सत्यमेव जयते

Ministry of Electronics
& Information Technology
Government of India

Cyber Security Guidelines for Smart City Infrastructure

certin
Enhancing Cyber Security in India

In collaboration with

kaspersky

Table of Contents

1. Introduction

Smart cities are a cornerstone of modern urban development, especially in a rapidly growing economy like India. The concept of smart cities goes beyond mere technological advancements, aiming to improve the quality of life for residents, ensure sustainability, and drive economic growth. Smart cities provide sustainable solutions to manage resources and infrastructure effectively.

Smart Cities Mission was launched by the Hon'ble Prime Minister of India on 25 June, 2015. The main objective of the Mission is to promote cities that provide core infrastructure, clean and sustainable environment and give a decent quality of life to their citizens through the application of 'smart solutions'. The Mission aims to drive economic growth and improve quality of life through comprehensive work on social, economic, physical and institutional pillars of the city. The focus is on sustainable and inclusive development by creation of replicable models which act as lighthouses to other aspiring cities. 100 cities have been selected to be developed as Smart Cities through a two-stage competition.

The objective of Smart Cities Mission under Ministry of Housing and Urban Affairs is to promote cities that provide core infrastructure and give a decent quality of life to its citizens, a clean and sustainable environment and application of 'Smart' Solutions. The focus is on sustainable and inclusive development and the idea is to look at compact areas, create a replicable model which will act like a light house to other aspiring cities

Smart Cities use the digital network as the platform to offer urban services and to be sustainable. Using the digital network as the fourth utility - along with electricity, water, and natural gas, smart cities can integrate multiple digital systems to deliver on-demand digital services over a highly secure Internet-

enabled cloud infrastructure. Such digital services and related digital networks can help cities address urban challenges as well as improve their liveability index.

The document aims to establish a foundational digitally resilient framework for protecting Smart City digital infrastructure against cyber threats. This document outlines good practices and architectural strategies for safeguarding Smart City systems by the State/Union Territory (UT) Computer Security Incident Response Team (CSIRT) and Smart City operators. Smart Cities rely heavily on interconnected digital services, IoT devices, and centralized command centres to optimize urban operations, making them particularly vulnerable to a range of cyber threats. This document is a joint initiative of Indian Computer Emergency Response Team (CERT-In) and M/s Kaspersky.

The building blocks of a smart city infrastructure consist of a digital network which deploys Internet Protocol (IP), including Wireless and Radio Frequency (RF) networks, Sensors, associated control systems / applications, Correlation platform & a mobile / web / application platforms for citizen interaction. The building blocks of a Smart City are as shown in Figure 1.

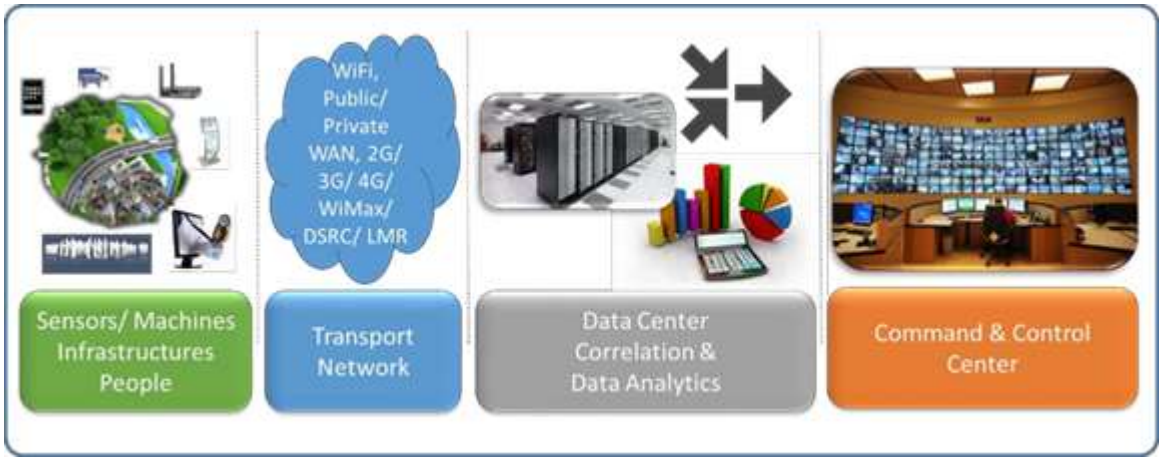

Figure. 1. Components of a Smart city infrastructure

1.1. Key Smart City Infrastructure components

The components of a Smart city infrastructure are briefly described below.

1.1.1. Sensors / Machines / Infrastructure / People:

These are the input / output devices in the smart city digital infrastructure and provide the information about the various parameters that are being tracked, and control the various parameters that are being monitored / controlled. These could be video cameras used for public safety and security surveillance, smart meters used for energy / water management, traffic counters used for monitoring traffic, Global Positioning System (GPS) devices to provide location information about public transport, traffic light actuators used to control traffic lights, large variable message displays used to provide / disseminate information to the citizens, public address systems used to unicast/ multicast/ broadcast local announcements, telemedicine facility etc.

1.1.2. Transport network

The transport network provides a ubiquitous IP network (mostly IP based, but can use other communication protocols as well) across the city which can be used by the various sensors, control systems etc. to send information to the desired destination. The information content, and hence the source and destination of the information would depend upon the application that is generating this information. For example, for a public safety and security surveillance application, the sources would be video cameras installed at multiple points in the city, and the destination could be the central control room where the video feeds are being monitored. Similarly, for an Energy management application, the sources could be smart meters installed at the consumer premises, and the destination could be the central power station where the utilization is being monitored and controlled. The different types of sensors would use different access mechanisms for sending information to the Data Centre (DC) e.g. Public safety and security surveillance cameras might use a captive network / MPLS /

Wi-Fi infrastructure, water & energy management sensors might use LoRa/ ZigBee based access while garbage bin sensors which are scattered across the city might use 3G/ 4G access mechanisms.

1.1.3. Data Centre

The sensor network generates lots of information that needs to be analyzed and processed before it can become actionable. The information also might need to be stored for a certain duration of time for historical analysis or forensic purposes. Other advanced use cases for data stored in DC would be Machine learning and AI for planning, forecasting, etc. Hence, a smart city infrastructure requires to have a DC that can store the information, and run the applications that can convert the raw data from the sensor network into actionable information. Further, as the degree of 'smartness' increases, there would be multiple applications and sets of sensors that would send information about the city with respect to multiple dimensions. All this information might not be useful unless it is correlated among the multiple sources to eliminate redundant information, and dwell on the intelligence of other applications to make the applications 'smarter' e.g. the video feeds form the public safety and security surveillance systems can be used to augment the traffic management systems.

1.1.4. Command and Control Centre

This is the place where the processed information is being monitored and actions being authorized based upon the information received. The term Command and Control Centre can combine several components as probably the separate parts may be controlled by different centres but report to the same governing authority. Smart city can be envisaged as the composition of parts (infrastructures) related to smart transportation, smart energy, communal services, notification, entertainment and information services, and many other systems and services. They might have different owners and relate to different areas of responsibility. In this case there would be no single command and control centre.

1.2. Target Audience

The audience for this document includes urban infrastructure managers, policy makers, Smart City technology providers and cybersecurity professionals who must work together to ensure a resilient and secure environment. The document's scope covers the lifecycle of Smart City development from planning and implementation to maintenance, and continuous improvement, highlighting the need for cybersecurity practices to be integrated at every stage.

The document aims to provide a high-level overview of the role that cybersecurity plays in Smart Cities and why it is essential for maintaining public trust, ensuring safety, and preventing operational disruptions. Key challenges, such as the need for interoperability across diverse systems and the potential for cyber-physical harm, are also emphasized. The document also addresses how emerging technologies, including IoT, cloud computing and artificial intelligence (AI), heighten both the potential and vulnerabilities of Smart City initiatives.

2. Threat Landscape for Smart Cities

The Smart City ecosystem, with its integration of IoT, cloud computing, and artificial intelligence, creates a complex attack surface vulnerable to a wide range of cyber threats.

By interconnecting different systems, a smart city creates a "system of systems". Primary challenge with respect to security solution for Smart cities are heterogeneity of data types, interfaces and carrier types. The complexity of such collaborating systems increases exponentially to manage data and privacy of a Smart City implementation. This creates a huge and complex attack surface with a cascade effect as there are numerous points of attack because of the interconnected sensors and devices creating an Internet of Everything.

Understanding the threat landscape is vital for developing robust defensive strategies. Key cyber threats include cyber-physical attacks where adversaries

target infrastructure components like energy grids, water systems, large message public displays, public address systems and public transportation, which can have severe consequences for urban safety and functionality. Another major threat is data privacy and breach risks, as Smart Cities handle large volumes of sensitive data on citizens, making them attractive targets for hackers seeking to steal or misuse personal information.

Denial of Service (DoS) attacks pose another critical risk, where essential city services can be rendered inoperative, causing widespread disruption to daily life. Similarly, malware and ransomware attacks can infiltrate Smart City systems, encrypt data, and demand ransom payments to restore access, potentially crippling municipal operations. The insider threat should not be overlooked, as malicious insiders or negligent employees with privileged access could intentionally or unintentionally compromise security.

There is no common risk assessment framework for Smart Cities. For each and every Smart City operator risk assessment exercise should be done. The risk assessment helps to identify high-priority risks, assess vulnerabilities, and determine their potential impact on the Smart City infrastructure. It is essential for developing tailored security controls that align with the unique needs of each Smart City. Understanding these threats provides Smart City operators with the insights needed to prioritize cybersecurity investments and prepare for an evolving threat landscape. The list of types of risks connected to cybersecurity might be as follows (but not limited to):

- Safety, including public safety risks
- Privacy risks
- Unlawful surveillance
- Wrongful announcement
- Data tampering

- Property risks
- Risks of service unavailability (DoS) / Defacement
- Financial and operational risks for the service operators
- Risks connected to the use of infrastructure for unintended purpose.

