भारत इलेक्ट्रॉनिक्स
BHARAT ELECTRONICS

Role of PSUs for Smart City Ecosystem

By Ravikumar D

elets
www.eletsonline.com

Smart City Definition

The smart city: where people want to live, participate and get a better life – with technology as an enabler

Ministry of urban development

E-Governance and Citizen Services

1. Public Information, Grievance Redressa
2. Electronic Service Delivery
3. Citizen Engagement
4. Citizens - City's Eyes and Ears
5. Video Crime Monitoring

Waste Management

6. Waste to Energy & fuel
7. Waste to Compost
8. Every Drop to be Treated
9. Treatment of C&D Waste

Water Management

10. Smart meters & management
11. Leakage Identification, Preventive Maint.
12. Water Quality Monitoring

Energy Management

13. Smart Meters & Management
14. Renewable Sources of Energy
15. Energy Efficient & Green Buildings

Urban Mobility

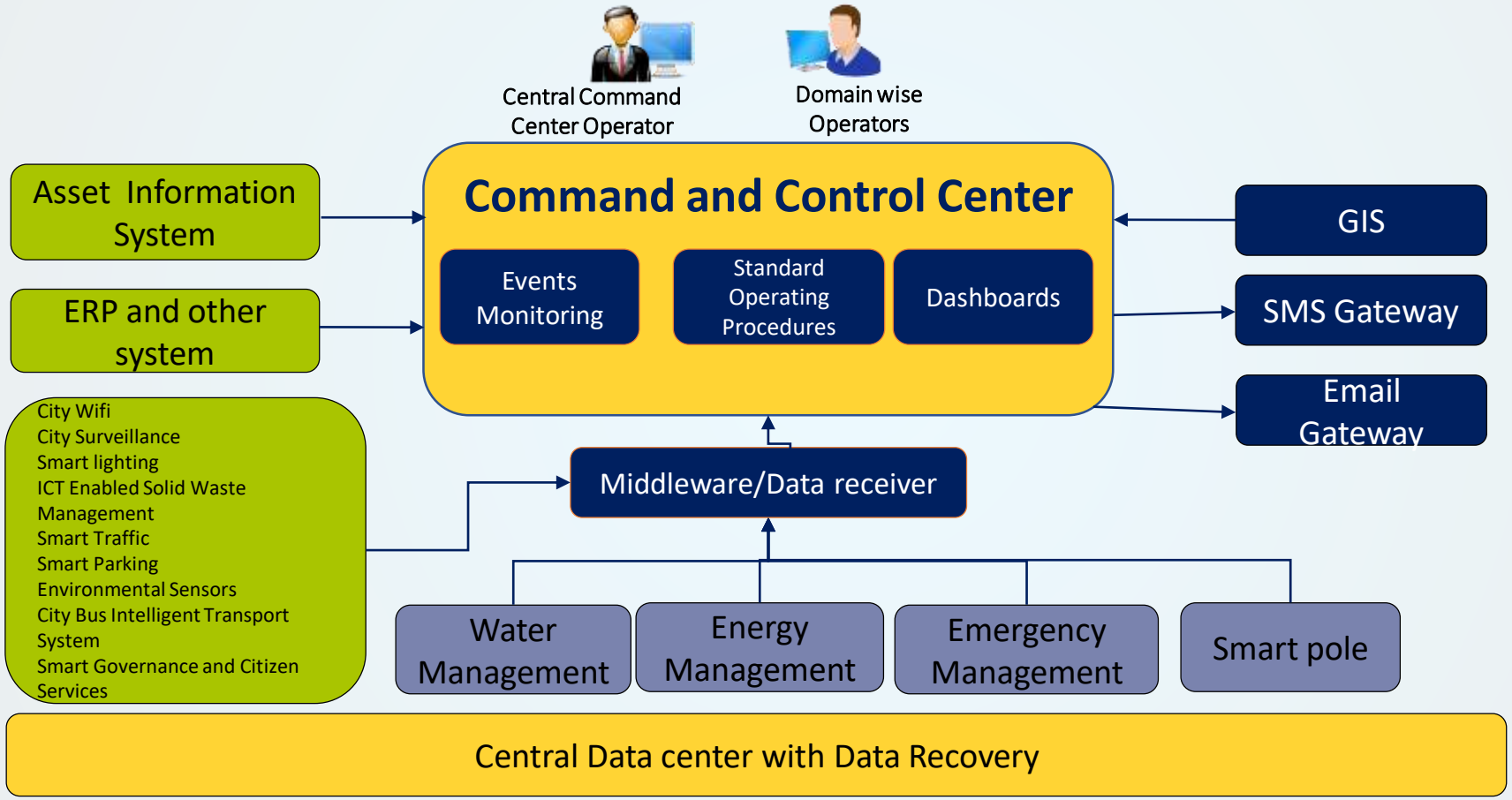
16. Smart Parking
17. Intelligent Traffic Management
18. Integrated Multi-Modal Transport

