**SMART CITIES AND RISING CONCERN OF DATA SECURITY AND PRIVACY**

*“If we don't carefully prepare these smart city projects, our economies could face catastrophic repercussions, from massive degradation of infrastructure to life becoming an Orwellian nightmare.*“-------[*Josh Lake*](https://www.comparitech.com/author/joshlake/)*[[1]](#footnote-1)*

*Abstract-* With a combination of sensors, data, and algorithms, urban centers around the world are now optimizing how they work, with the intention of improving their citizens ' lives. Smart city innovations have the ability to transform how we live and communicate in cities from traffic control to law enforcement, making communities more productive, reducing water use and much more.

The smart cities model deals with public data which at various stages of smart cities architecture are vulnerable to different protection and privacy risks. Hence in this model the importance of maintaining security and privacy is paramount. Significant issues of risk include the large quantities of data gathered and the possible effect on citizens' safety, the likelihood that hackers would steal this data, and enemies exploiting this distributed infrastructure to conduct attacks, bringing cities to a halt.

This paper reflects on problems related to security and privacy in the smart cities. The paper discusses the main uses of smart cities, and then examines their architecture from a security viewpoint. The paper also discusses the latest protection and privacy strategies for smart cities.

**Introduction**

India's government has initiated a 'National Smart Cities Project' seeking to build 100 smart cities around the world. Prime Minister Narendra Modi unveiled the project on June 25, 2015, with a budget of 48,000 Rs crore. About Rs 50,000 crore was distributed under what is known as the 'Atal Mission for Rejuvenation and Urban Transformation (AMRUT) for rejuvenation of 500 other cities.

The drive toward greater inclusion of smart cities seems imminent. Industries are now using technology in nearly every area of industry you can think about, and it's only a matter of time before policymakers truly adopt the method and adapt those innovations to daily facets of urban life.

**Meaning of a Smart City**

Due to the broad variety of methods and technology that can be called "smart," the precise concept of a smart city is a little fuzzy. Basically, they are cities that uses Information Technology to automate their operations particularly where the method includes collecting input from multiple sources, processing this data with algorithms, and then using it to enhance an assortment of different items[[2]](#footnote-2).

In addition to their technology expertise, they seek to take advantage of the new technical advances, use the unified strategy to enhance people’s lives, raise competitiveness and performance, minimize resource use, decrease prices, increase adaptability and make facilities more convenient[[3]](#footnote-3).

This data-focused approach offers a means for communities to make the most of their available wealth, facilities, and infrastructure, allowing them to provide people with a high quality of life. Such strategies would be critical frameworks for addressing the threats predicted from population booms and environmental pressures.

For smart cities to work successfully the following components are critical:

Collection of Data

Cities require knowledge to be knowledgeable, which they will use to make more informed decisions. They capture data from persons, their computers, appliances, sensors, cameras, RFID (Radio-frequency identification) processors, smart meters and other points of interest.

Together, these various sensors allow cities to see what is going on in real time, and also to collect historical data that can be used to make smarter decisions. Each of this detail is then used to make more detailed decisions in the latter stages. Such data collection points work in about the same way as our own senses, capturing and transmitting information about the world around us so we can behave accordingly based on the latest developments.

Communication

To connect smart cities, it is important that knowledge flow to where it is required. This is enabled by the Internet of Things (IoT) and other networking technologies that allow rapid communication between computers, servers, and points of action that collect data[[4]](#footnote-4).

In order to control their behavior, data may be sent to central servers where decisions are taken or sent to other smart devices. Such means of communication are close to our nerves, directing input from where it is found to where choices can be taken and also transmitting responses about where they need to go.

Analyzing data and taking steps

The various data streams come together to provide a more detailed image of what happens in a region. Often, real-time data can be paired with historical data to help make more detailed choices. Algorithms take into account the necessary details to assess the correct response, while human operators can be involved in such processes.

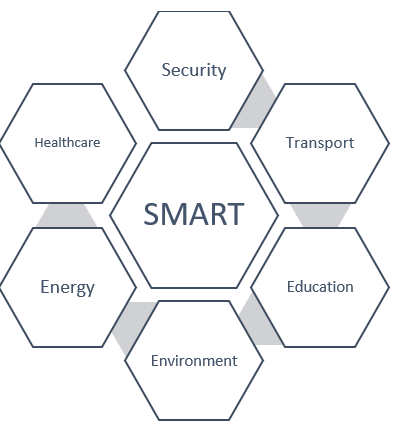
This technique can be used to address a variety of specific issues and optimize infrastructure, such as deciding the best time to turn a light green for a traffic control system, or when a street light will glow when a pedestrian walk by. When a decision is taken on the basis of the applicable evidence, the directive moves to the point of operation and the correct adjustment is made. The whole cycle is what makes a smart city[[5]](#footnote-5). A traffic light in a stupid city will only turn green depending on a timer, not taking into account local conditions and potentially causing traffic jams worse.

By seeing what is going on in a city and incorporating reliable, real-time knowledge into its decision-making processes, a smart city will behave in ways that help to provide better infrastructure, improve performance, cut costs, and more. Continuing our connection with the human body, the core of data processing is the brain, taking our sensory feedback and using our prior experience to make choices on the right action to take in a given situation. Much as our brains tell us the right moment to kick a soccer ball based on the feedback from our feet, the smart city decision-making process will send out garbage trucks just where and when they're needed, jumping over empty trash cans to make the collection process more effective.

Given the enormous gains that can come from smart city projects, there's a lot we need to be vigilant about as well. Key issues of risk include the large quantities of data gathered and the possible effect on peoples' safety, the likelihood that hackers would steal this data, and enemies exploiting this distributed infrastructure to conduct attacks, bringing cities to a halt.

Usage of Smart City Technology

Smart city model unlocks up doors for innovative technologies by connecting the real world to the ICT networks. The data collected from these physical spaces are processed and made available in the form of various services which allow applications to use the sensed data or control the physical world[[6]](#footnote-6), as shown in Fig. 1. This segment discusses the specifics of only a few main application categories in a smart city.



*Fig 1: Usage of smart city technology*

Transportation

The idea of intelligent transport is the materialization of the Intelligent Transport Network (ITS). This program uses the data collected by the smart city to handle a city's mobility requirements such as congestion control, real-time forecasts of urban transit departures, parking room management and real-time auto management[[7]](#footnote-7) etc.

Energy

Reducing energy use and stopping a city or individual user from breaching an power grid are only a couple of the other obstacles a city management authority faces. Smart technology systems use the commonly used sensor data to track and control technology from producing to using it. The apps allow authorities to keep all entities responsible for their energy consumption and carbon footprint.

Healthcare

Smart healthcare applications aim to improve the quality of the current healthcare systems by continuously monitoring the real-time data of patients for early diagnosis of infectious diseases. In fact, it offers patient monitoring capabilities for people suffering from chronic illnesses and online consultation. The systems access the cloud resources that contain the safety data transmitted, such as the ECG and EIT signals obtained by monitoring devices and other sensors. The big data element allows smart healthcare applications to track trends so that infections and plagues do not spread.

Education

Smart Education apps take advantage of the data gathered from numerous field sources to allow successful learning in a smart town. The data is gathered from the infrastructure, people and information processed by big data technologies[[8]](#footnote-8). The education process is enhanced with the provision of smart services. Moreover, this knowledge-based culture is being spread further to rural areas to better people's lives.

Environment

This category of applications deals with the creation of different environments, intelligently by controlling vastly deployed sensors. These applications manage climate intelligently, using omnipresent sensing and actuation. Building management, city noise management, CO2 heavy area detection and management, green reserve management, and resource waste control systems are few examples of such applications.

Security

Such technologies rely on context-aware protection systems focused on the sensors to provide technologies for risk reduction. Such technologies offer a defense approach that is ever needed to ensure public protection against serious natural disasters and terrorists.

System Faults and device attacks

Smart cities incorporate many things that make them insecure, too. These seem to require centralization, convergence and internet access. Online connectivity also offers attackers windows of opportunity which will allow them to access these critical systems[[9]](#footnote-9). Centralization and convergence open up the ability for them to cause significant damage.

In earlier days, when networks were more unavailable and utilities such as power grids were more localized, mass disruption without an invasion or systemic conflict was practically impossible to inflict. The attackers may have been able to penetrate and hack a power plant, but people continue to remember when suspicious persons loiter around critical facilities, making these techniques harder[[10]](#footnote-10). Likewise, the lack of centralization made it more difficult to plan threats that would create global disruption.

As we push into convergence with smart cities, more and more of our critical infrastructure and facilities are theoretically opening up for attack. What's more troubling is that not all the suspects appear to be in the same area[[11]](#footnote-11). While such threats can come from organized criminal cartels, the greater challenge comes from national-state-funded organizations who aim to interrupt public services or inflict economic damage.

Many of the best cases in real life haven't addressed high-tech cities, but they are also strong models from which we can extrapolate. In 2015, a Russian-linked cyber-attack shut off power for up to six hours for 230,000 Ukrainians, and an attack traced to Iran interrupted electricity for 40 million Turks[[12]](#footnote-12). All of these attacks have impacted regional facilities, turning electricity off from hospitals and traffic lights and critical elements in the cities. The disturbances not only inconvenienced people, but also caused economic harm and could also have resulted in deaths.

If you think these sound-like challenges affecting only developed world nations, bear in mind that Russia has been investigating vulnerabilities on the US power grid. Just because it hasn't happened yet doesn't mean it's not something we need not to worry about.  It's not an effort to dissuade the community from embracing smart city technologies to mention these past threats. Actually, it's just to highlight how important cybersecurity is in any smart city growth. When we create a smart environment without protecting it, we could end up suffering disorderly attacks.

**How do smart cities pose privacy risks?**

The privacy threats that could arise from data falling into the wrong hands are well known, but what can happen if data is right where it should be, forced into the systems of the processor and placed on databases? Smart cities have the ability to generate large amounts of data on their structures, data that may be insidiously used.

Next, it's important to consider where the data could end up. It might be under government jurisdiction, or it might also be in the possession of a private company. That is because many smart city projects are mostly carried out as public-private partnerships, or are initiated by completely private companies.

What comes next cannot be unequivocally told, because we are still in the data protection legislation Wild West days and there are not adequate regulation mechanisms in many countries that state[[13]](#footnote-13):

• What data form to receive, while gathering info.

• Which data should be obtained under what circumstances.

• To what purpose data may be used.

• How people can control the data

• How individuals can opt out of collecting the data.

• If anonymization of the data is needed.

• How to store Data.

• How long does it take to store info.

• How to erase data when it's no longer needed.

There are of course major differences depending on nation and society, but in many ways, we end up with scenarios where either corporations or the government have enormous quantities of data and a very long run to do whatever they want with it. It will have major implications for our safety, as well as the way we go about our everyday lives in a smart world.

Sadly, merely announcing that these technical advances have the ability to inflict major infringements on our privacy is not enough, and that we need to properly manage them. In a culture where policymakers and paternalistic journalists still echo the same old adage that "if you don't do something illegal, you shouldn't have something to hide,"[[14]](#footnote-14) we need to think about why privacy is such an important aspect of society and our lives. This line of reasoning bounces around the consciousness of the public, and has become a conviction held by others, making it necessary to unpack why this statement is false.

Privacy is a crucial aspect of life, as times of no outside control or fear of being watched are essential to our personal growth. This is in these empowering days when we accept ourselves as people with the freedom to make decisions, have interests and live our lives according to our own point of view. Privacy allows us the right to discover our own identities and grants us sovereignty, dignity and honesty[[15]](#footnote-15).

When you've been under relentless scrutiny all your life, would you ever have meddled on the boundaries of respectability? Either right or wrong, behaving like teenage defiance, moving against our parents' desires and defying authority figures may be vital to our moral growth and crucial experiences that lead to who we are today. Our mistakes shape us just as much as our successes and if a supervisory society discourages people from this experiment, would it also deprive them of an opportunity to learn and grow?[[16]](#footnote-16)

The risks can be classified as follows:

Surveillance or data collection[[17]](#footnote-17): Where is the line?

No rational one would question the extremely importance of data collection and interpretation when it comes to improving a city's infrastructure. How can officials find out the best route for a new line of trains without data? You put on a blindfold and drag a marker over the map?

We need data collection to make our towns safer and more efficient. The concern is that we have become fascinated with data gathering, to the extent where we neglect how it can affect the rights and lives of the people living in a community. Unless that is taken to the full, we could end up living in a surveillance state with cameras monitoring our every breath, having our DNA on file and extensive computer records of our network activities closely monitored by government machines and operatives.

This will lead to power asymmetry between the people and their government if something is registered and scrutinized. If the government knows everything about the people, while people know nothing about their government because of lack of accountability, it will use the intelligence capacity to force people to behave according to their wishes.

Therefore, surveillance is a weapon of exploitation. People fear the omniscience of the government, and act out of concern along narrow lines, maybe restricting their political activity and not sharing their true views. The end result would be the repression of opposition parties and an end to democracy, a chilling influence on the freedom and choice of people, and the anxiety that comes with living in fear society.

Some of the best recent examples of this is in *Xinjiang Province*, where the Chinese Communist Party employs smart town monitoring methods to intimidate the Muslim minority. The omnipresent monitoring systems make extensive use of CCTV[[18]](#footnote-18) – including inside homes and mosques, tracking by facial recognition technologies, gathering DNA and other biometric evidence, as well as the IJOP software, which police use to monitor individuals and capture large quantities of data on them.

In Xinjiang, many of the innovations that are frequently associated with smart cities have been used to establish a state of repression where people can no longer freely exercise their faith or claim the human freedoms that we take for granted[[19]](#footnote-19).

The centralization of Data

If data is consolidated without de-identification, it may be used to decide the schedule of a person to whom they are associating, and much more. If the image is sufficiently realistic, it may also be compared to anonymized individual data, showing that the two data sets accurately depict the same entity. This can lead to previously anonymized data being identified.

Once again, we need to be careful about how we collect, analyze and store data to protect people from possible negative impacts. This involves separating different data streams as soon as it is no longer needed for its original purpose, unless absolutely necessary, proper encryption, and disposal of the data. When it comes to major invaders of privacy, like Facebook[[20]](#footnote-20), at least you can choose not to use them. You can face social repercussions, fail to sign in to other programs, and still be somewhat watched, but there's a decision, although a hard one.

With smart cities collecting data the only choice a resident has is to leave. People can't opt out of being seen by CCTV cameras[[21]](#footnote-21), tracking their movements on public transit, and using a compulsory smart meter that tracks their consumption of electricity. When it stands, there are in many cases no fair choices for those who wish to retain a private life, or fear that too intense data processing could end up adversely impacting them.

Regulatory System

Despite this era of mass data gathering and algorithmic wizardry, policymakers have been reluctant to respond, ensuring that most countries don't have sufficient laws to shield their people from the possible negative effects associated with smart cities[[22]](#footnote-22).

In certain cases, corporations or states themselves are free to gather data on whatever they like, however they want to use it in the manner they want, with little concern on how it affects those being tracked. If we are to address the transition to smart cities seamlessly and without compromising citizens' lives, then policymakers need to closely analyze the present situation, where it is likely to be going, the solutions in use and the possible damage that such strategies might cause on individuals[[23]](#footnote-23).

Only after this deep thinking will they come up with a fitting legislative system that offers people the advantages of living in a smart city without the possibility of major breaches of privacy and cyber-attacks.

Major Privacy Violations

A smart city's health criteria can be broken down into two groups. The operational safety requirement is to ensure that the technology and infrastructure employed are secure and are immune to cyber-attacks. The second is linked to the data produced and shared through various technologies within the infrastructure. Information encryption[[24]](#footnote-24) and privacy, however, is based on organizational integrity, because anybody who hacks into a network would be able to violate the data access policy.

Privacy, the state of being separated from undesired criticism and care, is a basic human right as illustrated in many declarations and jurisdictions. The definition of privacy, however, varies based on the various cultures, circumstances and type of information. Privacy has various facets[[25]](#footnote-25) of it:

• The security of sensitive details pertaining to an individual's identification

• The security of physical dimensions of corporate privacy

• Territorial sovereignty covers individual's personal properties and resources

• Privacy Security aims at securing location coordinates and monitoring security

Communications privacy is about protecting channels of communication from eavesdropping. These networks include, but not limited to, hardware devices that allow either wired or wireless data sharing, networking media. Security transfers are geared to shielding questions and answers from surveillance[[26]](#footnote-26).

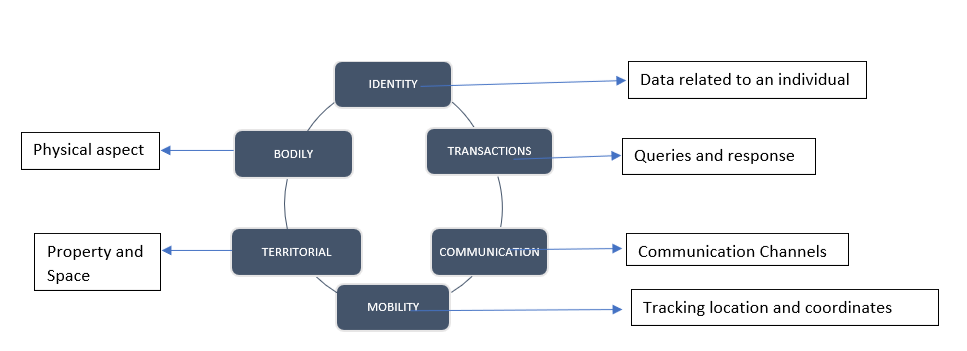
Attack Categories

The cyber-attacks are typically categorized into one of the three attacks[[27]](#footnote-27):

1. Attacks on availability: This term is about threats that either refuse any services or tear down the network entirely.

2. Attacks on confidentiality: These attacks involve illegal surveillance and access to information.

3. Attacks on integrity: These attacks try to hack into network and amalgamate or change the information stored. Such attacks also change systems such as halting essential programs, infecting the network with malware or rendering the network unreliable. Privacy aspects and violations attached to it are depicted in Figure 2 below.

****

*Fig 2: Privacy aspects and violations*

**Current legal framework to protect privacy violations in India**

In India, there are actually 31 per cent of the population living in cities. The figure continues to climb, with more residents moving to urban cities for greater work prospects, healthcare and educational services, and a higher living level. This trend is expected to continue in the years to come, with city population growth expected to reach nearly 50 percent by 2030[[28]](#footnote-28).

Having recognized this move, the Indian government-initiated measures to build 100 smart cities under the 2015 Smart Cities Programme[[29]](#footnote-29). The smart cities harness technologies and use current and proposed improvements in services to give people a better standard of life. Smart cities are powered by emerging technology, such as the Internet of Things (IoT) and sensors, along with existing IT and OT systems and equipment. Both innovative and conventional systems, spread throughout the smart community, operate in an interconnected fashion to produce intelligent and actionable intelligence to aid in effectively and sustainably delivering services to people.

India's efforts to secure its smart cities are opportune. To secure the smart city system from cyberattacks, a series of policies and regulations were planned. Some of the existing / coming security and privacy regulations also apply to smart cities and thus help build safe cities.

1. On 20 May 2016, the Ministry of Housing and Urban Affairs (MoHUA) Guidelines MoHUA[[30]](#footnote-30), the Government of India, published a model framework for cyber security in smart cities. This covers protection across various layers of smart cities, including sensor layer, application layer, data layer and communication layer. The key recommendations include but are not limited to:

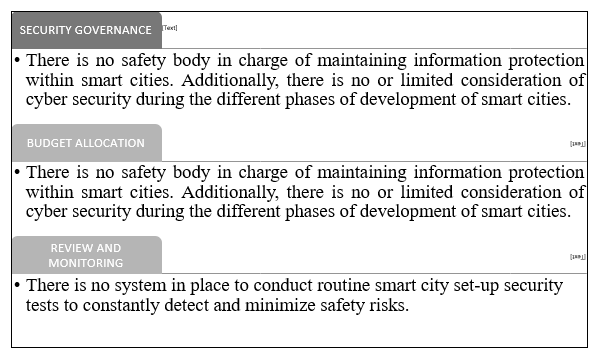
* Implementation of a stable network infrastructure based on the standard IT infrastructure of the National Institute of Standards & Technology (NIST).
* Security solutions that need to be considered as a smart city develops.
* Safe storage and data sharing between the multiple structures and applications deployed in the smart city.
* Health review of the facilities before and after live activities.
* Compliance with specifications such as ISO 27001, ISO 22301, ISO 37120, ISO 3712, ISO 27017, ISO 27018, BSI PAS 180, BSI PAS 182, Protected Extensive Authentication Protocol (PEAP) and 3rd Generation Partnership Project (3GPP), as applicable;
* Provision of safety management for smart city networks, apps, and sensors.
* Cyber incident notification to appropriate agencies such as the Computer Emergency Response Team – India (CERT-In) and the National Critical Information Intelligence Infrastructure Center (NCIIPC);

1. The National Critical Information Protection Infrastructure Center (NCIIPC), 2014: NCIIPC has been identified as the nodal agency for the protection of critical information infrastructure within the National Technical Research Organization. The NCIIPC ‘s formal functions and duties include collaboration plans, protocols, meetings and for CERT-In collaboration. The NCIIPC defined security enhancement controls for the critical infrastructure sectors.
2. NCSP, 2013: The strategy aims to establish a stable cyber environment in the country and improve the regulatory mechanism
3. Information Technology Act (IT Act), 2000[[31]](#footnote-31), and its amendments: The IT Act provides regulations on the protection of confidential personal data or information and requirements for the delivery of online facilities, the dissemination on the Internet of relevant material and the sanctions imposed in the event of any breach.
4. Aadhaar Act, 2016[[32]](#footnote-32), and its regulations: The Aadhaar Act, 2016, specifies how to collect, preserve and process data pertaining to Aadhaar. Aadhaar data not only contains biometric information (fingerprints, iris, and photograph) but also resident demographic details. The Aadhaar Act, 2016, forms the basis for various e-governance initiatives such as the delivery of services and benefits to Indian residents.
5. Draft Personal Data Privacy Act[[33]](#footnote-33): The Personal Data Protection Bill provides provisions for the preservation of sensitive data as an integral feature of data privacy. In other things, the bill includes guidance on the data collection criteria, data principal privileges, fines and exemptions. The law seeks to protect citizens ‘rights from State and private data privacy violations. When introduced, the bill will affect how personal / sensitive data is collected and accessed by smart city information systems.
6. Data Protection in Healthcare Act (DISHA)[[34]](#footnote-34): Recently the draft DISHA paper was released for review in the public domain. This aims at creating a National Health Authority in India to implement privacy and protection controls for electronic health records, and to control the collection and sharing of data

Indian smart cities face different obstacles

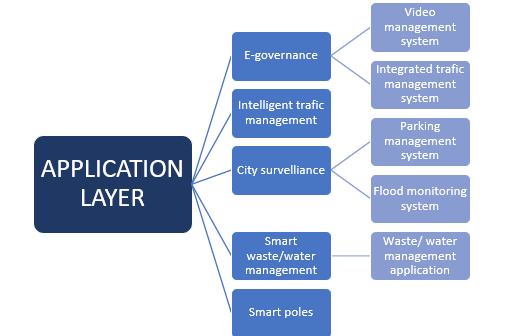
Indian-specific challenges hinder attempts to introduce the information infrastructure of smart cities. The key issues were

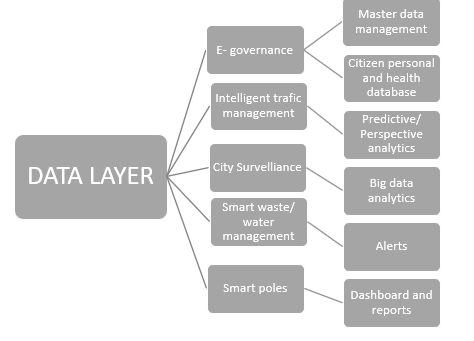
1. non-figuring information protection among top targets and
2. insufficient understanding of cyber security among stakeholders. Whilst protection should be a requirement, it is always an afterthought in the Indian context. Safety takes a backseat, as cities put their weight behind schedules for integrating programs. The smart cities today face several obstacles in integrating information security, based on our research and on-ground evaluations.



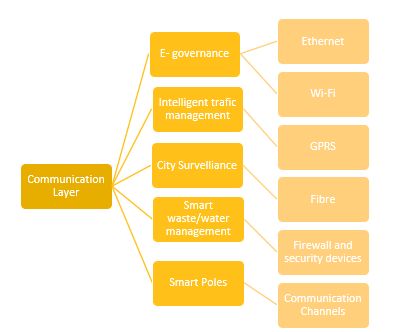
*Fig 3: Indian smart city obstacles*

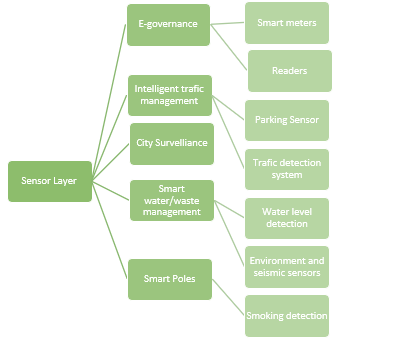
**Indian smart city ICT architecture**

****

****

*Fig 4: Application Layer Fig 5: Data Layer*

****

****

*Fig 6: Communication Layer Fig 7: Sensor Layer*

Figure 4, 5, 6, 7 gives the architectural structure of Indian smart city technology

The Indian Smart City technology architecture can be understood through the four logical layers[[35]](#footnote-35): sensor, communication, data and application layers. The infrastructure within these four layers operates in an interconnected way to provide Smart City services. smart cities indicate that the technologies driving the Indian smart city systems are very much vulnerable to bugs, which can contribute to future social, environmental, economic and/or reputational risks.

The emergence of intrinsic barriers, lack of granular rules and legislation, and India-specific concerns add to the uncertainty of the risk environment for Indian smart cities.

**E-governance**

*Vulnerabilities with associated systems*

• Unencrypted storage and transmission of citizen data.

• Lack of user rights and authorization controls.

• Several flaws leading to non-adherence to app development life cycle, (SDLC) phase.

• Obsolete version vulnerable to new threats like ransomware.

*Potential risks*

• Citizen personal data, including financial and health data, can be compromised.

• E-governance services can be shut down, denying services to citizens.

**Surveillance and monitoring of cities**

*Vulnerabilities with associated systems*

• Default login and setup

• Surveillance cameras available over the Internet with low access controls

• Unreliable sharing of video feeds

*Potential Risks*

• Video monitoring can provide intelligence on vulnerable security areas that can be used for sinister antisocial purposes, and plan and execute an attack at the city level

• Audio clips can be manipulated / deleted to impede criminal investigation

**Managing Smart Waste**

*Vulnerabilities with associated systems*

• Insufficient cryptographic tagging strategies for radiofrequency identification (RFID) defense

• The spoofing and cloning of tags

• Site termination attribute attacks

*Potential Risks*

• Smart sewage system may be breached by opening / closing intelligent valves and releasing untreated sewage water into freshwater bodies

• Denial of service attack may be carried out to interrupt waste collection, posing a risk to the safety of citizens' health

**Smart checkpoints and poles**

*Vulnerabilities with associated systems*

**•** Smart pole edge devices (e.g. Wi-Fi, sensors) default password and configuration;

• Inappropriate testing method for edge communication (e.g. Wi-Fi) devices;

• Remote sensor access at the terminal.

*Potential Risks*

• Attackers can connect to Wi-Fi and send anti-social emails to the town to create unrest

• Anti-political video can be projected in public areas by means of automated billboards to cause civil unrest

• Lights should be turned off at night so that the security cameras don't catch a crime.

**Water management**

*Vulnerabilities with associated systems*

• Misuse of data during retrieval / transition

• The spoofing and cloning

• Service denial attacks

*Potential Risks*

• False water management data can lead to water shortages, unrecognized wastage of drinking water and lack of water quality control metrics

**Smart traffic management system**

*Vulnerabilities with associated systems*

• Man-in-the-middle of sensor-reader attack

• The spoofing and cloning

• Service denial attacks

*Potential Risks*

• Miscreants can monitor bus locations and other parameters when planning an attack

• Traffic signals can be manipulated to create in-city traffic jams.

The Smart City Information Safety System

Although the action points will help the smart city SPVs keep the communities secure, adopting a comprehensive information protection system would have integrated security coverage. MoHUA's Smart City Information Security Principles have been used to develop a cyber security system for smart cities. This includes several aspects — data policy, data goods and services delivery and operation, and security assurance. The system is capable of securing all levels of infrastructure, empowering each smart city to balance its needs and helping to address the growing regulatory environment[[36]](#footnote-36).

Project and Governance Management

* 1. Appoint a CISO-led security agency to ensure information protection in the smart region.
  2. Set out a business-driven risk evaluation and determine the information protection criteria adequately.
  3. Develop a framework for security and privacy including policies, procedures and minimum-security guidelines covering systems, network devices, and edge devices including IoT, sensors, etc.
  4. Create a framework for the regular evaluation and enhancement of information protection for the smart city;
  5. In-smart city information security understanding and capacity building program.
  6. Maintain contact with various security agencies such as CERT-In and NCIIPC and other Cyberthreat Advisory and Incident Reporting security experts.

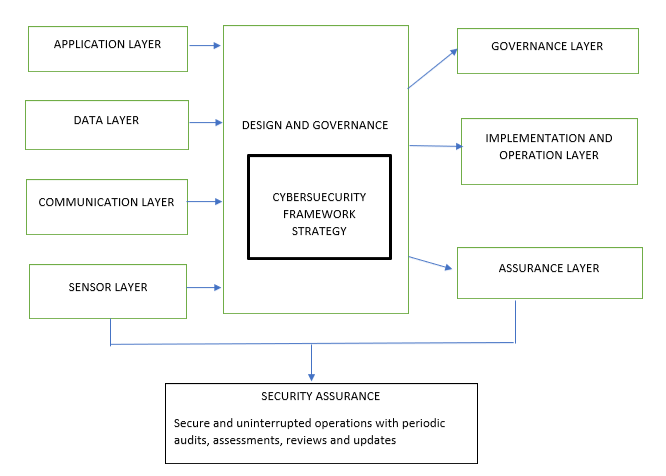
Implementing Security

* 1. Build and introduce smart city technology infrastructure based on risk evaluation, technology budget, and MoHUA guidance to exploit COTS / Make in India / open source security products;
  2. Security products are implemented across various layers: sensor layer, communication layer, data layer and application layer;
  3. Ensure that all systems, network and edge devices are configured to the minimum safety guidelines for the baseline.
  4. Carry out service safety assessments and close identified gaps before Go-live.

Operating Security

1. Compliance activities are carried out according to compliance protocols — change control, crisis management, etc.
2. Design, implement and operate a Security Operations Center (SOC) with advanced analytical capabilities and integrate, where possible, with all systems and edge devices; Operate the SOC 24x7 to identify, track and respond to security incidents
3. Develop a robust patch management process involving routine and timely upgrading of both firmware and operating systems;
4. Regularly checking Smart Management enterprise continuity and emergency response programs.

Conclusion



*Fig 8: Smart city architectural structure and solutions[[37]](#footnote-37)*

Creating a smart city is not just a dream any more, it is similar to a reality. Several organizations, policy departments, and research institutes are moving for the creation of integrated, instrumented, and urban smart cities. Such cities will provide its citizens with intelligent and advanced services education, transportation, surveillance, housing, health care, energy, and other services to improve the quality of life. This comes at an expense, though, of gathering, preserving, sorting, and reviewing a large amount of heterogeneous data that is sensed from the atmosphere and also contributed by the people. The emergence of the Internet of Things, cloud computing, social networking, and other influencers in business is moving technologies into the smart community structure, and also introduces new gaps in smart city results, infrastructure, and applications. These flaws also lead to questions about how the citizens' data is transferred and stored safely, whether it is kept confidential and inaccessible to unauthorized access, and whether the services delivered are safe and effective.

There is a lot of effort underway to address these security, privacy and trust concerns. Existing protection and privacy approaches operate fairly well in multiple situations, but we are seeing an increasing effort by hackers and intruders to show it differently sometimes. Therefore, supplying smart city data, infrastructure, and software with protection and privacy will entail further research into evolving technologies. In addition to security and privacy, smart city services and applications must be trustworthy and reliable against all odds so that any attacks on security or privacy breaches are detected and resolved immediately; this is a challenging task.

The various areas where technology will be used under smart city model were discussed in this paper along with possible threats it poses. It was also developed that the Indian smart city architecture including Application Layer, Data Layer, Communication Layer and Sensor Layer must be closely adhered to with Governance Layer, Deployment and Service Layer and Assurance Layer in order to avoid threats and violations to privacy. Implementing Personal Data Privacy laws in India is also significant, as the existing law is not well prepared to handle evolving technical developments.