Different stakeholders are involved and they can bear different kinds of risks. This is quite important for the proper consideration of the threat landscape. It might be useful to consider different risks and concerns for the different groups of stakeholders.

Each and every system or group of systems within a Smart City may be of interest to attackers – from adversarial states to cybercriminals, saboteurs, hacktivists and even cyber terrorists. Some examples of Smart City functional areas with corresponding threats list is provided here.

2.1. Intelligent Transportation System

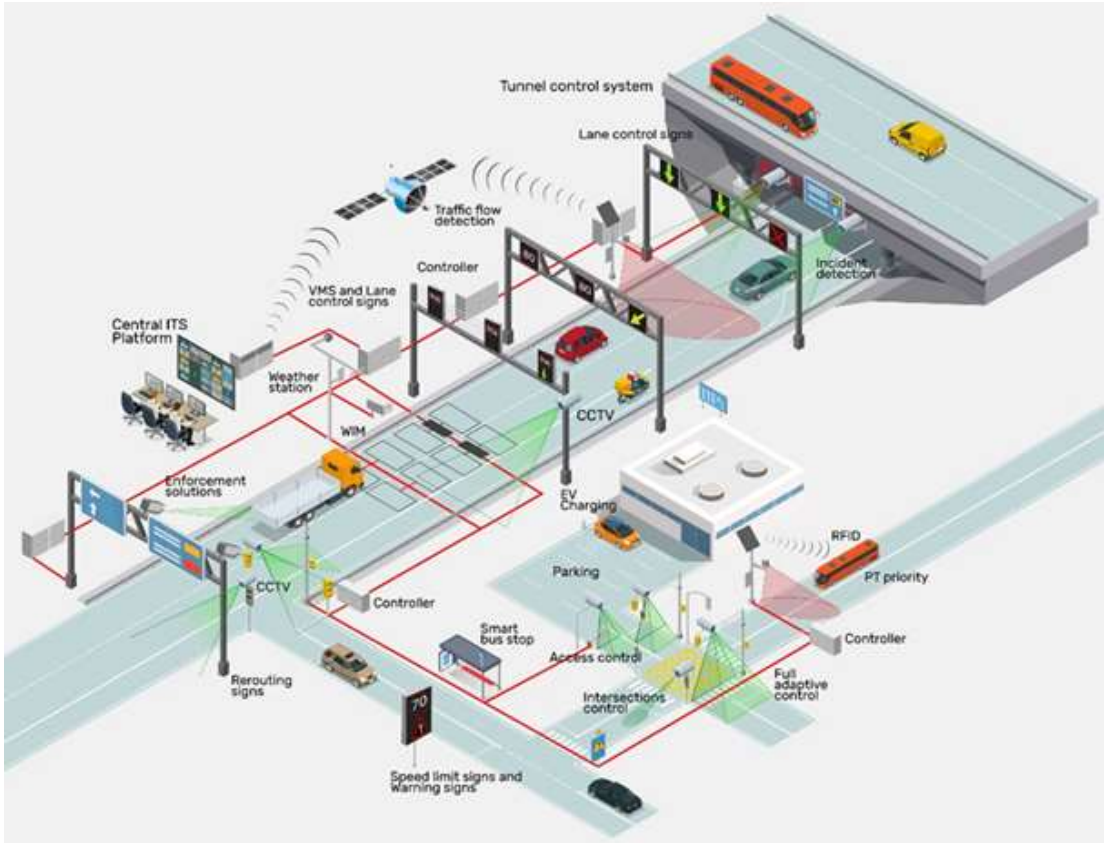

Figure. 2. Intelligent Transport System

Intelligent Transportation System (ITS) can comprise of many components as presented in Figure 2. Each element of ITS plays a key role in ensuring safe and efficient urban mobility. However, their interconnectivity and reliance on digital systems expose them to distinct cyber and physical threats.

From privacy violations in CCTV systems to infrastructure takeovers and potential operational disruption by exploitation of the central ITS platform, it is essential to have robust security measures that address these vulnerabilities comprehensively to safeguard urban transportation. The ITS encompass multiple integrated elements to optimize urban mobility and each component faces distinct threats as follows:

2.1.1. CCTV

- Privacy Violation: Unauthorized access to video feeds could lead to a violation of citizens' privacy, with footage being used for malicious purposes or unlawful activity.
- Denial of Service (DoS): Attackers could flood the CCTV system with excess traffic to make cameras non-functional, preventing effective monitoring during crucial incidents.
- Evidence Compromise: CCTV footage can be crucial for law enforcement. Attackers could tamper with or delete recordings, compromising their value as evidence during investigations.

2.1.2. Parking / Charging / Access Control Systems

- Parking Fraud: Attackers could exploit vulnerabilities in payment systems to commit parking fee evasion or misuse parking permits, leading to revenue losses.
- Vehicle Damage: Cyber or physical attacks on automated parking systems could lead to damages to vehicles, either by manipulating the parking mechanism or gaining unauthorized control over automated parking structures.

- Unauthorized Access: Poorly secured systems can be vulnerable to unauthorized access, allowing attackers to access restricted areas or alter parking and charging data.

2.1.3. Central ITS Platform

- Transport Infrastructure Takeover: A compromise of the central ITS platform can allow attackers to control critical transportation elements like traffic signals, communication infrastructure and public safety and security surveillance systems, potentially leading to widespread disruption.
- Pivot Point to Attack Municipal Agencies: The ITS platform often integrates with other municipal services, making it a potential pivot point for attackers to infiltrate other governmental systems and disrupt broader services.
- Public safety and security surveillance: Exploiting the ITS to monitor and track public safety and security of individuals could lead to unauthorized mass surveillance, raising significant privacy concerns.
- Operational disruption: Control over the central ITS can facilitate acts of serious disruption, where an attacker may orchestrate traffic chaos, prevent emergency responses, or cause life-threatening incidents in densely populated areas.

2.1.4. Traffic Controllers

- Road Accidents: Malicious actors could manipulate traffic controllers (e.g., traffic lights) to cause confusion at intersections, resulting in increased road accidents.
- Traffic Jams: Attackers may alter traffic light sequences or road signals to create artificial congestion, which can severely affect daily commutes and productivity.
- Impact on Emergency Services: Deliberate interference with traffic signals could delay or obstruct emergency vehicles, preventing them from reaching critical locations, leading to potentially life-threatening consequences.

2.2. Public Service Systems

The Public service systems represent a critical backbone for effective governance, citizen welfare, and infrastructure management. However, they face a broad spectrum of cyber and physical threats, including data breaches, service disruptions, fraud, and unauthorized surveillance. These threats necessitate a robust security posture involving strong identity management, access controls, system resilience, and continuous monitoring to safeguard public interests and maintain the trust and safety of all citizens in a Smart City.

Public services in a Smart City typically involve integrated digital platforms that manage citizen services, welfare programs, administrative tasks, and public safety. Listed below are specific threats faced by various elements of public service systems:

2.2.1. Citizen Portals and Digital Services

- Identity Theft: Attackers could exploit vulnerabilities to steal personal information, which can be used for fraudulent activities or impersonation, severely compromising citizen trust.

Figure 3: Government Services Systems

- Denial of Service (DoS): Malicious actors could overload government portals, making critical citizen services (e.g., healthcare, benefits, permits) unavailable, causing public inconvenience.
- Unauthorized Access to Sensitive Data: Weak access controls could lead to unauthorized access to sensitive citizen data, such as personal details, health records, and welfare information, causing privacy breaches.

2.2.2. e-Government Administrative Platforms

- Personally Identifiable Information (PII) data leaks: Platforms holding administrative records, such as birth certificates, property records, PAN Card details, Aadhaar Card details, Driving License Card and voter information, etc. are attractive targets for data breaches, compromising citizens' personal data. Compromise of stored sensitive information, including citizen records, can lead to data exposure and privacy violations, eroding public trust.
- Malware and Spyware Infiltration: Malware could be introduced by malicious actors into government networks to monitor activities, gather sensitive data, or disrupt essential functions, potentially affecting service delivery and confidentiality.
- System Manipulation: Attackers might manipulate public records for fraudulent purposes, such as altering property titles or modifying business registration data, leading to legal and financial complications.

2.2.3. Data Centres

- Physical Security Threats: Data centres store vast amounts of sensitive information. Physical intrusions or sabotage attempts pose a risk of data theft, damage, or complete service outage.
- Insider Threats: Employees or contractors with privileged access might misuse their roles to exfiltrate sensitive data, alter configurations, or insert malicious software to compromise system integrity.

- Unpatched Systems: Servers and workstations with outdated software are susceptible to exploitation through known vulnerabilities, leading to unauthorized access, data exfiltration, ransomware or data manipulation.
- Targeted Cyberattacks (APT): Data centres may be targeted by Advanced Persistent Threats (APTs) involving sophisticated and sustained attacks, aimed at gaining unauthorized long-term access to extract valuable information.

2.3. Malware and Vulnerable Systems analysis

CERT-In carried out an analysis of 20 smart cities located in different parts of the country to understand the types of malware and vulnerable systems for the year 2024.

In Western India, Central India and Northern India the majority of the malware was trojans (a malicious digital pest whose sole aim is to wreak havoc on its victims' computers unnoticed. It does this by reading passwords, recording keyboard strokes or opening the door for further malware that can even take the entire computer hostage – as defined by Kaspersky). The top trojans were avalanche-andromeda (the main functionality of this malware family is downloading of other malware, which is most often used to electronically spy on users) and gamarue (a malware family that is used as a botnet and modular backdoor. It can spread through malicious email attachments, external drives, and other malware. It can steal information, download and execute other malware, and create a backdoor for remote access). The most prevalent vulnerability observed was allowing remote connections to unauthorized computers.