Others

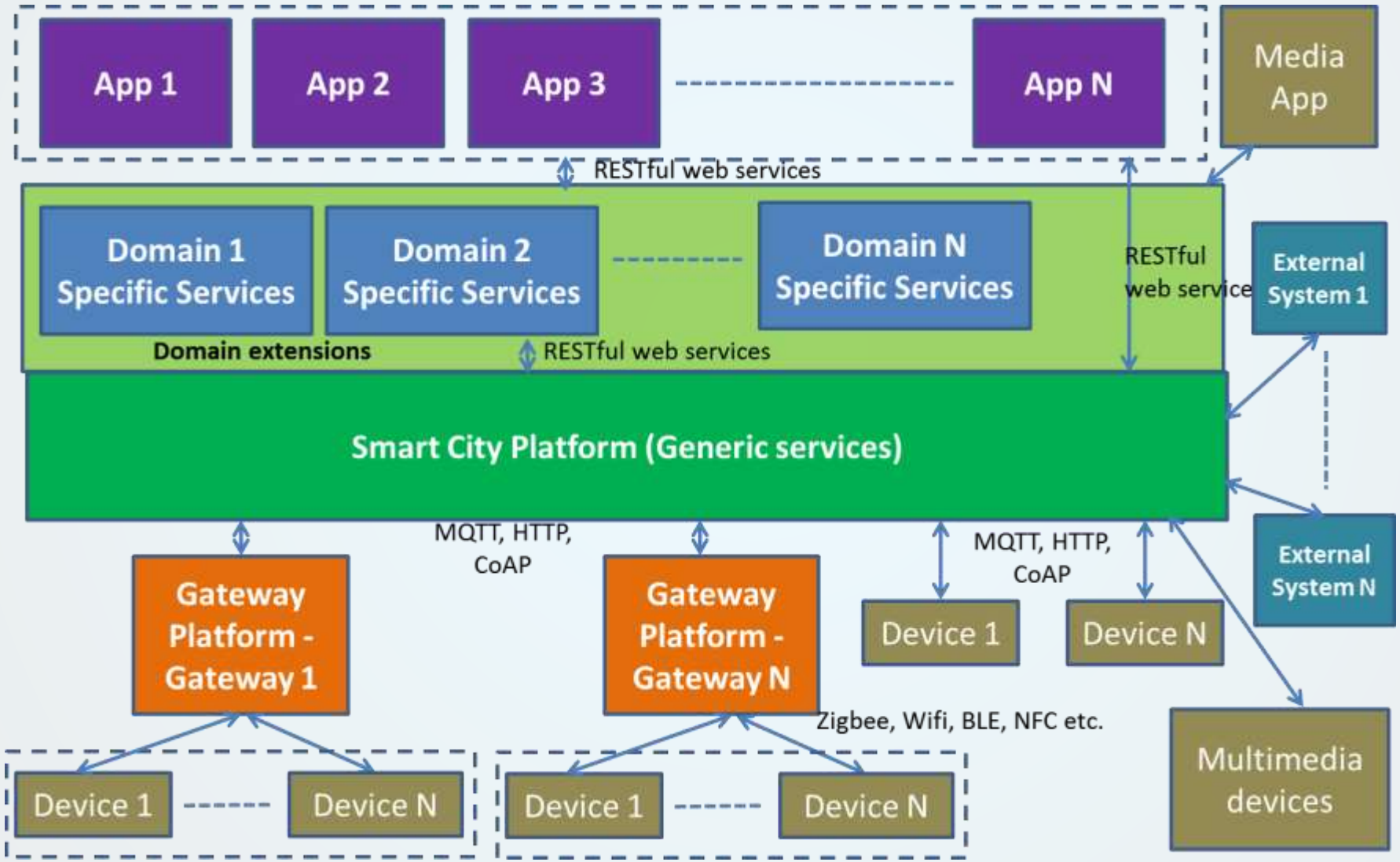
19. Tele-Medicine
20. Incubation/Trade Facilitation Centers
21. Skill Development Centers

