Enhance Smart Cities Security by Mitigating IoT Vulnerabilities

Bhupendra Dhakrey[1], Dr. Hari Om Sharan[2]

Research Scholar, Department of Computer Science & Engineering, Rama University Kanpur, Uttar Pradesh, India
Associate Professor, Department of Computer Science & Engineering, Rama University Kanpur,
Uttar Pradesh, India

Abstract - *Smart cities deals in a large volume of real-time data. Smart Cities have many resources which produce a different type of data. Smart cities use IoT sensors to gather data for various resources and this data is used by backend systems to manage resources efficiently. This data can be private or public nature. It's necessary to maintain the privacy of public and personal data. There is lots of focus on smart cities by various countries and lots of money being invested in this area. IoT based smart cities are highly venerable to different security threats and hence a lot to do in the area of smart city security.*

This paper provides a basic overview of smart city and key component of smart cities along with potential threats to smart cities. This paper also provided a high-level overview of the OCTAVE Allegro methodology [12] to analyze and mitigate risks associated with the smart city.

Key Words: Smart Cities, Security, IoT, privacy, Internet of Things.

1. INTRODUCTION

A Smart city [1] is a municipality or urban area that use large amount and different type of sensors to collect and process data to analyze, manage and monitor information about different systems like traffic, power plants, transport, school, library, transport, waste, law enforcement, and other community services. The smart city integrates information and communication technology (ICT) and other physical devices connected to the network to optimize the efficiency of services and operations of the city for citizens.

The aim of using ICT to enhance performance, interactivity, and quality of urban services to increase connections between citizen and government to reduce resource consumption and cost.

Smart cities [3] deal in a large volume of real-time data. Smart Cities have many resources which produce a different type of data. It's necessary to maintain the privacy of public and personal data hence smart cities security is a very important issue that can affect data and privacy issues like Theft, Eavesdropping, Denial of Service (DoS), Phishing, Spoofing Attacks on Data Integrity, Identification, and Secondary use. Personal data can be sensitive or non-sensitive. The non-sensitive data can be transmitted without encryption and it won't harm to the person which it belongs to however if sensitive data/information passed without encryption it could harm the person it belongs to. This information is Biometric, Medical, Financial, passport, PAN, UIDAI Aadhaar number or any other personal information [2]

Key examples of smart city technologies and programs are Singapore, Dubai, Milton Keynes, Amsterdam, Barcelona, New York, and Stockholm.

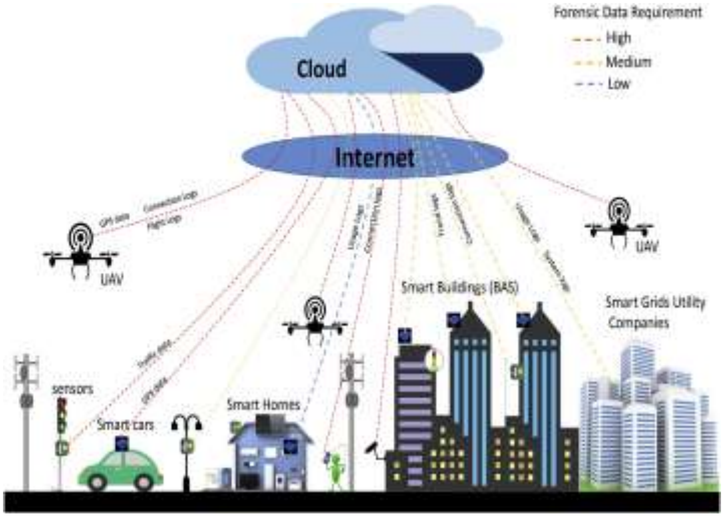

Fig -1: Smart City[3]

1.1 Smart Cities Components

1) Smart Grids: [6] Smart grid is for power supply. This is the smart version of the traditional power grid. It offers reducing energy demand and offers utility costs, connectivity to smart meters to collect energy requirement and report generation. Key features offered by smart grids are reliability, efficiency, flexibility in network topology, load balancing, and sustainability.

2) Smart Homes: [7] Building automation for home is called smart homes. It provides light controlling, entertainment and climate control, alarm controlling and control to appliances like Heating, ventilation and air conditioning (HVAC), central locking, Leak detection, Lighting control system, Remote surveillance of security cameras over the Internet smoke and CO detectors, Air quality control, Home automation for the elderly and disabled.