In Southern India the majority of the malware was botnets (networks of hijacked computer devices used to carry out various scams and cyberattacks. They serve as a tool to automate mass attacks, such as data theft, server crashing, and malware distribution – as defined by Kaspersky), the widely found botnet was Socks5Systemz, that allows the infected system to be used as a proxy thus causing

the infected systems to unwittingly become participants in criminal activities and the most prevalent vulnerability observed was misconfiguration of Simple Network Management Protocol (SNMP) which is at the core of the network devices leading to unauthorized access or execution of malicious commands or interception of network traffic or a denial of service attack.

3. Cybersecurity Standards and Frameworks for Smart Cities

Smart Cities Mission (SCM), under Ministry of Housing and Urban Affairs (MoHUA), Government of India has undertaken several initiatives including, inter alia projects that use digital technologies extensively for various facets of urban governance. One such initiative is establishment of Integrated Command and Control Centres (ICCCs), being set up in many smart cities to act as decision support systems in day-to-day and emergent situations. Many other ICT initiatives are being rolled out in different sectors like mobility, water etc. In order to facilitate procurement of these ICCCs / ICT solutions, a Model ICCC RFP document was developed in year 2016. Model RFP 2.0 was released in 2021.

As per the Advisory on Standard Operating Procedure for cyber security of smart city infrastructure (Advisory no.22) released by Smart Cities Mission (SCM), under Ministry of Housing and Urban Affairs (MoHUA), ICCCs were advised to adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. The advisory also provides the Base line Security Measures that need to be taken at Sensor layer, communication layer, Data and Application layer. The advisory on Strengthening Cybersecurity of ICCC Infrastructure in Smart Cities (Advisory no. 24) focusses on the Vulnerability Assessment and Penetration Testing, End point security, Trusted Electronics value Chain, and Process Audit. The Advisory on Essential Cyber-security Protocols for ICCC Infrastructure in Smart Cities (Advisory No: 25) focusses on the General Cyber Security Protocols, Malware Defense, Password

policies, Incident Prevention and detection, Securing conference cameras and email security best practices.

4. Smart City Cybersecurity Architecture

A secure Smart City architecture is critical in ensuring the resilience and protection of interconnected urban services. This principles of security-by-design, resilience, scalability, and interoperability not only help to secure the smart city systems but also make them adaptable to future requirements and evolving threats.

4.1. Security by design

Security must be embedded into the architecture and development of Smart City systems from the outset, rather than being added later as an afterthought. This includes:

- Threat modelling during design to identify potential vulnerabilities and attack vectors early in development.
- Zero Trust Architecture (ZTA) to ensure strict identity verification and least privilege access across networks.
- Secure coding practices to minimize software vulnerabilities and prevent common threats such as injection attacks and buffer overflows.
- Multi-layered defense mechanisms, such as firewalls, endpoint protection, and intrusion detection/prevention systems (IDS/IPS), to provide in-depth security.
- Privacy-by-Design principles to ensure that personal data is protected, anonymized where necessary, and processed in compliance with regulatory requirements.

4.2. Resilience and continuity

Smart Cities must be designed to withstand, adapt to, and recover from cyber incidents, natural disasters, or technical failures. This includes:

- Redundant and distributed architectures to ensure continuous operation, even if a key component is compromised.
- Automated failover mechanisms to switch to backup systems seamlessly in the event of an attack or failure.
- Cyber-physical resilience planning, ensuring that both digital and physical infrastructure (e.g., power grids, traffic systems) remain operational during crises.
- Real-time anomaly detection and automated incident response to detect cyber threats early and mitigate them swiftly.
- Regular penetration testing and disaster recovery drills to test preparedness and improve response strategies.
- Scalability: Smart Cities must accommodate growing populations, emerging technologies, and evolving cyber threats. This requires:
- Modular architecture to support new technologies, services, and regulatory changes without requiring a complete overhaul.
- Cloud-native and edge computing to efficiently handle large-scale data processing with flexibility and redundancy.
- Adoption of Software-Defined Networking (SDN) to dynamically manage and scale network security policies as infrastructure grows.
- Use of AI-driven security analytics to continuously adapt defenses based on emerging threats.
- Interoperable and vendor-neutral frameworks to prevent vendor lock-in and allow seamless integration of new solutions.

4.3 Interoperability and Standardization

Smart Cities consist of diverse systems that must work together securely and efficiently. This requires the following.

- Open standards and APIs to ensure seamless communication between IoT devices, government services, and enterprise systems.
- Common security protocols such as TLS, WPA3, and encrypted communication for all connected systems.
- Identity and access management (IAM) frameworks that work across different platforms and services.
- Cross-agency and cross-sector collaboration, ensuring that cybersecurity policies apply uniformly across transportation, healthcare, utilities, and other Smart City services.

4.4 Network segmentation and isolation strategies

The core components of Smart City typically include several interconnected layers: The Edge Computing and IoT Layer, Communication and Data Transmission Layer, Cloud and Data Storage Layer, and Command and Control Centres. Each layer requires specific security controls tailored to its unique role within the ecosystem. For instance, IoT devices at the edge layer are often more vulnerable due to limited processing power, making them potential entry points for attackers.

Proper segmentation and isolation strategies can reduce the attack surface by isolating critical systems and sensitive data. Effective segmentation prevents unauthorized access and limits the lateral movement of threats within the network. Implementing real-time monitoring, anomaly detection, and intrusion prevention by Smart City operators can significantly reduce the risk of attacks compromising essential services or affecting citizen safety. Dedicated tools such as EDR, NDR, XDR and MDR needs to be deployed according to the infrastructure to have a better proactive posture for IT and ICS environments.

The unique attributes of Smart Cities—interconnected IoT sensors, integrated mobility systems, and centralized command centres – significantly amplify the

need for robust segmentation strategies. IoT devices deployed across traffic management, public utilities, and environmental monitoring create vast networks of endpoints that are inherently vulnerable due to limited processing capabilities and insufficient security measures. Without appropriate segmentation, a single compromised sensor could act as an entry point, enabling attackers to traverse networks and potentially access critical infrastructure.

To address these challenges, segmentation strategies must strike a balance between security and operational efficiency. Effective separation and network isolation are critical to reduce the attack surface in Smart City infrastructure by isolating critical systems and sensitive data. Physical segmentation, including dedicated hardware or air-gapped networks, offers the highest degree of separation. This approach ensures that critical systems, like water treatment plants or energy grids, are entirely isolated from broader network ecosystems, making unauthorized access significantly more difficult. Logical isolation, on the other hand, relies on methods such as virtual LANs (VLANs) and subnetting, which allow administrators to logically partition devices and functions within shared physical infrastructure. Communication within different VLANs should be disabled by default and only be allowed on need basis with per port / application basis. Intra-VLAN and inter-zone / Inter-VLAN Access Control Lists (ACLs) add an additional layer of filtering, controlling traffic between devices within a segment and across segments. Although these are highly scalable solutions, their complexity in design and ongoing maintenance may lead to misconfigurations that attackers may exploit.

Firewalls play a central role in isolating functional areas by implementing granular traffic controls between segmented zones. These strategies can be further bolstered by micro-segmentation, using network, host (agent-based) or hypervisor-layer controls to establish security boundaries even at the device level. Modern technologies like Software-Defined Networking (SDN) can overlay

automated, dynamically adaptable segmentation, optimizing resource use while enhancing isolation. In scenarios where ultra-sensitive operations are involved – such as Smart City command and control centres – air gaps or data diode-based unidirectional connections may provide higher level of defense.

Segmentation and isolation are vital for Smart Cities due to their diverse systems – IoT devices, critical infrastructure, and citizen-facing services – all interconnected in complex architectures. By designing robust networking architectures from the get-go and implementing strong policies, Smart City operators can limit the potential impact of threats, contain lateral movement, and ensure the resilience of urban infrastructure.

5. Network Security in Smart City Environments

Network security is fundamental to protecting the interconnected systems that comprise a Smart City. Network segmentation and micro-segmentation are crucial for containing threats and preventing lateral movement across the network. By dividing networks into smaller, isolated segments, Smart City operators can limit the potential impact of an attack on a specific segment and reduce exposure to unauthorized access.

The use of secure communication protocols is vital, as it ensures data integrity and confidentiality during transmission. CCTV cameras should send video streams to storage and analytics server over encrypted channel. Secure protocols, such as TLS and VPNs, provide robust encryption, preventing unauthorized entities from intercepting or tampering with data. Vulnerability testing of Video Management System (VMS) is very much essential for safeguarding against possible Man in The Middle (MiTM) attack. Firewalls, Intrusion Detection and Prevention Systems (IDPS) and Privilege Access Management (PAM) play a key role in protecting network perimeters and identifying malicious activities.

Regular configuration and audit should be performed for network and security devices. Default factory settings of the devices must be changed and configured as per the business requirement of the smart city.

Implementing Zero-Trust Model which is an approach based on the principle of never trusting any device or user inside or outside the network without continuous verification is highly needed in Smart Cities due to diverse and dynamic environments where systems, devices, and users frequently interact. Additionally, encryption and data protection mechanisms ensure sensitive information remains secure, irrespective of the data in transit or at rest. By implementing these strategies, Smart Cities can maintain a robust network security posture that mitigates the risk of intrusions and data breaches. Kindly refer to CERT-In's Guidelines on Information Security Best Practices for Government Entities (Section 4 – Network and infrastructure security) for further details.

6. Identity and Access Management (IAM)

Identity and Access Management (IAM) is essential for controlling access to Smart City systems and data, ensuring only authorized users and devices can access critical resources. Continuous access monitoring by regularly reviewing access logs and detecting anomalies that may indicate unauthorized access attempts is important in a smart city environment. IAM solutions can help Smart City operators maintain robust access controls with geo-fencing and protect against unauthorized or malicious actions within their networks. By implementing IAM best practices, Smart Cities can significantly reduce risks associated with human error, insider threats, and compromised credentials. Some of the IAM best practices include:

6.1. Implement Multi-Factor Authentication (MFA)

- Require at least two authentication factors: passwords, biometrics, TOTP (time based OTP) or security tokens.

- Use adaptive authentication to assess risk based on user behaviour and location.
- Encourage passwordless authentication (FIDO2, hardware keys) for enhanced security.

6.2. Enforce Strong Password Policies

- Require long (12+ characters), complex, and unique passwords with periodic updates.
- Prevent password reuse and implement account lockouts after multiple failed attempts.
- Promote the use of password managers and passkeys to improve security.

6.3. Use Secure Biometric Authentication

- Implement liveness detection to prevent spoofing (e.g., fake fingerprints, deep fakes).
- Encrypt biometric data and comply with privacy laws.
- Combine biometrics with other authentication factors for higher accuracy.

6.4. Deploy Digital Certificates and Public Key Infrastructure (PKI)

- Issue digital certificates for all devices and users to verify authenticity.
- Use mutual TLS (mTLS) authentication for secure system communication.
- Automate certificate lifecycle management to prevent expired credentials.

6.5. Secure IoT and Device Authentication

- Assign unique cryptographic credentials to each device.
- Enforce Zero Trust policies—no device is trusted by default.
- Use regular firmware updates and network segmentation to mitigate attacks.

6.6. Implement Risk-Based & Adaptive Authentication

- Detect unusual login behaviour (e.g., login from a new location) and require extra verification.
- Continuously assess risk using AI-driven analytics and behavioural monitoring.

6.7. Enable Single Sign-On (SSO) & Federated Identity

- Use SAML, OAuth 2.0, and OpenID Connect for seamless authentication.
- Secure SSO sessions to prevent hijacking and enforce role-based access control.
- Role-Based Access Control (RBAC) is another key concept that can provide operators with a structured approach to assign permissions based on job roles. RBAC helps minimize the risk of privilege abuse by limiting user access to only those systems or data required for their role. Multi-Factor Authentication (MFA) is recommended for critical operations and accounts with elevated privileges, adding an additional security layer to mitigate risks from compromised credentials.
- For Government services, it may be ensured that Websites and Applications are integrated with a common Single Sign On (SSO) for login purpose. It also needs to ensure that passwords are encrypted while transmission and the passwords are forced to change at regular intervals.
- Care must be taken to ensure that default login credentials of devices such as routers, firewall, storage equipment etc., are changed prior to the deployment of such devices in the operational environment.

7. Data Security and Privacy

Protecting data within Smart City systems is critical, as these digital infrastructures collect vast amounts of personal and operational information. It is necessary to have mechanisms for data classification and sensitivity management, where data is categorized based on its sensitivity level to determine appropriate security measures. By distinguishing between public, internal, and confidential data, Smart Cities can apply different security protocols that align with the risks associated with each category.

Encryption standards for data at rest and in transit are essential for preventing unauthorized access and ensuring data integrity. Encryption algorithms such as

AES for data storage and TLS for data transmission help maintain the confidentiality of data within Smart City networks. Data minimization and retention policies are also addressed here, focusing on collecting only necessary information and limiting data retention periods to reduce the risk of unauthorized exposure over time. It is also necessary to have mechanisms to ensure that files do not contain executable code that could potentially harm the system. Server security is crucial to protect servers from unauthorized access, data breaches, and malicious attacks. Care must be taken for hardening and configuring the servers and other devices.

Privacy-by-Design principles and compliance to Digital Personal Data Protection Act (DPDP Act) are critical considerations in Smart City development. Privacy-by-Design ensures that privacy measures are integrated into systems from the beginning, rather than as an afterthought. This approach reduces the chances of data breaches and aligns data protection best practices. Ensuring data security and privacy builds public trust, as citizens are more likely to accept Smart City technologies when they perceive that their data is protected.

8. Operational Security for Smart City Command and Control Centres

Not only individual components of a Smart City present potential vulnerabilities, but the emergent properties of such a complex, interconnected system can also give rise to unforeseen and often unpredictable security challenges. Operational Security (OpSec) is crucial for the command and control centres that manage Smart City operations. These centres are responsible for monitoring, decision-making, and coordinating various urban services, so their security must be airtight.

8.1 Legacy Technologies

Integrating outdated legacy systems with modern technologies often results in performance bottlenecks and creates weak links in the overall security chain.

These legacy components may lack proper security updates, making them easy targets for exploitation. Additionally, limited visibility into these older systems and inadequate architectural choices for integration can drag down the security posture of the entire Smart City ecosystem, effectively reducing it to the weakest and most neglected elements.

8.2 New Technologies

Emerging technologies can introduce risks, especially when they are developed and deployed without a robust security framework. If security is an afterthought—due to a rush to market, poor planning, or prioritizing rapid deployment over durability—new technologies introduce potential vulnerabilities. Insufficient testing or a lack of resilience measures can leave these technologies susceptible to attacks, amplifying risk throughout the interconnected infrastructure.

8.3 Team Coordination

The involvement of multiple teams in Smart City projects, spanning integration, deployment, and maintenance, often highlights serious management shortcomings. Lack of well-defined responsibilities and coordination among these teams can lead to fragmented efforts, duplicated tasks, and gaps in coverage. Without a clear, unified vision, teams may inadvertently pursue disparate objectives, reducing overall project cohesion and effectiveness. This disunity risks creating blind spots and inconsistencies, both of which can significantly weaken the Smart City's defenses.

8.4 Incident Detection and Response

Poor coordination in detecting, reporting, and responding to security incidents can result in delayed or even entirely missed responses, significantly undermining the city's security. The inability to respond swiftly and effectively can escalate minor issues into significant breaches. Inadequate documentation—such as

missing or poorly defined policies, security guidelines, and communication plans—exacerbates these issues by creating confusion during a crisis. Without a properly tailored incident response plan, Smart City operators may struggle to minimize damage and restore services quickly, ultimately eroding public trust.

Incident response and recovery plans are vital for maintaining operations during and after a cyber-incident. These plans outline procedures for isolating affected systems, restoring services, and conducting post-incident analyses to improve resilience. Supply chain security plays a critical role in Smart City operations, as threat actors try to compromise through third-party vendors. Secure procurement practices and vendor audits help ensure that third-party products and services meet strict security standards. Effective operational security protects the core functions of Smart Cities and minimizes the risk of service interruptions that could impact public safety.

8.5 Continuous monitoring and logging

Monitoring and logging infrastructure is essential for operational security. Continuous monitoring of network traffic, system activities, and user access can reveal abnormal behaviour indicative of a potential security incident. Integrating real-time threat intelligence provides command centres with insights into emerging threats, allowing them to adapt security protocols dynamically. All network, security and applications shall forward logs to centralised server where analytics, monitoring and correlation could be performed. The logs need to be maintained as per CERT-In directions published on 28 April 2022.

9. Internet of Things (IoT) Security in Smart Cities

IoT devices are central to Smart City ecosystems, enabling services such as traffic management, waste collection, and public safety monitoring. However, IoT devices often have limited processing capabilities and are prone to vulnerabilities. IoT and industrial control systems (ICS) are integral to the smooth functioning of

Smart City infrastructure, but they face vulnerabilities like unauthorized access, data manipulation, and operational disruptions. It is crucial to implement stronger network security, timely updates, and secure communication protocols to ensure these systems operate safely and effectively, maintaining reliable city services.

9.1 Internet of Things (IoT) Devices

- Unauthorized Access: Weak authentication makes IoT devices vulnerable to remote takeover, compromising various systems, including those that manage utilities like smart lighting, traffic controls, and resource meters.
- Data Interception: Poor encryption could lead to the interception of sensitive information, such as data from sensors monitoring resource distribution, compromising privacy and potentially revealing exploitable patterns.
- Botnet Attacks: Infected devices can be recruited into botnets, capable of launching large-scale DDoS attacks that disrupt digital infrastructure.

9.2 Industrial Control Systems (ICS)

- Operational Disruption: ICS disruptions can lead to major service outages, particularly in essential sectors like water distribution and power supply, affecting the city's ability to maintain smooth operations.
- Manipulation of Control Logic: Attackers targeting programmable logic controllers (PLCs) can manipulate control settings, which can lead to malicious operation of equipment such as pumps, valves, and electrical systems – disrupting essential functions.
- Ransomware: Targeting ICS with ransomware can lead to the shutdown of crucial services, halting operations with potentially dire consequences for residents.

9.3 Communications Vulnerabilities:

- Man-in-the-Middle (MITM) Attacks: Data manipulation between IoT devices and ICS could result in incorrect operational commands, impacting critical services and leading to reduced efficiency or unsafe conditions.
- Protocol Weaknesses: Weaknesses in commonly used ICS communication protocols may allow unauthorized control over vital systems, potentially endangering public safety by affecting service reliability. The IoT, ICS, data centre and cloud computing protocols also have vulnerabilities and care needs to be taken during implementation of these protocols. The best practices that need to be followed while using these technologies are placed in Annexure I.

9.4 Vulnerability management

IoT vulnerability management is another critical component, as identifying and mitigating vulnerabilities in IoT devices reduces the risk of exploitation. It is recommended to have network segmentation to isolate IoT devices from other critical systems, limiting the potential impact of a compromised device. By addressing these aspects, Smart Cities can reduce the attack surface associated with IoT devices and ensure that the benefits of IoT-driven services. The commonly exploited vulnerabilities in different smart systems is provided in Annexure-II.

Firmware and patch management are essential for maintaining device security, as outdated firmware may contain vulnerabilities that attackers can exploit. Establishing a regular patch management process, including automated updates where possible, ensures that devices are protected against known threats. The default factory settings of the IoT devices must be changed before deployment and access to the device must be limited to authorised users / devices. Secure device identity and credential management also play a significant role, ensuring that only authenticated and authorized devices can connect to the network.

10. Artificial Intelligence (AI) and Machine Learning (ML) Security

AI is used in Smart Cities to optimize traffic flow and reduce congestion by analyzing real-time data from cameras, IoT sensors, and GPS devices. It also supports autonomous vehicle navigation and enhances public transportation scheduling for smoother urban mobility. However, this brings certain risks. Attackers could manipulate traffic data, leading to incorrect AI predictions that result in congestion or accidents. Additionally, adversarial inputs could confuse sensors used in autonomous vehicles, compromising their safety and reliability.

In the energy sector, AI-driven smart grids help optimize energy distribution and consumption by predicting peak usage, managing demand response, and effectively integrating renewable energy sources. Yet, AI models in energy management are not without vulnerabilities. A compromised model could lead to energy imbalances or blackouts, particularly during periods of peak demand. Similarly, incorrect demand response actions triggered by an attacker could destabilize the power grid.

AI is also used to enhance public safety through automated surveillance, anomaly detection, and facial recognition, allowing for proactive crime prevention and real-time alerting. However, attackers manipulating training data could cause the AI system to misclassify threats, leading to either ignoring real incidents or flagging normal behaviors as potential threats.

AI-powered environmental monitoring analyzes data from sensors to assess air quality, water quality, and noise levels. Predictive models help implement timely interventions to mitigate environmental issues. Nevertheless, attackers could alter sensor data, resulting in false alerts or missed opportunities to address pollution, ultimately impacting public health. Misleading data fed to AI systems can also result in poor decision-making.

Citizen engagement is improved by AI-driven chatbots and virtual assistants, which provide quick responses to queries, manage service requests, and enhance communication between citizens and city administrations. However, these chatbots can be exploited to spread misinformation or provide unauthorized access to services. In cases where AI systems are compromised, sensitive citizen data may be exposed, eroding public trust.

AI systems are also used to predict maintenance needs for essential public infrastructure, such as bridges, roads, and utilities, by analyzing sensor data. This helps prevent failures and optimizes resource allocation. But attackers could manipulate sensor data, leading to false maintenance alerts that either trigger unnecessary interventions or miss genuine issues, resulting in increased downtime. Additionally, compromised predictive maintenance systems could make infrastructure vulnerable to deliberate failures or sabotage, disrupting key services.

AI plays a critical role in optimizing urban operations, enhancing public safety, improving resource management, and streamlining citizen services in Smart Cities. However, every AI application has inherent risks – such as data manipulation, adversarial attacks, privacy concerns, and operational disruptions. These must be addressed through robust security measures, including encryption, data integrity verification, and proactive monitoring to ensure the resilience and reliability of city services.

Artificial Intelligence (AI) and Machine Learning (ML) are increasingly used in Smart City applications for predictive analytics, anomaly detection, and automated decision-making. However, these technologies introduce unique security risks. Protecting ML models from adversarial attacks is crucial. Techniques such as input sanitization, model validation, and adversarial training help mitigate the risk of attacks that could cause AI-driven systems to malfunction. Monitoring and detecting AI anomalies in real-time is also

emphasized, as AI systems may behave unpredictably under attack or if data patterns change unexpectedly.

10.1 AI ethical considerations

To build ethical AI systems in Smart Cities, it is essential to address biases, maintain transparency, respect privacy, and emphasize human-centered design and accountability. When these principles are embedded throughout the development and deployment process, AI can enhance urban life equitably, maintaining public trust and ensuring ethical decision-making at every stage.

Smart Cities can enhance the security and resilience of AI-driven applications while mitigating risks associated with their use in urban environments by ensuring the AI solutions are developed with transparency and ethical approach.

The accuracy and fairness of AI systems in Smart Cities depend heavily on the quality and representativeness of the data they process. If training datasets contain biases, these biases easily manifest in the system's outputs, leading to unequal treatment or opportunities. Addressing these risks involves incorporating fairness metrics, auditing datasets for potential biases, and introducing diverse datasets that reflect the varied realities of a city's population.

AI systems deployed in Smart Cities must not only perform their tasks effectively but also offer clear and understandable reasoning behind their decisions. A lack of clarity can foster mistrust and resistance to AI-powered services. Explainability ensures that both officials and the public have confidence in these systems. Additionally, the ability to review AI decisions should be integrated into the process to rectify errors and promoting a sense of trust. Clear communication about how these systems work and their decision criteria is essential to maintaining public support and ensuring ethical usage.

Smart Cities generate vast amounts of data through IoT devices, surveillance systems, and interconnected platforms, enabling administrators to gain valuable

insights for improving urban planning, safety, and resource management. However, these same data collection practices can infringe on privacy and human rights if not carefully controlled. The data collected often includes personal details such as movement patterns, behavioural tendencies, and interactions with city infrastructure. Without proper safeguards, this sensitive information could be misused for intrusive surveillance or fall victim to breaches, putting citizens at risk. Addressing these concerns requires anonymization techniques, encryption protocols, and strict data governance policies that minimize the risk of misuse. Policies governing data retention periods and access permissions are also critical to ensure compliance with privacy standards. By focusing on these protective measures, Smart Cities can strike a balance between leveraging AI for collective benefits and preserving the fundamental rights of their residents.

AI systems in Smart Cities must prioritize the welfare and needs of the people they are designed to serve. This means designing systems that are accessible, inclusive, and fair for all citizens. For example, public-facing systems should accommodate diverse user needs, including language support and accessibility for individuals with special needs. While AI can automate decision-making at scale, final authority over critical decisions must remain with human operators. Automated recommendations for resource allocation, public safety actions, or penalties should always be subject to review, enabling human discretion to override machine-generated outputs when needed. Furthermore, accountability frameworks must clarify who is responsible for decisions made or supported by AI, particularly in cases where errors lead to harm. Transparent accountability mechanisms and robust oversight processes ensure that ethical principles guide both the design and deployment of Smart City technologies.

11. Disaster Recovery and Business Continuity Planning

A Disaster Recovery and Business Continuity Plan (DR/BCP) is essential for ensuring that Smart City services remain operational during emergencies. Smart

cities need to develop resilience planning with a detailed approach to assess the resilience of each system component and develop contingency plans for various scenarios, including cyber incidents, natural disasters, and equipment failures.

Data backup and recovery processes are the foundational elements of disaster recovery, ensuring that data can be restored quickly and accurately after an incident. The redundancy and failover strategies, such as using geographically distributed data centres and redundant network paths to prevent single points of failure must also be made part of the recovery plan. Offline tape backups should also be taken regularly in case the whole system needs to be restored from scratch.

Regular testing of disaster recovery plans is emphasized to ensure that DR/BCP procedures are effective and can be executed quickly when needed. Testing scenarios should simulate real-world conditions, helping Smart City operators identify weaknesses and improve their response times. By establishing comprehensive disaster recovery and continuity plans, Smart Cities can reduce downtime, minimize service disruption, and maintain critical functions in times of crisis.

12. Compliance and Legal Considerations

Compliance with regulatory requirements is critical for Smart City operations to ensure security, privacy, and accountability. Cybersecurity compliance and audits play a key role in verifying that Smart City operators adhere to these regulations. Regular audits, both internal and external, help identify areas of non-compliance and provide a roadmap for addressing security gaps.

Any service provider, intermediary, data centre, body corporate and Government organization shall mandatorily report cyber incidents to CERT-In within 6 hours of noticing such incidents or being brought to notice about such incidents. The incidents can be reported to CERT-In via email (incident@cert-in.org.in), Phone (1800-11-4949) and Fax (1800-11-6969). The details regarding methods and

formats of reporting cyber security incidents is also published on the website of CERT-In (www.cert-in.org.in) and will be updated from time to time. The service providers, intermediaries, data centres, body corporate and Government organisations should designate a Point of Contact to interface with CERT-In. All communications from CERT-In seeking information and providing directions for compliance shall be sent to the said Point of Contact.

All service providers, intermediaries, data centres, body corporate and Government organisations shall mandatorily enable logs of all their ICT systems and maintain them securely for a rolling period of 180 days and the same shall be maintained within the Indian jurisdiction. These should be provided to CERT-In along with reporting of any incident or when ordered / directed by CERT-In.

Data Centres, Virtual Private Server (VPS) providers, Cloud Service providers and Virtual Private Network Service (VPN Service) providers, shall be required to register accurate user information as notified in CERT-In's direction issued in April 2022 and must be maintained by them for a period of 5 years or longer duration as mandated by the law after any cancellation or withdrawal of the registration as the case may be.

13. API security

APIs (Application Programming Interfaces) are the backbone of smart cities, enabling seamless communication and data exchange between various systems, devices, and stakeholders. They serve as the key enabler for integrating diverse technologies, fostering innovation, and ensuring efficient delivery of services in a smart city ecosystem. APIs play a key role in Data Integration and Interoperability, Real-Time Data Exchange, Optimized Resource Management, E-Governance, Smart Infrastructure, Open Data Platforms, Security and Privacy. This increasing dependence on API, in turn, is leading to API security becoming a serious concern as it not only expands the attack surface but also introduces new

security risks. In addition, there could be severe consequences for consumers, businesses, and third-party providers in case of API breaches. Some of the common API security issues are listed below.

- Broken Object Level Authorization: Exposing endpoints that handle object identifiers can lead to access control issues.
- Broken Authentication: Flaws in authentication mechanisms can allow attackers to compromise user identities.
- Broken Object Property Level Authorization: Lack of proper authorization at the object property level can lead to information exposure or manipulation.
- Unrestricted Resource Consumption: API requests can overconsume resources, causing denial of service or increased operational costs.
- Broken Function Level Authorization: Complex access control policies can result in authorization flaws, enabling unauthorized access.
- Unrestricted Access to Sensitive Business Flows: APIs exposing business flows without safeguards can be exploited for malicious purposes.
- Server-Side Request Forgery (SSRF): APIs fetching remote resources without validation can be manipulated to send requests to unintended destinations.
- Security Misconfiguration: Improper API configurations can open vulnerabilities, leading to potential exploitation.
- Improper Inventory Management: Poor documentation and management of API endpoints and versions increase security risks.
- Unsafe Consumption of APIs: Trusting third-party APIs without proper security measures can lead to indirect compromises.

The API security best practices that smart cities needs to follow include

- Implement strong authentication and authorization.
- Use encryption for data in transit and at rest.
- Validate and sanitize inputs to prevent injection attacks.

- Limit data exposure with response filtering and access controls.
- Throttle and rate-limit API requests.
- Monitor and log API activities for auditing and threat detection.
- Secure API endpoints using IP whitelisting and API gateways.
- Keep APIs and dependencies up-to-date.
- Use security tokens for session management.
- Protect against unintended resource consumption with quotas and safeguards.
- Adopt security-first development practices.
- Educate and train stakeholders on API security.
- Conduct regular risk assessments.
- Implement security by design during the API development phase.
- Leverage AI and machine learning for threat detection and response.

14. Training and Awareness

Cybersecurity training and awareness are essential for equipping Smart City personnel with the knowledge and skills needed to identify and respond to cyber threats. It is necessary to organize cybersecurity awareness programs for operators and stakeholders, focusing on educating staff about common threats, such as phishing, social engineering, and malware.

Most of the cyber incidents are caused by human error. Enterprises suffer financial losses from staff-related incidents. Human factor of breaches appears in different ways. Most common are the download of malware, using weak passwords or not changing passwords often enough, visiting unsecured websites and using unauthorized systems to share data. Training is essential to raise awareness among employees – motivating them to pay attention to cyber threats and mitigating them. Accordingly, it is important to raise awareness among employees supporting the functioning of Smart Cities.

In today's ever-changing threat landscape, it is essential to ensure that Smart City ICT security specialists maintain up-to-date skills in threat hunting and incident response. Security experts must be trained to implement security monitoring processes and key security operations to effectively detect and investigate malicious activity and threat hunting. It is also important to master the skills of incident analysis, evidence collection, log file analysis, network analysis, creating indicators of compromise (IoC) and memory forensics.

By investing in cybersecurity training and awareness, Smart Cities can strengthen their first line of defense against cyber threats, as well-trained employees are better equipped to prevent and respond to incidents. A culture of cybersecurity awareness fosters proactive security practices and reduces the likelihood of human error contributing to security incidents.

15. Crisis Management & Incident Response

A Cyber Crisis Management Plan (CCMP) is a structured framework designed to prepare organizations for responding effectively to cybersecurity incidents, minimizing their impact, and ensuring rapid recovery. It encompasses proactive measures, incident response protocols, and recovery strategies to mitigate the risks associated with cyberattacks, data breaches, and other digital threats. CERT-In, MeitY has formulated Cyber Crisis Management Plan (CCMP) for countering cyber-attacks and cyber terrorism for implementation by all Ministries/Departments of Central Government, State Governments/UTs and organizations under their administrative control. Along with the CCMP, CERT-In has developed "Guidance Framework for CCMP" which may be used as a template by various entities including Central Government Ministries/Departments/States/UTs and entities under their administrative control to prepare & implement their own CCMP. CCMP outlines a framework for dealing with cyber related incidents for a coordinated, multi-disciplinary and broad based approach for rapid identification, information exchange, swift

response and remedial actions to mitigate and recover from malicious cyber incidents. The CCMP needs to be developed in line with the National CCMP template for effective crisis management.

Incident response is a critical component of a robust cybersecurity strategy, as Smart Cities must be prepared to detect, contain, and mitigate cyber incidents to maintain public safety and service continuity. A comprehensive incident response framework is required to guide operators through each stage of managing a cyber-incident. The framework should include preparation, detection, containment, eradication, recovery, and post-incident review phases, each with detailed actions and responsibilities for team members.

Incident Response (IR) framework should describe the following aspects:

- IR Methodology
- IR participants
- Internal and External communication matrix
- IR metrics and SLAs
- Incident definition, severity levels, prioritization, and categorization
- Guidelines for the analysts to prioritize incidents
- Crisis management procedures covering triggers to involve internal and external parties
- Corresponding IR procedures
- Connection with relevant processes of organization

IR Playbooks should be tailored for the chosen cyber threats and existing IR processes describe in detail all phases of incident handling, from initial preparation to post-incident activities. IR playbooks should define the Who, What, When, Where, and How to act in case of a cyber-security incident and which tools should be used.

Detection and analysis involve identifying unusual activities or potential breaches. This stage requires effective monitoring systems, threat intelligence, and log analysis to rapidly identify suspicious events. Once an incident is detected, the containment phase focuses on isolating affected systems to prevent further spread. For example, in the case of a malware attack, operators might disconnect compromised devices from the network.

Eradication and recovery are the next steps, where the source of the incident is removed, systems are restored, and normal operations are resumed. Post-incident analysis plays a crucial role in identifying lessons learned and improving incident response procedures. Implementing these incident response best practices allows Smart City operators to minimize the impact of cyber incidents and continually improve their response capabilities.

Testing the readiness of Smart City to respond to a cyber-attack in terms of stakeholder communication and coordination is necessary to build confidence in everyone's ability to respond swiftly and appropriately in a crisis situation. It allows to confirm the effectiveness of incident response plans and playbooks and make sure, that in case of a breach all defined steps, roles and responsibilities of the incident response team members are defined, known and the overall tasks match the desired output in response to a particular incident.

16. Continuous Monitoring and Threat Intelligence

Continuous monitoring is essential for maintaining situational awareness and identifying threats before they can cause harm. Real-time system and network monitoring, as well as behavioural analytics can help to detect unusual activities. These tools help operators gain visibility into system health, network traffic, and potential anomalies that may indicate a cyber-threat.

Threat intelligence integration enables Smart Cities to stay ahead of emerging threats. Threat intelligence includes information on known vulnerabilities, attack

vectors, and evolving tactics used by malicious actors. By subscribing to CERT-In's threat intelligence feeds and other IT & OT feeds from relevant stakeholders, operators can keep their defenses up-to-date and prioritize high-risk threats. Integrating Security Information and Event Management (SIEM) systems with these feeds can effectively help to protect by aggregating and analysing data from multiple sources to provide a centralized view of security activities.

Furthermore, automated threat detection and response mechanisms, such as Security Orchestration, Automation, and Response (SOAR), can enhance the efficiency and accuracy of incident response by automating routine actions and alerting operators to high-priority threats. Continuous monitoring and threat intelligence integration ensure that Smart Cities remain vigilant, resilient, and responsive to potential cyber threats, providing early warning signals that prevent small issues from escalating into major incidents.

Entities in smart cities can also get onboarded onto CERT-In's services like CERT-In's Malware Threat eXchange (CMTX) – Cyber Threat Intelligence, Cyber Swachhta Kendra (CSK), National Cyber Coordination Centre and Cyber security alerts.

17. Supply Chain Security, Vendor Management and SBOM

As Smart Cities rely on numerous third-party vendors for software, hardware, and services, securing the supply chain is vital to avoid introducing vulnerabilities. Evaluating vendor security practices and ensuring that suppliers adhere to strong cybersecurity standards is one of the important aspects of ensuring supply chain security. Smart City operators should conduct due diligence assessments for vendors, covering aspects such as data handling practices, access control, incident response capabilities, and adherence to relevant cybersecurity frameworks.

Supply chain risk management practices, such as setting clear security expectations in contracts, regular vendor audits, and continuous risk assessment,

are recommended to monitor and enforce security compliance. In secure procurement processes, cybersecurity is factored into purchasing decisions, and it helps to reduce the risk of integrating compromised or untested products into the Smart City infrastructure.

To further mitigate risks, vendor access control policies must be developed to ensure that third-party access to systems and data is restricted, monitored, and regularly reviewed. By implementing these supply chain security measures, Smart Cities can protect themselves from vulnerabilities or malicious actions originating from their vendors, minimizing risks associated with external dependencies in urban infrastructure.

Indian Computer Emergency Response Team (CERT-In) has released the Technical Guidelines on Software Bill of Material (SBOM) for entities, particularly those in the public sector, government, essential services, organizations involved in software export and software services industry. Departments and organizations in smart cities are encouraged to make the creation and provision of SBOM a mandatory standard practice as part of software procurement and software development in order to enhance security and reduce the risk of cyber threats.

18. Penetration Testing and Vulnerability Management

Regular penetration testing and vulnerability assessments are essential for identifying and addressing security weaknesses within Smart City systems. Industry standard best practices for conducting penetration tests, including both internal and external assessments must be carried out to uncover potential vulnerabilities. These tests should be tightly controlled and performed by qualified professionals who can provide an objective analysis of the system's security posture.

These tests can reveal security shortcomings which could be exploited to gain unauthorized access to critical network components. Penetration testing provides understanding of security flaws in IT infrastructure, revealing vulnerabilities, analyzing the possible consequences of different forms of attack, evaluating the effectiveness of current security measures and suggesting remedial actions and improvements. These tests should be tightly controlled and performed by qualified professionals with full regard to Smart City systems' confidentiality, integrity and availability.

Smart City critical applications should be analyzed in more detail. Application security assessment involves identifying and testing vulnerabilities and weaknesses of various risk levels that could potentially pose threats to the Smart City's applications and data. Assessment should take into consideration not just technological and functional capabilities of the application, but also should dive deeper into business logic of the application to identify issues that may be missed when using conventional vulnerability assessment approach.

The outcome of the analysis, which includes information about existing security flaws and corresponding recommendations for their elimination, allows to eliminate vulnerabilities in a timely manner and thus avoid possible negative consequences for the application from external attackers or insider actions.