Different Cities – Different Smart Solutions Leveraging Local Innovations

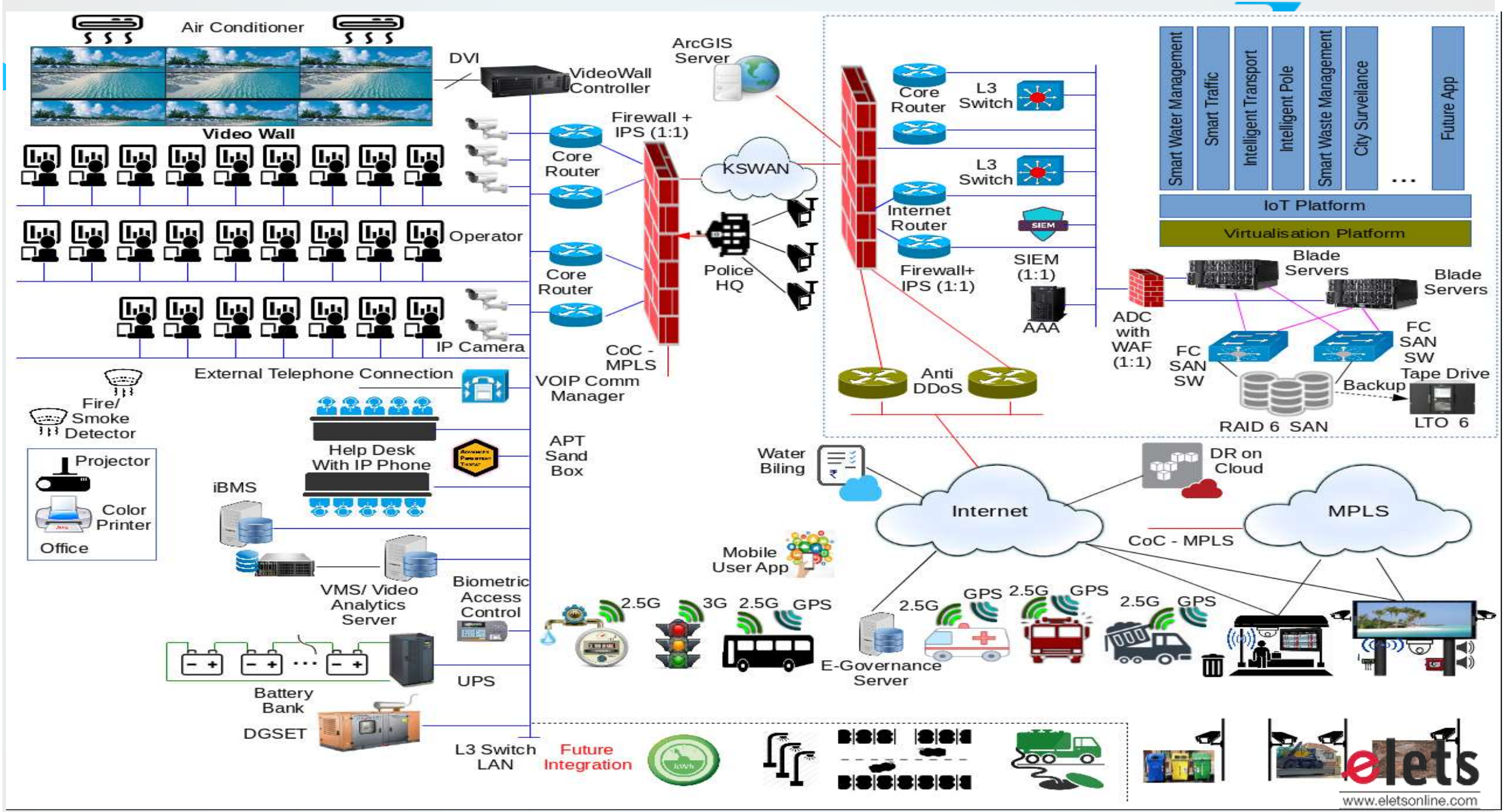
Command and Control Center Architecture Overview



Typical Smart City Middleware Components



OVERALL BLOCK DIAGRAM OF A SMART CITY



Complexity of Smart City Systems

A Smart Cities reference architecture should follow a holistic view of a Smart City ecosystem.

Challenges arise from the complexity of such systems.

- They are used in a wide range of application domains – such as transport, energy, health, public safety, education – and

- Demonstrate complex operations and maintenance processes. In addition, the needs of stakeholders from different disciplines and domains must be taken into account.

- Besides the operational complexity, Smart City systems have to fulfill strict quality requirements for reliability, availability, maintainability, security and privacy.

General Requirements of Cost Effective Smartcity

- Avoid getting locked-in to particular platform providers
- Support to the implementation of replaceable Smart City solutions.
- Choose who will operate your applications and host your data.
- Be part of a market for cities large enough to attract investment by a larger community of developers and entrepreneurs thus fostering innovation, economy growth and creation of jobs.
- Develop and test Smart city applications in one city that can be ported and adapted to other cities, which means scale opportunities for developers and lower costs for cities.