1. Specialist in security, privacy and encryption. [↑](#footnote-ref-1)
2. Lilian Edwards, *Privacy,Sec, Data Protection in Smart City*, 11 Designing Smart Cities? Opportunities and Regulatory Challenges 39 (2015) [↑](#footnote-ref-2)
3. Talal Ashraf Butt & Muhammad Afzaal, *Security and Privacy in Smart Cities: Issues and Current Solutions*, 317–323 (2019) [↑](#footnote-ref-3)
4. Rong Wenge et al., *Smart City Architecture : A Technology Guide for Implementation and Design Challenges*, 56–69 (2014) [↑](#footnote-ref-4)
5. Manishree Bhattacharya Sivarama Krishnan, Rahul Aggarwal, Anas Viquar, Vikas Sood, Suman Bhunia, Amit Verma, *Creating cyber secure smart cities*, (2018) [↑](#footnote-ref-5)
6. David Eckhoff & Isabel Wagner, *Privacy in the Smart City - Applications, Technologies, Challenges, and Solutions*, 20 IEEE Communications Surveys and Tutorials 489–516 (2018) [↑](#footnote-ref-6)
7. Liesbet van Zoonen, *Privacy concerns in smart cities*, 33 Government Information Quarterly 472–480 (2016), http://dx.doi.org/10.1016/j.giq.2016.06.004 [↑](#footnote-ref-7)
8. <https://www.comparitech.com/blog/vpn-privacy/smart-cities-privacy-risks/> [↑](#footnote-ref-8)
9. Steven M Janosik, ‘済無 (2005) 42 NASPA Journal 1. [↑](#footnote-ref-9)
10. Christos Beretas, *Smart Cities and Smart Devices : The Back Door to Privacy and Data Breaches*, 21221–21223 (2020) [↑](#footnote-ref-10)
11. E-newsline January et al., *Smart Cities : Need for a regulatory framework*, 1–4 (2020) [↑](#footnote-ref-11)
12. Robert M. Lee et al., *Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case*, Electricity Information Sharing and Analysis Center 36 (2016), https://ics.sans.org/media/E-ISAC\_SANS\_Ukraine\_DUC\_5.pdf [↑](#footnote-ref-12)
13. S Rahmansyah, D. and Tahir, Data Protection Law in Indonesia: An Overview (2017), https://uk.practicallaw.thomsonreuters.com/4-583-2387?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1 [↑](#footnote-ref-13)
14. <https://www.nytimes.com/wirecutter/blog/security-cameras-ethics-and-the-law/> [↑](#footnote-ref-14)
15. van Zoonen [↑](#footnote-ref-15)
16. Fahd AlDosari, *Security and Privacy Challenges in Cyber-Physical Systems*, 08 Journal of Information Security 285–295 (2017) [↑](#footnote-ref-16)
17. January et al. [↑](#footnote-ref-17)
18. Ronald Deibert Xiao Qiang Steven Feldstein Larry Diamond et al., *The Road to Digital Unfreedom lliberal Democracy and the Struggle on the Right The Fates of Third-Wave Democracies Bolsonaro and Brazil’s Illiberal Backlash*, 30 (2019) [↑](#footnote-ref-18)
19. Wenge et al. [↑](#footnote-ref-19)
20. Ari Ezra Waldman, *Privacy, Trust, and the Propensity to Disclose*, 67 SSRN Electronic Journal (2016) [↑](#footnote-ref-20)
21. Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and  the Right to Anonymity*, 213 SSRN Electronic Journal (2005) [↑](#footnote-ref-21)
22. January et al. [↑](#footnote-ref-22)
23. Slobogin [↑](#footnote-ref-23)
24. Eckhoff & Wagner [↑](#footnote-ref-24)
25. Basant Kumar, *Data Security and Privacy Management; Addressing Meticulous Crime Strategies in Smart Cities*, 3 22–30 (2015), http://www.recentscientific.com/sites/default/files/5456.pdf [↑](#footnote-ref-25)
26. Beretas [↑](#footnote-ref-26)
27. AlDosari [↑](#footnote-ref-27)
28. Sivarama Krishnan, Rahul Aggarwal, Anas Viquar, Vikas Sood, Suman Bhunia, Amit Verma [↑](#footnote-ref-28)
29. Reference Framework, *Reconceptualising Smart Cities :*, [↑](#footnote-ref-29)
30. Smart Cities, *Ministry of Housing and Urban Affairs*, 1 1–7 (2020) [↑](#footnote-ref-30)
31. M. A. Yadugiri & Geetha Bhasker, *The Information Technology Act, 2000*, English for Law 482–511 (2011) [↑](#footnote-ref-31)
32. Arrangement O F Clauses et al., *the Aadhaar ( Targeted Delivery of Financial and Other Subsidies , Benefits and Services ) Bill , 2016*, 1–25 (2016) [↑](#footnote-ref-32)
33. Lothar Determann & Chetan Gupta, *Indian Personal Data Protection Act, 2018: Draft Bill and Its History, Compared to EU GDPR and California Privacy Law*, SSRN Electronic Journal (2018) [↑](#footnote-ref-33)
34. Ministry of Health and Family Welfare; Government of India, *Draft “Digital lnformation Security in Healthcare Act (DISHA),”* (2018) [↑](#footnote-ref-34)
35. Wenge et al. [↑](#footnote-ref-35)
36. Cities [↑](#footnote-ref-36)
37. Eckhoff & Wagner [↑](#footnote-ref-37)