Vulnerability management involves systematically identifying, classifying, and remediating security weaknesses in hardware, software, and network components. Smart City operators should implement a vulnerability assessment schedule to ensure that new vulnerabilities are detected and addressed promptly. Patch management is also critical in this process, as timely application of patches minimizes the risk of exploitation by attackers. Utilizing automated vulnerability scanning tools can enhance efficiency by providing continuous assessments and alerts for emerging risks. Regular penetration testing and vulnerability management efforts enable Smart Cities to maintain a proactive security stance,

continuously improving defenses and reducing the likelihood of successful cyberattacks.

19. Security Audits and Compliance Checks

Cyber Security audits and compliance checks are essential for verifying that Smart City infrastructures adhere to regulatory requirements and internal cybersecurity policies. It is necessary to conduct regular, thorough security audits, focusing on evaluating policies, procedures, technical configurations, and user practices. These audits help identify non-compliance areas and gaps that may introduce security risks.

Internal and external audit processes are both recommended for a comprehensive assessment, with external audits providing an impartial evaluation from third-party experts. Smart City operators should also implement continuous compliance monitoring to ensure that systems remain in alignment with relevant regulations, such as data protection laws, industry standards, and critical infrastructure security requirements. The scope of audit should be comprehensive so as to cover entire ICT infrastructure. Internal information security audit should be performed at least once in six months. Third party security audits must be conducted periodically at least once a year to ensure compliance with security policy, guidelines, and procedures, and to determine the minimum set of controls required to address the Smart city security. Security audit should be performed prior to and after implementation or installation or major enhancements in the ICT infrastructure.

Corrective action plans should follow each audit to address identified gaps, with clear timelines and responsibilities for remediation. By performing regular security audits and compliance checks, Smart Cities demonstrate accountability, maintain a high standard of security, and adapt their practices to comply with evolving regulations and industry standards.

20. Conclusion

The document aims to provide a comprehensive, forward-looking approach to support the secure growth of Smart Cities by enhancing their ability to serve citizens in an increasingly digital world. It also emphasises the importance of a proactive, layered, and adaptable cybersecurity strategy for Smart Cities. As urban areas become increasingly dependent on digital infrastructure, cybersecurity must be integrated into every aspect of Smart City development, from the design phase to daily operations. The document reiterates that Smart Cities are not just technological innovations but essential services that support citizens' well-being and safety.

We need to understand the importance of collaborative efforts among various stakeholders namely - CERT-In, smart city operators, technology providers, and Government bodies. By working together, all the stakeholders can ensure that Smart City systems are not only innovative but also secure, resilient, and compliant with regulatory standards.

References

1. https://mohua.gov.in/cms/smart-cities.php
2. https://smartcities.gov.in/advisory
3. www.iiconsortium.org
4. www.nist.gov

Useful Guidelines and Materials

a) CERT-In Directions.

https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

b) Technical Guidelines on SBOM

https://www.cert-in.org.in/PDF/SBOM_Guidelines.pdf

c) Information Security Best Practices for Government entities

https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf

d) Cyber Security Awareness Booklets

https://www.cert-in.org.in/AwarenessBooklets.jsp

e) Free Botnet removal tools

https://www.csk.gov.in/security-tools.html

f) Guidelines for Secure Application Design, Development, Implementation & Operations

https://www.cert-in.org.in/PDF/Application_Security_Guidelines.pdf

CERT-In's 24/7 Cyber security Incident Response Help Desk

Tel: 1800-11-4949 (Toll free)

Fax: 1800-11-6969 (Toll free)

E-mail: incident@cert-in.org.in

Annexure I

a) ICS protocols

S.No	ICS Protocol	Purpose of Use	Common Exploitation of Vulnerabilities	Best Practices for Implementation
1	Modbus	Communication between master and slave devices in industrial systems.	Lack of authentication and encryption; data interception or tampering.	Use Modbus TCP with TLS; encrypt traffic using VPNs; isolate Modbus devices in secure network zones.
2	DNP3	Communication in utilities like power and water distribution.	Replay attacks, lack of encryption; unauthorized command execution.	Implement DNP3 Secure Authentication; segment networks; encrypt communication.
3	Profibus/Profinet	Automation in factory environments.	Packet injection, denial-of-service attacks.	Use Profinet with secure network configurations; enforce access controls.
4	OPC/OPC UA	Interoperability between devices and systems in industrial environments.	Lack of secure configuration; exploitation of legacy OPC vulnerabilities.	Use OPC UA for enhanced security; enforce secure-by-default configurations.
5	BACnet	Building automation for HVAC, lighting, and security systems.	Exploitation of open ports; unauthorized device access.	Use secure network segmentation; apply strong access controls.
6	IEC 61850	Substation automation and communication in smart grids.	Spoofing and unauthorized access due to unencrypted communication.	Implement TLS for communication; use strong authentication mechanisms.
7	HART	Communication with field instruments like sensors and actuators.	Man-in-the-middle attacks on analog/digital data.	Encrypt HART traffic using secure tunneling; use strong device authentication.

8	CAN Bus	Real-time communication in automotive and industrial systems.	Injection of malicious CAN frames; lack of authentication.	Implement message authentication codes (MACs); monitor CAN traffic for anomalies.
9	EtherCAT	High-speed communication for real-time automation.	Denial-of-service and packet manipulation attacks.	Use firewalls to restrict EtherCAT traffic; implement secure firmware updates.
10	MMS	Supervisory control communication in power systems.	Data tampering due to lack of encryption.	Use TLS for secure communication; enforce strict access controls.

b) IoT Protocols

S.No	IoT Protocol	Purpose of Use	Common Exploitation of Vulnerabilities	Best Practices for Implementation
1	MQTT (Message Queuing Telemetry Transport)	Lightweight messaging protocol for IoT devices.	Lack of encryption; unauthorized access; spoofed messages.	Use MQTT over TLS; implement authentication and access control.
2	CoAP (Constrained Application Protocol)	Communication for constrained devices in IoT networks.	Replay attacks; lack of encryption; denial-of-service attacks.	Use DTLS for secure communication; restrict access to trusted sources.
3	AMQP (Advanced Message Queuing Protocol)	Middleware for reliable message queuing and routing.	Exploitation of misconfigured brokers; interception of messages.	Use AMQP over TLS; enforce strict access control and monitoring.
4	HTTP/HTTPS	Communication between IoT devices and cloud servers.	Interception of unencrypted HTTP traffic; session hijacking.	Always use HTTPS; implement strong authentication and token-based access.

5	XMPP (Extensible Messaging and Presence Protocol)	Messaging and presence notifications in IoT systems.	Unauthorized access; spoofing attacks.	Use TLS for encryption; deploy server-to-server authentication.
6	Zigbee	Wireless communication for smart home devices.	Weak encryption keys; jamming attacks; device spoofing.	Use strong encryption keys; implement network key rotation.
7	Z-Wave	Wireless communication for home automation devices.	Exploitation of default keys; device impersonation.	Use secure mode (S2); replace default keys with unique ones.
8	LoRaWAN	Low-power wide-area network communication.	Replay attacks; weak device authentication.	Use LoRaWAN 1.1+ for enhanced security; ensure unique device credentials.
9	BLE (Bluetooth Low Energy)	Short-range communication for IoT devices.	Sniffing attacks; pairing vulnerabilities.	Use secure pairing modes; enforce strong encryption (AES-CCM).
10	NB-IoT (Narrowband IoT)	Cellular-based IoT communication for wide coverage.	SIM-based attacks; interception of unencrypted data.	Encrypt data at the application layer; use device-based authentication.
11	LWM2M (Lightweight Machine-to-Machine)	Device management for IoT systems.	Man-in-the-middle attacks; lack of authentication.	Use DTLS for communication; implement client-server authentication.
12	DDS (Data Distribution Service)	Real-time data sharing in IoT and edge systems.	Unauthorized access; denial-of-service attacks.	Apply encryption (TLS/DTLS); enforce role-based access control.

c) Data Centre Protocols

S.No	Data Centre Protocol	Purpose of Use	Common Exploitation of Vulnerabilities	Best Practices for Implementation
1	TCP (Transmission	Reliable, connection-	Packet injection, session	Use firewalls to limit SYN

	Control Protocol)	oriented data transport.	hijacking, SYN flooding attacks.	flooding; implement TLS for encryption.
2	UDP (User Datagram Protocol)	Low-latency, connectionless communication.	Amplification attacks, packet spoofing.	Use rate limiting and access control; monitor for anomalous traffic.
3	HTTP/HTTPS	Communication for web services and APIs.	Man-in-the-middle (MITM) attacks, insecure cookies, cross-site scripting.	Enforce HTTPS with TLS; implement secure headers; use web application firewalls (WAFs).
4	BGP (Border Gateway Protocol)	Routing between data centers and external networks.	Route hijacking, prefix leaking, denial-of-service attacks.	Use BGP route filtering, prefix validation, and monitoring.
5	VXLAN (Virtual Extensible LAN)	Network virtualization for Layer 2 over Layer 3.	Unauthorized access to VLANs, spoofing.	Isolate VXLANs; use strong authentication and network segmentation.
6	iSCSI (Internet Small Computer Systems Interface)	Storage access over IP networks.	Data interception, weak authentication.	Encrypt traffic with IPsec; enforce mutual authentication.
7	Fibre Channel	High-speed data transport in SANs.	Unauthorized access, traffic interception.	Use Fibre Channel zoning and LUN masking for access control.
8	NFS (Network File System)	File sharing between servers and clients.	Exploitation of insecure exports, man-in-the-middle attacks.	Restrict access to trusted hosts; enable Kerberos authentication.
9	SNMP (Simple Network Management Protocol)	Device monitoring and management.	Exploitation of default community strings, data interception.	Use SNMPv3 with strong credentials; restrict access by IP.
10	LACP (Link Aggregation Control Protocol)	Aggregates multiple links for redundancy and higher throughput.	Exploitation of misconfigured LACP; traffic disruption.	Configure LACP securely; monitor for anomalous behavior.