Strengths of PSUs from Smart City Perspective

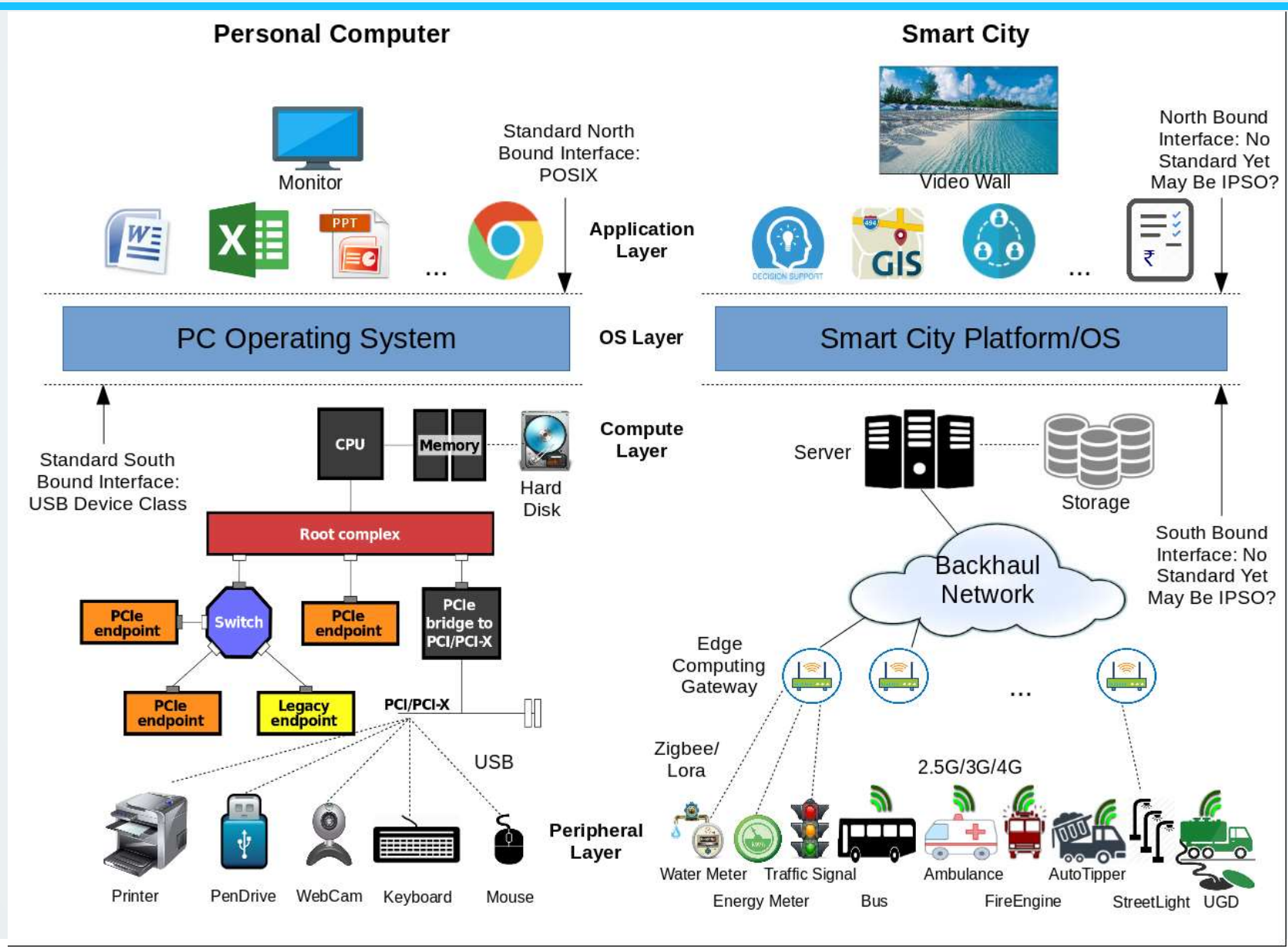
1. Huge Infrastructure is available
2. Core expertise in different verticals of technologies like electronics, mechanical, IT etc.
3. Government organization
4. Data and information security
5. Well established process flows
6. Transparency
7. Auditable
8. Investment capabilities
9. Well established skill development centers to promote and support youth.

Two Important Requirements of Smartcity

1. Standardization

2. Security

Analogy Between PC & Smart city



Standardization

When we standardize our IT, or in other words adopt uniform systems across the enterprise:

❖ We reduce complexity

❖ Lower the associated costs

❖ Adopting the same make and/or model of hardware devices (means that parts and accessories can be shared, swapped, and deployed more easily within the organization)

❖Standards played an important role in the industrial revolution. Standardization of parts made supplier specialization possible and increased efficiency over the entire product life cycle by facilitating part repair or replacement.

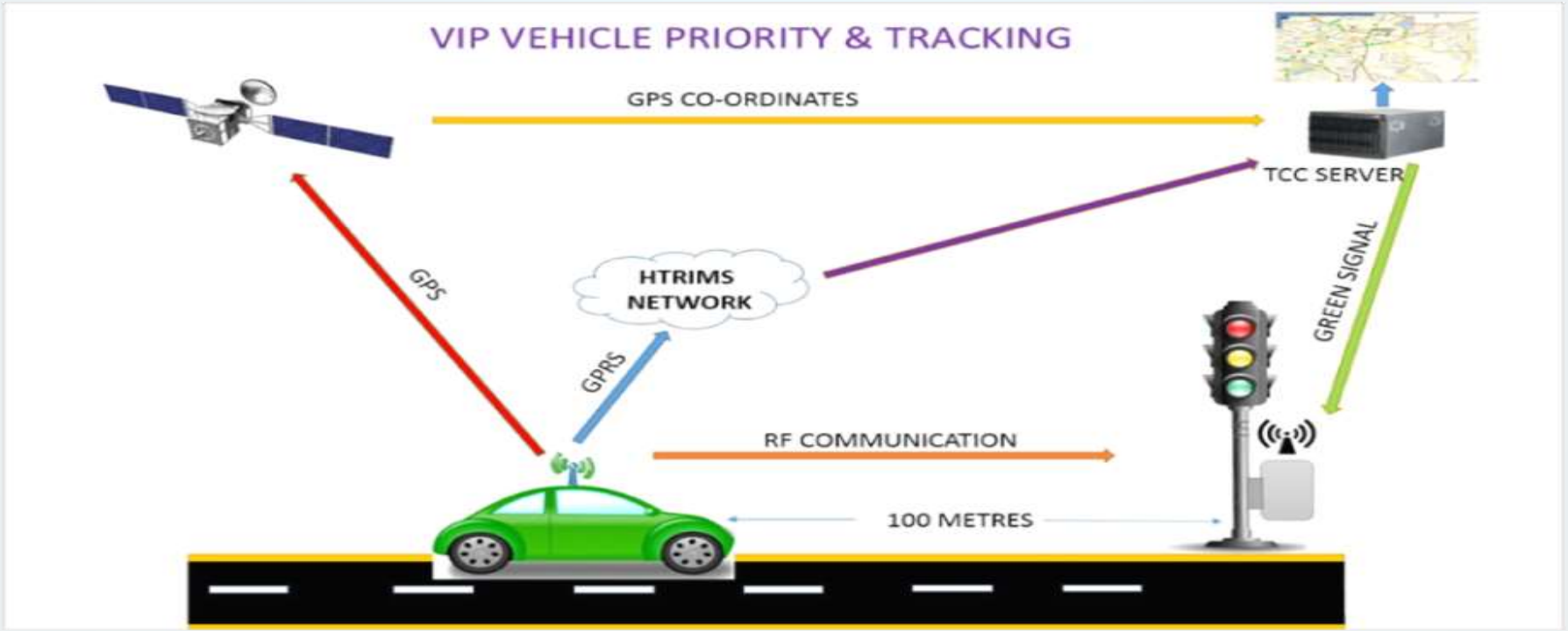
❖Standards will create a foundation of interoperability upon which next-generation technologies and capabilities can be cost-effectively and seamlessly layered.

Issues In Smarcity Solutions

- Multiple offerings from different IOT platform vendors. Every vendors has got their own proprietary API and device model
- Device manufacturer has to customize or adapt to multiple IoT platform resulting in time and resource wastage
- Monopoly - new device manufacturer not able to enter the business because there is no single standard for IoT platform integration
- Issues of Non standard
- Lack of competition, repetition of work, high cost, maintenance issue, vendor locking
- Patchwork of expensive and un-scalable solutions in smart city realization poses a big threat to achieve true value of such efforts.
- Large platform-like implementations are typically slow in adapting new industry standards since it involves complex release cycles

Use Case of non-standardization (Vehicle Priority and Tracking)

The objective is to provide free flow path for VIP and Emergency Vehicles. The vehicle equipped with GPS, GPRS and RF devices can be tracked from each junction having a RF modem as a receiving unit which establishes RF communication between traffic junction controller and vehicle.



Why an open standard platform is required

- Avoid vendor lock-in
- Standard Southbound APIs for sensor providers
- Standard Northbound APIs offered to applications
- Portability across platform providers
- Interoperability of apps on top of different providers
- Larger community of developers (critical mass, economies of scale)
- True innovation
- More competition, leading to cost savings
- Modularity
- Allow different business models
- Integration with standard open data platform
- Non-intrusive (smooth integration with legacies)

Benefits of Standardization

- Will bring more competition which reduces the cost
- Provides a level playing field for all including near entrant
- Develop eco-system to meet the needs of smart city
- Develop plug and play devices and operations
- Promotes Innovation which suits Indian conditions/situations
- Needs interoperability to build systems and create systems of systems
- To keep costs low, reduce risk, spur innovation
- **Scalable and flexible:** More module offerings can be applied to the same platform.

Security Issues In Smartcity

- Lack of Cyber Security Testing
- Poor or Nonexistent Security
- Encryption Issues
- Lack of Computer Emergency Response Teams
- Large and Complex Attack Surfaces
- Patch Deployment Issues
- Insecure Legacy Systems
- Simple Bugs with Huge Impact
- Lack of Cyber Attack Emergency Plans
- Susceptibility to Denial of Service
- **Supervisory control and data aquition(SCADA) SYSTEM**, are particularly susceptible to frequent hacks due to poor security protocols. Though SCADA systems control large-scale processes

Data Flow From End Device To Cloud

Device Hardware

- Physical tampering
- Open ports

Device Software

- Identity management
- Anomaly detection
- Firewall
- Safe reboot
- Data encryption at rest and during transfer
- Patches

Communications

- Encryption
- Secure networks (VPN, private networks)
- Secure access to the network (i.e. Wi-Fi drive-by)

Cloud Platform

- Best practices in IT security
- Secure hosting
- Patches
- Encryption
- Identity management
- User management - right people, right permissions
- API authentication and authorization
- Multiple layers of authentication for critical items

Cloud Applications

- Authentication & authorization
- Injection

FBI: Smart Meter Hacks Likely to Spread

FEDERAL BUREAU OF INVESTIGATION
INTELLIGENCE BULLETIN
Cyber Intelligence Section

(U//FOUO) Smart Grid Electric Meters Altered to Steal Electricity

(U//FOUO) This intelligence bulletin satisfies requirements contained in the FBI's Cyber Intrusions against the US Standing Collection Requirements USA-CYBR-CYD-SR-0085-09, USA-CYBR-CYD-SR-0004-10, and USA-CYBR-CYD-SR-0061-10.

(U//FOUO) Smart Grid electric meters[a] in Puerto Rico are being exploited to under-report the amount of electricity used by consumers and businesses, according to FBI case information.[1] The Puerto Rican utility estimates their losses could reach $400,000,000 annually. This is the first report that criminals have compromised Smart Grid meters and the first time the FBI has investigated meter fraud.

UNCLASSIFIED

(U) Source Summary Statement

(U//FOUO) The information contained in this Intelligence Bulletin is derived from confidential sources with direct access who the FBI judges to be accurate, reliable, and credible, despite the fact that they have not reported previously. We would deem this reporting more reliable, if it could be independently verified.

(U//FOUO) The FBI assesses with medium confidence[b] that as Smart Grid use continues to spread throughout the country, this type of fraud will also spread because of the ease of intrusion and the economic benefit to both the hacker and the electric customer.

(U) Smart Grid meters are intended to improve efficiency, reliability, and allow the electric authority to charge different rates for electricity at different times of the day. The Smart Grid also improves a utility's ability to remotely read meters to determine electric usage.[2]

(U//FOUO) Meters are being compromised in the following ways, according to a contact with good access

hakers threw 20 percent of the Ukrainian city of Kiev into total darkness

One million IoT devices infected by Bashlite malware-driven DDoS botnet
The DDoS botnet targets Taiwan, Brazil and Colombia.

Smart cities can be vulnerable: That Dallas emergency siren hack is a warning of things to come

Smart City Sensor Network

Smart city systems rely heavily on sensor data to make decisions and take action.

Most sensors use wireless technologies Hacking wireless sensors is an easy way to remotely launch cyber attacks over a city's critical infrastructure

Attacks that involve compromising sensors and sending fake data can directly affect systems since decisions and actions will be based on fake data.

This could have great impact depending on how the affected systems use the data and interact with other systems.

Attackers could even fake an earthquake, tunnel, or bridge breakage, flood, gun shooting, and so on, raising alarms and causing general panic.

Mirai Botnet

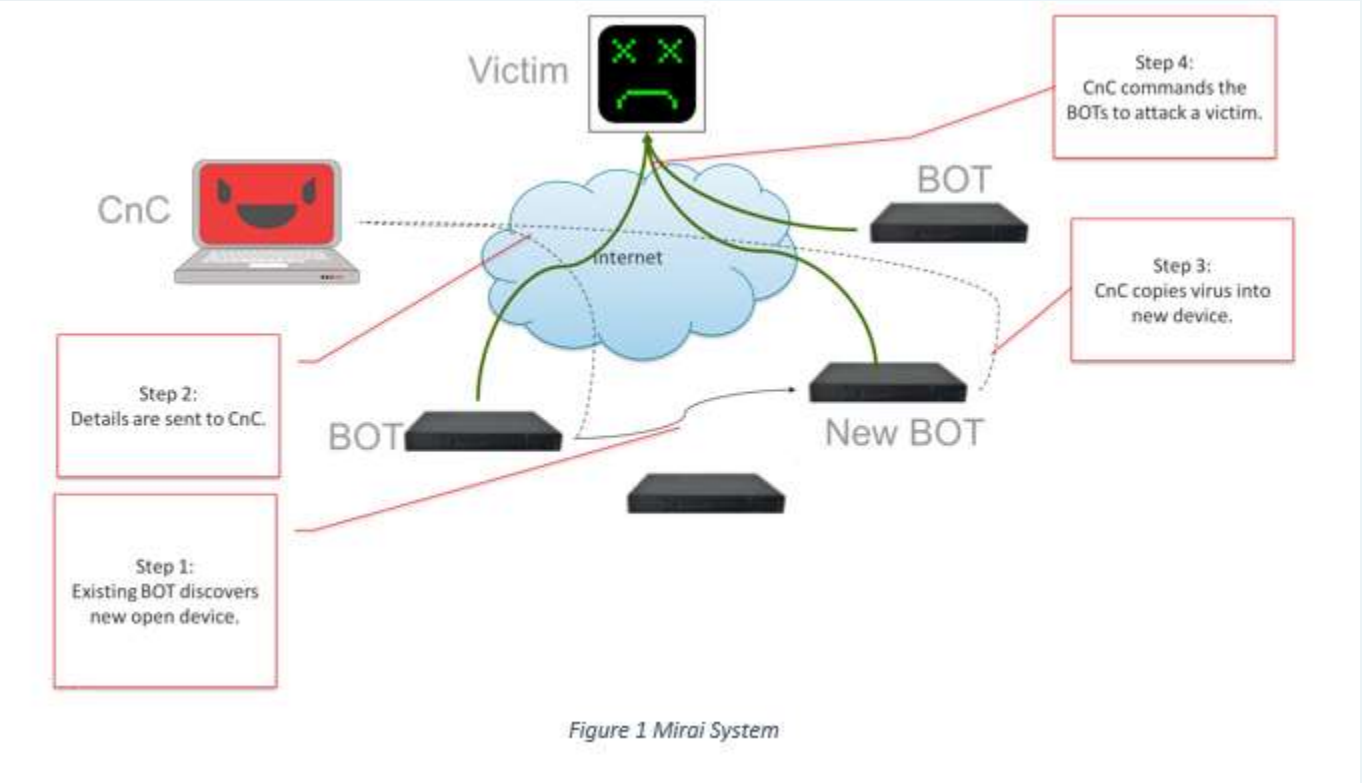
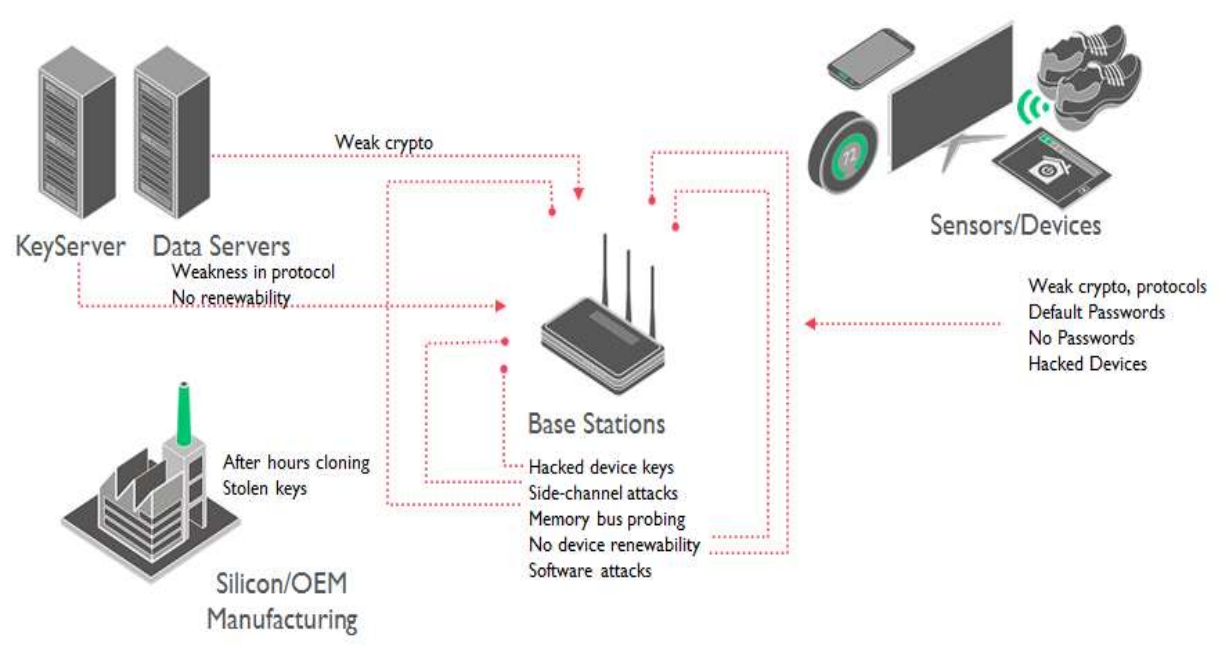


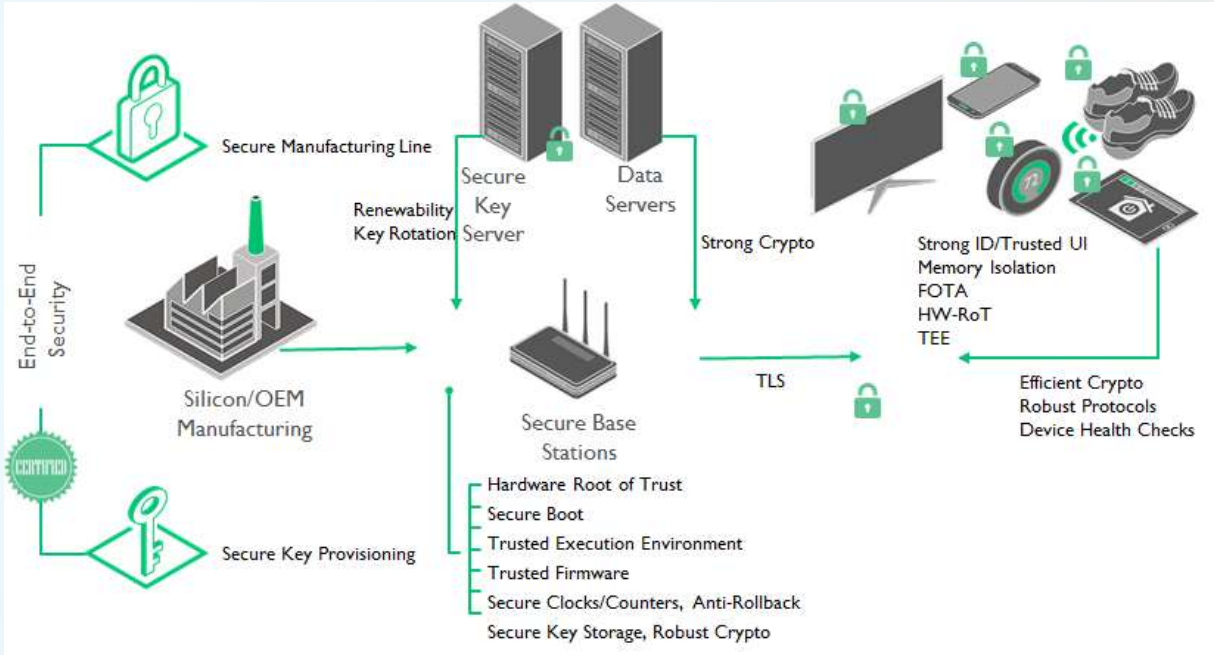
Figure 1 Mirai System

The outbreak of Mirai and find the botnet infected nearly 65,000 IoT devices in its first 20 hours before reaching a steady state population of 200,000– 300,000 infections. These bots fell into a narrow band of geographic regions and autonomous systems, with Brazil, Columbia, and Vietnam disproportionately accounting for 41.5% of infections

Securing the embedded IoT world



The Internet of Things is vulnerable to attack from many angles



When security is implemented across the cloud

Reference Model for Smart City Solution

भारत इलेक्ट्रॉनिक्स
BHARAT ELECTRONICS

STANDARD

Compliant

with Industry Standards.

Open

avoiding being captive by closed platforms.

Accessible

enabling access to data by third parties.

Modular

enabling re-utilization.

HORIZONTAL

Non-intrusive

integrating different services and solutions from service suppliers.

Interoperable

integrating different technologies, devices and protocols.

SCALABLE

Cloud-based

easily scalable.

Service models

Robust

tolerant to failures.

Adaptable

to technological changes.

Managing Security and privacy concerns

PSU Roles to address the above cited issues

•Security of Smart City: The PSU bodies should recommend guidelines on security of the smart city platform with more emphasis on smart element protection

•Standardization of Smart City Platform Interface to avoid vendor lock-in, encourage competition and promote innovation

•Make In India Mission: Development of key component/module of Smart City indigenously through open hardware imitative.

•Setting up of Open Standard IoT Test Bed for Startup to experiment and Innovate using PSU cloud infrastructure

•Reference Smart City Model with all the above features to be implemented and showcased in all public sector undertaking campuses/colony.

भारत इलेक्ट्रॉनिक्स
BHARAT ELECTRONICS

Thank You

elets
www.eletsonline.com