore putting in place a reliable cyber security apparatus to defend the infrastructure will need a concerted and joint effort involving both the local administration and private sector organizations.

References

[1]. https://unhabitat.org/wcr

[2]. Rumi Aijaz, “India's Smart Cities Mission, 2015-2021: A Stocktaking,” ORF Special Report No. 155, August 2021, Observer Research Foundation.

[3]. United Nations Department of Economic and Social Affairs News, New York, dated 16 May 2018; https://www.un.org/development/desa/en/news/population/2018-revision-of-worldurbanization-prospects.html

[4]. https://niti.gov.in/planningcommission.gov.in/docs/reports/sereport/ser/vision2025/urban.doc

[5]. https://smartcities.gov.in

[6]. https://www.ieee-pes.org/pes-communities/ieee-smart-cities

[7]. “Creating cyber secure smart cities” – A report co-authored by Sivarama Krishnan etal, Year 2018; Data Security Council of India & PWC; https://www.dsci.in/ ucch/resource/download attachment/9/Creating%20cyber%20secure%20smart%20cities

[8]. M. Ali-ud-din Khan, M. F. Uddin and N. Gupta, "Seven V's of Big Data understanding BigData to extract value," Proceedings of the 2014 Zone 1 Conference of the American Society for Engineering Education, 2014, pp. 1-5, doi: 10.1109/ASEEZone1.2014.6820689

[9]. Gohar, Ali and Nencioni, Gianfranco. The Role of 5G Technologies in a Smart City: The Case for intelligent Transportation System. Journals Sustainability. Vol.13, Issue 9, 10.3390/su13095188; Year 2021.

[10]. 5G Technology, Applications And 5G's Current Status in India and the World By ShailjaPurohit Updated: Friday, May 20, 2022, 0:11 [IST]; https://www.careerindia.com/general-knowledge/5g-technology-applications-and-5g-s-current-status-in-india-and-the-world-031749.html

[11]. India gears up for 5G but challenges remain: Article by Aaron Tan, Published: 30 June 2022; https://www.computerweekly.comnews/252522190/India-gears-up-for-5G-but- challenges-remain

[12]. News/Magazine/Corporate/” Here's What the Next Steps in India's 5G Path Could Look Like” by Krishna Gopalan; Print Edition: Sep 04, 2022; https://www.businesstoday.in/magazine/corporate/story/heres-what-the-next-steps-in indias-5g-path-could-look-like-345411-2022-08-24

[13]. Article “The way forward on 5G”:Economics, Mains Paper 3: Effects Of Liberalization On The Economy, Changes In Industrial Policy and their effects on Industrial Growth, Post date: une 14, 2022, The Indian Express; https://www.civilsdaily.com/news/the-way-forward-on-5/