3) Building Automation System (BAS) [5]: BAS provide centralize monitoring controls for citizen, climates, access, visitor management, etc. It's the core feature of smart city systems. Main features Offred by BAS are control of a building's heating, ventilation and air conditioning, lighting and other systems, building climate within a specified range, provides light to rooms based on an occupancy schedule (in the absence of overt switches to the contrary), monitors performance and device failures in all systems and provides malfunction alarms to building maintenance staff.

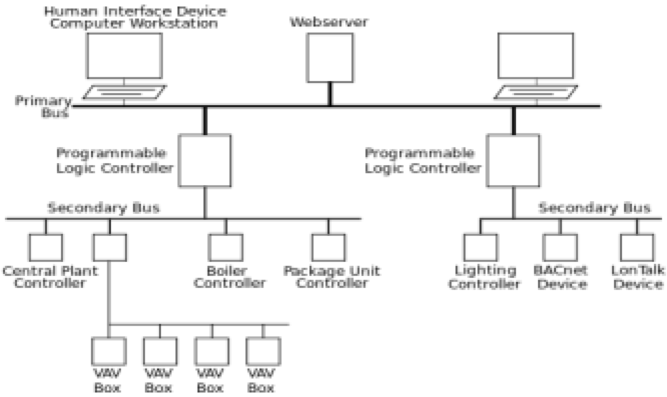

Fig -2: Building Automation System

4) Unmanned Aerial Vehicles (UAVs): This is also known as drones [8] and can be used for delivery of goods, peacekeeping, surveillance, product deliveries, aerial photography, agriculture, smuggling, and drone racing, Arial monitoring, and other purposes. UAVs are component of unmanned aircraft system (UAS), which include a UAV, ground-based controller, and a system of communication between two. UAV flight can operate and control by either human or computer system.

Fig -3: UAV

5) Smarts Vehicles: This is for transportation. It may provide features like driverless cars, self-parking, optimize route finding. A smart vehicle like modern vehicles also contains telematics systems such as GPS and integrated infotainment system which can link cloud and the smart devices. Intelligent vehicles [4] regularly report their co-ordinates and status to bases stations placed on the perimeter of a road network. Data can be transmitted live or periodically based on communication channel availability and governing policy. Information collected for vehicle location can be used for investigations like homicide and burglary.

6) IoT Sensors: This is for connecting IoT devices to exchange and data. [4] IoT sensors are deployed and maintained to monitor various phenomena and to respond to changes in the smart cities to operate efficiently. Key applications of IoT sensors are in Smart Parking to monitor the location of available parking slots, Sensor for traffic monitoring, sensors for smart grids, lighting, road, dustbin, sound monitoring, and smart devices detection. Sensors provide data for capturing events like movement pattern of the smart vehicle or mobile devices over the period. We usually keep sensors data into the cloud for availability to citizens and for other devices.

Top IoT sensors [9] includes Temperature, Proximity, Water quality, Humidity, Chemical, Gas, Smoke, Infrared (IR), Level (amount of fluid, liquid or other substances), Image, Motion, Optical, Accelerometer, and Gyroscope.

Table -1: Sensors Types

Sensors Types in Smart Cities	
Category	**Description**
Smart Parking	Monitoring of parking spaces availability
Structure health	Monitoring of material condition in bridges, monuments, and building.
Noise urban map	Monitoring of sound
Smartphone detection	Detect devices which work with Bluetooth, Wi-Fi or cellular interfaces.
Electromagnetics field levels	Monitoring and measurement of RF capable devices.
Traffic congestion	Monitoring of traffic
Smart lighting	Weather adaptive lighting in street
Waste management	Detection of trash in smart bins
Smart roads	Sensors to detect temperature, humidity, and appearance of ice plates in real times

7) Cloud: The data produced by each smart city component storied in Cloud for easy access by stockholders. Data stored in the cloud may affect the security of hardware and software of the smart city. If data security is compromised then it may result in Malware Injection, Denial of Service Attacks (DoS), Application/system vulnerabilities, Malicious insider threats