11	TLS (Transport Layer Security)	Encryption for secure communication.	Exploitation of weak ciphers, outdated versions.	Use strong cipher suites; enforce TLS 1.2 or 1.3.
12	SSH (Secure Shell)	Secure remote access and command-line operations.	Exploitation of weak credentials, brute-force attacks.	Use key-based authentication; disable root login; use strong passwords.
13	NVMe-oF (NVMe over Fabrics)	High-performance storage access over RDMA, Ethernet, or Fibre Channel.	Data interception, unauthorized access.	Implement encryption and secure zoning; enforce strong authentication.
14	OpenFlow	SDN control for forwarding plane management.	Unauthorized controller access, packet manipulation.	Secure OpenFlow controllers with authentication and encryption.
15	Zigbee	Communication in low-power environments (e.g., IoT in data centers).	Exploitation of default keys, jamming attacks.	Use strong encryption keys; implement frequent key rotations.
16	NetFlow/sFlow	Network traffic monitoring and analysis.	Spoofing attacks, exploitation of unprotected traffic data.	Encrypt exported data; limit NetFlow access to trusted systems.
17	ICMP (Internet Control Message Protocol)	Diagnosing network issues (e.g., ping).	Smurf attacks, ICMP tunneling.	Limit ICMP traffic; block unnecessary ICMP types.
18	LoRaWAN	Low-power, wide-area communication for IoT.	Replay attacks, weak device authentication.	Use LoRaWAN 1.1+; ensure unique device credentials.
19	HTTP/3 (QUIC)	Web content delivery with reduced latency.	Exploitation of unencrypted fallback mechanisms, injection attacks.	Enforce encryption; implement strict transport security policies.
20	RESTful APIs	Managing cloud and data center resources.	Exploitation of insecure endpoints, improper authentication.	Use API gateways; secure endpoints with OAuth2 and HTTPS.

d) Cloud Protocols

S.No	Cloud Protocol	Purpose of Use	Common Exploitation of Vulnerabilities	Best Practices for Implementation
1	HTTP/HTTPS	Communication for web applications and APIs.	Man-in-the-middle (MITM) attacks, insecure cookies, cross-site scripting.	Enforce HTTPS with TLS, implement secure headers, and use WAFs.
2	REST (Representational State Transfer)	API communication for cloud services and applications.	Exploitation of insecure endpoints, lack of authentication.	Use HTTPS for transport, implement OAuth2, and validate API inputs.
3	SOAP (Simple Object Access Protocol)	Messaging protocol for cloud-based web services.	Exploitation of insecure XML parsing, MITM attacks.	Use WS-Security standards; validate XML inputs; enforce encryption.
4	AMQP (Advanced Message Queuing Protocol)	Messaging for distributed cloud applications.	Message interception, unauthorized message injection.	Use TLS for encryption; implement authentication mechanisms.
5	MQTT (Message Queuing Telemetry Transport)	Lightweight protocol for IoT and cloud communication.	Unauthorized access, weak authentication.	Implement TLS and mutual authentication; enforce access control.
6	DNS (Domain Name System)	Resolving domain names to IP addresses in cloud services.	DNS spoofing, DNS amplification attacks.	Use DNSSEC; implement rate limiting and monitor for anomalies.
7	IPsec (Internet Protocol Security)	Secure communication over IP networks in	Weak key management, improper configuration.	Use strong encryption algorithms and manage keys securely.

		cloud environments.		
8	TLS (Transport Layer Security)	Encrypting communication for secure cloud data transfers.	Exploitation of weak ciphers, outdated versions.	Use strong cipher suites and TLS 1.2 or 1.3; avoid deprecated versions.
9	SSH (Secure Shell)	Secure remote access to cloud infrastructure.	Brute-force attacks, exploitation of weak credentials.	Use key-based authentication; enforce strong passwords; disable root login.
10	S3 API (Amazon Simple Storage Service API)	Interfacing with AWS S3 for object storage.	Exploitation of open buckets, unauthorized access.	Use access control policies; enable bucket encryption and versioning.
11	OpenStack APIs	Managing OpenStack cloud resources.	Exploitation of insecure endpoints, improper access control.	Use role-based access control (RBAC); secure API endpoints with HTTPS.
12	CloudFormation/ARM Templates	Infrastructure-as-Code (IaC) for cloud resource provisioning.	Misconfigured templates leading to insecure deployments.	Review and validate templates; enforce least privilege policies.
13	IAM (Identity and Access Management)	Access control and authentication for cloud resources.	Privilege escalation, weak role definitions.	Enforce least privilege, enable MFA, and monitor access logs.
14	Kerberos	Authentication for secure cloud resource access.	Ticket replay attacks, credential theft.	Use strong encryption; ensure synchronized time between servers.
15	RDP (Remote Desktop Protocol)	Remote access to cloud virtual machines.	Brute-force attacks, exploitation of weak credentials.	Use strong passwords; enable network-level authentication

				(NLA); restrict RDP access.
16	VDI (Virtual Desktop Infrastructure)	Delivering desktop environments via the cloud.	Exploitation of insecure connections, session hijacking.	Use TLS to secure connections; enforce user session timeouts.
17	OAuth2	Authorization for cloud services and APIs.	Token theft, token reuse attacks.	Use short-lived tokens; implement secure storage for tokens.
18	OIDC (OpenID Connect)	Authentication for cloud applications.	Exploitation of misconfigured redirect URIs.	Validate redirect URIs; enforce strong authentication policies.
19	NetFlow/sFlow/IPFIX	Monitoring cloud network traffic and analyzing performance.	Exploitation of unencrypted traffic data.	Encrypt monitoring data; restrict access to trusted systems.
20	IAM Federation (SAML/OIDC)	Federated identity for single sign-on in cloud environments.	Exploitation of weak trust relationships between identity providers.	Monitor SAML assertions; enforce secure token exchanges.

Annexure-II

IoT Device threats

S.No	IoT Device	Purpose	Security Threat	Best Practices
1	Smart Traffic Lights	Manage traffic flow by adjusting light timings based on real-time data.	Traffic manipulation, unauthorized access to control systems.	Use encrypted communication, secure access control, and implement regular software updates.
2	Traffic Cameras	Monitor traffic conditions, capture incidents, and detect violations.	Privacy violations, data tampering, and unauthorized access.	Encrypt video data, secure storage, and ensure compliance with privacy laws.
3	Parking Sensors	Detect availability of parking spaces and guide drivers.	Data interception, spoofing sensor data.	Use encrypted communication, ensure device integrity, and regular firmware updates.
4	Air Quality Sensors	Monitor air pollution levels and provide real-time data on air quality.	Data spoofing or manipulation, denial of service attacks.	Use secure data transmission, monitor sensor integrity, and implement access control for data.
5	Water Quality Sensors	Monitor parameters like pH, turbidity, and temperature in water systems.	Tampering with sensor data, physical sabotage.	Ensure physical security, use encryption for data transmission, and implement regular maintenance.
6	Smart Street Lighting	Adjust lighting based on environmental conditions and motion.	Hacking light control systems, physical attacks on devices.	Secure the communication networks, use resilient devices, and install physical tamper-proof enclosures.
7	Smart Water Meters	Monitor water consumption and detect leaks or inefficiencies.	Unauthorized access, data manipulation.	Encrypt communication, implement user authentication, and maintain firmware updates.

8	Smart Grids	Optimize energy distribution, detect faults, and balance loads.	Cyberattacks on grid control systems, data manipulation.	Apply strong encryption, use multi-factor authentication, and monitor systems continuously.
9	Surveillance Cameras (CCTV)	Provide real-time monitoring of public spaces and critical infrastructure.	Privacy violations, unauthorized access to footage, data breaches.	Use encrypted video feeds, restrict access, and ensure compliance with data protection laws.
10	Smart Fire Detection Systems	Detect fires early by monitoring smoke, heat, or gas levels.	False alarms, hacking of alert systems.	Regularly test systems, use encrypted communication, and ensure proper alarm protocols.
11	Emergency Alert Systems	Notify citizens of emergencies such as natural disasters or accidents.	Hacking of alert messages, denial of service attacks.	Implement redundancy, use encryption, and regularly audit system security.
12	Wearable Health Devices	Track health metrics such as heart rate, blood pressure, and activity levels.	Data privacy breaches, device tampering, unauthorized access to health data.	Use end-to-end encryption, enforce strict access control, and ensure secure cloud storage.
13	Public Transit Tracking	Track public transport vehicles for real-time location data.	GPS spoofing, unauthorized data access.	Encrypt GPS data, implement real-time monitoring, and secure network communication.
14	Smart Waste Bins	Monitor waste levels and optimize waste collection.	Data manipulation, hacking of bin data.	Ensure secure communication, use encrypted data transmission, and maintain regular system checks.
15	Smart Solar Panels	Monitor energy production and optimize performance.	Data interception, unauthorized access to control systems.	Use secure communication protocols, monitor system integrity, and regularly update firmware.

16	Electric Vehicle Charging Stations	Provide data on usage, availability, and energy consumption of EVs.	Hacking of charging station controls, payment system vulnerabilities.	Use secure payment protocols, encrypt data, and maintain regular software updates.
17	Smart Kiosks	Provide public information such as maps, schedules, and government services.	Physical tampering, unauthorized access to system.	Secure physical locations, use encrypted communications, and regularly update software.
18	Citizen Feedback Systems	Allow citizens to report issues such as infrastructure problems.	Data tampering, unauthorized access to feedback data.	Encrypt feedback data, limit access to authorized personnel, and ensure system integrity.
19	Smart Bikes and Scooters	Track and manage shared bike/scooter rentals in cities.	GPS spoofing, unauthorized access to rental system.	Use encrypted GPS tracking, secure rental system data, and implement authentication for users.