1.2 Potential threats with each smart city components [4]

Table -2: Main Security Threats

Security Threats	
Component	**Threats**
Smart Grids	• Privacy • Protocol • Infected devices • Eavesdropping
BAS	• Insecure protocol • High trusting devices Lack of source authentication • Highly trusting devices
UAV	• Communication injection, interception and jamming
Smart Vehicles	• Data security • Physical threat • Communication interception, jamming, and DoS
IoT Sensors	• Data confidentially, security, storage, and management • Remote exploitation and sensor failure.
Cloud	• System and application vulnerabilities • Insecure API • Data leakage, locations and regulation boundaries • Malware injections and DoS attacks

1.3 Analyze threat and Mitigation [11]

OCTAVE [12] (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a methodology for identifying and evaluating information security risks. We can use the OCTAVE Allegro methodology to analyze and mitigate threats related to IoT based smart cities.

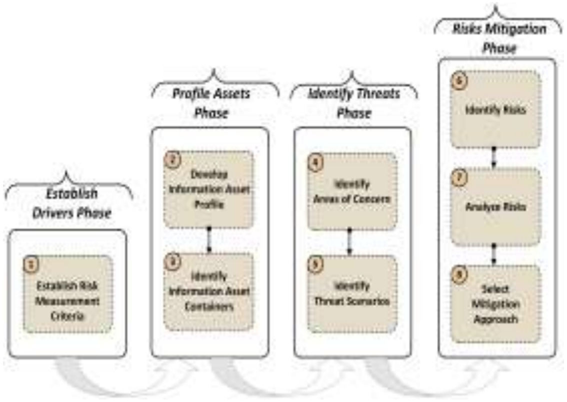
Establish Drivers Phase
1
Establish Risk Measurement Criteria
Profile Assets Phase
2
Develop Information Asset Profile
3
Identify Information Asset Containers
Identify Threats Phase
4
Identify Areas of Concern
5
Identify Threat Scenarios
Risks Mitigation Phase
6
Identify Risks
7
Analyze Risks
8
Select Mitigation Approach

Fig -4: Steps and phases in OCTAVE Allegro methodology

2. CONCLUSIONS

Using IoT to the smart city has both opportunity and risk. IoT based smart city is highly venerable to different security threats. There is high risk in terms of privacy and personal data hence security is a key area in Smart city technology.

Smart cities are scalable and dynamic and hence we can't apply traditional cybersecurity directly. This requires a survey of current security threats, prioritize based on severity. There has been some work done on IoT based smart homes by Bako and Awad [11].

OCTAVE Allegro methodology [12] can be used to analyze and mitigate risks associated with smart cities using the learning of IoT based smart home security.

We can use the learning of this research work for careful assessment of security risks to ensure all potential problems are discovered and we can plan mitigations in well advance. This will help in saving cost and life of human being. The future research will provide risk assessment, prioritization, analyze and mitigation of security threats associated with smart cities.

ACKNOWLEDGMENT

I appreciate help from my guide and university to provide me all the necessary guidance.

REFERENCES

[1] Smart City, https://en.wikipedia.org/wiki/Smart_city

[2] The (in)security of smart cities: vulnerabilities, risks, mitigation and prevention, Rob Kitchin and Martin Dodge.

[3] https://internetofthingsagenda.techtarget.com/definition/smart-city

[4] Future challenges for smart cities: Cyber-security and digital forensics, Zubair A. Baig, Patryk Szewczyk, Craig Valli, Priya Rabadia, Peter Hannay, Maxim Chernyshev, Mike Johnstone, Paresh Kerai, Ahmed Ibrahim, Krishnun Sansurooah, Naeem Syed, Matthew PeacockY.

[5] Building Automation System (BAS), https://en.wikipedia.org/wiki/Building_automation

[6] Smart Grids, https://en.wikipedia.org/wiki/Smart_grid

[7] Smart Homes, https://en.wikipedia.org/wiki/Building_automation

[8] UAV, https://en.wikipedia.org/wiki/Unmanned_aerial_vehicle

[9] IoT sensors, https://www.finoit.com/blog/top-15-sensor-types-used-iot/

[10] Risk ranking, https://www.projectsmart.co.uk/ranking-risks-rare-to-certain-negligible-to-catastrophic.php

[11] Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes, Bako Ali and Ali Ismail Awad

[12] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson